Blockchain technology based e-voting system.

Prof. Anita A. Lahane[1,*], *Junaid* Patel[1,**] , *Talif* Pathan[1,***] and *Prathmesh* Potdar[1,****].

[1]Juhu Versova Link Rd, behind HDFC Bank, Gharkul Society, Bharat Nagar, Versova, Andheri West, Mumbai, Maharashtra 400053.

Abstract.
Election could be a important event during a trendy democracy however massive sections of society round the world don't trust their election system that is major concern for the democracy. Even the world's largest democracies like Republic of India, us, and Japan still suffer from a blemished legal system. Vote rigging, hacking of the EVM (Electronic vote machine), election manipulation, and booth capturing square measure the key problems within the current electoral system. during this system, we tend to square measure work the problems|the problems within the election vote systems and attempting to propose the E-voting model which might resolve these issues. The system can highlight a number of the popular blockchain frameworks that provide blockchain as a service and associated electronic E-voting system that is predicated on blockchain that addresses all limitations severally, it additionally preserve participant's obscurity whereas still being hospitable public examination.

Building Associate in Nursing electronic electoral system that satisfies the legal necessities of legislators has been a challenge for an extended time. Distributed ledger technologies is Associate in Nursing exciting technological advancement within the info technology world. Blockchain technologies supply Associate in Nursing infinite vary of applications cashing in on sharing economies.

Blockchain could be a unquiet technology of current era and guarantees to enhance the resilience of e-voting systems. this technique presents a shot to leverage edges of blockchain like cryptological foundations and transparency to attain an efficient theme for e-voting. The projected theme conforms to the elemental necessities for e-voting schemes and achieves end-to-end verifiability. The system presents in-depth analysis of the theme that with success demonstrates its effectiveness to attain Associate in Nursing end-to-end verifiable e-voting theme.

Keywords.
Blockchain, Electronic Voting System and E-voting.

1 Introduction

In each democracy, the protection of AN election may be a matter of national security. the pc security field has for a decade studied the probabilities of electronic choice systems, with the goal of minimizing the price of getting a national election, whereas fulfilling ANd increasing the protection conditions of an election. From the dawn of democratically electing candidates, the legal system has been supported pen and paper. commutation the normal pen and paper theme with a replacement election system is essential to limit fraud and having the choice method traceable and verifiable. Electronic choice machines are viewed as blemished, by the protection community, based totally on physical security considerations. Anyone with physical access to such machine will sabotage the machine, thereby moving all votes run up the said machine. Enter blockchain technology.

A blockchain could be a distributed, immutable, incontrovertible, public ledger. This new technology works through four main features:

1. The ledger exists in many different locations: No single point of failure in the maintenance of the distributed ledger.

2. There is distributed management over United Nations agency will append new transactions to the ledger.

3. Any projected "new block" to the ledger should reference the previous version of the ledger, making a changeless chain from wherever the blockchain gets its name, and so preventing meddling with the integrity of previous entries.

4. A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger.

These technological options operate through advanced cryptography, providing a security level equal and/or bigger than any antecedently notable information. The

[*]e-mail: anita.lahane@mctrgit.ac.in
[**]e-mail: junaidpatel1998@gmail.com
[***]e-mail: talifpathan13@gmail.com
[****]e-mail: prathmeshpotdar08@gmail.com

blockchain technology is thus thought of by several, together with America, to be the best tool, to be accustomed produce the new fashionable democratic ballot method. This paper evaluates the employment of blockchain as a service to implement associate degree electronic ballot (e-voting) system. The system makes the subsequent original contributions:

1. research existing blockchain frameworks suited to constructing blockchain primarily based e-voting system,

2. propose a blockchain-based e-voting system that uses “permissioned blockchain” to alter liquid democracy.[4]

2 Literature Survey

2.1 Survey Existing system

1. Adida, B., Helios (2008).**“Web-based open-audit voting.”**, in Proceedings of the 17th Conference on Security Symposium, ser. SS’08. Berkeley, CA, USA: USENIX Association, 2008.

   This paper proposes associated justify an adequate security model and criteria to judge comprehensibility. It additionally describe a web ballot theme, Pretty graspable Democracy, show that it satisfies the adequate security model which it’s a lot of graspable than Pretty smart Democracy, presently the sole theme that additionally satisfies the planned security model.

2. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008).**“Scantegrity: End-to-end voter-veriable optical- scan voting."**, IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.

   This paper describes Scantegrity that minimally impacts election procedures and is the first independent E2E verification mechanism that preserves optical scan as the underlying voting system and doesn’t interfere with a manual recount.

3. Dalia, K., Ben, R. , Peter Y. A, and Feng, H. (2012). **“A fair and robust voting system by broadcast.”**, 5th International Conference on E-voting, 2012.

   This paper proposes a recovery round to enable the election result to be announced if voters abort and also added a commitment round to ensure fairness. In addition, it also provided a computational security proof of ballot secrecy.

4. Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013).**“Star-vote: A secure, transparent, auditable, and reliable voting system.”**, in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.

   This paper describes the STAR-Vote design, that may preferably be the next-generation electoral system for Travis County and maybe elsewhere.

Recent major technical challenges relating to e-voting systems embrace, however not restricted to secure digital identity management. Any potential citizen ought to are registered to the electoral system before the elections. Their data ought to be in a very digitally processable format. Besides, their identity data ought to be unbroken personal in any involving information. ancient E-voting system could face following problems:

- Anonymous vote-casting.
- Individualized ballot processes.
- Ballot casting verifiability by (and only by) the voter.
- High initial setup costs.
- Increasing security problems.
- Lack of transparency and trust.
- Voting delays or inefficiencies related to remote/absentee voting.[7]

2.2 Limitations of Existing system or Research gap

Recent major technical challenges relating to e-voting systems embody, however not restricted to secure digital identity management. Any potential citizen ought to are registered to the electoral system before the elections. Their data ought to be during a digitally processable format. Besides, their identity data ought to be unbroken non-public in any involving info. ancient E-voting system might face following problems:

- **Anonymous vote-casting:** Each vote may or may not contain any choice per candidate, should be anonymous to everyone including the system administrators, after the vote is submitted through the system.
- **Individualized ballot processes:** How a vote are depicted within the involving net applications or databases continues to be AN open discussion. whereas a transparent text message is that the worst plan, a hashed token is wont to offer obscurity and integrity. Meanwhile, the vote ought to be non-reputable, that can’t be bonded by the token resolution.
- **Ballot casting verifiability by (and only by) the voter:** The elector ought to be ready to see and verify his/her own vote, when he/she submitted the vote. this is often vital to realize so as to forestall, or a minimum of to note, any potential malicious activity. This counter live, except for providing suggests that of non-repudiation, can sure boost the sensation of trust of the voters. These issues area unit partly self-addressed in some recent applications. Yet, suggests that of e-voting is presently in use in many countries together with Brazil, uk, Japan, and Republic of Estonia. Republic of Estonia

ought to be evaluated otherwise than the others, since they supply a full e-voting resolution that's, said to be, equivalent of ancient paper-based elections.

- **High initial setup costs:** Though sustaining and maintaining on-line selection systems is way cheaper than ancient elections, initial deployments could be pricy, particularly for businesses.
- **Increasing security problems:**Cyber attacks cause an excellent threat to the general public polls. nobody would settle for the responsibility if associate degreey hacking try succeeds throughout an election. The DDoS attacks ar documented and largely not the case within the elections. The citizen integrity commission of the u. s. gave an affidavit concerning the state of the elections within the North American country recently. Accordingly; Ronald Rivest explicit that "hackers have myriad ways in which of assaultive pick machines". As associate degree example; barcodes on ballots and smartphones in pick locations may be utilized in the hacking method. Apple explicit that we tend to mustn't ignore the actual fact that computers ar hackable, and also the evidences will simply be deleted. Double-voting or voters from the opposite regions also are some common issues.[8]

To mitigate these threats, software mechanisms which promise the following should be deployed:

1. Prevention of evidence deletion.
2. Transparency with privacy.
    - **Lack of transparency and trust:** How can people surely trust the results, when everything is done online? Perceptual problems cannot be ignored.
    - **Voting delays or inefficiencies related to remote voting:** Timing is very important in voting schemes; technical capabilities and the infrastructures should be reliable and run at the highest possible performance to let remote voting be synchronous.[5]

2.2.1 *Problem Statement and objectives*

Our objective is to solve the issues of digital voting by using blockchain technology.Blockchain enabled e-voting could reduce viter fraud and increase voter access.

2.3 Objectives

Thus, the voting system that is hereby conceived must satisfy the following requirements:

1. The election system must be openly verifiable and transparent.
2. The election system must ensure that the vote cast by the voter has been recorded.
3. Only eligible voters must be allowed to vote.
4. The election system should be tamper-proof.
5. No power-hungry organization must be able to manipulate and rig the election process.

Using a Blockchain, the most important requirements are satisfied :

- **Authentication:** Only registered voters will be allowed to vote.
- **Anonymity:** The system prevents any interaction between the votes casted by the voters and their identities.
- **Accuracy:** Votes once cast are permanently recorded and cannot be modified or changed under any circumstances.
- **Verifiability:** The system will be verifiable such that the number of votes is accounted for.[6]

3 Proposed System

The simple rationalization could be a 'chain' of blocks. A block is associate degree mass set of information. knowledge square measure collected and methoded to suit in an exceedingly block through a process known as mining. every block may be known employing a science hash (also referred to as a digital fingerprint). The block shaped can contain a hash of the previous block, so blocks will kind a sequence from the primary block ever (known because the Genesis Block) to the shaped block. during this method, all the information may be connected via a connected list structure.

3.1 Analysis/Framework/Algorithm

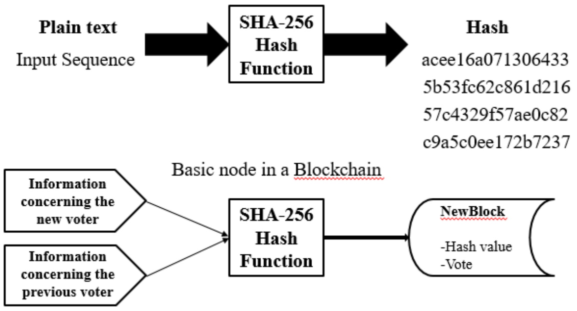


Figure 1. SHA-256 Algorithm Working

Working:

- The SHA-256 algorithm takes an input of any random length and produces an output of a fixed length(256 bits).
- In the case of SHA-256 algorithm no matter how big or small is the input, the output is of fixed length(256 bits).

A cryptographic hash function has the following properties:

1. **Deterministic:**This means that no matter how many times we enter the same input we will get te sam e result.
2. **Quick Computation:**This means that the result is generated quickly and this leads to an increase in the system effiency.
3. **Pre-Image resistance:**Suppose we are rolling a dot(1-6) and instead of getting a specific number we get the hash vaalue.Now we calculate the hash value of each number and then compare it with the result.And for a larger data sets it is possible to break pre-Image resistance by brute force method and this takes too long that it does not matter.
4. **Small changes in Input change the whole Output:** A minor change in the input significantly changes the whole output.
5. **Collision Resistant:**Every input will have a unique hash value.
6. **Puzzle friendly:**The combination of two values gives the hash value of new variable.

The need of hashing in blockchain:

- The blockchain is a sequence of blocks that contain data.
- Each block has a hash pointer that contains previous block's data.
- So if a hacker tries to attack a particular block, the changes will be reflected to the entire chain of blocks.
- Therefore, the blockchain concept is so revolutionary.

3.2 Details of Hardware and Software

3.2.1 Software Requirements

- **OS:** Windows 10.
- **Framework:** Visual Studio.
- **Server:** Localhost.
- **Database:** MS-SQL Server 2012/2014.

3.2.2 Hardware Requirements

- **Processor:** Intel Quad core 1.7 GHZ Processor or above.
- **HD:** Minimum 10 GB of HD.
- **RAM:** Minimum 8 GB of RAM.

3.3 Design Details

The .NET Framework is Microsoft's Managed Code programming model for building applications on Windows shoppers, servers, and mobile or embedded devices. Microsoft's .NET Framework could be a computer code technology that's on the market with many Microsoft Windows operative systems. within the following sections describes, the fundamentals of Microsoft .Net Frame work Technology and its connected programming models.

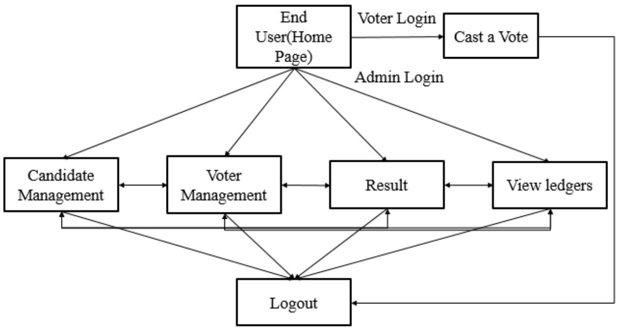


Figure 2. The Proposed System/System Architecture

C# may be a language for skilled programming. C# (pronounced C sharp) may be a programing language designed for building a large vary of enterprise applications that run on the .NET Framework. The goal of C# is to produce a straightforward, safe, modern, object-oriented, superior and sturdy language.

.NET development. conjointly it allows developers to make solutions for the broadest vary of purchasers, as well as net applications, Microsoft Windows Forms-based applications, and thin- and smart-client devices.[4]

- **Microsoft SQL Server 2008:**

Business nowadays demands a special quite knowledge management resolution. Performance measurability, and dependability ar essential, however businesses currently expect additional from their key IT investment.

SQL Server 2008 exceeds reliableness necessities and provides innovative capabilities that increase worker effectiveness, integrate heterogeneous IT ecosystems, and maximize capital and operative budgets. SQL Server 2008 provides the enterprise knowledge management platform your organization has to adapt quickly in an exceedingly quick ever-changing surroundings.

Benchmarked for scalability, speed, and performance, SQL Server 2008 is a fully enterprise-class database product, providing core support for Extensible Mark-up Language (XML) and Internet queries.[4]

- **Easy-to-use Business Intelligence(BI) Tools:**

Through wealthy information analysis and data processing capabilities that integrate with acquainted applications like Microsoft workplace, SQL Server 2008 permits you to produce all of your staff with vital, timely business data tailored to their specific data desires. each copy of SQL Server 2008 ships with a collection of metallic element services.[4]

- **Self-Tuning and Management Capabilities:**

Revolutionary self-tuning and dynamic self-config uring options optimize info performance, whereas man agement tools automatise customary activities. Graphical tools and performance, wizards change setup, info style, and performance watching, permitting info directors to tar get meeting strategic business desires.[4]

3.3.1 Detailed Design

The following usecase diagram explains the flow of the project from user end and backend.

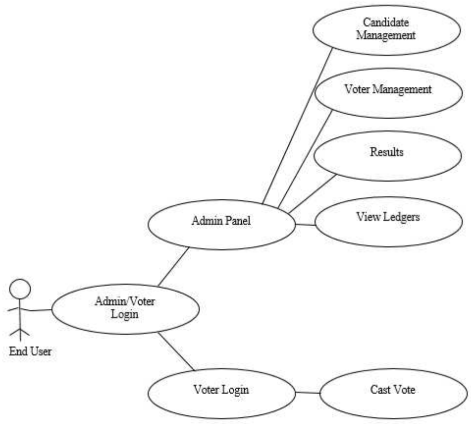


Figure 3. Use Case Diagram

The user firstly need to register to the website.Then the user can go to the voting page where he/she enters the OTP that they have received through e-mail blockchainev@gmail.com. Once the user enters the OTP, then he will be get access to cast a vote.After, the user casts a vote they will be acknowledged by a prompt stating that successfully voted.Finally, the user can logout after voting.

3.4 Methodology/Procedures(Approach to solve the problem)

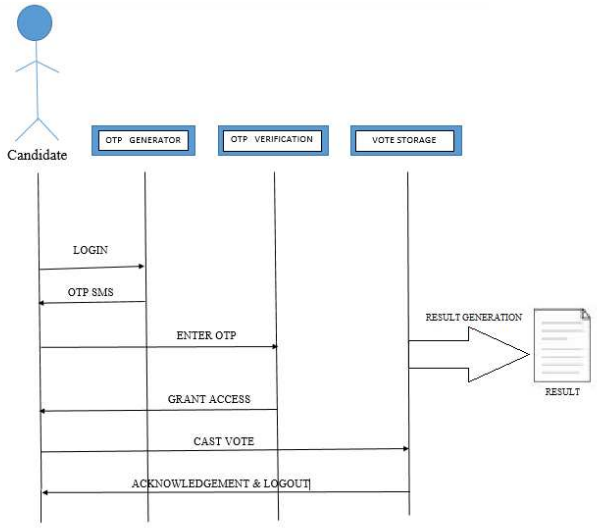
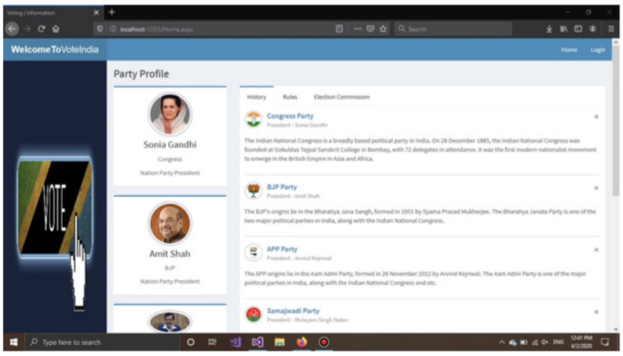


Figure 4. Sequence Diagram

4 Results

This is the home page that consists of different parties.



Party Profile

Sonia Gandhi
Congress
Nation Party President

Amit Shah
BJP
Nation Party President

Congress Party
President - Sonia Gandhi

The Indian National Congress is a broadly based political party in India. On 28 December 1885, the Indian National Congress was founded at Gokuldas Tejpal Sanskrit College in Bombay, with 72 delegates in attendance. It was the first modern nationalist movement to emerge in the British Empire in Asia and Africa.

BJP Party
President - Amit Shah

The BJP's origins lie in the Bharatiya Jana Sangh, formed in 1951 by Syama Prasad Mukherjee. The Bharatiya Janata Party is one of the two major political parties in India, along with the Indian National Congress.

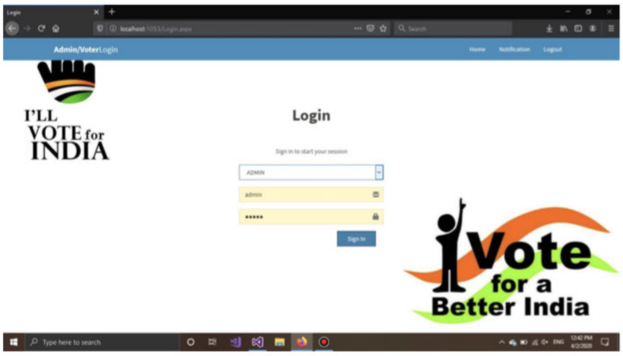
APP Party
President - Arvind Kejriwal

The APP origins lie in the Aam Admi Party, formed in 26 November 2012 by Arvind Kejriwal. The Aam Admi Party is one of the major political parties in India, along with the Indian National Congress and etc.

Samajwadi Party
President - Mulayam Singh Yadav

Figure 5. Home Page

This page allows the admin or voter to login(Admin).



Login

Sign in to start your session

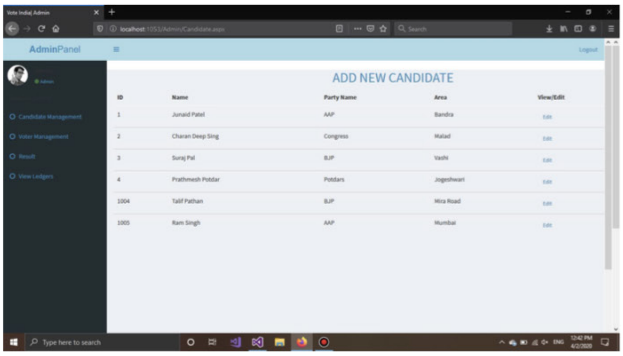
ADMIN

admin

•••••

Figure 6. Admin or Voter Login

This page allows to view,add or edit new candidate.

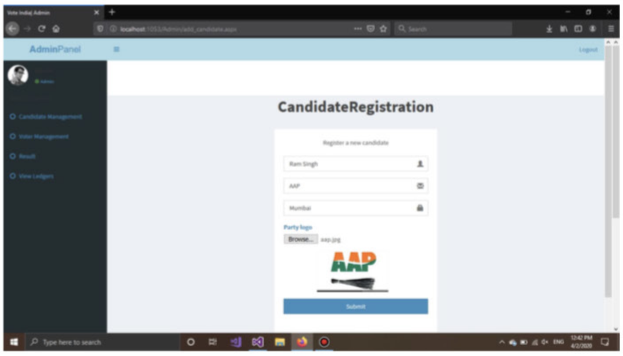


ADD NEW CANDIDATE

ID	Name	Party Name	Area	View/Edit
1	Junaid Patel	AAP	Bandra	Edit
2	Charan Deep Sing	Congress	Malad	Edit
3	Suraj Pal	BJP	Vashi	Edit
4	Prathmesh Potdar	Potdars	Jogeshwari	Edit
1004	Talif Pathan	BJP	Mira Road	Edit
1005	Ram Singh	AAP	Mumbai	Edit

Figure 7. Candidate Management Page

This page allow a new candidate to register.



CandidateRegistration

Register a new candidate

Ram Singh

AAP

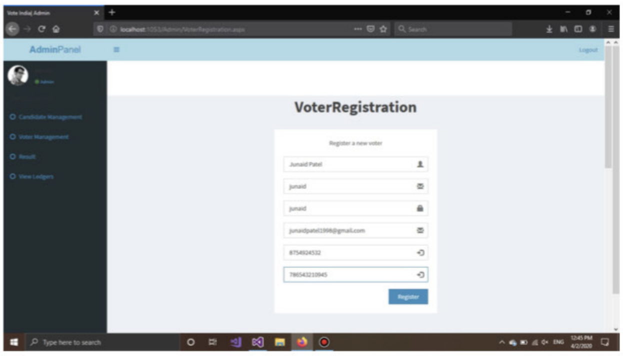
Mumbai

Party logo

Browse... aap.jpg

Figure 8. Candidate Registration Page

This page allows a new voter to register.



VoterRegistration

Register a new voter

Junaid Patel

junaid

junaid

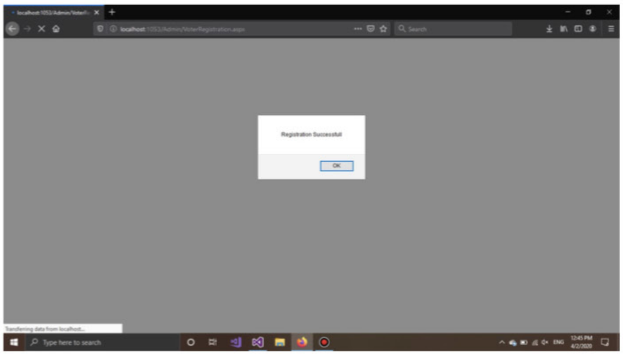
junaidpatel1998@gmail.com

8754924532

786543210945

Figure 9. Voter Registration Page

This prompt shows that a new voter is successfully registered.

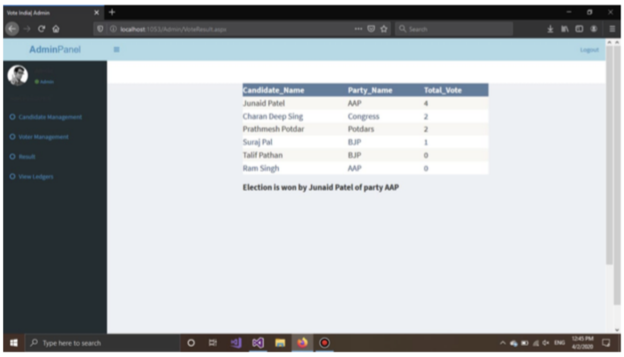

localhost:1053/Admin/VoterR...
localhost:1053/Admin/VoterRegistration.aspx
OK
Type here to search
12:45 PM
4/2/2020

Registration Successfull

Transferring data from localhost...

Figure 10. Voter Registration Prompt

This is the result page that displays the winner of the election.

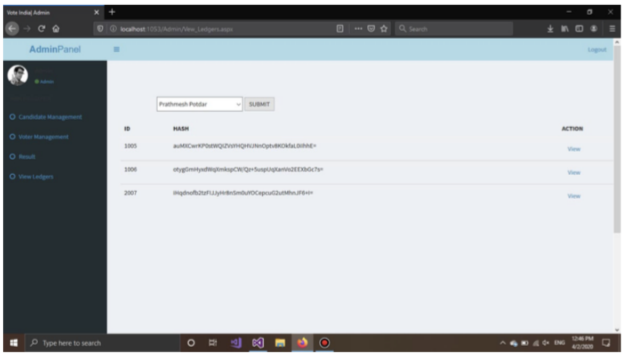


Candidate_Name	Party_Name	Total_Vote
Junaid Patel	AAP	4
Charan Deep Sing	Congress	2
Prathmesh Potdar	Potdars	2
Suraj Pal	BJP	1
Talif Pathan	BJP	0
Ram Singh	AAP	0

Election is won by Junaid Patel of party AAP

Figure 11. Result Page

This page shows the blockchain implementation for a particular candidate.



ID	HASH	ACTION
1005	auMXCwrKP0stWQIZVsYHQHVJNnOptv8KOkfaL0iIhhE=	View
1006	otygGmHyxdWqXmkspCW/Qz+5uspUqXanVo2EEXbGc7s=	View
2007	iHqdnofb2tzFIJJyHr8nSm0uYOCepcuG2utMhnJF6+I=	View

Figure 12. View Ledgers

This page allows the voter to cast a vote.

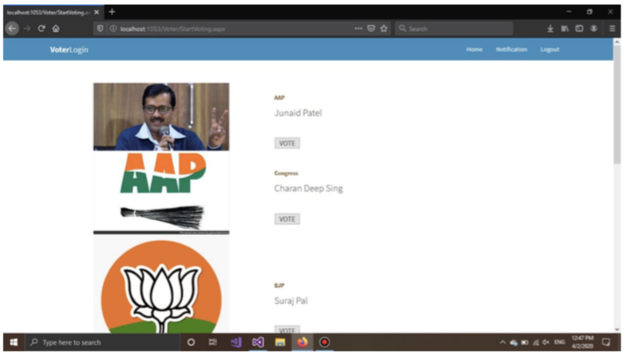
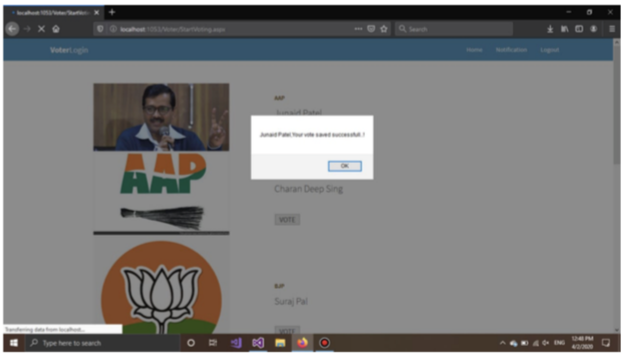


Figure 13. Voting Page

This prompt shows that the voter has successfully voted.

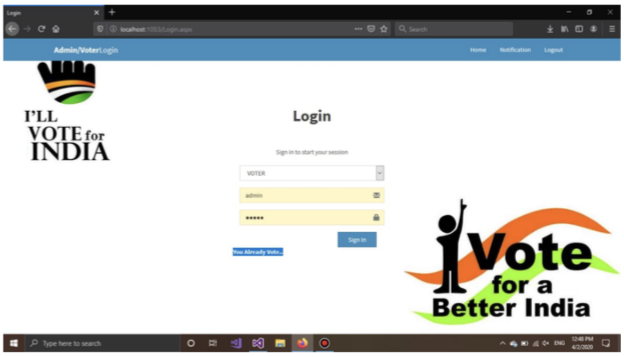


Junaid Patel,Your vote saved successfull..!

OK

Figure 14. Vote Saved Prompt

This message tells that the voter has already voted.



You Already Vote...

Figure 15. Already Voted Message

5 Discussion-Comparative study/Analysis

Table 1. Results Calculated Using Proposed Voting System

No of voters	Correct verification	Correct voting count	Accuracy
3	3	3	100%
5	5	5	100%
10	10	10	100%
30	30	30	100%

6 Conclusion

The transparency of the block-chain allows additional auditing and understanding of elections. These attributes square measure a number of the wants of a legal system.

These characteristics come back from redistributed network, and may bring additional democratic processes to elections, particularly to direct election systems. For e-voting to become additional open, clear, and severally auditable, a possible answer would be base it on blockchain technology. This paper explores the potential of the blockchain technology and its quality within the e-voting theme. The blockchain are going to be in public verifiable and distributed during a manner that nobody are going to be able to corrupt it.

The idea of adapting digital selection systems to create the general public electoral method cheaper, quicker and easier, could be a compelling one in trendy society. creating the electoral method low cost and fast, normalizes it within the eyes of the voters, removes an explicit power barrier between the elector and therefore the functionary and puts an explicit quantity of pressure on the functionary. It additionally opens the door for a additional direct sort of democracy, permitting voters to precise their can on individual bills and propositions.[5]

7 Scope

The following improvements can be made to the system,

- Adding Aadhar number verification system.
- Linking application with Government voting system data.
- Making the system more secure.
- Enhnacing the Graphical User Interface(GUI) of the application.
- Local languages can be included which will play a vital role for people living in rural areas as well as uneducated people.
- A Candidate's earlier social work and candidate qualification's can be added for a voter to have better choice.
- Also, adding suggestion system for voters that enables the public to give suggestions to the current winner.
- A complaint system can be included, that allows the people to file complaint against a candidate.

References

[1] Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). "**Star-vote: A secure, transparent, auditable, and reliable voting system.**", in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.

[2] Dalia, K., Ben, R. , Peter Y. A, and Feng, H. (2012). "**A fair and robust voting system.**" by broadcast, 5th International Conference on E-voting, 2012.

[3] Adida, B.; 'Helios (2008). "**Web-based open-audit voting.**", in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335348.

[4] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008). "**Scantegrity: End-to-end voter-veriable optical-scan voting.**" , IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.

[5] Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). "**Bingo voting: Secure and coercion- free voting using a trusted random number generator.**", in Proceedings of the 1st International Conference on E-voting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.

[6] Adida B. and Rivest, R. L. (2006). "**Scratch and vote: Self-contained paper-based cryptographic voting.**", in Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, ser. WPES '06. New York, NY, USA: ACM, 2006, pp. 29-40.

[7] Chaum, D., Ryan, P. Y. A. and Schneider, P. Y. A. (2005). "**A practical voter-verifiable election scheme.**", in Proceedings of the 10th European Conference on Research in Computer Security, ser. ESORICS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 118-139.

[8] Chaum, D. (2004)."**Secret-ballot receipts: True voter-verifiable elections.**" , IEEE Security Privacy, vol. 2, no. 1, pp. 38-47, Jan 2004.

[9] Chaum, D. (1981)."**Untraceable electronic mail, return addresses, and digital pseudonym.**", Commun. ACM, vol. 24, no. 2, pp. 84-90, Feb.