

AN ENHANCED SECURITY MECHANISM THROUGH BLOCKCHAIN FOR E- POLLING/COUNTING PROCESS

A Major Project Report
submitted in partial fulfillment of the
requirements of VIII-Semester for the degree
of
Bachelor of Technology
in
COMPUTER SCIENCE & ENGINEERING

By
Chandrashekhar Gupta Somisetty

Reg. No. **16115081**

Veda Nandan Gandhi

Reg. No. **16115085**

P Varshani Reddy

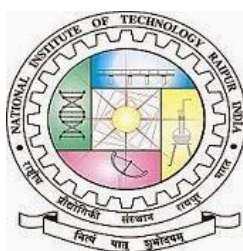
Reg. No. **16115053**

Under the guidance of

Dr. Preeti Chandrakar

Assistant Professor

NIT-RAIPUR



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY

RAIPUR, CG (INDIA)

APRIL 2020

DECLARATION

We hereby declare that the work described in this thesis, entitled “**An Enhanced Security Mechanism Through Blockchain For E-Polling/Counting Process**” which is being submitted by us in partial fulfillment for the VIII-Semester of the degree of Bachelor of Technology in the Department of **Computer Science and Engineering** to the National Institute of Technology Raipur is the result of investigations carried out by me under the guidance of **Dr. Preeti Chandrakar**. The work is original and has not been submitted for any Degree/Diploma of this or any other Institute/university.

Signature

Chandrashekhar Gupta Somisetty

Roll No.: **16115081**

Veda Nandan Gandhi

Roll No.: **16115085**

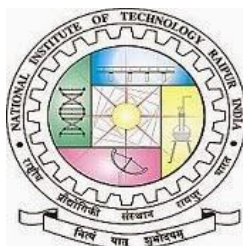
P Varshani Reddy

Roll No.: **16115053**

Place: Raipur

Date: 30.04.2020

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY**



CERTIFICATE

This is to certify that the project entitled “**An Enhanced Security Mechanism Through Blockchain For E-Polling/Counting Process**”, that is being submitted by **Chandrashekar Gupta Somisetty (Roll No. 16115081)**, **Veda Nandan Gandhi (Roll No. 16115085)** and **P Varshani Reddy (Roll No. 16115053)** in partial fulfillment for VIII-Semester of the degree of **Bachelor of Technology in Computer Science & Engineering** to National Institute of Technology Raipur is a record of bonafide work carried out by her under my guidance and supervision.

The matter presented in this project document has not been submitted by her for the award of any other degree elsewhere.

Signature of Supervisor

Dr. Preeti Chandrakar

Assistant Professor

Department of Computer Science & Engineering

National Institute of Technology, Raipur

(CG.)

Project Coordinator

Dr. K. Jairam Naik

Department of Computer Science & Engineering

National Institute of Technology, Raipur (CG.)

H.O.D

Dr. Pradeep Singh

Department of C.S.E

NIT Raipur (CG.)

ACKNOWLEDGEMENT

We would like to acknowledge our college **National Institute of Technology, Raipur** for providing a holistic environment that nurtures creativity and research-based activities.

We express our sincere thanks to **Dr. Preeti Chandrakar, Assistant Professor, Department of Computer Science & Engineering, NIT Raipur**, the guide of the project for guiding and correcting throughout the process with attention and care. She has frequently suggested us creative ideas and guided through the major hurdles that occurred during the duration of the project.

We would also thank **Dr. Pradeep Singh, Head of the Department** and all the faculty members without whom this project would be a distant reality. We also extend our heartfelt thanks to my family and friends who supported us.

Thank You!

Chandrashekar Gupta Somisetty

Roll No.: **16115081**

Veda Nandan Gandhi

Roll No.: **16115085**

P Varshani Reddy

Roll No.: **16115053**

ABSTRACT

In this project we present our idea in developing an e-voting application that helps in unprejudiced election results with the help of Hyperledger Fabric and IBM Blockchain Platform. The aim of this project is to develop a web application where the voter can register with the help of his/her voter ID and cast their vote with the help of the unique voter ID. Then the vote is corresponded to the block chain and then the web application shows the latest standing of the election votes. After the registration process is done by the voter, we check for the previous registration of the similar voter identification number. If there is no difficulty in the above step, the voter gets created a public and private key with an authorized certificate which is running on the cloud and there we add the public and private keys to the wallet.

Then, we use our voter ID number to submit our vote, during which the application checks if this voter ID number has voted before and tells the user they have already submitted a vote if so. If all goes well, the political party which the voter has chosen is given a vote, and the world state gets updated. Now, the current standing of the candidates is updated by the web application to show the current number of votes a particular political party has. As every submitted transaction to the service of ordering is supposed to have a signature from a genuine public key and private key, in case of audit, the tracing back of the registered vote transaction can be achieved.

CONTENTS

<u>DESCRIPTION</u>	<u>PAGE NO.</u>
DECLARATION	ii
CERTIFICATE	iii
ACKNOWLEDGEMENT	iv
ABSTRACT	v
CONTENTS	vi
LIST OF FIGURES	vii
LIST OF TABLES	vii
1. INTRODUCTION	1
1.1 Overview	2
1.2 Objectives and Importance of the Project	6
1.3 Scope	9
1.4 Motivation	10
1.5 Organization of the Project	11
2. LITERATURE REVIEW	12
2.1 Existing Works	13
2.2 Literature Summary	14
3. PROPOSED METHODOLOGY	17
3.1 Proposed Methodology	18
3.2 Flowchart	19
3.3 Description of the Flow	20
3.4 Architecture	20
3.5 Terminating Conditions	21
4. EXPERIMENTAL RESULTS	22
4.1 Environment Setup and Tools Used	23
4.2 Prerequisites	23
4.3 Data Used	24
4.4 Results	25
5. CONCLUSION	29
6. FUTURE WORK	31
REFERENCES	33

LIST OF FIGURES

<u>FIGURE NAME</u>	<u>PAGE NO.</u>
3.1: Flowchart of e-voting web application	19
3.2: Architecture	20
3.3: Architecture Abstract	21
4.1: Home Page	25
4.2: Cast Ballot	26
4.3: Current Poll Standings	27
4.4 Attempt to vote multiple times	28

LIST OF TABLES

<u>TABLE NAME</u>	<u>PAGE NO.</u>
1. Summary of Literature Review	14

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

The major challenge in the political chaos is evident during the process of the election where the leaders do anything to gain power. Moreover, due to the violence during the polling process and tedious queues for casting their votes many of the citizens do not choose to give their opinion to abscond the inconvenience or chaos during the voting process. Authors have contributed towards developing various voting applications that are based on IOT or smartphones to reduce the problems during the voting process and increase the number of voters that participate and give their opinion. These days, hacking is a mainstream problem and many of the IOT devices can be hacked by superior hackers and there is the chance of malicious access to the device where the statistics of the votes can be changed without any notice [1]. In order to make sure that the voting process is secure we create a transparent mechanism with the help of a block chain where the polling process is entering the votes which are legitimate and not duplicated and not modified and without any manipulation in the calculation of the votes [2].

The current project will be on the basis of a security mechanism which is enhanced using the block chain in e-voting application where the user will create or register using their credentials such as voter ID, aadhar number or any other government issued numbers. This can be enhanced further using biometric methods on the smart device [3].

The minor will validate every transaction done through this account that is being registered. There are several validation and verification parameters such as response time and utilisation of the resources and processing of the requests are being taken into consideration in this particular mechanism of electronic polling with the help of block chain.

Blockchain is a system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network [4]. We can define the block chain as a growing list of records that contain the hash value of the previous block calculated

cryptographically, nonce, timestamp, transaction of the data which is represented as a Merkle tree in many cases. Each one of the records in this growing records list is called a block. Here, the first block in a block chain is called a genesis block. Every node in a network will have the block chain as this technology is decentralised and highly difficult to hack and enter malicious information.

The design pattern of the block chain is in such a way that it will not allow any modification in the data and is highly resistant to such kind of malicious activities. This software is highly effective for conducting the transaction between two persons for parties in a way which is verifiable and permanent [5]. The block chain uses the concept of distributed ledger where each node in the network will have the copy of the block chain. In this mechanism of a distributed ledger the block chain is typically controlled or managed by a peer to peer network sticking to a protocol for the communication between the nodes internally and validating any new block entering into the block chain. Once a record or a block years added or saved into the block chain is highly difficult to retroactively change its content without changing the consequent blocks because every change in a block chain should be accepted by the majority of the nodes in the network according to the algorithm. Albeit, this Blockchain mechanism is where there is no way to alter the data in the records it has to be considered perhaps that even this secure design which exemplifies a computing system which is distributed is highly Byzantine fault tolerant [6].

Block chain technology was invented in the year 2009. The block chain technology has been invented by Santoshi Nagamaki in order to help the cryptocurrency bitcoin's Ledger of public transaction. Santoshi Nagamaki is a person or a group of people whose identity is not known till date. After the invention of the block chain for the first time in the digital currency there is no double spending problem without the help of any authority which is trusted or a centralised server mechanism. Many applications drew their inspiration from the design of this block chain. The block chains that are readable are highly in use by the cryptocurrencies.

A single block in the block chain has more than one valid transaction. Each transaction undergoes the mechanism of encoding and hashing into a Merkle tree. Each block in the block chain has the hash or the cryptographic hash of the previous block in the blockchain. This way of saving the block hash into its next one is the method that is established to hold all the blocks together in the block chain. The very first Block in this block chain is called Genesis block. The integrity of the blockchain can be iteratively validated with the help of the concept of saving previous hash till we reach the first block or the genesis block from which the entire blockchain starts.

Smart contracts are the applications that can be tracked and not reversed in a system or environment that is decentralised i.e, there is no centralised server where each and every transaction has to go before it goes to the destination. As soon as a contract is deployed it can't be changed by any one in any way to change its performance or maliciously change the code content. There are several transactions that hold as an agreement between two parties [7]. The type of relation is highly trustworthy and does not depend on one party alone. The self verification and self execution of the blockchain in the car of smart contracts opens doors for the administration of digital transactions and agreements with trust.

Many frameworks, applications, libraries and business technologies using block chain are incubated and supported by Hyperledger. Various block chain frameworks, projects, including Hyperledger fabric are hosted by the Hyperledger project.

There are various private and permissioned business networks where the members in the network know each other's identity. These business networks somehow implement the open source framework of the Hyperledger fabric. The Hyperledger fabric is created for modular architecture solution development as a foundation to them. Various components such as the database of the ledger, mechanism of the consensus, to be plug-and-play, services of membership are permitted by the Hyperledger fabric. The container technology is leveraged,

enterprise ready network security is delivered, confidential and scalable products are achieved by the Hyperledger fabric [8].

There are several components for a hyperledger fabric. They are as follows:

- **Assets:** Something that has a value is an asset. Ownership and state are its features. They are a collection of key-value pairs in the hyperledger fabric.
- **Shared ledger.** This is the component that has a record of ownership and state of an asset. The ledger is comprised of two components:
 - The database of the ledger is world state. It has a record of the state of the ledger at any point in time.
 - Log history of the transactions is something that is stored in the blockchain.
- **Smart contract:** Hyperledger fabric's smart contracts may also be called by another name known as Chain Code. Chaincode defines assets and related transaction. The business logic of the system is contained in it. When the application is required to interact with ledger, it invokes Chaincode. Golang or Node.js is used to write Chaincode.
- **Peer nodes:** They are used to host smart contracts and ledgers and play a fundamental role. A peer is used to execute chaincode, make use of ledger data, endorses transactions, and interfaces with applications. An endorsement policy is specified by every Chaincode. Here, the endorsement policy defines all the conditions for a valid transaction endorsement.
- **Channel:** Collection or group of peers form a logical unit or structure which can be called as a channel. This ability permits a collection of peers to form a discrete ledger of the transactions.
- **Organizations:** The Hyperledger Fabric network is formed with the help of peers possessed and bestowed by the various organizations that are holding the membership of the network. These organizations contribute their individual resources to the collective network. A Membership Service Provider assigns an identity (digital certificate) to the peers from its owning organization.

- **Membership Services Provider:** The Membership service provider or MSP in short is implemented as a Certificate Authority to manage certificates used to authenticate member identity and roles. No unknown identities can transact in the Hyperledger Fabric network. It manages user IDs and authenticates all participants on the network which enables Hyperledger Fabric as a Private and Permissioned network.
- **Ordering service:** The ordering service encapsulates transactions into blocks to be delivered to peers on a channel. It guarantees the transaction delivery in the network. It communicates with peers and endorsing peers. The supported configuration mechanisms for the Ordering service are Solo and Kafka.

1.2 OBJECTIVES AND IMPORTANCE OF THE PROJECT

The e-polling machines have always been considered as faulty with flaws due to their inefficacy in case of physical attacks. The security community hence considered them less secure. Person who has the ability to access the machine can just vandalise the machine or hack it which alters all the votes submitted by the voters on the particular machine [9]. This resulted in a highly inefficient voting process.

Coming to the blockchain technology, a block chain follows the concept of immutable ledger. The block chain is public ledger. It cannot be converted and is a distributed ledger. This new technology follows the peer to peer decentralised distributed network protocols [10]. The four main characteristic working principles of this block chain technology are as follows:

- (i) The ledger exists in various locations: There is no single point of failure which can take place in the maintenance of the distributed ledger.
- (ii) The control is distributed over who can append new transactions to the ledger.

(iii) Any new block to the ledger references the ledger's previous version which creates an immutable chain, and thus helps to prevent tampering with the integrity of previous entries.

(iv) A consensus should be reached by a majority of nodes in the network before a new block can become a permanent part of the ledger.

The security provided by the characteristics of the blockchain mentioned above is very inflated in comparison to any other precursory database. Hence, it is so conspicuous that this is a perfect technological tool to be considered in provision of security in any voting application including this. Incorporation of such technology can be a revolutionary change in modern democracy [11].

This e-voting application helps in unprejudiced election results with the help of Hyperledger Fabric and IBM Blockchain Platform. The project's aim is to develop a web application where the voter can register with the help of his/her voter ID and cast their vote using his/her voter ID. Then the vote is corresponded to the block chain and then the web application shows the latest standing or update of the election votes submitted. The registration process is done by the voter where the credentials such as voter, aadhar ID, first and last name are submitted and we check for the previous registration of the similar voter identification number. In case if there is no difficulty in the above steps the voter gets created a public and private key with an authorized certificate which is running on the cloud and there we add the public and private keys to the wallet.

Then, we use our voter ID number to submit our vote, during which the application checks if this voter ID number has voted before and tells the user they have already submitted a vote if so. If all goes well, the political party which the voter has chosen is given a vote, and the updation of world state happens. Now the current standing of the candidates is updated by the web app to show the current number of votes a particular political party has. As every submitted transaction to the service of ordering is supposed to have a signature from a genuine public key and private key, in case of audit the tracing back of the registered vote transaction can be achieved.

This concept of block chain technology has the backend network incorporated with the network of Hyperledger fabric. The front end of the application communicates with this network of Hyperledger fabric. There are many software development kits that are incorporated in establishing the communication between the frontend and the back end. Some of these software development kits are Node.js and Java software development kits. Hence, these software development kits monitor the events between them, they perform the code of the block chain, they conduct transactions in the distributed network etc.

In order to create a blockchain app we have to:

- Use any programming language such as Go that supports blockchain and write the code for the blockchain.
- Create the frontend client part of the application using any software development kit.
- The programmed code of the blockchain has to be deployed on the network of Hyperledger fabric.

The topnotch level flow of the transaction requests on the network of Hyperledger fabric goes like this:

- The client uses any software development kit such as node or java and connects to the network of Hyper-ledger fabric. The user or the client uses this software development kit in order to send the transaction by underwriting it to the peer endorsing.
- This corresponding peer who is endorsing checks the sign of the sender. Now the transaction is simulated and an endorsement sign is sent.
- When the transaction is finally endorsed, the submission of the transaction to the ordering service happens. Else, the transaction is rejected.
- Now this particular transaction is sent to all other peers by the ordering service. Finally, the transaction is committed and applied by all the peers in the network. Now the updation of world state occurs in all the nodes or peers in the network.

1.3 SCOPE

These days the citizens of the nations are facing several issues in giving their opinion on whom to choose as the next deserved leader to their constituency, state or the nation through the traditional voting ballot system. The queues are very tedious and awful with the holloi polloi crushing, longer waiting times in the queues, travel to the voting booth, and discomfort in the polling booths.

In fact, every citizen wants the polling system to be easy and accessible such that even when there is a scenario where they are unable to reach their place because of the travel, health or other work issues they will be able to cast their vote through their digital device [12].

The blockchain solution using Hyperledger is an effective mechanism that defies multiple casting of votes with a secure voting mechanism. In this web application, the user is allowed to vote only once and any malicious attempts to login through fake ID or casting the vote for the second time is completely not possible. Albeit the solution is very secure digitally, its scope is bound to the educated and developed countries or places. In underdeveloped countries or countries with less literacy rate this method will not be very successful.

Immutable ledger is one of the most important features of the blockchain when the ledger data cannot be changed because the block chain is decentralized and every node in the block chain has the ledger. When the majority of the nodes disagree with ledger at one node then the malicious attempt to change the data will be a failure. In order to change the vote transactions the hacker will have to change the data at every node in the network at exactly the same time which is highly difficult and the impossibility probability is very high.

In order to consider other scenarios of cons of the digital method primarily the system may face inappropriate results in case of oppressive leaders who may force the voters by threatening them till they vote or by other means [13].

Blockchain technology is based on mining the hash of the particular block, where the perfect hash is found with a nonce which will be called golden nonce. The nonce and the transactions taken into the block will help in finding the hash of the

block. Here, each transaction pays the miner with some cryptocurrency and the miner will choose the transactions which he considers best and eventually change on the basis of hash by changing the nonce and in the worst case he will remove a transaction and choose another. So, this is a scenario where the government will have to take the budget for the voting process without any favorability or partiality.

But considering statistics from various years, the amount of population that cast the vote is very less compared to the entire population. So, this method when made sure the people are not forced to cast the vote other than their own opinion will open doors to a better democracy.

Every technology has its pros and cons but the major consideration will be on the basis of percentage of pros and chance to avoid the cons. So, in this technology of e-voting, the pros are on the side of the technology and cons are on the side of the literacy rate, oppression by leaders, paying the miners and other facts. So, with a possibility of a high percentage of efficiency in places of the country, this can be implemented. As time and again, the literacy rate and education opportunities with competition is improving worldwide this method can be incorporated with a wide scope in upcoming years and decades.

1.4 MOTIVATION

The main motivation behind the project is to create a hassle-free interface for voting. There are many other technologies in the current world and Block chain provides a secure mechanism through which the duplicity of the votes is highly impossible because of the concept of immutable ledger [14].

There is a lot of chaos involved in the voting system where the people had to stand in queues for a longer time and many do not choose to give their opinion because of the chaos so the project provides an online mechanism where the voters need not go to the ballots to cast their votes and it provides an interface to give their opinion even when they are abroad or in a position unable to reach the ballot.

According to the statistics from recent years, most of the population was unable to give their choice or they did not opt to give because of the difficulty involved in the voting mechanism. There were situations in which there was an operation that led to duplicity of the votes and invalid votes. The blockchain mechanism will make sure that there is no duplicity of the votes where each vote is stored as a transaction in a single block with other transactions which are validated when each time a new transaction is being initiated and will not allow a vote if the vote is already registered.

1.5 ORGANIZATION OF PROJECT REPORT

This project report is divided into seven different chapters which cover various details related to the project.

Chapter1. Introduction: This chapter deals with the introduction part of the project. It describes the overview, objectives, scope and motivation of the project.

Chapter2. Literature Review: The second chapter deals with the previous works related to the work done in this project. It consists of the summary of some important research works which were referred to in this project.

Chapter3. Proposed Methodology: This chapter explains the process and the working of the proposed method. It describes the details of how the work is to be done.

Chapter4. Experimental Results: This section of the report deals with the results generated after executing the algorithm on the given input. It gives the comparison of results with other models.

Chapter5. Conclusion: This chapter gives the conclusion of the project and the results achieved from the execution of the algorithm.

Chapter6. Future Work: This section describes some of the possible ways in which the current work could be improved and be integrated into other algorithms and gives some examples of its applications.

CHAPTER 2

LITERATURE REVIEW

2.1 EXISTING WORKS

Bin Yu et.al.[15] describes a Platform-Independent Secure Blockchain-Based Voting System. This particular project provides a high security platform that is corroborated irrespective of any platform whose deployment can be done in any blockchain that aid the running of the smart contract. Analysis of the accuracy and how resistant the coercion of the project methodology is done. The voting system is deployed and its performance is analysed numerically by the Hyperledger fabric's employment in the application.

Denis Kirillov et.al.[16] describes in Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain, an E-Voting Scheme in which blockchain is used to increase faith between the participants to use the electronic voting system. Here, the traditional and electronic voting can be incorporated at the same time. In this paper, the description and discussion of the architecture of the solution by incorporation on the basis of Hyperledger fabric platform and demonstration of the functions is done.

Emre Yavuz et.al.[17] describes in Secure e-voting using ethereum blockchain in which he developed a simple electronic voting application incorporating smart contracts with the help of Ethereum network using Ethereum wallets and solidity language. Even though the voters do not have an ethereum wallet, the application in androids lets them cast their vote. As soon as the election is completed, the block chain holds the data regarding the records of votes and ballots. The submission of the votes is done in two ways, one is using the android device and the other is using the directly from the ether coins from the ethereum wallets. The consensus of every node of ethereum handles the transactions done.

Friðrik Þ. Hjálmarsson et.al.[18] describes in Blockchain-Based E-Voting System his assessment of the concept of distributed ledger and its potentiality while describing the case studies. The case studies include election procedure, how the block chain app is implemented. This blockchain implementation was supposed to improve the efficiency and reduce the national wide election cost.

David Khoury et.al.[19] in Decentralized Voting Platform Based on Ethereum Blockchain used a new method to remove the inefficiency of voting using blockchain. This implementation removes trust issues. This ensures integrity of data by maintaining a transparent method of voting through mobiles phones with better privacy. Here the blockchain RTE is EVM which is ethereum virtual machine. Here the transparency and consistency of the chain will be deployed for events of voting to run voting rules.

2.2 LITERATURE SUMMARY

Table 1: Summary of Literature Review

S. NO.	TITLE	AUTHOR	YEAR OF PUBLIC ATION	PARAMETERS CONSIDERED	DESCRIPTION	LIMITATIONS
1	Platform-Independent Secure Blockchain-Based Voting System [15]	Bin Yu et.al.	2018	Verifiability, encryption, proof-of-knowledge, linkable ring signature	This particular project provides a high security platform that is corroborated irrespective of any platform whose deployment can be done in any blockchain that aid the running of the smart contract.	Illiterates cannot use it as it is digital. Authentication issues as one can illegally use anyone's ID and vote.

2	Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain [16]	Denis Kirillov et.al.	2019	Traditional paper voting and e-voting	Here, blockchain is used to increase faith between the participants to use the electronic voting system. Here, the traditional and electronic voting can be incorporated at the same time.	Complex implementation of both traditional and digital method implementation. Authentication issues as one can illegally use anyone's ID and vote.
3	Secure e-voting using ethereum blockchain [17]	Emre Yavuz, Ali Kaan	2018	Contracts, data privacy, electronic money, financial data processing, government data processing, mobile computing, Web services.	Developed a simple electronic voting application incorporating smart contracts with the help of Ethereum network.	The user can vote through android or through wallets directly. So, the problem occurs to those of non android users who have no knowledge regarding wallets and smart contracts to cast their votes. Authentication issues as one can illegally use anyone's ID and vote.

4	Blockchain-Based E-Voting System [18]	Friðrik Þ. Hjalmarsson et.al.	2018	Contracts, Electronic voting, Peer-to-peer computing, Privacy, Electronic voting systems	Assessment of the concept of distributed ledger and its potentiality while describing the case studies is being done in this paper.	It is completely digital and doesn't help in case of illiterates and people who can't afford digital devices. Authentication issues as one can illegally use anyone's ID and vote.
5	Decentralized Voting Platform Based on Ethereum Blockchain [19]	David Khoury et.al.	2018	Authorisation, data integrity, data privacy, distributed databases, government data - processing, message-authentication, virtual machines	The blockchain RTE is EVM which is ethereum virtual machine. Here the transparency and consistency of the chain will be deployed for events of voting to run voting rules.	Doesn't help in case of illiterates and people who can't afford digital devices in less developed nations.

CHAPTER 3

PROPOSED METHODOLOGY

3.1 PROPOSED METHODOLOGY

In this application we have incorporated Blockchain technology using Hyperledger fabric using IBM blockchain platform in Visual studio code. Here the voters are supposed to register with the help of their valid voter ID number if they are not a registered voter else will have to just login. Then they will be directed to a page where they will be allowed to vote if they have not cast their vote else they will not be able to cast. The Voter Peer node is used for conducting peer to peer transactions.

This method of e-voting avoid fraud to maximum extent because of the features of blockchain technology which is decentralized technology and incorporates the concept of immutable ledger as each node stores the entire transaction genuine block chain and hacking is highly impossible into more than 51 % of the nodes at the same time as the new chain is only incorporated into each only when majority of them accept the chain.

This e-voting application helps in unprejudiced election results with the help of Hyperledger Fabric and IBM Blockchain Platform. The aim of this project is to develop a web application where the voter can register with the help of his/her voter ID and cast their vote with the help of the unique voter ID. Then the vote is corresponded to the block chain and then the web application shows the latest standing of the election votes.

The registration process is done by the voter where the credentials such as voter ID, aadhar ID, first and last name are submitted. The details about the voter are stored locally. Then, we check for the previous registration of the similar voter identification number. This checking is done by a fabric network library which checks with the certificate authority whether the voter ID exists or not. The Voter CA acts as an approver and is used to approve a voter. If there is no difficulty in the above steps, the registered user is approved as a voter and that identity is imported into the wallet. The implementation of the wallet is done by creating separate folders for each voter ID which is registered. Then, the voter gets created a public and private key and these keys are added to the wallet according to their voter ID. These public and private keys present in the wallet are used to sign a

transaction when the voter casts his vote. In this way, a vote can be traced back to the voter in case of audit.

Then, we use our voter ID number to submit our vote, during which the application checks if this voter ID number has voted before and tells the user they have already submitted a vote if so. If all goes well, the political party which the voter has chosen is given a vote, and the updation of world state happens. Now the current standing of the candidates is updated by the web app to show the current number of votes a particular political party has. As every submitted transaction to the service of ordering is supposed to have a signature from a genuine public key and private key, in case of audit the tracing back of the registered vote transaction can be achieved.

3.2 FLOWCHART

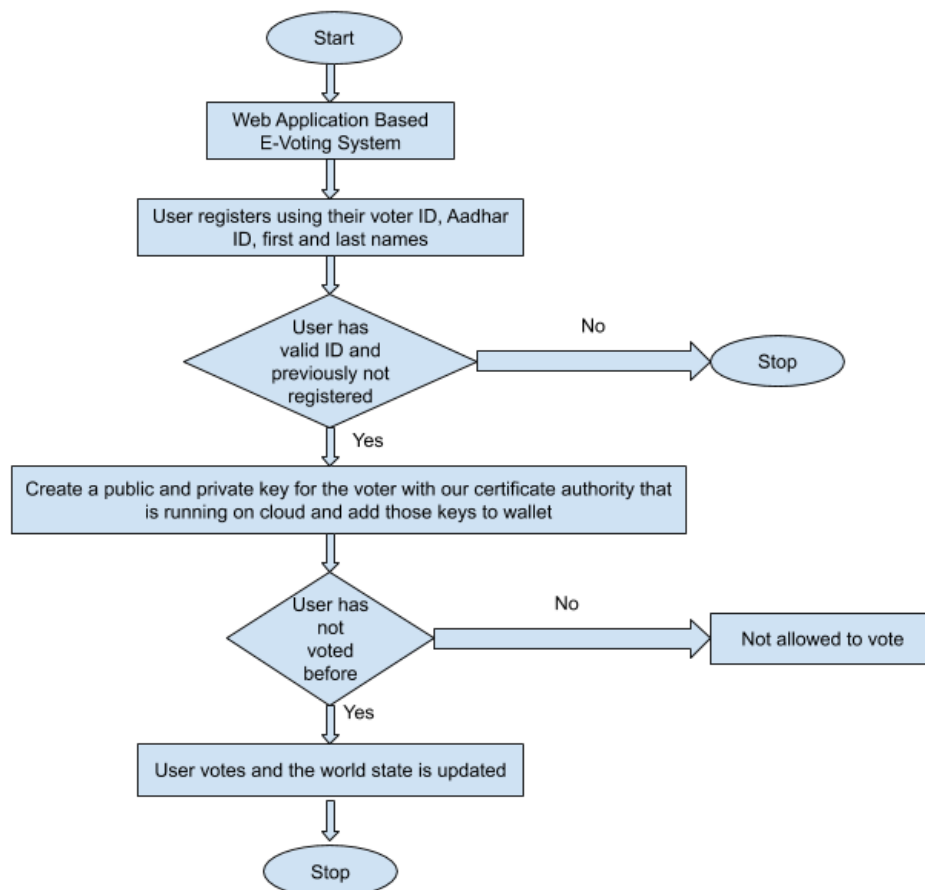


Fig 3.1: Flow chart of e-voting web application

3.3 DESCRIPTION OF THE FLOW

1. The IBM Blockchain platform 2.0 services are initialised by the one who operates the blockchain.
2. The IBM Kubernetes Service is where the IBM blockchain platform 2.0 forms the Hyperledger fabric network, and in this network the smart contract will be instantiated by the operator.
3. The Fabric SDK is used by the Node.js application server for the interaction with the network where deployment is done on IBM Blockchain platform 2.0 and then, APIs are created for the web client.
4. The network is interacted by Vue.js client with the help of Node.js application API.
5. Most casting the votes to the ballot and for knowing the current standing of the polls the user has to interact with the web interface of Vue.js.

3.4 ARCHITECTURE

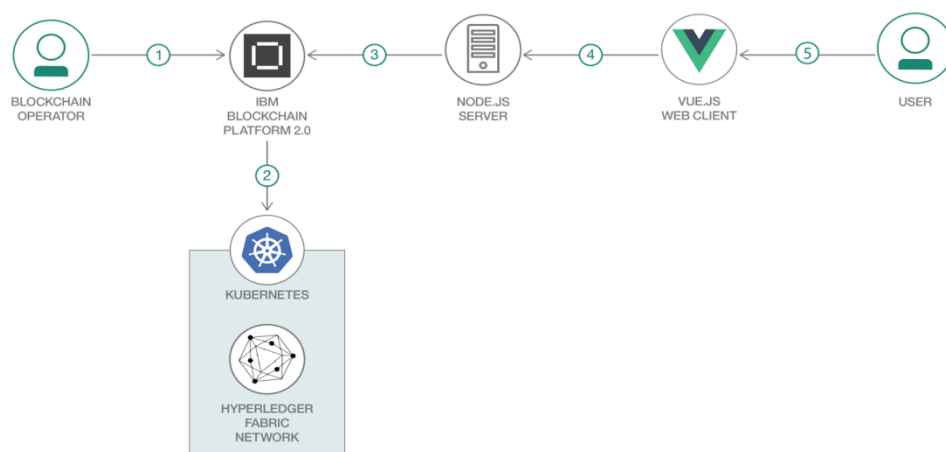


Fig 3.2: Architecture

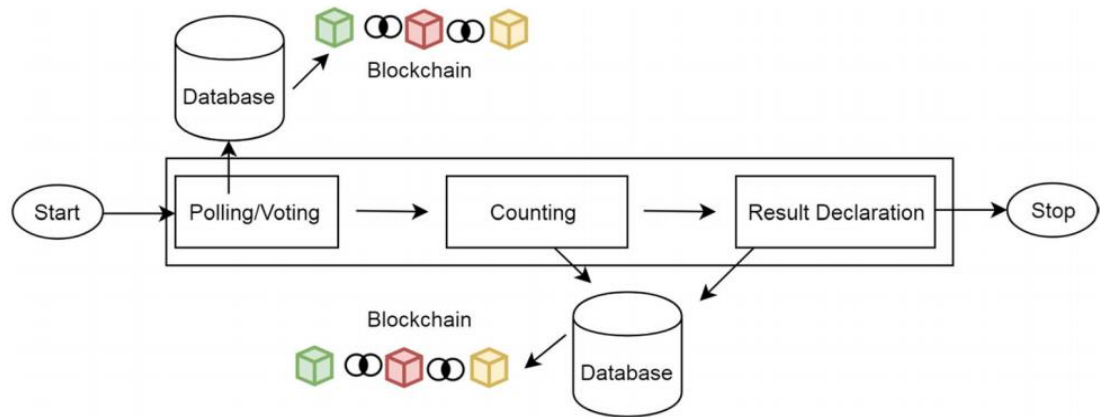


Fig 3.3: Architecture Abstract

3.5 TERMINATING CONDITIONS

There are few terminating conditions that will reject the voter if he tries to maliciously give duplicate votes or false information. They are:

- When the voter registers himself to vote he will have to give several information about his name, place and government issued ID number. In case this data is not present in the data of the government DB, then the user cannot cast his vote as he is considered as an illegitimate voter.
- When the registered voter casts his or her vote, then when they try to vote again for the second time then they will not be allowed to vote.

CHAPTER 4

EXPERIMENTAL RESULTS

4.1 ENVIRONMENT SETUP & TOOLS USED

- IBM Blockchain Platform [20]: Where u can control the blockchain from UI and adds an extra fuel for the deployment and management of block chain constituents on the kubernetes cloud service of IBM.
- IBM Cloud Kubernetes Service: Here a set of hosts are created and mostly available containers are deployed. Helps in deployment, updation and scaling of apps.
- IBM Blockchain Platform Extension for Visual Studio Code: Acts as an assistant for users in development, testing and deployment of smart contracts including the connection with Hyperledger fabric environment.
- Hyperledger Fabric v1.4: Helps in providing confidential, integral, resilient, flexible, scalable modular architecture in a distributed ledger platform.
- Node.js: Server side JS code is executed.
- Vue.js 2.6.10: For building UI and single page apps.

4.2 PREREQUISITES

- Visual Studio Code version 1.38.0 or greater
- IBM Blockchain Platform Extension for VSCode
- Node v8.x or greater and npm v5.x or greater

4.3 DATA USED

There are three types of data stored in the json files :

ballotData.json :

This has the data regarding the Race titles that are involved like Presidential race, Governor race, Mayor race etc. For each race it has data of its own description. Under each race, it has the data of each candidate participating and their respective agenda.


electionData.json :

This has all the data regarding the election that constitute the information regarding the Registrar of the election such as their name, organisation, locality, state, country etc and also has the data regarding the name of the election, the country where the elections are held and the year in which the election is conducted.

presElection.json :

This has all the data regarding the name and description of the candidates participating with their respective agendas.

4.4 RESULTS



[Home](#)
[Get Poll Standings](#)

Elections

If you are a registered voter, enter your voterId below

Otherwise, fill out the form below to register!

Fig 4.1: Home Page

The home page of the web application is where the voter registers and login to cast their vote. Here the voters are asked to submit their voter ID, aadhar number, first name and last name to register. If he or she is an authentic voter then they can login to cast their vote.



[Home](#)

[Get Poll Standings](#)

Cast Ballot

- ☐ Candidate 1
- ☐ Candidate 2
- ☐ Candidate 3
- ☐ Candidate 4
- ☐ Candidate 5

Fig 4.2: Cast Ballot

After logging-in into the web application they are directed to the ballot page. Here, they are supposed to choose the party that they want to support, and then submit it entering the voter ID.



[Home](#)

[Get Poll Standings](#)

Get the Current Poll Standings

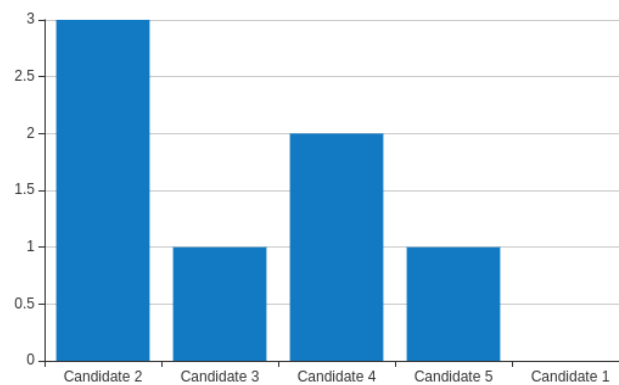


Fig 4.3: Current Poll Standings

The web application provides an option to acknowledge the voters with the current statistics of the votes casted. This is where we get the results of the current polling in the form of a bar chart.



[Home](#)

[Get Poll Standings](#)

Elections

If you are a registered voter, enter your voterId below

{ "error": "This voter has already cast a ballot, we cannot allow double-voting!" }

Otherwise, fill out the form below to register!

Enter Voter ID
Enter Aadhaar No.
Enter first name
Enter last name

Fig 4.4: Attempt to vote multiple times

When a voter tries to login to vote for the second time we meet a terminating condition where the voter will not be allowed to vote again. Here is an example of such a situation.

CHAPTER 5

CONCLUSION

5. CONCLUSION

According to the statistics from recent years, most of the population was unable to give their choice or they did not opt to give because of the difficulty involved in the voting mechanism. There is a lot of chaos involved in the voting system where the people had to stand in queues for a longer time and many do not choose to give their opinion because of the chaos so the project provides an online mechanism where the voters need not go to the ballots to cast their votes and it provides an interface to give their opinion even when they are abroad or in a position unable to reach the ballot.

The blockchain solution using Hyperledger is an effective mechanism that defies multiple casting of votes with a secure voting mechanism. In this web application, the user is allowed to vote only once and any malicious attempts to login through fake ID or casting the vote for the second time is completely not possible.

Albeit the solution is very secure digitally, its scope is bound to the educated and developed countries or places. In underdeveloped countries or countries with less literacy rate, this method will not be very successful.

Considering statistics from various years, the amount of population that cast their vote is very less compared to the entire population. So, this method when made sure the people are not forced to cast the vote other than their own opinion will open doors to a better democracy. As time and again, the literacy rate and education opportunities with competition is improving worldwide this method can be incorporated with a wide scope in upcoming years and decades.

CHAPTER 6

FUTURE WORK

6. FUTURE WORK

The current project uses only the basic validation of the data using a government issued ID number such as voter ID or aadhar card number. In future this method can be made easy with the help of an optional fingerprint sensor available in almost all the devices in the current world of technology.

This method of fingerprint scanning with the device's fingerprint sensor can be incorporated after a few years when the percentages of cell phones that are manufactured and used use the fingerprint sensor.

Albeit this is a web application, in order to consider secondary changes, we can also go for an application for the same mechanism for both ios and android devices.

The application also has to implement the mechanism where the government is able to add a fixed crypto currency to every node and automatically pay the miner when a transaction is performed such that the miner chooses the nodes without any favorability towards any transaction.

REFERENCES

- [1] Fraga-Lamas, P., & Ferná ndez-Caramé s, T. M. (2019). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE Access*, 7, 17578–17598.
- [2] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, 95(1), 118–127.
- [3] Khasawneh, M., Malkawi, M., Al-Jarrah, O., Barakat, L., Hayajneh, T. S., & Ebaid, M. S. (2008). A biometric-secure e-voting system for election processes. In 2008 5th international symposium on mechatronics and its applications (pp. 1–8). IEEE.
- [4] B. Singhal, G. Dhameja, and P. S. Panda, “How Blockchain Works,” in *Beginning Blockchain*, pp. 31–148, Berkeley, CA: Apress, 2018
- [5] Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software*, 35(4), 95–99. 14. Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security and Its Applications*, 9(3), 01–09.
- [6] Osgood, R. (2016). The future of democracy: Blockchain voting. In *COMP116: Information security* (pp. 1–21).
- [7] M. Pawlak, J. Guziur, and A. Poniszewska-Mara nda, “Voting Process with Blockchain Technology: Auditable Blockchain Voting System,” in *Lecture Notes on Data Engineering and Communications Technologies*, pp. 233–244, Springer, Cham, 2019.
- [8] Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D. I., & Zhao, J. (2019). Towards secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Transactions on Vehicular Technology*, 68, 2906–2920.
- [9] R. Anane, R. Freeland, and G. Theodoropoulos, “E-voting requirements and implementation,” in *The 9th IEEE CEC/EEE 2007*. IEEE, 2007, pp. 382–392.
- [10] A. B. Ayed, “A conceptual secure blockchain-based electronic voting system,” *International Journal of Network Security & Its Applications*, vol. 9, no. 3, 2017.

- [11] T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in Proceedings of the 18th Annual International Conference on Digital Government Research, ser. dg.o '17. New York, NY, USA: ACM, 2017, pp. 574–575. [Online]. Available: <http://doi.acm.org/10.1145/3085228.3085263>
- [12] Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-voting with an open cloud computing architecture. *Government Information Quarterly*, 28(2), 239–251.
- [13] K.-H. Wang, S. K. Mondal, K. Chan, and X. Xie, "A review of contemporary e-voting: Requirements, technology, systems and usability"
- [14] D. A. Gritzalis, "Principles and requirements for a secure e-voting system," *Computers & Security*, vol. 21, no. 6, pp. 539–556, 2002.
- [15] Bin Yu, Joseph K. Liu, Amin Skated, Surya Nepal, Ron Steinfeld, Paul Rimba, Man Ho Au Platform-Independent Secure Blockchain-Based Voting System(2018)
- [16] Denis Kirillov, Vladimir Korkhov, Vadim Petrunin, Mikhail Makarov, Ildar M. Khamitov, Victor Dostov Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain (2019)
- [17] Emre Yavuz, Ali Kaan Secure e-voting using ethereum blockchain(2018)
- [18] Hjalmarsson, F.P., Hreioarsson, G.K., Hamdaqa, M., & Hjalmtysson, G. (2018). Blockchain-based e-voting system. In *IEEE 11th international conference on cloud computing (CLOUD)* (pp. 983–986).
- [19] David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb Decentralized Voting Platform Based on Ethereum Blockchain (2018)
- [20] <https://developer.ibm.com/technologies/blockchain/patterns/how-to-create-a-secure-e-voting-application-on-hyperledger-fabric/>