International Journal of Latest Trends in Engineering and Technology
Vol.(17)Issue(1), pp.195-202
DOI: http://dx.doi.org/10.21172/1.171.27
e-ISSN:2278-621X

VSAP–VOTING SYSTEM FOR ALL PEOPLE

Prof. Aisha Begam[1], Mudit Nigam[1]

Abstract- **In this project, we aim to build an online voting system that complies with law, specifically voting principles in, facilitating the registered users to vote from anywhere, at any time within the time period using blockchain, cryptography and web technologies to provide a more transparent, secured and inexpensive alternative to the current voting system. We implement a model to allow voters with proper credentials to vote for their respective candidate using their mobiles or laptops and assess user responses. We intend to make the voting to be done remotely and the database public, and allow anyone to store a redundant copy of the database. In this way, everyone can be assured that their copy of the database is intact, simply by comparing it with everyone else's. We base our work by, taking signed votes using private keys from the registered and authorized users (using otp) and then storing them in blocks. After voting, the blocks are mined and the system analyses them for authenticity and generates a report stating the result of voting.**

Keywords: Blockchain, Cryptography, Web Technologies, Remote Login

I. INTRODUCTION

In a democratic country like India, a single authority is responsible for maintaining huge Voting Database, and that organization has complete control over it, including the ability to apply changes to the data. The organization which maintains the database has no reason to falsify the database's contents, however, the data being stored is too sensitive and the motive to manipulate it is too enticing to allow any single organization to have total control over it. Even if it could be guaranteed that the responsible organization would never enact a fraudulent change to the database (an assumption which, for many people, is already too much to ask), there is still the possibility that someone from outside could break in and manipulate the database to their own ends (EVM hack). Also,not all people are able to come and vote at the voting booths, as they might be living far from their respective election center, are busy on that day, etc.

This project aimsto decentralize the voting data, increase the transparency of the voting data and ensure that no entity can manipulate the database by making the database public, and allow anyone to store a redundant copy of the database. In this way, everyone can be assured that their copy of the database is intact, simply by comparing it with everyone else's. The registered users are allowed to do remote login, anywhere and anytime within the time frame from their mobiles and laptops using their credentials and one-time password and then vote for their chosen candidate. Their votes are sealed using their private key in ballots. After the voting is done, the ballots are mined into blocks and all the blocks are chainedto ensure the accuracyand integrity of every votei.e. with the help of Blockchain, wallets of the authenticated users will be created, and in the transaction, coins will be interpreted as their vote. The user can send their respective coin/vote from their wallet to their respective candidate wallet and these transactions will be zipped into the blocks of the distributed immutable ledger Blockchain.For getting the result of voting, all blocks and thetransactions are checked for integrity,authenticity and a report is generated, stating the result of voting.This providesa more transparent, secured and inexpensivealternative to the current voting system.

[1] Department of Information Science and Engineering , PES University, Bangalore, Karnataka

II. LITERATURESURVEY

This Literature Survey has been done to gain insights on the following divisions of our project: First, to check whether or not the use of blockchain technology will be useful and feasible in our application. Second, to study different existing similar applications and the drawbacks in them.

[1] This survey paper is about: if Blockchain technology is to be used or not in different cases? A study released by Juniper Research, shows more than half the world's largest companies are now researching blockchain. For decades companies like Oracle Corp. have expanded the functionality and hardened the security of relational databases. However, they suffer from one major constraint: They put the task of storing and updating entries in the hands of one or a few entities, whom you have to trust won't mess with the data or get hacked. But,Blockchain removes the need for a trusted authority. A group of anonymous strangers (and their computers) can work together to store, curateand secure a perpetually growing set of data without anyone having to trust anyone else.

Result-Blockchain technology will be very useful and feasible in our type of applications.

[2] This paper discusses different implementations for blockchain voting systems that have been proposed and use those to come to a conclusion about the best, most realistic implementation method.

Votebook- TheVotebookteam, consisting of NYU Masters students came in first place and offered one of the most thorough and effective case studies on how a block chain voting system might look like. Votebook made few design considerations when creating their system: 1. Individuals may check that their vote was counted (but cannot see their neighbour's vote). 2. The system should not enable coerce voting. 3. The system should either produce or hide interim results, as desired. 4. The system must be audible. 5. Only citizens can vote.

VoteWatcher-Most mature and tested blockchain voting implementation. After registering using current methods, voters are given a paper ballot at the voting station. This paper ballot willcontain three QR codes. Once the ballot is scanned, vote is sent to the proper candidate's unique address. Once the election is complete all the votes are added to the global blockchain.

[3]This paper presented two important case studies of the governments who have previously tried implementing the online voting system and their drawbacks as well as how blockchain voting system is the best option available.

Estonian I-Voting System- The ID card used in the elections was designed to run on an integrated circuit with 2048-bitPIN. The card is easily usable for authentication, encryption, and signatures the voter has to download the voting application, authenticate using the electronic ID.Candidates will be displayed and a vote could be cast. The vote will be encrypted using the election's public key and signed with the voter private key. As soon as the vote is cast it will be sent to a vote storage server controlled by the Estonian government

New South Wales State election- In 2015, about 280,000 eligible citizens placed their vote using iVote system in the New South Wales State election. The voter has to register with authorities, receive a voter ID and choose a six-digit PIN. The voter logins in the system using his ID and PIN, cast a vote, then receives a 12-digit receipt number as a confirmation.

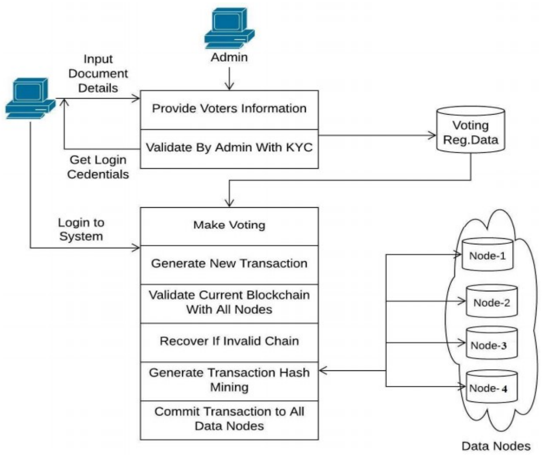
Drawbacks- Estonian model was dropped due to raising questions on the transparency and centralization of votes that could lead to a DDOS attack.Agencies with enough computing power can provide a potential alteration.

III. SYSTEM DESIGN

System Architecture- Firstly, we create a multiple distributed ledger and e-voting transnational data and store all transaction data into multiple data nodes. Each node will hold the specific block for each transaction. Same block has been placed for all the nodes, and generates a valid block chain. Now the System will retrieve data from all data nodes and commit the transaction, it should be any kind of transactional query. If any block is invalid during the validation of data servers, then the system will automatically recover the whole blockchain using majority of servers. We will address and eliminate the runtime server attacks and recover the blockchain. System will provide each transactional validation, for all servers.

In the admin module, we use the hash generation algorithm and the hash will be generated for the given data. Before executing any transaction, we use peer to peer verification to validate the data. If any chain is invalid then it will recover or update the current server blockchain. Mining algorithm is used for checking the hash generated for the query till the valid hash is generated.

In the block Generation and blockchain validation phase, the data is processed in multiple servers so that the transactions are processed in sequencing P2P distributed network. The Consensus algorithm is used by the network which will store the data to the block that is added to blockchain and all nodes in the network admit the respective block and extend the chain base on the block. In the results generation phase, firstly E-voting will be done successfully and secondly if attacker attacks the system, then the system will automatically recover the blocks using blockchain technology.



.

Figure 1. System architecture

IV. IMPLEMENTATION

Firstly, the voter provides his/her personal details: name, email address, phone number and Adhaar number.Afterwards a One-Time Password (OTP) and a public key-private key pair is generated with the help of Elliptic Curve Digital Signature Algorithm (ECDSA) and is sent to the voter email address and his respected mobile number. The voter enters the respective otp in order to vote into the system, the respective otp is validated by the system. If the entered otp is correct, then the authentic user is allowed to cast his/her vote and his ID (UUID) is generated to hide user's identity.

The user cast his/her by providing the private-key and selecting the candidate. The user private key is verified, if the private key is correct the vote is verified and store in the database using SHA-3.After the elections are over, all the votes are mined into the block of the immutable ledger blockchain. The election results are shown along with the block and vote description.

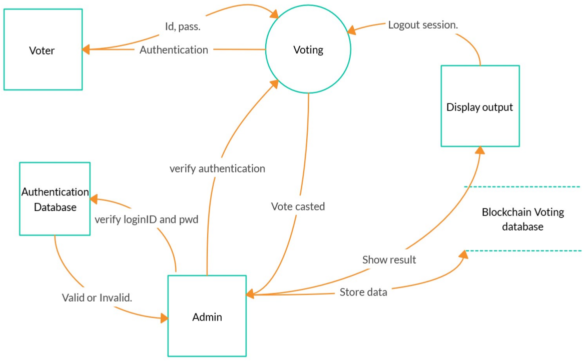


Figure 2. Implementation

4.1 Blockchain [4]

A blockchain, is a growing list of records, called *blocks*, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction dataas shown in Figure 3 (generally represented as a Merkle tree).

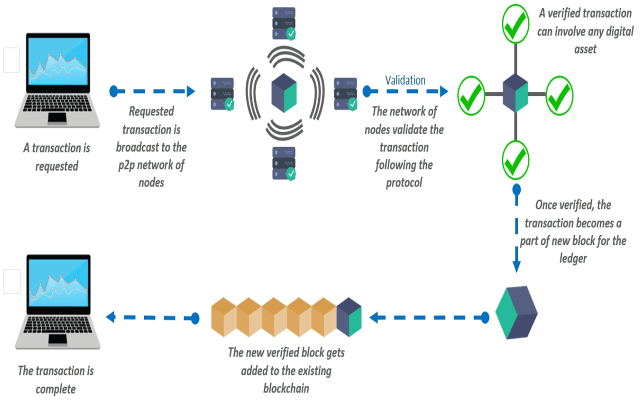

A transaction is requested
Requested transaction is broadcast to the p2p network of nodes
Validation
The network of nodes validate the transaction following the protocol
A verified transaction can involve any digital asset
Once verified, the transaction becomes a part of new block for the ledger
The new verified block gets added to the existing blockchain
The transaction is complete

Figure 3. Blockchain

A blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Blockchain may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

4.2 One-Time Password(OTP) [5]

An OTP, also known as one-time pin or dynamic password, is a password that is valid for only one login session or transaction, on a computer system or other digital deviceas shown in Figure 4. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication. In contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. And also, a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker.

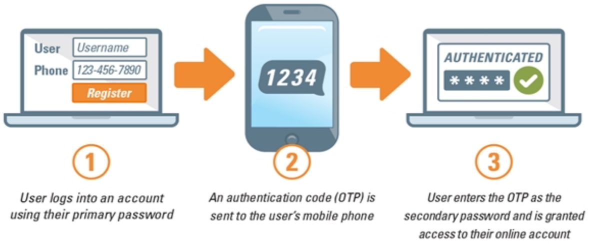

User
Username
Phone
123-456-7890
Register
1234
AUTHENTICATED
****
1
2
3
User logs into an account using their primary password
An authentication code (OTP) is sent to the user's mobile phone
User enters the OTP as the secondary password and is granted access to their online account

Figure 4. One-Time Password

4.3Secure Hash Algorithm 3 (SHA-3) [6]

SHA-3 is a latest member of secure hash algorithm standards. A cryptographic hash function is a one-way function that uses mathematical algorithm to map data of any size (message) to a fixed size bit string (hash). SHA-3 uses

Keccak algorithm. It is based on un-keyed permutations as opposed to other usual hash functions' constructions that used keyed permutations. A new approach called sponge and squeeze construction is used in Keccak, which is a random permutation model. The variant used in this project is SHA-3 with 256-bit of output (SHA3-256).

4.4 Universally Unique Identifier (UUID) [7]

A universally unique identifier (UUID) is a 128-bit number used to identify information in computer systems. The term globally unique identifier (GUID) is also used, typically in software created by Microsoft. When generated according to the standard methods, UUIDs are for practical purposes unique. Their uniqueness does not depend on a central registration authority or coordination between the parties generating them, unlike most other numbering schemes. While the probability that a UUID will be duplicated is not zero, it is close enough to zero to be negligible. Thus, anyone can create a UUID and use it to identify something with near certainty that the identifier does not duplicate one that has already been, or will be, created to identify something else. Information labelled with UUIDs by independent parties can therefore be later combined into a single database or transmitted on the same channel, with a negligible probability of duplication.

4.5 Elliptic Curve Digital Signature Algorithm (ECDSA) [8]

ECDSA is a cryptographic algorithm used to ensure that funds (here votes) can only be spent by their rightful owners. A few concepts related to ECDSA:

- private key: A secret number, known only to the person that generated it. A private key is essentially a randomly generated number. A private key is a single unsigned 256-bit integer (32 bytes).
- public key: A number that corresponds to a private key, but does not need to be kept secret. A public key can be calculated from a private key, but not vice versa. A public key can be used to determine if a signature is genuine (in other words, produced with the proper key) without requiring the private key to be divulged. The keys are 65 bytes, consisting of constant prefix (0x04), followed by two 256-bit integers called x and y (2 * 32 bytes). The prefix of a compressed key allows for the y value to be derived from the x value.
- signature: A number that proves that a signing operation took place. A signature is mathematically generated from a hash of something to be signed, plus a private key. The signature itself is two numbers known as r and s. With the public key, a mathematical algorithm can be used on the signature to determine that it was originally produced from the hash and the private key, without needing to know the private key. Resulting signatures are either 73, 72, or 71 bytes long.

4.6 Graphical User Interface

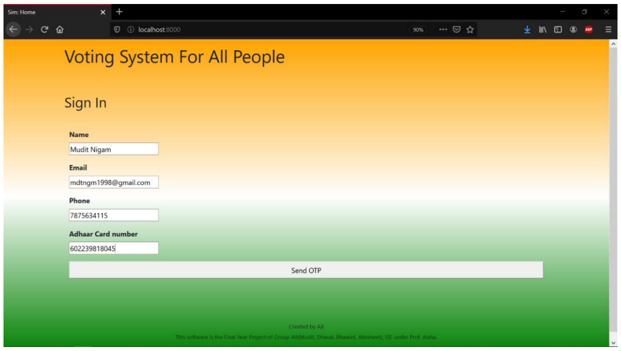
GUI of our project was developed using the Django web framework. It is a Python-based free and open-sourceweb framework that follows the model-template-view (MTV) architectural pattern. It is maintained by the Django Software Foundation (DSF), an American independent organization established as a 501(c)(3) non-profit.

V. EXPERIMENTAL RESULTS

The project is a web-based application, so, authenticated users will be able to cast vote remotely through their mobiles and desktops using their credentials.

5.1 The Login Page

The home pageof the applicationas shown in Figure 5(a) consists of the login page. In this page user has to provide his/her various details consisting of Name, Email-ID, phone number and Adhaar card number. After providing the necessary details, the user presses the Send OTP button for the verification and authentication purposesas shown in Figure 5(b) and Figure 5(c).



Voting System For All People

Sign In

Name
Mudit Nigam

Email
mdtngm1998@gmail.com

Phone
7875634115

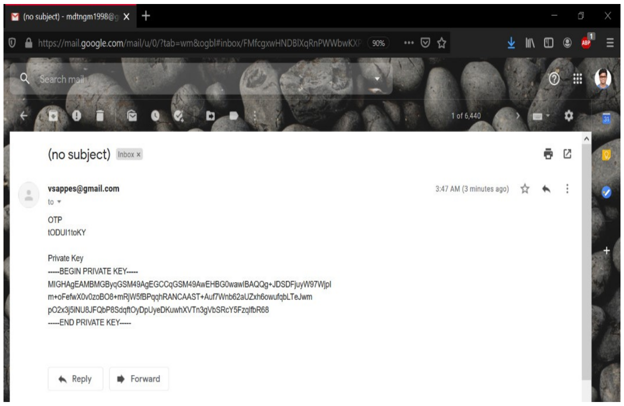
Adhaar Card number
602239818045

Send OTP

Created by A8

This software is the Final Year Project of Group A8(Mudit, Dhaval, Bhawini, Abhineet), ISE under Prof. Aisha.

Figure 5(a) Login Access


(no subject) - mdtngm1998@g
https://mail.google.com/mail/u/0/?tab=wm&ogbl#inbox/FMfcgxwHNDBlXqRnPWWbwKXP
90%
Search mail
1 of 6,440
Inbox ×
Reply
Forward

(no subject)

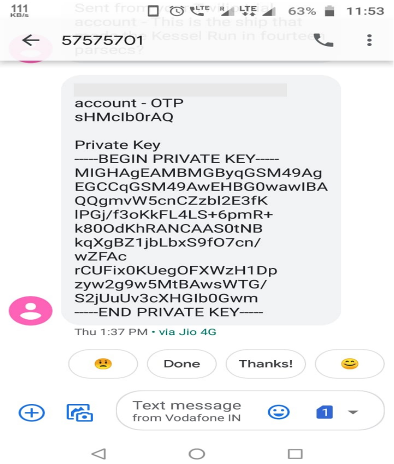
vsappes@gmail.com
to

3:47 AM (3 minutes ago)

OTP
tODUI1toKY

Private Key

```
-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQg+JDSDFjuyW97WjpI
m+oFefwX0v0zoBO8+mRjW5fBPqqhRANCAAST+Auf7Wnb62aUZxh6owufqbLTeJwm
pO2x3j5INU8JFQbP8SdqftOyDpUyeDKuwhXVTn3gVbSRcY5FzqlfbR68
-----END PRIVATE KEY-----
```



57575701

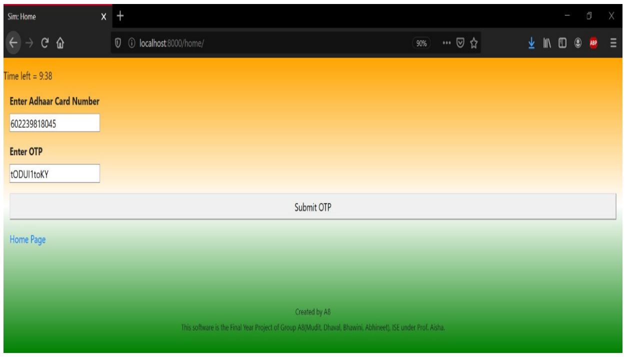
[redacted]
account - OTP
sHMcIb0rAQ

Private Key

```
-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49Ag
EGCCqGSM49AwEHBG0wawIBA
QQgmvW5cnCZzbl2E3fK
lPGj/f3oKkFL4LS+6pmR+
k80OdKhRANCAAS0tNB
kqXgBZ1jbLbxS9fO7cn/
wZFAc
rCUFix0KUegOFXWzH1Dp
zyw2g9w5MtBAwsWTG/
S2jUuUv3cXHGIb0Gwm
-----END PRIVATE KEY-----
```

Thu 1:37 PM • via Jio 4G

Figure 5(b) OTP security



Time left = 9:38

Enter Adhaar Card Number
602239818045

Enter OTP
tODUI1toKY

Submit OTP

Home Page

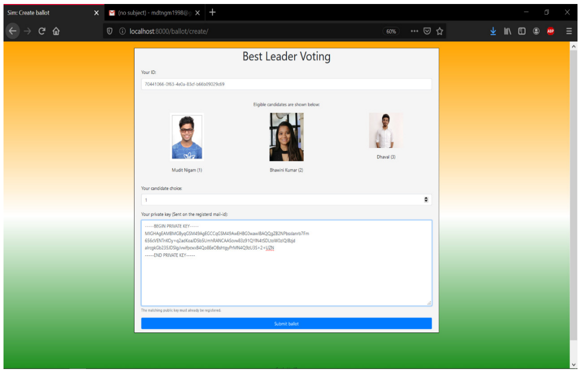
Created by A8

This software is the Final Year Project of Group A8(Mudit, Dhaval, Bhawini, Abhineet), ISE under Prof. Aisha.

Figure 5(c) OTP submission

5.2 The Voting Page

The voting page consists *of* the eligible candidates, and a text boxas shown in Figure 6, in which the user needs to provide his/her choice, if the private key entered is correct, the vote is counted for the respective candidate.



Best Leader Voting

Your ID:

70441066-0f63-4e0a-83cf-b66b09029c69

Eligible candidates are shown below:

Mudit Nigam (1)

Bhawini Kumar (2)

Dhaval (3)

Your candidate choice:

1

Your private key (Sent on the registerd mail-id):

```
-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQgZB2NPbsxlanrb7Fm
656cVENTnKOy+q2adKoaJD5b5UmhRANCAAScvw83z91QYIN4tSDLtoW0zIQIBzjd
alrcgkGb235JDSIg/vwifpcwxB4Qo8EeOBshtgyPrMN4Q9zU3S+2+UZN
-----END PRIVATE KEY-----
```

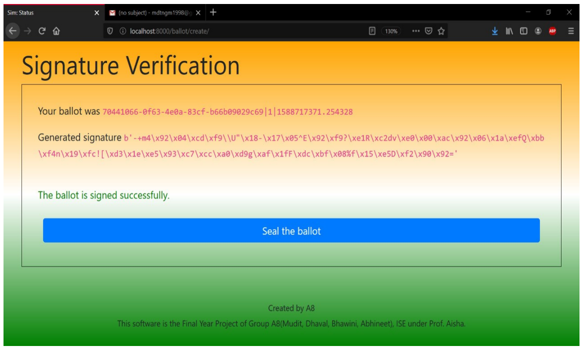
The matching public key must already be registered.

Submit ballot

Figure 6. Candidate Selection

5.3 The Vote Authentication Page

This part of the application is used to verify the eligibility of the votes and to check the authenticity of the stored votesas shown in Figure 7(a) and Figure 7(b).



Signature Verification

Your ballot was 70441066-0f63-4e0a-83cf-b66b09029c69|1|1588717371.254328

Generated signature b'-+m4\x92\x04\xcd\xf9\\U"\x18-\x17\x05^E\x92\xf9?\xe1R\xc2dv\xe0\x00\xac\x92\x06\x1a\xefQ\xbb\xf4n\x19\xfc![\xd3\x1e\xe5\x93\xc7\xcc\xa0\xd9g\xaf\x1fF\xdc\xbf\x08%f\x15\xe5D\xf2\x90\x92='

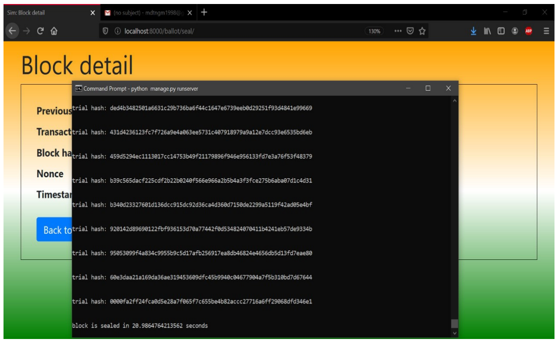
The ballot is signed successfully.

Seal the ballot

Created by A8

This software is the Final Year Project of Group A8(Mudit, Dhaval, Bhawini, Abhineet), ISE under Prof. Aisha.

Figure 7(a). Signature Verification

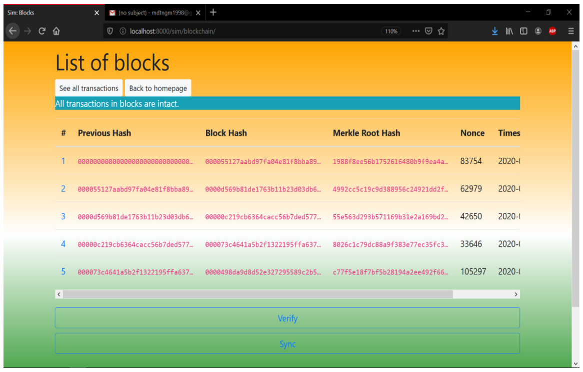

Sim: Block detail
(no subject) - mdtngm1998@g
localhost:8000/ballot/seal/
130%
Block detail
Previous
Transact
Block ha
Nonce
Timestar
Back to
Command Prompt - python manage.py runserver

```
trial hash: ded4b3482501a6631c29b736ba6f44c1647e6739eeb0d29251f93d4841e99669

trial hash: 431d4236123fc7f726a9e4a063ee5731c407918979a9a12e7dcc93e6535bd6eb

trial hash: 459d5294ec1113017cc14753b49f21179896f946e956133fd7e3a76f53f48379

trial hash: b39c565dacf225cdf2b22b0240f566e966a2b5b4a3f3fce275b6aba07d1c4d31

trial hash: b340d23327601d136dcc915dc92d36ca4d360d7150de2299a5119f42ad05e4bf

trial hash: 920142d89690122fbf936153d70a77442f0d534824070411b4241eb57de9334b

trial hash: 95053099f4a834c9955b9c5d17afb256917ea8db46824e4656db5d13fd7eae80

trial hash: 60e3daa21a169da36ae319453609dfc45b9940c04677904a7f5b310bd7d67644

trial hash: 0000fa2ff24fca0d5e28a7f065f7c655be4b82accc27716a6ff29068dfd346e1

block is sealed in 20.9864764213562 seconds
```

Figure 7(b). Mining of block

5.4 The Logout page:

After the voting process is over, user’s vote is displayed on the screen and the expires as shown in Figure 8(a) and Figure 8(b)



List of blocks

See all transactions | Back to homepage

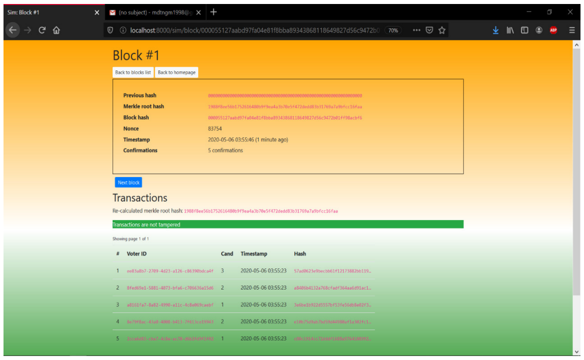
All transactions in blocks are intact.

#	Previous Hash	Block Hash	Merkle Root Hash	Nonce	Times
1	0000000000000000000000000000…	000055127aabd97fa04e81f8bba89…	1988f8ee56b1752616480b9f9ea4a…	83754	2020-(
2	000055127aabd97fa04e81f8bba89…	0000d569b81de1763b11b23d03db6…	4992cc5c19c9d388956c24921dd2f…	62979	2020-(
3	0000d569b81de1763b11b23d03db6…	00000c219cb6364cacc56b7ded577…	55e563d293b571169b31e2a169bd2…	42650	2020-(
4	00000c219cb6364cacc56b7ded577…	000073c4641a5b2f1322195ffa637…	8026c1c79dc88a9f383e77ec35fc3…	33646	2020-(
5	000073c4641a5b2f1322195ffa637…	0000498da9d8d52e327295589c2b5…	c77f5e18f7bf5b28194a2ee492f66…	105297	2020-(

Verify

Sync

Figure 8(a). List of blocks


Sim: Block #1
(no subject) - mdtngm1998@g
localhost:8000/sim/block/000055127aabd97fa04e81f8bba89343868118649827d56c9472b0
70%

Block #1

Back to blocks list | Back to homepage

Previous hash	0000000000000000000000000000000000000000000000000000000000000000
Merkle root hash	1988f8ee56b1752616480b9f9ea4a3b70e5f472dedd83b31769a7a9bfcc16faa
Block hash	000055127aabd97fa04e81f8bba89343868118649827d56c9472b01ff98acbf6
Nonce	83754
Timestamp	2020-05-06 03:55:46 (1 minute ago)
Confirmations	5 confirmations

Next block

Transactions

Re-calculated merkle root hash: 1988f8ee56b1752616480b9f9ea4a3b70e5f472dedd83b31769a7a9bfcc16faa

Transactions are not tampered

Showing page 1 of 1

#	Voter ID	Cand	Timestamp	Hash
1	ee83a8b7-2709-4d23-a126-c86390bdca4f	3	2020-05-06 03:55:23	57ad0623e9becbb61f12173882bb119…
2	8fed69e1-5881-4073-bfa6-c706636a15d6	2	2020-05-06 03:55:23	a8406b4132a768cfadf364aa6d91ac1…
3	a8161fa7-8a82-4990-a11c-4c8e069caebf	1	2020-05-06 03:55:23	3e6be1b922d5557bf53fe56db8e02f3…
4	8e79f8ac-43a0-4008-b413-7f613ce19943	2	2020-05-06 03:55:23	e10b75d9ab7bd59d44980af1a302fc1…
5	2cca6d83-cba7-4c8e-ac70-d6b2fd9f2f02	1	2020-05-06 03:55:23	c08c1914cc72dddf1688a9764108992…

Figure 8(b). Details of individual block

VI. CONCLUSION

We have implemented an online voting system which lets a voter vote from a remote location. With the help of Blockchain we have decentralized the database. Decentralized database will increase the security and transparency of the data and never allow anyone to make fraudulent changes to it. The system developed is user-friendly and can be easily used by a naive user with little overhead knowledge. Remote voting helps save resources and allow voters to vote from anywhere.

REFERENCES

[1] Morgen E. Peck. “Do You Need a Blockchain.” IEEE Spectrum
[2] Ryan Osgood. “The Future of Democracy: Block chain Voting.” COMP116: Information Security
[3] Ahmed Ben Ayed. “A Conceptual Secure Blockchain - Based Electronic Voting System” International Journal of Network Security & Its Applications (IJNSA)
[4] https://en.wikipedia.org/wiki/Blockchain
[5] https://en.wikipedia.org/wiki/One-time_password
[6] https://en.wikipedia.org/wiki/SHA-3
[7] https://en.wikipedia.org/wiki/Universally_unique_identifier
[8] https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm