

ONLINE VOTING USING BLOCKCHAIN

at

**Sathyabama Institute of Science and Technology
(DEEMED TO BE UNIVERSITY)**

Submitted in partial fulfillment of the requirements for the award of
Bachelor Engineering Degree in Computer Science and Engineering

By

DIPTANIL SAHA (Reg. No. 37110194)



***DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING***

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY (DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC | 12B Status by

UGC | Approved by AICTE

JEPPIAAR NAGAR, RAJIV GANDHI SALAI,

CHENNAI - 600 119

March - 2021



SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**



Accredited with Grade "A" by NAAC
(Established under Section 3 of UGC Act, 1956)
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI- 600119
www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this project report is the bonafide work of G DIPTANIL **SAHA** (Reg. No. 37110194) who carried out the project entitled "**ONLINE VOTING USING BLOCKCHAIN**" under my supervision from **August 2020** to **March 2021**.

Internal Guide

Dr.T.Judgi, M.E., PhD,

Head of the Department

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I **Diptanil Saha (37110194)** hereby declare that the Project Report entitled **“ONLINE VOTING USING BLOCKCHAIN”** is done by me under the guidance of **Dr.T.Judgi, M.E., PhD**, Department of Computer Science and Engineering at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala, M.E., Ph.D., Dean**, School of Computing, **Dr. S. Vigneswari, M.E., Ph.D., and Dr. L. Lakshmanan, M.E., Ph.D., Heads of the Department** of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.T.Judgi, M.E., PhD, Professor** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

The aim of this report is to outline our proposal to solving the issues of digital voting by using blockchain technology. The report starts by introducing the problems with current voting practices, it then goes into a brief explanation of what blockchain technology is and how it is currently used. The following section looks at present day deployments of digital voting and the issues they face. The main section of the report is a detailed breakdown of our proposed design followed by an analysis of potential flaws and threats. The final section is a conclusion of how we feel our design solves the issue at hand. First we voted in online, then will RSA key generation to validate the votes. finally blockchain concept will rectifying the problem.

TABLE OF CONTENTS

CHAPTER No	TITLE	PAGE
1	INTRODUCTION	1
2	SYSTEM ANALYSIS	2
2.1	Existing system	2
2.2	Proposed system	2
3	REQUIREMENTS SPECIFICATION	3
3.1	Introduction	3
3.2	Hardware and Software specification	6
3.3	Technologies Used	6
4.1	Design and Implementation Constraints	24
4.2	Other Nonfunctional Requirements	25
5	Architecture Diagram	27
5.1	Result	29
5.2	Conclusion	30
5.3	Future Enhancement	31
	SCREENSHOTS	44
	REFERENCES	45

CHAPTER 1

INTRODUCTION

Aim:

This paper aim to give online voting using blockchain.

Synopsis:

Building an electronic voting system that satisfies the legal requirements of legislators has been a challenge for a long time. Distributed ledger technologies is an exciting technological advancement in the information technology world. Block chain technologies offer an infinite range of applications benefiting from sharing economies. This paper aims to evaluate the application of blockchain as service to implement distributed electronic voting systems. The paper elicitates the requirements of building electronic voting systems and identifies the legal and technological limitations of using blockchain as a service for realizing such systems. The paper starts by evaluating some of the popular blockchain frameworks that offer blockchain as a service. We then propose a novel electronic voting system based on blockchain that addresses all limitations we discovered. More generally this paper evaluates the potential of distributed ledger technologies through the description of a case study, namely the process of an election and implementing a blockchain-based application which improves the security and decreases the cost of hosting a nationwide election.

CHAPTER 2

SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

It evaluates the use of blockchain as a service to implement an electronic voting (e-voting) system. The paper makes the following original contributions

- (i) research existing blockchain frameworks suited for constructing blockchain based e-voting system.
- (ii) In existing use only blockchain for retrieve the data's.
- (iii) User can voted twice or thrice.
- (iv) No attackers used in previous process.

Disadvantages of Existing System

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

2.2 PROPOSED SYSTEM

- 1) A blockchain-based evoting system that uses “permissioned blockchain” to enable liquid democracy
- 2) Rsa key used
- 3) generate hashing values accuracy

REQUIREMENT

SPECIFICATIONS

3.1 INTRODUCTION

Building an electronic voting system that satisfies the legal requirements of legislators has been a challenge for a long time. Distributed ledger technologies is an exciting technological advancement in the information technology world. Block chain technologies offer an infinite range of applications benefiting from sharing economies. This paper aims to evaluate the application of blockchain as service to implement distributed electronic voting systems. The paper elicitates the requirements of building electronic voting systems and identifies the legal and technological limitations of using blockchain as a service for realizing such systems. The paper starts by evaluating some of the popular blockchain frameworks that offer blockchain as a service. We then propose a novel electronic voting system based on blockchain that addresses all limitations we discovered. More generally this paper evaluates the potential of distributed ledger technologies through the description of a case study, namely the process of an election and implementing a blockchain-based application which improves the security and decreases the cost of hosting a nationwide election.

1. Ali KaanKoc, EmreYavuz,Umut Can Cabuk,GokhanDalkoloc "Towards Secure E-Voting Using EthereumBlockchain", 978-1-5386-3449-3/18/\$31.00 ©2018 IEEE.

Ali KaanKoc, EmreYavuz,Umut Can Cabuk,Gokhan Dalkoloc, building smart contract of ours, we have succeeded in moving e-voting to the blockchain platform and we addressed some of the fundamental issues that traditional e- voting systems have, by using the potential

of the Ethereum network and the blockchain structure. As a result of trials, the concept of blockchain and the security methodology which it uses, namely immovable hash chains, has become adaptable to polls and elections.

2. F. Hao and P.Y.A. Ryan, Real-World Electronic Voting: Design, Analysis and Deployment, CRC Press, pp. 143-170, 2017.

The idea of e-voting is considerably older than blockchain. So that, all celebrated examples to this point used suggests that of centralized computation and storage models. Esthonia may be a excellent example, since the govt of Esthonia is one in every of the primary to implement a totally on-line and comprehensive evoting resolution.

3. Rifa Hanifatunnisa,Budi Rahardjo”Blockchain Based E-Voting Recording System Design”
978-1-5386-3546-9/17/\$31.00 ©2017 IEEE

The utilization of the grouping proposed in the blockchain creation process in this framework considers that in a constituent framework not required for mining as in the Bitcoin framework in light of the fact that the voter information and numbers are clear and are not permitted to choose more than once, the proposed succession guarantees that all hubs Which is legitimately associated and can maintain a strategic distance from impact in transportation. Likewise ensure all hubs that have enrolled the outcomes are incorporated into the figuring procedure. As far as expense can likewise be more effective on the grounds that it doesn't require hardware that is dependably changed in every race did. In light of the structure and the consequences of research led, it very well may be presumed that the framework is effective usefulness of chronicle the e-casting a ballot framework dependent on Blockchain

innovation.

4. Sathya V. ; Arpan Sarkar ; Aritra Paul ; Sanchay Mishra “Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting”IEEE 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)

Voting is a tedious task in this nation. The highest amount of controversies and corruptions are involved along this path. A nation needs a fair and unbiased election for the masses to redeem their right to elect the leader of their choice. The latest trends of EVM (Electronic Voting Machine) hacking has taken over the ability to hold a clear and transparent election. In this paper, we discuss an innovative approach by imbibing the latest technologies with the traditional voting methods. The technology involves a secure data storage technique named as block chain which is used for cryptocurrencies and is proven [7] for its security. The votes which are recorded by the EVM will be updated with the cloud-based storage (SAAS). Any changes made to the voting panel or tampering with the votes will cause the hash to break the link and by detecting the manipulated votes, any discrepancy can be removed by marking them as NOTA, hence not affecting the polling by any means. Blockchain technology has a significant feature of Proof-of-Work which does not allow the continuous creation of data blocks hence protecting the rapid manipulation of data. Also, this system only requires uploading the hashes created along with the blocks which are stored in a hash table [12] on the cloud. The data of the EVM, when tallied with the hash table, can help in identifying the point of manipulation. Moreover, the areas with no broadband internet connection can also implement these techniques as it required only a few kilobytes of upload data rate to update the hash values. The already existing UIDAI based biometric system already adds an extra

layer of security to the voting system. Each vote will be treated as a single block of data. Also, as added features of block chain technology, the P2P (Peer to Peer) network allows only communication between two already connected peers. Man-in-Middle attacks are impossible in this case as the blockchain proof-of-work does not allow mass updating of data ...

5. Dina MOLOJA, Noluntu MPEKOA, "Securing M-voting Using Cloud Intrusion Detection and Prevention System: A New Dawn", ST-Africa 2017 IEEE Conference Proceedings.

Democracy has been transformed by the introduction of ICT, which is known as e-voting. E-voting is the use of computerised equipment to cast votes. M-voting is a subset of e-voting and is the use of mobile phones to cast a vote outside the restricted electoral boundaries. M-voting has a feature that is different from other e-voting solutions: the mobile-phone. Mobile-phones are pervasive; they offer connection everywhere at any time. However, using a fast growing device such as mobile-phone as a tool to cast a vote can raise questions when coming to its security. This paper designed and developed a security solution termed a cloud intrusion detection and prevention system which endeavours to secure the voters' mobile phone while casting their vote. The security system was developed using android version 6.0 for android phones and MySQL. Simulations were used to evaluate the system and results indicate that the proposed system is efficient, reliable and secure.

6.A Comparative Analysis on E-Voting System Using Blockchain

Authors: Kanika Garg ; Pavi Saraswat ; Sachin Bisht ; Sahil Kr. Aggarwal ; Sai Krishna Kothuri ; Sahil Gupta, 2019 4th International Conference on Internet of Things: Smart

Innovation and Usages (IoT-SIU)

In a democratic country like India (which is the largest democracy in the world), Voting plays a major role in the selection of government officials as well as showing our opinion how the governing body to be formed. Time to time, researches are conducted in order to tackle the difficulties in the centralized voting system to make it more anonymous, reliable and secure while preventing any kind of frauding. Even though the use of e-voting through the electronic medium, we have to face well-known problems of maintenance and fraud. Currently, various researches are conducting in-order to make secure and reliable voting system while tackling issues of anonymity and security. Through Decentralized System, focus is drifting towards making Voting Process simple, secure and anonymity in the hand of the public. This paper presents a literature review on the papers and the techniques used to tackle voting challenges.

7.Decentralized E-Voting Portal Using Blockchain

Authors: Kriti Patidar ; Swapnil Jain, 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)

Online voting is an alternative to age old paper ballot system and the currently popular electronic voting machines (EVM). An electronic voting portal should offer security and integrity along with the transparency of votes and privacy of voters. This paper proposes an e-voting system based on blockchain that eliminates some of the limitations in existing voting systems. The paper also presents state of art of some blockchain frameworks for e-voting. The presented implementation is suitable for small scale elections like inside corporate houses, board rooms etc. The implementation uses smart contract from Ethereum. Truffle framework is used in this paper for development, testing and deploying smart contracts.

Ganache is used as Ethereum client for testing. Here Meta-mask is used as browser wallet.

8.E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy

Authors: Freya Sheer Hardwick ; Apostolos Gioulis ; Raja Naeem Akram ; Konstantinos Markantonakis

2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData)

Technology has positive impacts on many aspects of our social life. Designing a 24 hour globally connected architecture enables ease of access to a variety of resources and services. Furthermore, technology like the Internet has been a fertile ground for innovation and creativity. One such disruptive innovation is blockchain - a keystone of cryptocurrencies. The blockchain technology is presented as a game changer for many of the existing and emerging technologies/services. With its immutability property and decentralised architecture, it is taking centre stage in many services as an equalisation factor to the current parity between consumers and large corporations/governments. One potential application of the blockchain is in e-voting schemes. The objective of such a scheme would be to provide a decentralised architecture to run and support a voting scheme that is open, fair, and independently verifiable. In this paper, we propose a potential new e-voting protocol that utilises the blockchain as a transparent ballot box. The protocol has been designed to adhere to fundamental e-voting properties as well as offer a degree of decentralisation and allow for the voter to change/update their vote (within the permissible voting period). This paper highlights

the pros and cons of using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts. Concluding the paper is a potential roadmap for blockchain technology to be able to support complex applications.

9. VoteChain: A Blockchain Based E-Voting System

Archit Pandey ; Mohit Bhasi ; K. Chandrasekaran

2019 Global Conference for Advancement in Technology (GCAT)

In the past, electronic voting systems have not seen widespread adoption due to data privacy concerns. Previously proposed e-voting systems make use of a central database to store data, resulting in the servers used to store these databases being a single point of failure. These systems have also been found to be vulnerable to DoS attacks, leading to concerns over their reliability. Blockchains have been used to build secure and scalable distributed systems which have shown several benefits over centralized systems. They have seen uses in sectors ranging from finance and healthcare to food and energy. In this paper, we present VoteChain, a blockchain based voting system to help bring transparency and security to polls. We report on our implementation of VoteChain, as well as the results obtained in testing the system in a real-world poll which prove that such a system can be used in practice for large-scale elections

10. Towards secure e-voting using ethereum blockchain

Authors; Emre Yavuz ; Ali Kaan Koç ; Umut Can Çabuk ; Gökhan Dalkılıç, 2018 6th International Symposium on Digital Forensic and Security (ISDFS)

There is no doubt that the revolutionary concept of the blockchain, which is the underlying technology behind the famous cryptocurrency Bitcoin and its successors, is triggering the start of a new era in the Internet and the online services. While most people focus only at cryptocurrencies; in fact, many administrative operations, fintech procedures, and everyday services that can only be done offline and/or in person, can now safely be moved to the Internet as online services. What makes it a powerful tool for digitalizing everyday services is the introduction of smart contracts, as in the Ethereum platform. Smart contracts are meaningful pieces of codes, to be integrated in the blockchain and executed as scheduled in every step of blockchain updates. E-voting on the other hand, is another trending, yet critical, topic related to the online services. The blockchain with the smart contracts, emerges as a good candidate to use in developments of safer, cheaper, more secure, more transparent, and easier-to-use e-voting systems. Ethereum and its network is one of the most suitable ones, due to its consistency, widespread use, and provision of smart contracts logic. An e-voting system must be secure, as it should not allow duplicated votes and be fully transparent, while protecting the privacy of the attendees. In this work, we have implemented and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language. Android platform is also considered to allow voting for people who do not have an Ethereum wallet. After an election is held, eventually, the Ethereum blockchain will hold the records of ballots and votes. Users can submit their votes via an Android device or directly from their Ethereum wallets, and these transaction requests are handled with the consensus of every single Ethereum node.

3.2 HARDWARE AND SOFTWARE SPECIFICATION

3.2.1 HARDWARE REQUIREMENTS

Hard Disk	:	500GB and Above
RAM	:	4GB and Above
Processor	:	I3 and Above
Webcam	-	1

3.2.2 SOFTWARE REQUIREMENTS

- ✓ Operating System : Windows 7 , 8, 10 (64 bit)
- ✓ Software : Python
- ✓ Tools : Python 3.7 IDLE, jupyter Note Book and Spyder

3.3 TECHNOLOGIES USED

BLOCK CHAIN

3.3.1 Introduction to Python

Python is a widely used general-purpose, high level programming language. It was initially designed by Guido van Rossum in 1991 and developed by Python Software Foundation. It was mainly developed for emphasis on code readability, and its syntax allows programmers to express concepts in fewer lines of code.

Python is a programming language that lets you work quickly and integrate systems more efficiently.

It is used for:

- web development (server-side),
- software development,
- mathematics,
- System scripting.

What can Python do?

- Python can be used on a server to create web applications.
- Python can be used alongside software to create workflows.
- Python can connect to database systems. It can also read and modify files.
- Python can be used to handle big data and perform complex mathematics.
- Python can be used for rapid prototyping, or for production-ready software development.

Why Python?

- Python works on different platforms (Windows, Mac, Linux, Raspberry Pi, etc).
- Python has a simple syntax similar to the English language.
- Python has syntax that allows developers to write programs with fewer lines than some other programming languages.
- Python runs on an interpreter system, meaning that code can be executed as soon as it is written. This means that prototyping can be very quick.
- Python can be treated in a procedural way, an object-orientated way or a functional way.

Good to know

- The most recent major version of Python is Python 3, which we shall be using in this tutorial. However, Python 2, although not being updated with anything other than security updates, is still quite popular.
- Python 2.0 was released in 2000, and the 2.x versions were the prevalent releases until December 2008. At that time, the development team made the decision to release version 3.0, which contained a few relatively small but significant changes that were not backward compatible with the 2.x versions. Python 2 and 3 are very similar, and some

features of Python 3 have been backported to Python 2. But in general, they remain not quite compatible.

- Both Python 2 and 3 have continued to be maintained and developed, with periodic release updates for both. As of this writing, the most recent versions available are 2.7.15 and 3.6.5. However, an official End Of Life date of January 1, 2020 has been established for Python 2, after which time it will no longer be maintained.
- Python is still maintained by a core development team at the Institute, and Guido is still in charge, having been given the title of BDFL (Benevolent Dictator For Life) by the Python community. The name Python, by the way, derives not from the snake, but from the British comedy troupe Monty Python's Flying Circus, of which Guido was, and presumably still is, a fan. It is common to find references to Monty Python sketches and movies scattered throughout the Python documentation.
- It is possible to write Python in an Integrated Development Environment, such as Thonny, Pycharm, Netbeans or Eclipse which are particularly useful when managing larger collections of Python files.

Python Syntax compared to other programming languages

- Python was designed to for readability, and has some similarities to the English language with influence from mathematics.
- Python uses new lines to complete a command, as opposed to other programming languages which often use semicolons or parentheses.
- Python relies on indentation, using whitespace, to define scope; such as the scope of loops, functions and classes. Other programming languages often use curly-brackets for this purpose.

Python is Interpreted

- Many languages are compiled, meaning the source code you create needs to be translated into machine code, the language of your computer's processor, before it can be run. Programs written in an interpreted language are passed straight to an interpreter that runs them directly.

- This makes for a quicker development cycle because you just type in your code and run it, without the intermediate compilation step.
- One potential downside to interpreted languages is execution speed. Programs that are compiled into the native language of the computer processor tend to run more quickly than interpreted programs. For some applications that are particularly computationally intensive, like graphics processing or intense number crunching, this can be limiting.
- In practice, however, for most programs, the difference in execution speed is measured in milliseconds, or seconds at most, and not appreciably noticeable to a human user. The expediency of coding in an interpreted language is typically worth it for most applications.
- For all its syntactical simplicity, Python supports most constructs that would be expected in a very high-level language, including complex dynamic data types, structured and functional programming, and object-oriented programming.
- Additionally, a very extensive library of classes and functions is available that provides capability well beyond what is built into the language, such as database manipulation or GUI programming.
- Python accomplishes what many programming languages don't: the language itself is simply designed, but it is very versatile in terms of what you can accomplish with it.

Block chain is a technology that is rapidly gaining momentum in era of industry 4.0. With high security and transparency provisions, it is being widely used in supply chain management systems, healthcare, payments, business, IoT, voting systems, etc.

Why do we need it?

Current voting systems like ballot box voting or electronic voting suffer from various security threats such as DDoS attacks, polling booth capturing, vote alteration and manipulation, malware attacks, etc, and also require huge amounts of paperwork, human resources, and time. This creates a sense of distrust among existing systems.

Some of the disadvantages are:

Long Queues during elections

Security Breaches like data leaks, vote tampering.

Lot of paperwork involved, hence less eco-friendly and time-consuming.

Difficult for differently-abled voters to reach polling booth.

Cost of expenditure on elections is high.

Solution :

Using blockchain, voting process can be made more secure, transparent, immutable, and reliable.

How? Let's take an example.

Permissioned blockchain

There are many benefits of permissioned blockchains.

1.Efficient performance: When we compared permissioned blockchains to public blockchains, they offer better performance. The core reason behind is the limited number of nodes on the platform. This removes the unnecessary computations required to reach consensus on the network, improving the overall performance. On top of that, permissioned networks have their own pre-determined nodes for validating a transaction.

2.Proper governance structure- Permissioned networks do come with an appropriate structure of governance. This means that they are organized. Administrators also require less time to update the rules over the network, which is considerably faster when compared to public blockchains. Public blockchain network suffers from the consensus problem as not all nodes work together to get the new update implemented. These nodes might place their self-interest above the needs of the blockchain, which, in return, means slower updates to the whole network. In comparison, permissioned blockchain doesn't have the problem, as the nodes work together to move the updates faster.

3.Decentralized storage: Permissioned networks also make proper use of blockchain, including utilizing its decentralized nature for data storage.

4.Cost Effective – There is no doubt that permissioned blockchains are more cost-effective

3.3 Blockchain:

A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data.

4.METHODOLOGY

4.1 SYSTEM DESIGN

System Design involves identification of classes their relationship as well as their collaboration. In object-oriented design, classes are divided into entity classes and control classes. The Computer Aided Software Engineering (CASE) tools that are available commercially do not provide any assistance in this transition. CASE tools take advantage of Meta modeling that is helpful only after the construction of the class diagram. In the FUSION method some object-oriented approach like Object Modeling Technique (OMT), Classes, and Responsibilities. Collaborators (CRC), etc, are used. Object-oriented design uses the term "agents" to represent some of the hardware and software system. In Fusion method, there is no requirement phase, where a user will supply the initial requirement document. Any software project is worked out by both the analyst and the designer. The analyst creates the user case diagram. The designer creates the class diagram. But the designer can do this only after the analyst creates the use case diagram. Once the design is over, it is essential to decide which software is suitable for the application

4.2 ALGORITHM USED:

🌐 SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA). They are built using the Merkle–Damgård structure, from a one-way compression function itself built using the Davies–Meyer structure from a (classified) specialized block cipher.

🌐 SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

🌐 SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words,

respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are truncated versions of SHA-256 and SHA-512 respectively, computed with different initial values.

🌐 Currently, the best public attacks break preimage resistance for 52 out of 64 rounds of SHA-256 or 57 out of 80 rounds of SHA-512, and collision resistance for 46 out of 64 rounds of SHA-256.

4.3 Modules description:

4.3.1 Modules:

Login:

User & admin are login to enter the system

✦ Username

✦ password

1. Voters detail module

Voter register their details to get username & password. They details are

🌐 Name

🌐 voter id

🌐 DOB

🌐 Username

🌐 Password

🌐 Login the system & voted the parties.voted only once,if do next means alert msg shown.

4.4 Blockchain module:

A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once,

solving the long-standing problem of double spending. A blockchain has been described as a value-exchange protocol. A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

4.5 project Process Description

we create a webpage(html/css) , use ASp.net code and connect sql database.

there are five modules

- ☞ register
- ☞ login
- ☞ hashing
- ☞ blockchain
- ☞ user verification

voters will register first, login and put a voting for any party at once. we try again, msg "you are already voted". once we voted it will be stored in database. sha-256 algorithm is for encryption. parties will hash on blockchain part and be stored.

4.6 Algorithm: SHA-256

SHA-256 is a one-way function that converts a text of any length into a string of 256 bits. This is known as a hashing function. In this case, it is a cryptographically secure hashing function, in that knowing the output tells you very little about the input. It is a modified version of SHA1, which in turn is a modified SHA0. All three are now broken, to some extent.

Note 1: All variables are 32 bit unsigned integers and addition is calculated modulo 2³²

Note 2: For each round, there is one round constant $k[i]$ and one entry in the message schedule array $w[i]$, $0 \leq i \leq 63$

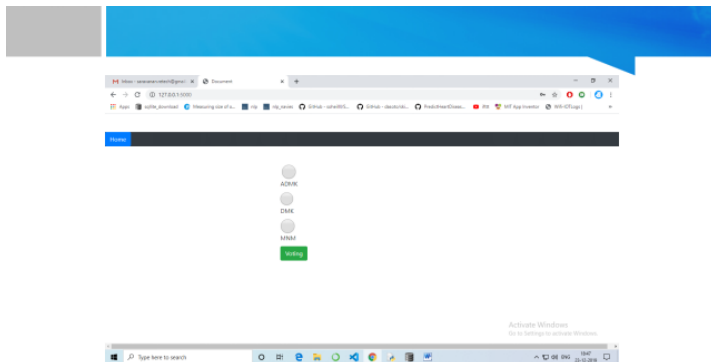
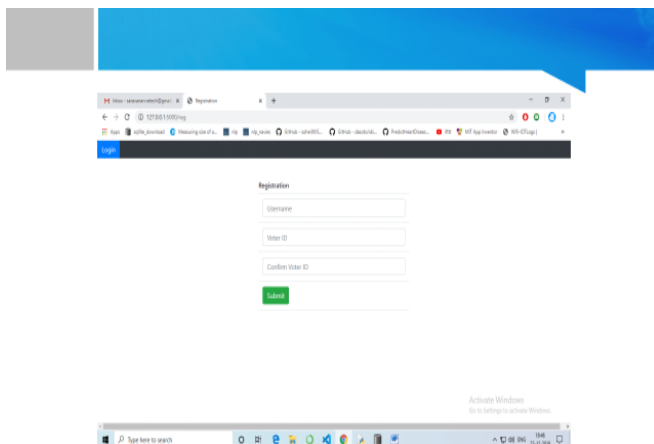
Note 3: The compression function uses 8 working variables, a through h

Note 4: Big-endian convention is used when expressing the constants in this pseudocode, and when parsing message block data from bytes to words, for example, the first word of the input message "abc" after padding is 0x61626380

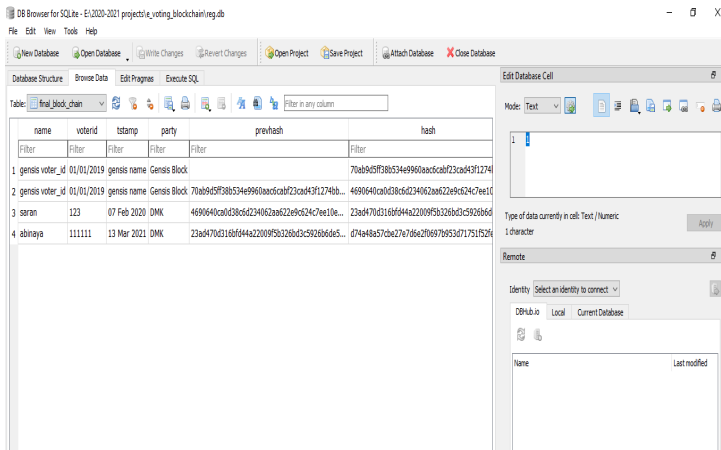
we apply sha-256 & Rsa key generation for digital voting
to hash the values & validate the vote

5.RESULT

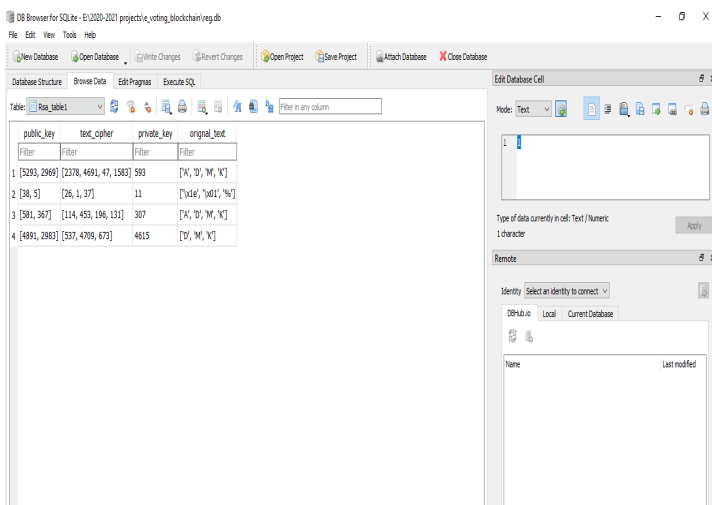
Screenshot:



```
3  #block.printHashes()
4
5  class Blockchain():
6      def __init__(self):
7          self.chain=[self.generateGenesisBlock(),]
8      def generateGenesisBlock(self):
9          return Block("genesis name","genesis voter_id","01/01/2019","Genesis Block")
10     def getLastBlock(self):
11         return self.chain[-1]
12     def addBlock(self,newBlock):
13         newBlock.prehash=self.getLastBlock().hash
14         newBlock.hash=newBlock.calcHash()
15         self.chain.append(newBlock)
16
```



Rsa:



5.1 CONCLUSION

Blockchain Technology is gaining popularity day by day. Using blockchain in voting system will help to achieve secure and cost-efficient election while guaranteeing voters privacy. Also, due to the encryption mechanism, it is impossible for any person to gain access to all the votes without first taking control of the entire service network. Everything that occurs on the blockchain is encrypted and it's possible to prove that data has not been altered. Also, it is decentralized. So it is too secure. Blockchain voting is just one of the many use cases of blockchain technology. As the world develops, the evolution of voting is imperative.

With the current voting system being so flawed and scrutinised, blockchain aims to introduce a new way for people to vote and communicate in their local and global elections.

FUTURE ENHANCEMENT

Applications to cast a ballot from cell phones can be assembled. There are two stages should have been considered to create them: Android and iOS. Appropriately, voters should download the casting a ballot application and introduce to their cell phones, at that point they will most likely vote. It is substantially more helpful in light of the fact that at the present, the vast majority use cell phones. All techniques ought to be bolstered to build up an expert E-voting framework for such stages.

REFERENCES

- [1] International Organization of Motor Vehicle Manufacturers. (2018). Pro-visional Registrations or Sales of New Vehicles. [Online]. Available: <http://www.oica.net/wp-content/uploads/>
- [2] Wards Intelligence. (2018). World Vehicles in Operation by Country, 2013_ 2017. [Online]. Available: <http://subscribers.wardsintelligence.com/databrowse- world>
- [3] National Highway Traf_c Safety Administration. (2018). Traf_c Safety Facts 2016. [Online]. Available: <https://crashstats.nhtsa.dot.gov>
- [4] G. Borghini, L. Astol_, G. Vecchiato, D. Mattia, and F. Babiloni, ``Measuring neurophysiological signals in aircraft pilots and car drivers for the assessment of mental workload, fatigue and drowsiness," *Neurosci. Biobehav. Rev.*, vol. 44, pp. 58_75, Jul. 2014.
- [5] Attention Technologies. (1999). S.a.m.g-3-Steering Attention Monitor. [Online]. Available: <https://www.zzzzalert.com>
- [6] Smart Eye. (2018). Smarteye. [Online]. Available: <https://smarteye.se/>
- [7] J. F. Henriques, R. Caseiro, P. Martins, and J. Batista, ``High-speed tracking with kernelized correlation _lters," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 37, no. 3, pp. 583_596, Mar. 2015.
- [8] P. F. Felzenszwalb, R. B. Girshick, D. McAllester, and D. Ramanan, ``Object detection with discriminatively trained part-based models," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 9, pp. 1627_1645, Sep. 2010.
- [9] Y. Sun, X. Wang, and X. Tang, ``Deep convolutional network cascade for facial point detection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2013, pp. 3476_3483.

- [10] S. Ren, X. Cao, Y. Wei, and J. Sun, "Face alignment at 3000 FPS via regressing local binary features," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2014, pp. 1685_1692.
- [11] E. Zhou, H. Fan, Z. Cao, Y. Jiang, and Q. Yin, "Extensive facial landmark localization with coarse-to-fine convolutional network cascade," in Proc. IEEE Int. Conf. Comput. Vis. Workshops, Dec. 2013, pp. 386_391.
- [12] W. Walter, "Overview of research on driver drowsiness definition and driver drowsiness detection," in Proc. Int. Tech. Conf. Enhanced Saf. Vehicles, 1995, pp. 462_468.
- [13] R. Grace, V. E. Byrne, D. M. Bierman, J.-M. Legrand, D. Gricourt, B. K. Davi, J. J. Staszewski, and B. Carnahan, "A drowsy driver detection system for heavy vehicles," in Proc. 17th AIAA/IEEE/SAE. Digit. Avionics Syst. Conf. (DASC), vol. 2, Oct. 1998, pp. I36-1_I36-8.
- [14] L. Li, Y. Chen, and Z. Li, "Yawning detection for monitoring driver fatigue based on two cameras," in Proc. 12th Int. IEEE Conf. Intell. Transp. Syst., Oct. 2009, pp. 1_6.
- [15] S. Abtahi, B. Hariri, and S. Shirmohammadi, "Driver drowsiness monitoring based on yawning detection," in Proc. IEEE Int. Instrum. Meas. Technol. Conf., May 2011, pp. 1_4.
- [16] X. Fan, B. Yin, and Y. Sun, "Yawning detection for monitoring driver fatigue," in Proc. Int. Conf. Mach. Learn. Cybern., vol. 2, Aug. 2007, pp. 664_668.
- [17] F. N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally, and K. Keutzer, "Squeezenet: Alexnet-level accuracy with 50x fewer parameters and <0.5mb model size," in Proc. ICLR, 2017, pp. 1_13.
- [18] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks," IEEE Signal Process. Lett., vol. 23, no. 10, pp.

1499_1503, Oct. 2016.

- [19] D. B. Lucas and T. Kanade, "An iterative image registration technique with an application to stereo vision," in Proc. 7th Int. Joint Conf. Artif. Intell., San Francisco, CA, USA, vol. 2, 1981, pp. 674_679.
- [20] D. S. Bolme, J. R. Beveridge, B. A. Draper, and Y. M. Lui, "Visual object tracking using adaptive correlation _lters," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., Jun. 2010, pp. 2544_2550.
- [21] F. J. Henriques, R. Caseiro, P. Martins, and J. Batista, "Exploiting the circulant structure of tracking-by-detection with kernels," in Proc. Eur. Conf. Comput. Vis., Berlin, Germany: Springer-Verlag, 2012, pp. 702_715.
- [22] Y. Li and J. Zhu, "A scale adaptive kernel correlation _lter tracker with feature integration," in Proc. Eur. Conf. Comput. Vis., L. Agapito, M. M. Bronstein, and C. Rother, Eds. Cham, Switzerland: Springer, 2015, pp. 254_265.
- [23] M. Danelljan, G. Häger, F. S. Khan, and M. Felsberg, "Discriminative scale space tracking," IEEE Trans. Pattern Anal. Mach. Intell., vol. 39, no. 8, pp. 1561_1575, Aug. 2017.
- [24] N.Wang and D.-Y.Yeung, "Learning a deep compact image representation for visual tracking," in Proc. 26th Int. Conf. Neural Inf. Process. Syst., New York, NY, USA: Curran Associates Inc., vol. 1, 2013, pp. 809_817.
- [25] M. Danelljan, G. Häger, F. S. Khan, and M. Felsberg, "Learning spatially regularized correlation _lters for visual tracking," in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Dec. 2015, pp. 4310_4318.
- [26] C. Ma, J. Huang, X. Yang, and M. Yang, "Robust visual tracking via hierarchical convolutional features," IEEE Trans. Pattern Anal. Mach. Intell., to be published.

- [27] M. Danelljan, G. Häger, F. S. Khan, and M. Felsberg, "Convolutional features for correlation filter based visual tracking," in Proc. IEEE Int. Conf. Comput. Vis. Workshop (ICCVW), Dec. 2015, pp. 621_629.
- [28] J. Valmadre, L. Bertinetto, J. Henriques, A. Vedaldi, and P. H. S. Torr, "End-to-end representation learning for correlation filter based tracking," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jul. 2017, pp. 5000_5008.
- [29] Y. Wu, T. Hassner, K. Kim, G. Medioni, and P. Natarajan, "Facial landmark detection with tweaked convolutional neural networks," IEEE Trans. Pattern Anal. Mach. Intell., vol. 40, no. 12, pp. 3067_3074, Dec. 2018.
- [30] M. Kowalski, J. Naruniec, and T. Trzcinski, "Deep alignment network: A convolutional neural network for robust face alignment," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jul. 2017, pp. 2034_2043.
- [31] D. E. King, "Dlib-ml: A machine learning toolkit," J. Mach. Learn. Res., vol. 10, pp. 1755_1758, Jul. 2009.
- [32] B. Warwick, N. Symons, X. Chen, and K. Xiong, "Detecting driver drowsiness using wireless wearables," in Proc. 12th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS), Oct. 2015, pp. 585_588.
- [33] G. Li, B.-L. Lee, and W.-Y. Chung, "Smartwatch-based wearable EEG system for driver drowsiness detection," IEEE Sensors J., vol. 15, no. 12, pp. 7169_7180, Dec. 2015.
- [34] S.-J. Jung, H.-S. Shin, and W.-Y. Chung, "Driver fatigue and drowsiness monitoring system with embedded electrocardiogram sensor on steering wheel," IET Intell. Transp. Syst., vol. 8, no. 1, pp. 43_50, 2014.

- [35] M. Omidyeganeh, A. Javadtalab, and S. Shirmohammadi, "Intelligent driver drowsiness detection through fusion of yawning and eye closure," in Proc. IEEE Int. Conf. Virtual Environ., Hum.-Comput. Interfaces Meas. Syst., Sep. 2011, pp. 1_6.
- A. Dasgupta, D. Rahman, and A. Routray, "A smartphone-based drowsiness detection and warning system for automotive drivers," IEEE Trans. Intell. Transp. Syst., to be published.
- [37] Y. Zhang and C. Hua, "Driver fatigue recognition based on facial expression analysis using local binary patterns," Optik, vol. 126, no. 23, pp. 4501_4505, Dec. 2015.
- [38] A. Picot, S. Charbonnier, A. Caplier, and N.-S. Vu, "Using retina modeling to characterize blinking: Comparison between EOG and video analysis," Mach. Vis. Appl., vol. 23, no. 6, pp. 1195_1208, Nov. 2012.
- [39] B. Akrouit and W. Mahdi, "Spatio-temporal features for the automatic control of driver drowsiness state and lack of concentration," Mach. Vis. Appl., vol. 26, no. 1, pp. 1_13, Jan. 2015.
- [40] R. O. Mbouna, S. G. Kong, and M.-G. Chun, "Visual analysis of eye state and head pose for driver alertness monitoring," IEEE Trans. Intell. Transp. Syst., vol. 14, no. 3, pp. 1462_1469, Sep. 2013,
- [41] S. M. Kamel and L. Guan, "Histogram equalization utilizing spatial correlation for image enhancement," Proc. SPIE, vol. 1199, pp. 712_723, Nov. 1989.
- [42] S. Kaplan, M. A. Guvensan, A. G. Yavuz, and Y. Karalurt, "Driver behavior analysis for safe driving: A survey," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 6, pp. 3017_3032, Dec. 2015.
- [43] R. K. Satzoda and M. M. Trivedi, "Drive analysis using vehicle dynamics and vision-based lane semantics," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 1, pp. 9_18, Feb. 2015.

- [44] J. Barbizet, "Yawning," *J. Neurol., Neurosurg. Psychiatry*, vol. 21, no. 3, pp. 203_209, Aug. 1958.
- [45] J. R. Eguibar, C. A. Uribe, C. Cortes, A. Bautista, and A. C. Gallup, "Yawning reduces facial temperature in the high-yawning subline of spraguedawley rats," *BMC Neurosci.*, vol. 18, no. 1, p. 3, Jan. 2017.
- [46] A. Franzen, S. Mader, and F. Winter, "Contagious yawning, empathy, and their relation to prosocial behavior," *J. Exp. Psychol., Gen.*, vol. 147, no. 12, pp. 1950_1958, Dec. 2018.
- [47] Z. Liu, P. Luo, X. Wang, and X. Tang, "Deep learning face attributes in the wild," in *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, Dec. 2015,