A Thesis/Project/Dissertation Report

on

BLOCKCHAIN BASED E-VOTING SYSTEM

Submitted in partial fulfillment of the

requirement for the award of the degree of

Bachelor of Technology in Computer Science and Engineering

GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

Under The Supervision of
SHOBHA TYAGI
ASSISTANT PROFESSOR

Submitted By

ABHILASH CHAUDHARY
18SCSE1010637
SHAURYA SINGH
18SCSE1010478

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY, GREATER NOIDA
INDIA
DECEMBER, 2021

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY, GREATER NOIDA

CANDIDATE'S DECLARATION

I/We hereby certify that the work which is being presented in the project, entitled " Ur Info: Blockchain based E-voting System " in partial fulfillment of the requirements for the award of the BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING submitted in the School of Computing Science and Engineering of Galgotias University, Greater Noida, is an original work carried out during the period of JULY-2021 to DECEMBER-2021, under the supervision of Dr. Shobha Tyagi, Assistant Professor, Department of Computer Science and Engineering of School of Computing Science and Engineering , Galgotias University, Greater Noida

The matter presented in the project has not been submitted by me/us for the award of any other degree of this or any other places.

18SCSE1010637 – Abhilash Chaudhary

18SCSE1010478 – Shaurya Singh

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Supervisor

(Dr.Shobha Tyagi, Assistant Professor)

CERTIFICATE

The Final Thesis/Project/ Dissertation Viva-Voce examination of 18SCSE1010637 – ABHILASH CHAUDHARY, 18SCSE1010478 – SHAURYA SINGH has been held on _____ and his/her work is recommended for the award of BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING.

Signature of Examiner(s) Signature of Supervisor(s)

Signature of Project Coordinator Signature of Dean

Date:

Place: Galgotias Univeristy

Abstract

In this Minor Project first we are going to research on Blockchain technology, some ways to secure data with the help of Python Language . We are going through research papers, documentations, and several other stuff.

After the Successful research , we will implement e-voting system using this technology. We will implement this technology in a web app that will be creating using django (a python supported framework for web). The aim of this project is to outline our proposal to solve the issues of digital voting by using blockchain.

Democratic voting is a crucial and serious event in any country. The most common way in which a country votes is through a paper based system, but is it not time to bring voting into the 21st century of modern technology? Digital voting is the use of electronic devices, such as voting machines or an internet browser, to cast votes. These are sometimes referred to as e-voting when voting using a machine in a polling station, and e-voting when using a web browser. Security of digital voting is always the biggest concern when considering to implement a digital voting system. With such monumental decisions at stake, there can be no doubt about the system's ability to secure data and defend against potential attacks. One way the security issues can be potentially solved is through the technology of blockchains.

Table of Contents

Declaration ..... **ii**

Acknowledgements ..... **iii**

Abstract ..... **iv**

Contents ..... **vi**

List of Tables/Figures ..... **vii**

1. Introduction **1**

2. Requirements, Feasibility and Scope/Objective **3**

2.1 Requirements 3

2.2 Feasibility 5

2.3 Scope/Objective 5

3. Analysis, Activity Time Schedule (PERT) **6**

3.1 Analysis 6

4. Design **7**

5. Implementation & Testing **9**

6. Limitations and Future Scope of the Project **13**

Conclusion **15**

Refrences **16**

List of Figures

Figure No.	Title	Page No.
1.	This is the home page of the application	15
2.	This is the voting page , where voter can select his candidate.	16
3.	User's Signature verification	16
4.	Block Generation page	17
5.	Transactions Page	17
6.	Voters registration page where the data is stored in database.	18

List of Table

S.No.	Caption	Page No.
1	Comparison of current blockchain-based electronic voting systems	14
2	Scalability analysis of famous blockchain platforms	15

Acronyms

py	Python
HTML	Hyper Text Markup Language
E-voting	Electronic Voting
Sql	Structured query Language

Chapter 1: Introduction

Blockchain has revolutionized the exchange of information and media after the Internet. Blockchain technology is pertained to as a path-breaking innovation and the forerunner of a fresh economic period. Many sectors, like finance, medicine, manufacturing, and education, use blockchain applications to profit from the unique bundle of characteristics of this technology. Blockchain technology (BT) promises benefits in trustability, collaboration, organization, identification, credibility, and transparency. When talking about BT, the distributed ledger technology needs to get mentioned since it is an umbrella term that includes blockchains as one type . A distributed ledger uses independent systems (nodes) to record, share, and synchronize transactions in a decentralized network. A blockchain network works without a centralized server. Transactions made in such a network are verified by the decentralized nodes and stored in so-called blocks with a timestamp . The size limit of blocks can differ between varying blockchains. The blocks are getting linked in chronological order because every one of them (except the first ―genesis‖ block) contains the cryptographic hash of the previous one, so they form a chain . The block hash considers not only structural data of a specific block but also its content like, for example, transactions. It depends on the blockchain whether users can store complete files on-chain or they need to use offchain solutions like a cloud or an InterPlanetary File System (IPFS) due to file sizes. Verification: Once the owner of the coin has broadcasted their transaction into the peer-to-peer network, it must undergo a verification process called ―mining‖ before it can become a part of the public ledger. For efficiency, these transactions are grouped into blocks for verification - hence the name blockchain. Verification is then performed by miners who devote computing power to solving a puzzle. This is the ―proof of work‖ mechanism . Double Spend and Decentralisation: Attempts by the owner of a Bitcoin to double spend a coin by issuing two transactions for the same coin are thwarted via the verification

process. If a node completes a proof of work puzzle on a block that contains a coin that has already been spent, it will be rejected by the rest of the nodes in the network, and subsequently will not be added to the blockchain. □Scalability: Much discussion currently surrounds Bitcoin's block size limit, which restricts blocks to 1Mb of transaction and header data. As blocks are mined every 10 minutes this limits the number of transactions per second (TPS) to a theoretical limit of 7 TPS [7]. As Blockchain became more popular and more nodes joined the network, the number of transactions increased and this limit became a significant problem. If the transaction creation rate increases too much it could surpass the rate at which transactions are added to the blockchain, creating a backlog of transactions.

Chapter 2: Requirements, Feasibility and Scope/Objective

Requirement

- **Technology Used**

1. **Python-** Python is an interpreted, high-level, general-purpose programming language. Created by Guido van Rossum and first released in 1991, Python's design philosophy emphasizes code readability with its notable use of significant whitespace. Its language constructs and object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects. Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including procedural, object-oriented, and functional programming. Python is often described as a "batteries included" language due to its comprehensive standard library.
2. **Jupyter Notebook-** The Jupyter Notebook is an open-source web application that allows you to create and share documents that contain live code, equations, visualizations and narrative text. Uses include: data cleaning and transformation, numerical simulation, statistical modeling, data visualization, machine learning, and much more.
3. **HTML**: Hypertext Markup Language is the standard markup language for documents designed to be displayed in a web browser. It can be assisted by technologies such as Cascading Style Sheets and scripting languages such asJavaScript.
4. **CSS:** Cascading Style Sheets is a style sheet language used for describing the presentation of a document written in a markup language such as HTML. CSSis a cornerstone technology of the World Wide Web, alongside HTML and JavaScript. Django: Django is a Python-based free and open-source web framework that follows the modeltemplate-views architectural pattern.

5. **SQL lite Database:** SQLite is a relational database management system contained in a C library. In contrast to many other database management systems, SQLite is not a client–server database engine. Rather, it is embedded into the end program

Feasibility

By speaking of feasibility, we mean a cost-effective, scalable, secure, and easy-to- deploy system (or subsystem). Any blockchain-based solution should be (noticeably) cheaper than the traditional elections in the long term, say in a 3-years period with at least 1 elections per year.

It should not be more expensive than non-blockchain solutions either. The system should support millions of people, depending on the country, business size or target group population. The security level should not be lower than non-blockchain solutions. Blockchain solutions are suitable, when the following characteristics are present in the legacy subject systems:

- Shared data: When there is structured information which should be sharedbetween entities.
- Multiple parties: When there is a need for more than one entity which reads orwrites the data.
- Low trust: When there is no presumed full trust between the members of thesystem.
- No trusted third party: If it is not available or not preferred due toimplementation difficulties or costs.
- Auditability: If we want the records to be immutable (not to be changed ordeleted after recording.

- Financial Aspects

  Undoubtedly, using automated electronic systems, including web portals and mobile applications, will lower the administrative costs in the long term, despite their higher initial investment costs . A previous study showing a rough comparison regarding infrastructure and maintenance costs of traditional and electronic elections was recently made . Per to the study, the advantages of switching to an online elections system may provide savings up to several times per year.

- Security and Reliability

  The security services that the blockchain provides is compared with other database solutions. The blockchain provides transparency with anonymity. The privacy is not aimed but can be implemented. In blockchain Each block keeps the hash of the previous block and this eventually provides a chain of blocks that are linked to each thus any change in any block leads to the change of the hash of that block and there is a change in whole blockchain. Merkle tree is used in order to keep the integrity of the records.

Scope/Objective

Traditional elections satisfy neither citizens nor political authorities in recent years. They are not fully secure since it is easy to attack votes. It threatens also privacy and transparency of voters. Additionally, it takes too much time to count the votes. This paper proposes a solution using Blockchain to eliminate all disadvantages of conventional elections. Security and data integrity of votes is absolutely provided theoretically. Voter privacy is another requirement that is ensured in the system. Lastly, waiting time for results decreased significantly in proposed Blockchain voting system.

Considering today's technology, blockchain may create one of the most prominent alternative to traditional voting in terms of security, consistency and speed. While designing a chain for voting in a crowded country, the system should be secure. Many aspects should be considered in order to construct a secure blockchain-based election system. First factor is human for such a system. In the solution, human interference is absolutely prohibited. The proposed system will be consisting of nodes (computers in design) that is closed to human interference. Any input that cannot be considered as

vote will be ignored in this system. For such a system, stealing votes or changing votes are totally blocked. Second issue is saving system from hackers. In order to manipulate votes, hackers need to enter the system as a citizen at proposed solution. Also, it is guaranteed that a citizen can only vote for one time. When citizen cast a ballot, e- government system will be informed without revealing any information about vote. Then, egovernment system marks that person as voted. In a blockchain system, every transaction is related to the previous one. So, changing an accepted transaction is impossible for such a system. Due to the consistency of the blockchain, data will always be consistent and voting will be reliable.

Table 1. Comparison of current blockchain-based electronic voting systems.

Online Voting Platforms	Framework	Language	Cryptographic Algorithm	Consensus Protocol	Main Features (Online Blockchain Voting System)							
					Audit	Anonymity	Verifiability by Voter	Integrity	Accessibility	Scalability	Accuracy/ Correctness	Affordability
Follow My Vote	Bitcoin	C++/Python	ECC	PoW	✓	✓	✓	✓	✓	✗	✓	✓
Voatz	Hyperledger Fabric	Go/JavaScript	AES/GCM	PBFT	✓	✓	✓	✓	✓	✗	✓	✓
Polyas	Private/local Blockchains	NP	ECC	PET	✓	✓	✓	✓	✓	✗	✓	NA
Luxoft	Hyperledger Fabric	Go/JavaScript	ECC/ElGamal	PBFT	✓	✓	✓	✓	✓	✗	✓	✓
Polys	Ethereum	Solidity	Shamir's Secret Sharing	PoW	✓	✓	✓	✓	✓	✗	✓	✓
Agora	Bitcoin	Python	ElGamal	BFT-r	✓	✓	✓	✓	✓	✗	✓	✓

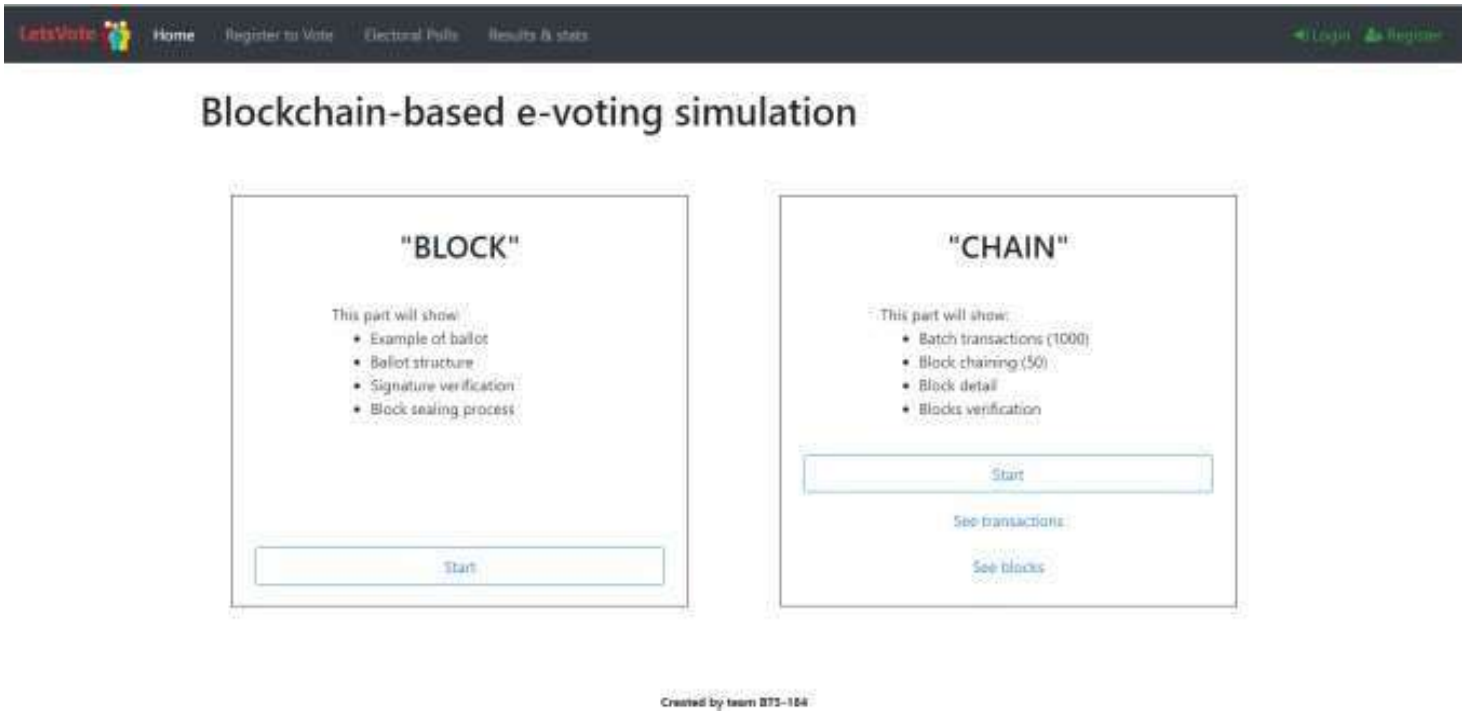
Table 2. Scalability analysis of famous blockchain platforms.

Framework	Year Release	Generation Time	Hash Rate	Transactions Per Sec	Cryptographic Algorithm	Mining Difficulty	Power Consumption	Reward/Block	Scalability
Bitcoin	2008	9.7 min	899.624 Th/s	4.6 max 7	ECDSA	High (around 165,496,835,118)	Very High	25 BTC	Very Low
Ethereum	2015	10 to 19 s	168.59 Th/s	15	ECDSA	High (around 10,382,102)	High	5 ether	Low
Hyperledger Fabric	2015	10 ms	NA	3500	ECC	No mining required	Very Low	No built-in cryptocurrency	Good
Litecoin	2011	2.5 min	1.307 Th/s	56	Scrypt	Low 55,067	Moderate	25 LTC	Moderate
Ripple	2012	3.5 s	NA	1500	RPCA	No mining required	Very Low	Base Fee	Good
Dogecoin	2013	1 min	1.4 Th/s	33	Scrypt	Low 21,462	Low	10,000 Doge	Low
Peercoin	2012	10 min	693.098 Th/s	8	Hybrid	Moderate (476,560,083)	Low	67.12 PPC	Low

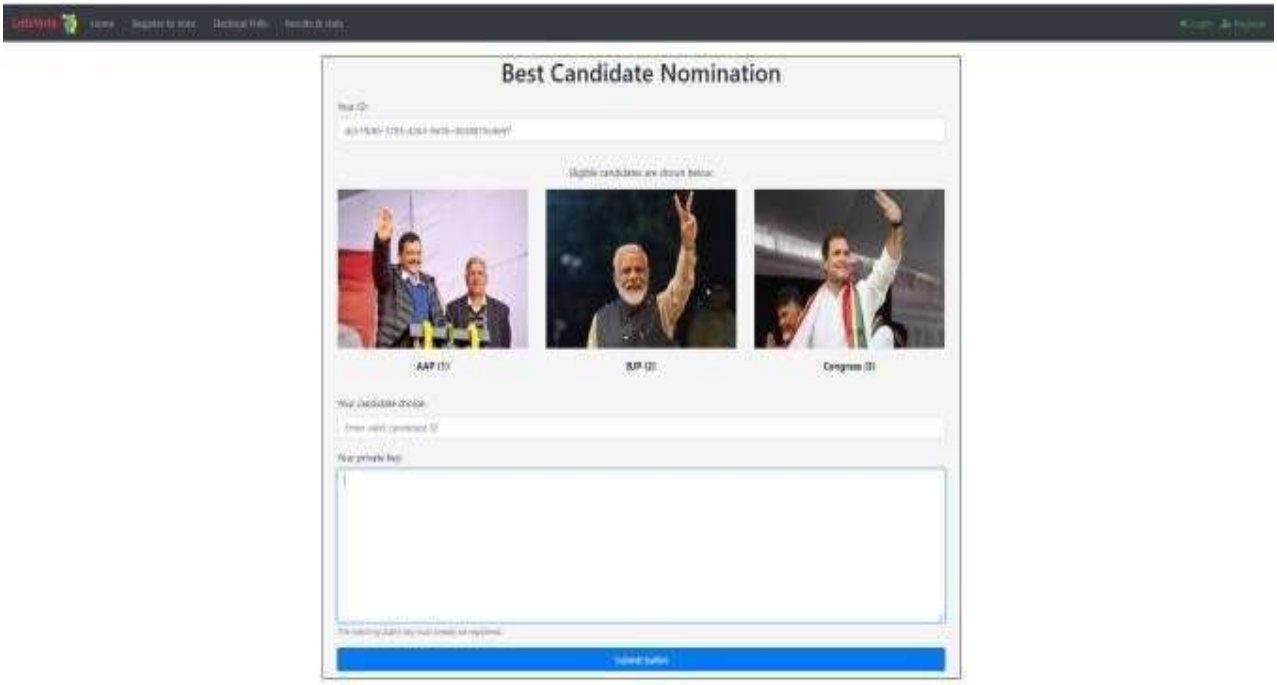
Chapter 4: Design

IX Results

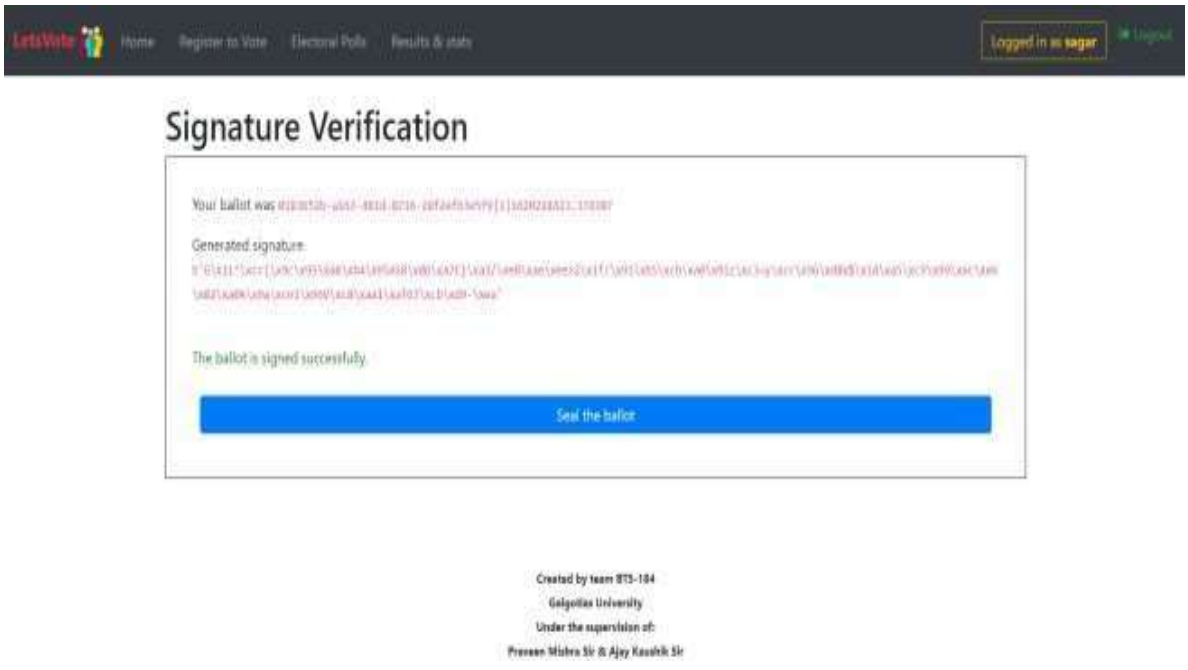
- This is the home page of the application.



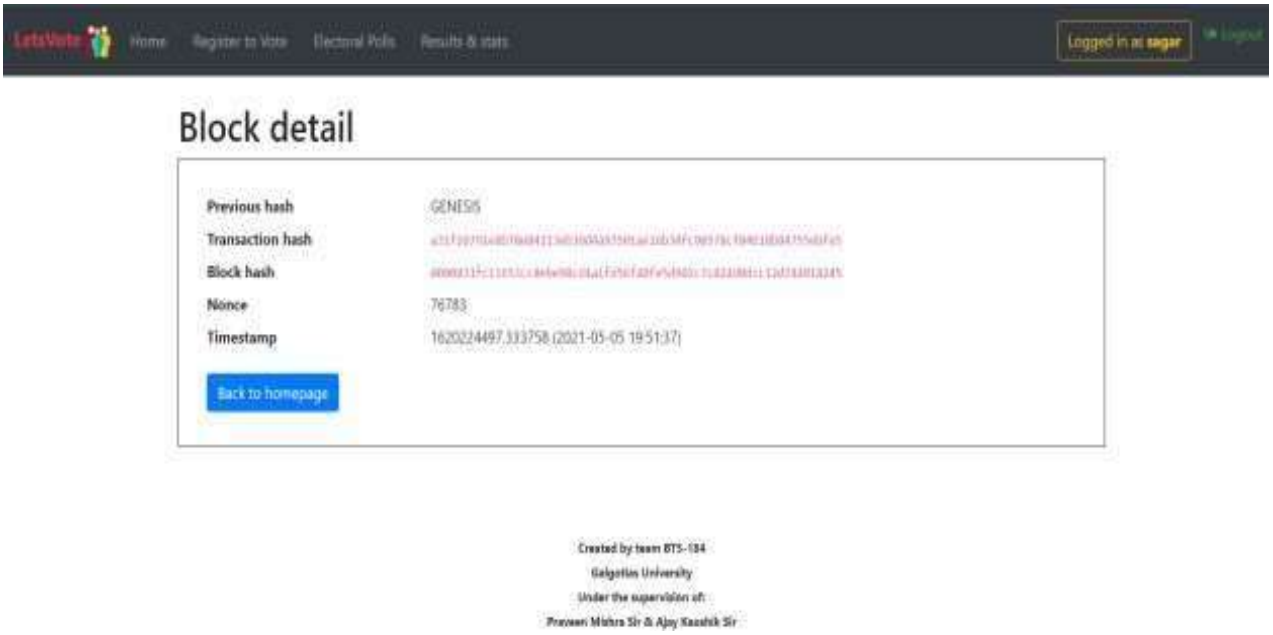
- This is the voting page , where voter can select his candidate.



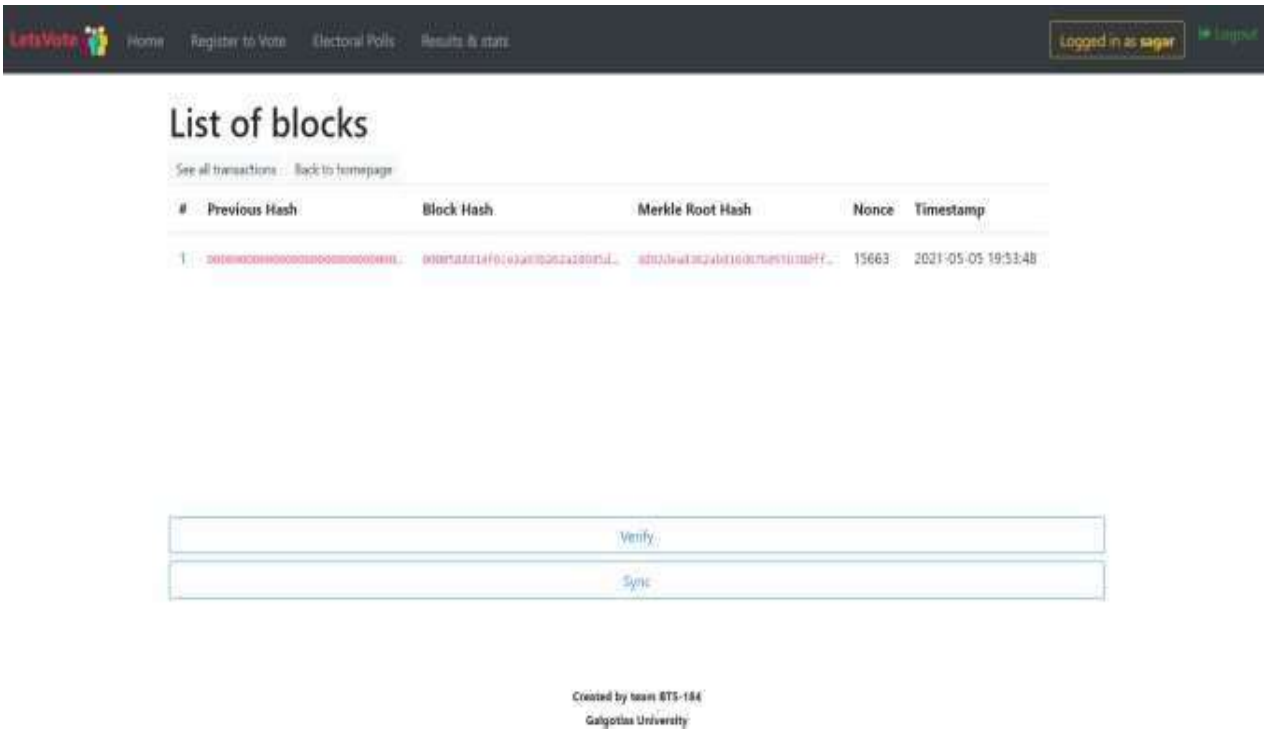
- User's Signature verification



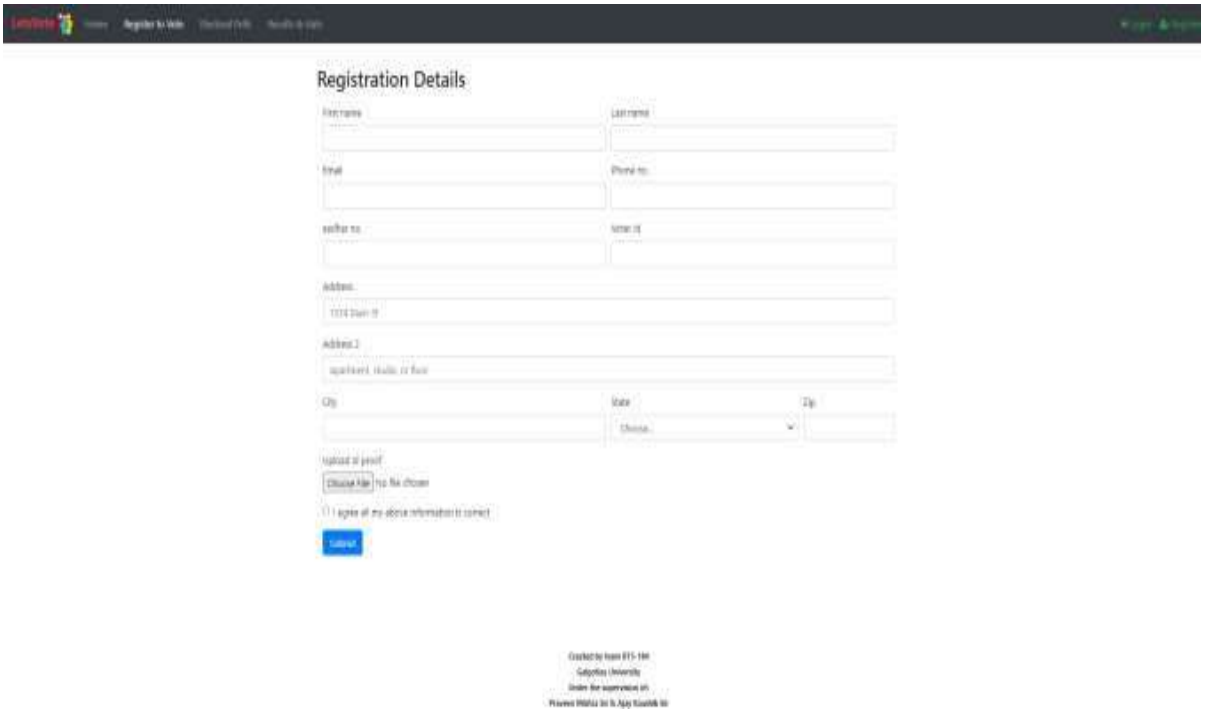
- Block Generation page



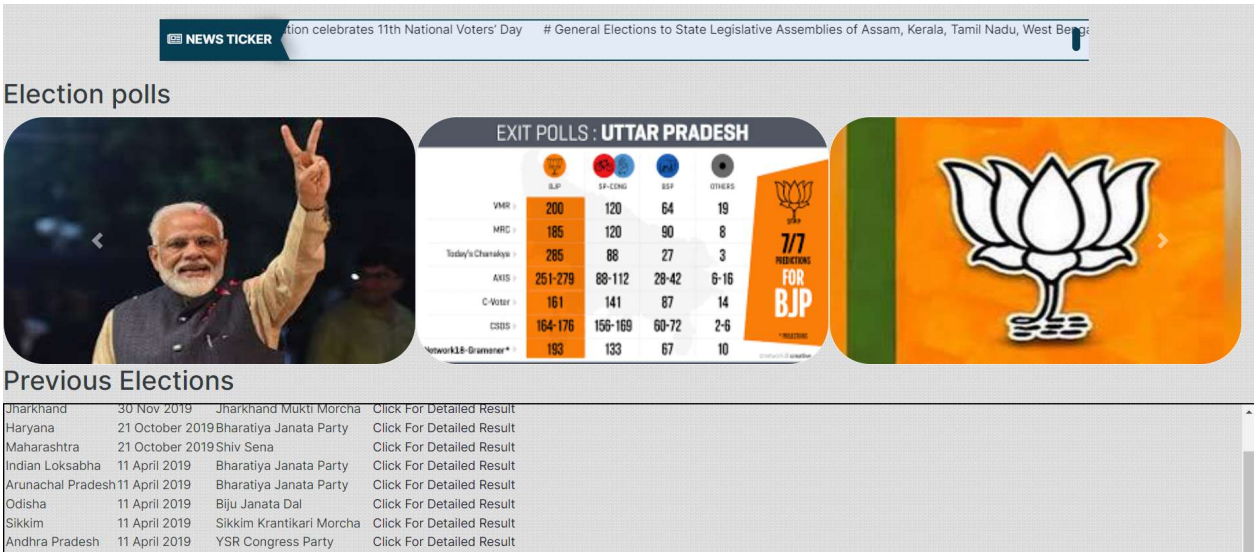
- Transactions Page



- This is the voters registration page where the data is stored in database.



- This is the polling page, where public opinion polls before actual elections are pubished.



Chapter 5: Implementation & Testing

Login Module

User Login is the first form users connected when the voting page is loaded from the internet.It will have a connection to the database to validate the user credentials. User types are either voters or Administrators. It is assumed that users have used another interface or form to register for voting. In the same login page there will be Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) validation with random numbers. Six digit random numbers will be created each time the page is loaded to be able to stop any kind of computer attacks to the voting site.

Start Election : This is automated phase. Durinng the stipulated date and time election is started . Voter can cast their vote within this time period .If anyone wants to cast vote before then he/she will be directed to page that displays correct date and time for the elections to be conducted.

Register User : In this module the user can register to the goverments database by entering the details and uploading the documents like (government ids to verify the identity of the user).

Chapter 6: Limitations and Future Scope of the Project

The voting systems that are in use till now are not as effective as they should. There are numerous problems that are discussed further in this paper
The traditional voting systems are facing the problems like:

Anonymous voting :
When a voter votes then his choice must be confidential that must not be known to anyone exceot the voter . The people involved with the maintaining of the voting machines should also be unaware of the voter's choice.

Individualised balloting process :

All the votes casted are being stored in the databases where the voterid's are mapped with the casted votes . This is a big question on the election's integrity. This can be resolved in blockchain technology by using hashing techniques to hide the choices and identities of the voters.

High costs of setup :
To conduct elections with traditional methods like EVM's require high amount of funds as there are the costs of setting up of the electronic voting machines, then their maintenance also it requires costs to provide protection to these EVM's till the election. results are declared. Thus this is not an economic way to conduct elections.

• Problems with the security :
This is the biggest problem when it comes to conductig elections in an unbiased way as fair elections decide the future of the nation. There are various attacks possible thatcould easily give hackers access to databases where the casted votes are stored. Also there are some external chips that are installed in the voting machines that manipulates the votes after the voter has voted his choice. To avoid these attacks there should be a system that prevents it and if tried to tamper anything with the votes it gets caught. Blockchain technology premits it as all the

blocks are linked together , a change in hash of a block will notify the whole next blocks as manipulated or tampered and this could be easily verified by the other blockchains running on other nodes.

Conclusions

The concept of adapting these virtual vote casting mechanisms to conduct the elections in more cheaper way and in an unibiased manner with trust using blockchain technology is mere a difficult task but not impossible. This being the most advantageous of all techniques and being the future of technology should be implemented and take these procedures to a higher level of advancements.

References

[1] M. Daniel, “Blockchain Technology: The Key to Secure Online Voting”, BitcoinMagazine, Jun. 2015.

[2] U.S. Official: Hackers targeted voter registration systems of 20 states, AssociatedPress, Sep. 2016.

[3] R. Osgood, “The Future of Democracy: Blockchain Voting,” 2016.
[4] K.Hegadekatti, “Democracy 3.0: Voting Through the Blockchain,” 2017.

[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.

[5] 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.

[6] 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.

[7] A. Barnes, C. Brake, and T. Perry, “Digital Voting with the use of Blockchain Technology,” Available: https://www.economist.com/sites/default/files/plymouth.pdf [Nov. 20, 2018]

[8] M. Pawlak, A. Poniszewska-Marańda and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Procedia Computer Science, vol. 141, pp. 239- 246, 2018.

[9] P. Tarasov and H. Tewari, "The Future of E-voting," IADIS International Journal on Computer Science and Information Systems, vol. 12, no. 2, pp. 148-165.

[10] Bartolucci, S., Bernat, P., & Joseph, D. (2018). SHARVOT: Secret SHARe-Based VOTing on the Blockchain. 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 30-34.

[11] A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", Future Generation Computer Systems, vol. 88, pp. 173-190, 2018.

[12] B. Wang, J. Sun, Y. He, D. Pang and N. Lu, "Large-scale Election Based On Blockchain", Procedia Computer Science, vol. 129, pp. 234- 237, 2018.