BLOCKCHAIN BASED VOTING SYSTEM

Project report submitted in fulfilment of the requirement of the major Project

for the degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

By

Ujjwal Jain (171014)

And

Shubham Kumar (171031)

UNDER THE GUIDANCE OF

Dr Alok Kumar

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

WAKNAGHAT

May 2021

TABLE OF CONTENTS

DECLARATION

We hereby declare that the work presented in the report entitled “ Blockchain based Voting System” in the partial fulfilment of the requirements for major project of Bachelor of Technology in electronics and communication engineering submitted in the department of ELECTRONICS AND COMMUNICATION, Jaypee University of Information and Technology, Waknaghat is an authentic record of our own work carried out over a time from June 2020 to May 2021 under the supervision of Dr. Alok Kumar .

Ujjwal

Ujjwal Jain (171014)

Shubham Kumar (171031)

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

Alok kumar 21/05/2021

Dr. Alok Kumar

ACKNOWLEDGEMENT

We would like to express my deepest appreciation to Dr Alok Kumar for helping us throughout the project and without whom this project would have been a very difficult task. We are highly indebted to sir for his guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in doing project. He consistently motivated and guided us towards the completion of the project. We would like to express our gratitude towards my parents & members of JUIT for their kind co-operation and encouragement which helped me in doing this project. My thanks and appreciations also go to our colleagues who have helped us out with their abilities in developing the project.

LIST OF ACRONYMS & ABREVIATIONS

I-VOTING	Internet Voting
E-VOTING	Electronic Voting System
EVM	Electronic Voting Machine
DRE	Digital Rectal Exam
DDoS	Distributed Denial of Service
Daaps	Decentralized applications
VVPAT	Voter Verifiable Paper Audit Trail
PoW	Proof of Stake
PoS	Proof of Work
DAO	Data Access Object
XP	Experience points generated through mining in Blockchain

LIST OF FIGURES

ABSTRACT

Elections are a means of electing members by justice, honesty and electoral legislation. The voting system enables approved voters to cast their ballots for candidates during the election. Essentially, many areas of political science, social science and economics can be directly affected by the voting system. Thus the definition of the voting system must respond and rigorously considered before the election is held. E-voting is the most commonly used method in the world and it is a tool that also reflects electoral democracy. Most nations, however, continue to study and develop the method of e-voting. The present voting system is ultimately, however far from what it should deliver. Blockchain technology delivers a decentralized architecture that synchronously distributes digital information without a central database through the P2P network. Blockchain has become a mainstream application thanks to technology innovation that solves problems such as "perfect online privacy" and Platform 3.0 dApps. The analysis therefore proposes that the Blockchain-based Online Voting System (BOVS) improves legitimacy, optimizes the voting process, delivers consistent voting outcomes and enhances the voting system's accountability. Finally, the report addressed the shortcomings of the existing I-voting system and successfully applied the technology of Blockchain to overcome those weaknesses.

CHAPTER 1 INTRODUCTION

First and foremost, there are the paper voting and e-voting schemes, all of which require voters to go to a designated polling place to cast their ballots. After the polling procedure, the paper vote counting system was used, which was performed manually or by machine (physical counting). E-voting, on the other hand, keeps track of each vote as it is counted. The next step will be to combine all of the candidate counts from the polling stations, which would be the same for all of the elections. After 1999, India has been one of the countries that has used electronic voting machines (EVMs) in elections. When opposed to other e-voting companies in India, EVMs are unquestionably more cost-effective. I-voting allows electors to vote from anywhere via a browser (web application) or a mobile application. Since 2005, Estonia has become the country for the election using I-voting [2] Election. Thanks to its dominance in terms of simplicity and cost-effectiveness, the reason for using I-voting outplayed the other voting system. An election is not just about security, but about authentication, auditability, openness, confidentiality, availability and reliability.

- The electoral mechanism should usually be able to perform the following functions:
- Registered electors should be able to vote (equal opportunity about accessibility and place).
- • The cost of voting should be fair.
- • Voters can check to see whether their vote was counted and whether the results will be tallied during the election process.
- The vote is immutable, which prohibits the third party from being influenced and active.
- The results should be the same as the numbers voted by the voters approved.
- Nobody other than themselves should refer to their decision.
- The votes should be audited after the poll.
- All voters should be able to validate the voting process.

As a result, it has not been the best option for democracy until now, with the exception of e-voting usability, which can be mitigated. Physical access (evaluated by researchers and the security community) that results in the voting process makes it unauditable[3].

I-voting was meant to overcome the shortcomings of e-voting. Nevertheless, up to now the Internet vulnerability like DDoS has represented an obstacle that is almost difficult to solve, making its power much of the weaknesses [4].

The blockchain platform is an irreplaceable life to overcome I-voting shortcomings. The essence of blockchain technologies, such as an incontrovertible, transparent and public ledger[5]. Blockchain technology's main features are:

Remove the core archive. P2P network in which each node has the same blockchain (data), but it is distributed across the network, resulting in no single point of failure[6].

The previous block will be referenced when a new data are so-called block is generated by the new block that has built an eternal chain that prevents information from tampering [6].

Control of half of the network nodes (51 percent) which made the device highly secure (Greatest wins the game.). It is difficult to concurrently launch DDoS to several nodes in the network[6].

In addition, Ethereum brings new changes, while the blockchain features remain:

1. Enable the creator to configure the blockchain (i.e. smart contracts) [7] and configure it.
2. Least output cost of CPU resources [8].

In comparison, the decentralized system with its consensus algorithm carries the degree of protection to a greater level than the centralized architecture of blockchain technologies (client-server).

New research therefore aims to examine the relevance of Blockchain technologies for automated voting in order to boost the Integrity, improving the election process, delivering predictable voting outcomes, and strengthening the voting system's accountability.

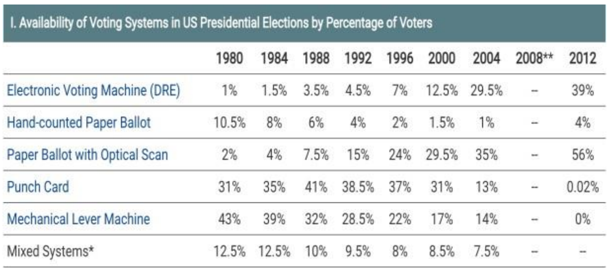
CHAPTER 2 MATERIALS AND METHODS

2.1PAPER BALLOTS

The voting system's history is extraordinarily long, beginning with paper ballots, then e-voting, and eventually i-voting. Paper ballots that represent the first voting method developed since 1856 by South Australia and Victoria, also known as the Australian vote, or secret ballot [9].

Figure 2.1: Paper Ballots [10]

The idea of paper ballots was to allow electors to use marking methods i.e. pen, pencil) to decide their vote (Figure 2.1) and the counting process would use a hand-counted or optical scanner[10]. Particularly after several years, paper ballots are still one of the most "trusted" voting systems. As seen in Figure 2.1, "optical scan paper ballots" reflect the highest supply during U.S. presidential elections in 2012. Moreover, the researchers constantly compare the EVM with the paper ballots.



I. Availability of Voting Systems in US Presidential Elections by Percentage of Voters

	1980	1984	1988	1992	1996	2000	2004	2008**	2012
Electronic Voting Machine (DRE)	1%	1.5%	3.5%	4.5%	7%	12.5%	29.5%	–	39%
Hand-counted Paper Ballot	10.5%	8%	6%	4%	2%	1.5%	1%	–	4%
Paper Ballot with Optical Scan	2%	4%	7.5%	15%	24%	29.5%	35%	–	56%
Punch Card	31%	35%	41%	38.5%	37%	31%	13%	–	0.02%
Mechanical Lever Machine	43%	39%	32%	28.5%	22%	17%	14%	–	0%
Mixed Systems*	12.5%	12.5%	10%	9.5%	8%	8.5%	7.5%	–	–

Figure 2.2: Availability Statistics in U.S. Presidential Elections (1980 – 2012) [10]

Phase of Voting

- Voters drive to the polling station named for them.
- Official survey to check the identity of a voter.
- The official survey issues a ballot paper to the electors.
- The elector goes to the position where the document is marked.
- Voter Paper Folding.
- By labeling the text, the elector decides the result.
- Unfolding the paper by the voter.
- The elector puts the document inside a box.

In comparison to EVM, there are a number of main advantages.

- Since the proposal was designed mainly without the use of electronic circuitry, no hijacked during the election.
- Votes reflect records in a physical format with no risk of losing votes.
- • Invulnerability in terms of both hardware and software security. Hackers, for example, have little interest in paper ballots.
- The corruption in hardware that could influence the election process is not a threat.

2.2 E-VOTING

According to recent studies (Figure 2.3), 31 countries are experienced with the E-voting system and 20 countries have been listed as using EVMs. The method of e-voting has been widely used and most used in Asia. The biggest country in the world was India. Privacy, honesty and accountability in e-voting schemes have been a significant issue that it has been abandoned by several nations (i.e. France, Netherland). In several parts of democracy, EVM/DRE is the most used e-voting system. EVM was first introduced by U.S since 1974. (Historical Timeline - Voting Machines - ProCon.org, 2013).

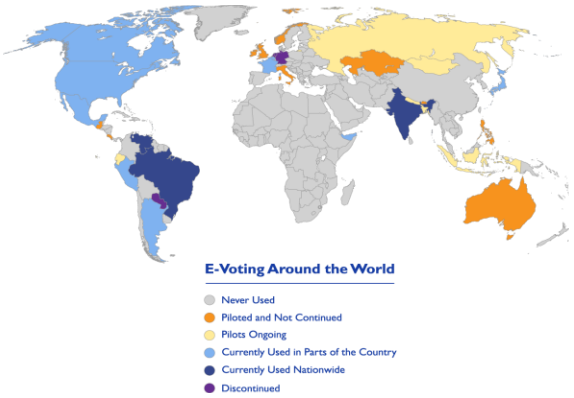

E-Voting Around the World
Never Used
Piloted and Not Continued
Pilots Ongoing
Currently Used in Parts of the Country
Currently Used Nationwide
Discontinued

Figure 2.3: Status of E-voting Around the World [11]

Three types of EVM can be described as dials, touchscreens and buttons (Figure 2.4)[10]. Over all, one thing in particular is that they stored the vote in CPU memory. The aim is to incorporate the method of voting and counting, which simply involves tracking the vote as cast by the elector. In addition, VVPAT will be an add-on to any of the EVMs to deliver authentication and auditability.

Figure 2.4 EVM/DRE [10]

Phase of Voting

- Voters drive to the polling station named for them.
- Official survey to check the identity of a voter.
- Voters switch to the cast-voting spot.
- Click any of the buttons representing the candidate on the EVM to cast a ballot.

Main benefits relative to paper ballots

The polling system is easier than paper ballots.

Better efficiency, so when the elector pushed a button on the EVM, the vote was counted. In addition, after the election process was over, the counting process of paper ballots began.

The price of paper ballots is greater than the price of EVM, like printing, paper, etc (Pathak, 2018).

2.3 I-VOTING

Since 2000, the United States has become the first country to use i-voting (Figure 2.5)[12]. Following that, 14 countries used the I-voting scheme, with a further 10 countries able to carry it out in the future [12]. Estonia, Canada, Switzerland, and France are the most relevant countries[12]. Estonia, on the other hand, is the first nation to fully implement the I-voting scheme.

Figure 2.5: Online I-Voting [13]

As seen in Figure 2.6, 31 states in the U.S. recently used I-voting in 2018. I-voting can be done in many areas, such as an online site, email, fax, and so on, leading to any remote-based electronic transmission, i.e. the root of the term "remote E-voting." I-voting is the evolution of e-voting in general. In fact, however there are crucial vulnerabilities such as DDoS, and voter PC virus infections, data tampering, spoofing, and so on as E-voting has been concerned [14]. For what I-voting does, cost, usability and usability concerns are merely solved. The aim of an election, according to Dr. Vanessa Teague, is not merely to pick a winner, but to persuade the looser and his followers that they have lost. Therefore, confidence in the democratic mechanism is an integral feature of every voting scheme.' [15]. While the Internet's flaws are well established, the use of the I-voting method persists in certain democracies. Nevertheless, there is little gap in the accountability of the polling process from the e-voting system i.e. no signs of data accuracy.

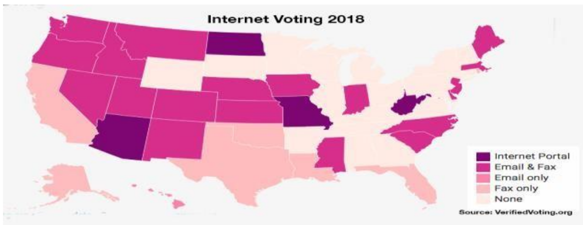


Figure 2.6: I-voting 2018 in U.S. [14]

Voting Process

- Voters have access to the voting system through electronic devices (i.e. desktops, laptops) that can connect to the Internet.
- The elector goes through the method of identity checking advised by the scheme.
- Via the UI, the elector decides the result.

Key Advantages over Electronic Voting Machines (EVMs) and Paper Ballots

Getting the fastest process of voting and the highest usability. With only a few taps, the elector will decide the vote anytime and at any moment (Elections Canada Online | A Comparative Evaluation of Electronic Voting, 2018). Furthermore, aside from In order to decide their vote, people who are out of the city, restless, and other so-called absentees will turn out to determine their vote.

Adopt affordability. No paper or EVM demands that the cost-effectiveness be significantly improved (Elections Canada Online | A Comparative Electronic Voting Evaluation, 2018).

The elector was completely directed by the device UI with I-voting to eliminate human error (i.e. incorrect choice, invalid vote). For paper ballots, when marking or the ballot paper given was null, the voter would make errors.

In addition, the elector can click the wrong button when using the EVM Encourage generations of young people to cast ballots (comfortable with technology).

Key disadvantages

- It can be useful for only as an online e-voting system, but cannot by the "national." By accessing the Internet, there is no perfect reliability, it has the greatest and deadly security flaws relative to the other forms of the voting system.
- For a general referendum, even though there are anything called flaws or glitches, it is a small problem that will significantly deter people from "believe" in the scheme.

According to the above facts and inquiries, while the I-voting system had overcome the shortcomings of the other modes of the e-voting system, and another story is stability.

Protection is the most critical obstacle for the I-voting method, and some countries are studying or adopting the "architecture" that could minimize the problems, but turned out to be the optimal solution. Any of the "architecture" countries that could minimize the issues but turned out to be the unidirectional approach, that is one of the reasons why the public started to adopt blockchain technology. In this situation, The Blockchain represents a technology that is most appropriate to get the concept behind the proposed framework, both "transparency" and "security."

CHAPTER 3 BLOCKCHAIN

3.1 BLOCKCHAIN

Bitcoin, the first and most well-known example of the use of blockchain software, has been quietly arriving in the blockchain technology movement since 2009. Furthermore, the Bitcoin creator remained anonymous, but an alias called Satoshi Nakamoto was left behind (bitcoin white paper).). "Bitcoin makes Blockchain, and email builds the internet," writes Sally Davies of the Financial Times. With just one currency, the developer of Bitcoin software is aided by a massive electronic system. [16.] Soon after, in 2014, it was revealed that blockchain technology can be used by organisations rather than cryptocurrency exchanges. Nonetheless, several individuals felt that both Bitcoin and blockchaiin were the same throughout 2018. The aim of blockchain technologies is to redefine the system's "confidence" that replaces intermediaries such as governments and companies, i.e. the framework of the next generations, decentralization[17]. With blockchain technologies, instead of intermediaries that are responsible for both data protection and stability, the 'trust' would be on the framework or so-called smart code.

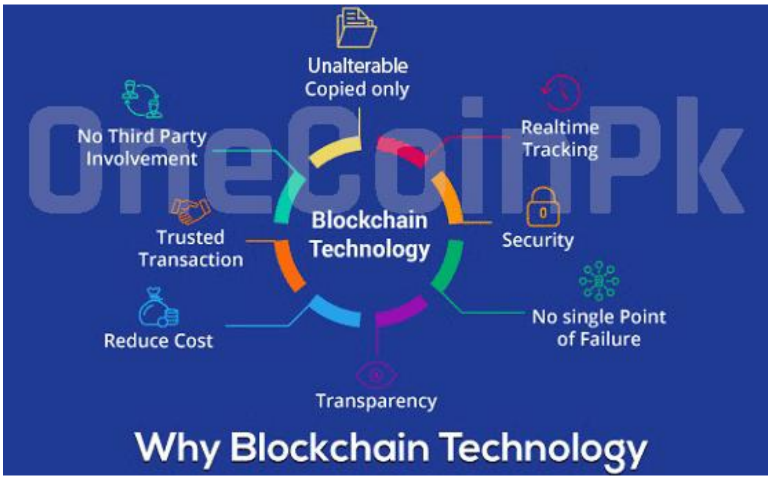


FIGURE 3.1: BLOCKCHAIN CAPABILITY [18]

Blockchain technology skills, however are what inevitably require clarity, immutability, and so on in the I-voting system (Figure 3.1). Currently numerous forms of blockchain, multiple consensus algorithms (i.e. PoW, PoS), and the new so-called "smart contracts" breakthrough have been established.

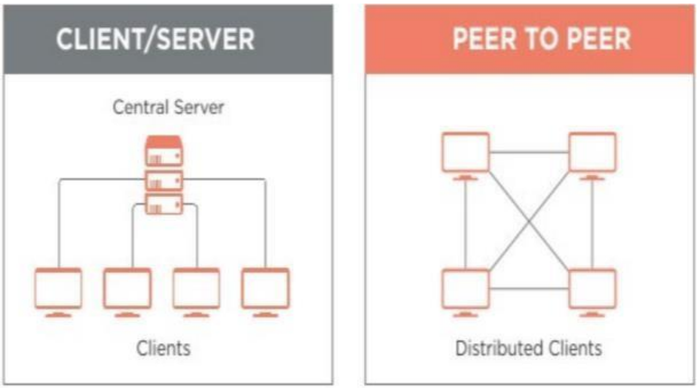
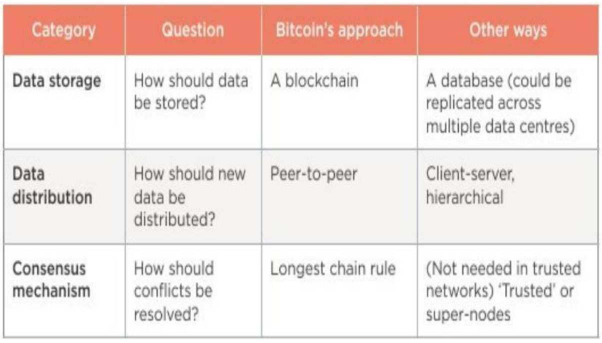


Figure 3.2: Centralization vs. Decentralization Architecture [19]

The server in the centralization architecture has maximum power, while the clients in the decentralisation architecture have full power, as seen in Figure 3.2. Theoretically, blockchain technology resembles a peer-to-peer network, with each peer having a distributed database and all peers maintaining the network's corresponding level." This also indicates that the nearest thing to government is blockchain technology.



Category	Question	Bitcoin's approach	Other ways
Data storage	How should data be stored?	A blockchain	A database (could be replicated across multiple data centres)
Data distribution	How should new data be distributed?	Peer-to-peer	Client-server, hierarchical
Consensus mechanism	How should conflicts be resolved?	Longest chain rule	(Not needed in trusted networks) 'Trusted' or super-nodes

Figure 3.3: Difference of dApps and Centralized Apps[19]

The simple comparison between dApps and centralized apps is as seen in Figure 3.3. In the P2P network, all nodes that are made sure that they keep the same copy can be synchronously distributed to blockchains.

The blockchain is a computer structure that allows for the insertion of processes but not their modification or removal. Figure 3.4 shows the new vote appended to the end of the candidate chain, and the reference (hash key) to the new vote will remain the same as before.

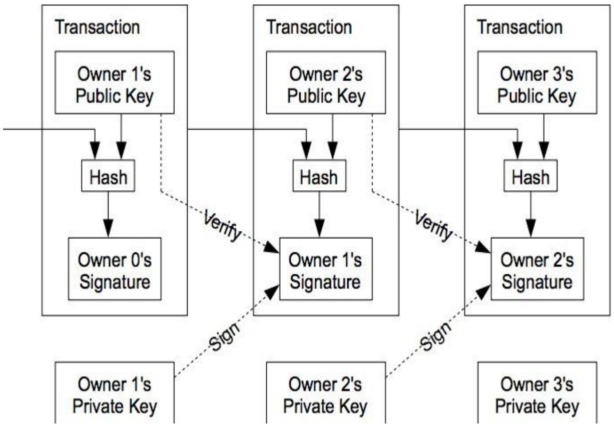


Figure 3.4: Cryptography Block [6]

Blockchain technology uses are called PoW consensus algorithm in the process. In the P2P Network, the longest chain will still be considered as unique and honest. PoW can detect tampering with votes and reject other nodes in the P2P Network.

3.2 CONSENSUS

A consensus, by definition, is an agreement within a party or community achieved in a complex manner [20]. PoW, invented by the inventor of Bitcoin, Satoshi Nakamoto [20], is one of the standard blockchain consensus algorithms.

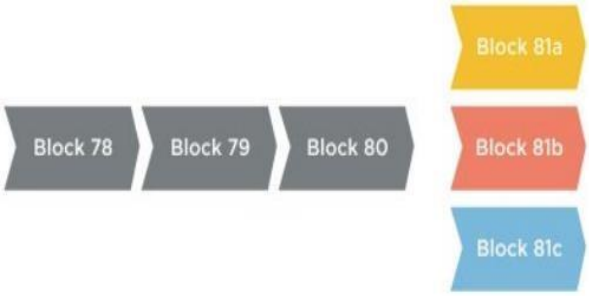


Figure 3.5: Block Conflict [19]

Assume only few electors cast their ballots concurrently, while the blockchain candidate is spread synchronously to all P2P network nodes (Figure 3.5). Both votes are known to have separate details i.e. voter information), which can create confusion in votes.

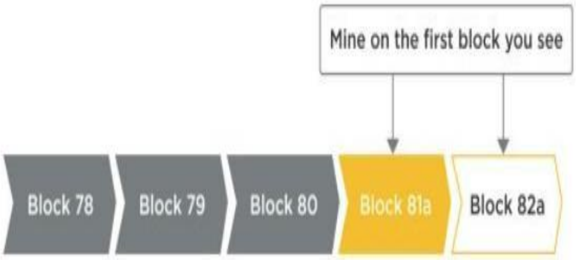


Figure 3.6: Lucky Block [19]

Around here the "longest chain rule" consensus process steps in to settle the disagreement. The first valid" vote to be applied at the end of the applicant blockchain would be chosen through this method (Figure 3.6).

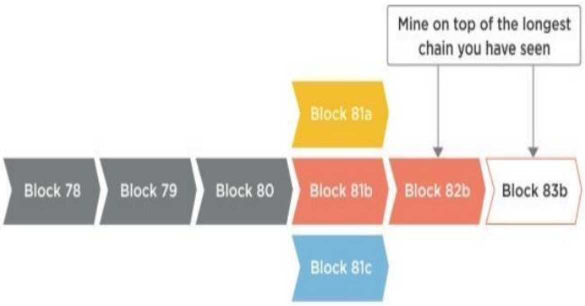


Figure 3.7: Longest Chain [19]

After that, as seen in Figure 3.7, the chosen candidate chain becomes the longest chain and the majority of the ballot will begin to be attached to this candidate chain, resulting in the accuracy of the votes.

3.3 TYPES OF BLOCKCHAIN

Owing to the large and diverse application styles i.e. (P2P trading and P2P freelancing), which have been generated to result in multiple forms of blockchain. The primary reason behind the scene which activates the blockchain's numerous properties. The Smart Contracts, is a brand-new programmable transaction that is provided by the Ethereum, is one example. There are private ones afterward,

The DLT of the blockchain was found by organizations such as banks, and a Permissioned Blockchain arose.

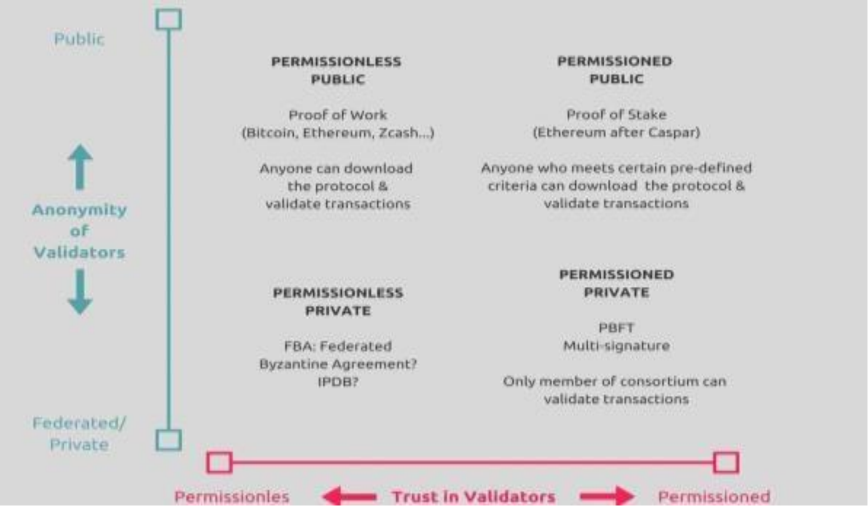

Public
PERMISSIONLESS PUBLIC
Proof of Work
(Bitcoin, Ethereum, Zcash...)
Anyone can download the protocol & validate transactions
PERMISSIONED PUBLIC
Proof of Stake
(Ethereum after Caspar)
Anyone who meets certain pre-defined criteria can download the protocol & validate transactions
Anonymity of Validators
PERMISSIONLESS PRIVATE
FBA: Federated Byzantine Agreement?
IPDB?
PERMISSIONED PRIVATE
PBFT
Multi-signature
Only member of consortium can validate transactions
Federated/ Private
Permissionles
Trust in Validators
Permissioned

Figure 3.8: Types of Blockchain [21]

Figure 3.8 indicates that the blockchain consists of different forms. In comparison, in the voting method, the different forms occur as follows:

• Public Blockchain without authorization. Open to the public without authorization to cast and check the ballot and to display the results (FFA).

• Public approved blockchain. Limit the casting and checking of the ballot to registered electors, and see the results.

The suggested scheme would use the Public Permissioned Blockchain as follows, which is ideally tailored to the scenario:

- After the voting is over, the registered elector can cast and check their vote and inspect the results.
- A poll/election that requires the registered elector to join and display the results during the process can be produced by the organizer.

PUBLIC AND PRIVATE BLOCKCHAINS

A public blockchain is one that anybody may view, transmit transactions to, and expect them to be included in the consensus process if they are legitimate. Cryptoeconomics, or the consensus process and transaction costs, protect public blockchains. This effectively means that the quantity of economic resources miners can have is proportionate to their level of influence in the consensus process.

Aside from public blockchains, there are also consortium blockchains, which include a pre-selected set of nodes that govern the consensus process. They are classified as private blockchains, with write access centralised to a single entity and read permissions open to the public or confined.

3.4 SMART CONTRACTS

A smart contract, by definition, entirely represents the collection of set of rules or requirements that are stored on ledger of a blockchain that enables the "eligible partty" to join. Smart contracts have traditionally been used to trade items such as land, money, and so on in a clear manner [22]. In addition, the smart contract is capable of real-time operation, authentication and protection of data tampering [23].

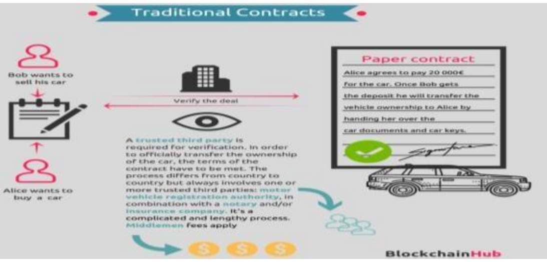

Traditional Contracts
Bob wants to sell his car
Alice wants to buy a car
Verify the deal
A trusted third party is required for verification. In order to officially transfer the ownership of the car, the terms of the contract have to be met. The process differs from country to country but always involves one or more trusted third parties: motor vehicle registration authority, in combination with a notary and/or insurance company. It's a complicated and lengthy process. Middlemen fees apply
Paper contract
Alice agrees to pay 20 000€ for the car. Once Bob gets the deposit he will transfer the vehicle ownership to Alice by handing her over the car documents and car keys.
BlockchainHub

Figure 3.9: Traditional Contracts in Trading [23]

Figure 3.9 demonstrates how conventional contracts work in trade. The election official serves as intermediaries, generally according to e-voting procedure discussed in section 2.2, just to do the authentication and allow the voter to decide their vote. For conventional contracts, as the third-party moves in the process will stay lengthy.

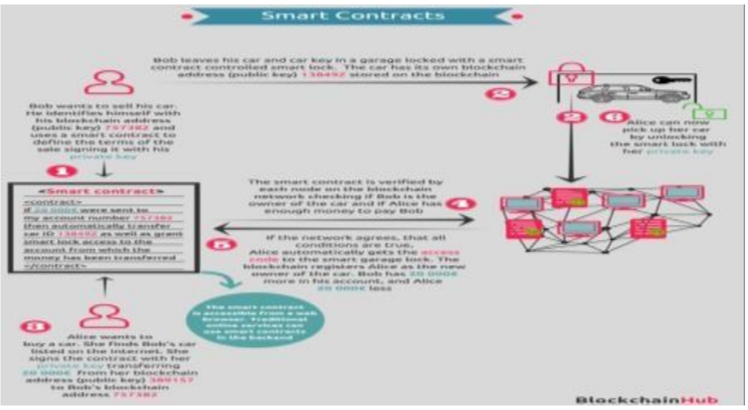


Figure 3.10: Smart Contracts in Trading [23]

Fig 3.10, on the other hand shows how smart contracts operate in trade. The measures as follows for the current method are:

- The blockchain of applicants was created by the admin or officer.
- A elector who wishes to cast vote to one of the candidates' ballots.
- Smart contract (PoV) validate the identity of the elector, "If an voter is eligible (i.e. identity) casts a vote on that candidate, increments one vote to the blockchain candidate ".
- Which candidate gets the majority wins.

The voting method was incredibly transparent for smart contracts, which immediately confirmed the elector without the middleman with such criteria.

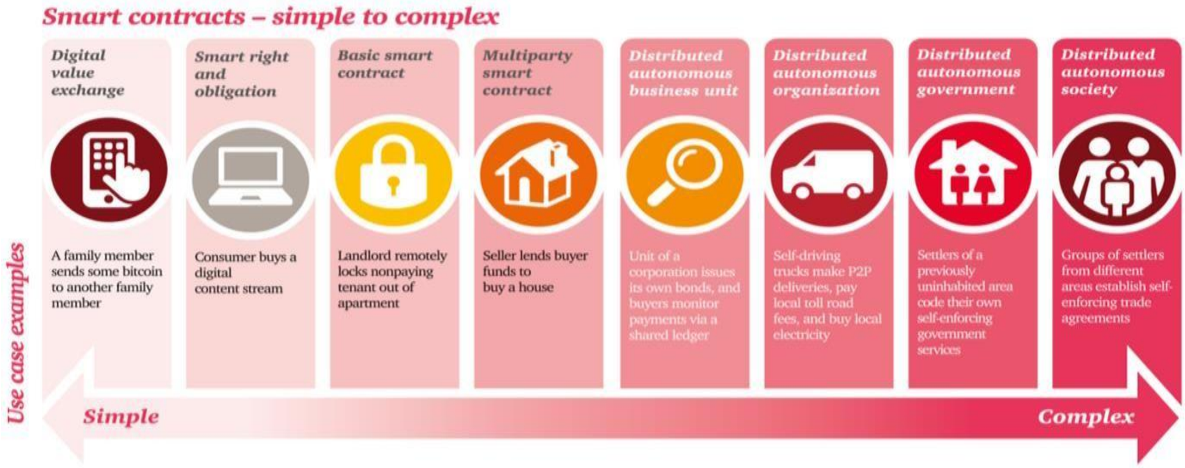

Smart contracts – simple to complex
Digital value exchange
Smart right and obligation
Basic smart contract
Multiparty smart contract
Distributed autonomous business unit
Distributed autonomous organization
Distributed autonomous government
Distributed autonomous society
A family member sends some bitcoin to another family member
Consumer buys a digital content stream
Landlord remotely locks nonpaying tenant out of apartment
Seller lends buyer funds to buy a house
Unit of a corporation issues its own bonds, and buyers monitor payments via a shared ledger
Self-driving trucks make P2P deliveries, pay local toll road fees, and buy local electricity
Settlers of a previously uninhabited area code their own self-enforcing government services
Groups of settlers from different areas establish self-enforcing trade agreements
Use case examples
Simple
Complex

Figure 3.11: Use Case of Smart Contracts [24]

As seen in Figure 3.11, there are different kinds of smart contracts based on difficulty. While the proposed framework represents a governance-like program, the developer would implement the simple smart contract instead of DAO according to the environment of confusion (i.e. time).

As the software creation approach, XP Methodology will be the better methodology for the proposed scheme. Since the proposed an incredibly small context (time) to build the huge system [25]. In addition, in contrast, RAD and XP are relatively similar, but the crucial aspect is that RAD is not consistent with the whole device.

One of the advantages of XP to eliminate needless labour and pitfall that meets the most prescribed procedure. The XP approach, even though it is an independent endeavour, is consistent with the proposed scheme. Accordingly, “pair programming” will be unconducted during the life cycle which directly overcomes one of the XP’s weakness.scheme has been perceived as broad and complex, brief deadline. XP is thus fully adapted to the present situation. The XP Technique is shown in figure 2.4.4.1. Briefly, XP was used under.

3.5 TRANSACTION

A transaction is a collection of instructions for changing the blockchain's state. In order for transactions to be processed by specialised nodes, or so-called miners, and confirmed by the network, transaction fees are a feature of public blockchain networks (See 2.1.4). Miners put forth a good show.

For a monetary incentive, you must perform computational effort.

For the following reason, it is important to briefly present Unspent Transaction Outputs (UTXOs for short) in order to truly comprehend what a blockchain state is.Transactions are the means through which value is transferred in Bitcoin. The current situation of Bitcoin is depicted.

Bitcoin, by virtue of its worldwide collection of UTXOs, does not keep track of user account balances. The cumulative total of each individual UTXO that a user has is the user's account balance.the private key that corresponds to it Other blockchains, on the other hand, can handle large amounts of data account balances and more, such as Ethereum, which is a state machine based on transactions. It may be used to build any transaction-based state machine notion.

3.6 DIGITAL WALLETS

An asymmetric key pair, consisting of a private key and a public key, is associated with each user who wishes to conduct a transaction. The public key is linked to a digital wallet, which acts as a user's address but has no relation to the user's identity. It is open to the public and may be accessed by anybody. The private key, on the other hand, is kept private to ensure that only the wallet's owner may sign legal transactions.

Transactions are regarded legitimate when they are signed with the user's private key, resulting in an unforgeable digital signature. As a result, transactions are one-of-a-kind, and only the owner may produce a one-of-a-kind digital signature.

3.7 ETHEREUM

A new age began soon after blockchain technology was established and applied with Bitcoin. Cryptoeconomics, from which Ethereum is derived, was formed as a result of the birth of digital currency.It is, however, an adaption of its essential principles with the goal of creating a decentralised system.For a wide range of different uses, combine a network with memory. Ethereum is a general-purpose blockchain that can be programmed in any computer language. It has the ability to store data and enforce the protocol's correct execution.

In 2015, Ethereum was introduced as a foundation for applications that required decentralisation and a shared memory notion. It enables programmers to create smart contracts and store them on the blockchain.

3.8 SOLIDITY

Solidity is a specialised programming language that may be used to create such contracts. It's a high-level, object-oriented language for creating smart contracts that are expressed in the same way that classes are in object-oriented languages. The contracts are made up of code and information in the variables of state Its operation and state are encapsulated in these.

On the Ethereum blockchain, the contracts are deployed to a specific address. Contracts include specific rules that specify who and what is allowed to read and write on the contract. For functions and state variables, there are four categories of visibility: external, public, internal, and private. They must be unique and provide a comparable role to those found in other object-oriented systems.

It's critical to remember that anyone watching a contract can see anything inside it. The term "blockchain" refers to a A private variable merely stops other people from seeing and changing the data. Outside of the blockchain, though, it is still visible.

3.9 TRANSACTION

It's also important to remember that Ethereum has a fixed fee each computational step performed on the contract. This entails either running a function on a contract or installing a contract on the Ethereum blockchain, both of which are basically transactions. When a contract is completed, all instructions on every node of the network are carried out, resulting in a cost. The price is expressed in gas units and paid in Ether, Ethereum's native money.

The ECDSA method, specifically Bitcoin's secp256k1 curve, is used to sign all Ethereum transactions. Without requiring a third party, the encoding of the set of rules that comes with a mechanism and the cryptographic features maintain it appropriately safe.

Essentially, it enables the creation and execution of an application with immutable rules once it has been deployed.The contracts are transparent and cannot be changed, ensuring accuracy.

3.10 MINING

Ethereum's mining process uses the same basic features as Bitcoin's. However, rather than the SHA-256 method used by Bitcoin, Ethereum employs the Ethash mining method, which employs the Keccak hash function. Furthermore, not all miners will approve every transaction, since some may have regulations that only allow transactions with a particular minimum gas price to be accepted.

If a transaction has a predetermined gas price that is less than that limit, those miners will be penalised. It's possible that your transaction will be ignored. The transaction is more likely to be included in the following block if the gas price is greater. Every 14-16 seconds, a new block is added to the Ethereum network. A miner, for example, can configure his node to aid the network by mining only low-gas transactions.

3.11 ARCHITECTURE

Unlike Bitcoin, Ethereum has the feature of containing the state root in every block. Merkle trees are a specific type of data structure that holds the whole state of the system. It lets a node to instantly synchronise with the blockchain using only the most recent block, without having to process any previous transactions. Any piece of data inside the tree must be properly validated against a root hash, much as the basic Merkle tree [2]. It also has the feature of allowing data to be swiftly added, deleted, or modified in the tree without affecting the overall structure. In Ethereum, the tree is used to record transactions, receipts, accounts, and account storage.

3.12 ENVIRONMENTAL ASPECTS

The paper, printing, and transportation are the environmental effects of a traditional paper-based election. Specifically, voting cards, ballots, and envelopes. While the CO2 emissions from the power required are the environmental implications of a blockchain-based election. Some calculations will be required to determine if a blockchain-based election is viable.

Because the percentage of emissions from electricity and heat cannot be distinguished in this case, the result will be larger than the real figure. However, it is assumed that power production is responsible for the majority of those emissions. If, on the other hand, a percentage difference between electricity and heat is assumed, the ultimate result may simply be divided by the proportion.

CHAPTER 4 VOTING SYSTEM USING BLOCKCHAIN

The design of the decentralised voting system is further explained in this section. The nature of this project was investigative, and it was completed in a week-long iterative process. The end aim was to meet the requirements indicated in the issue definition, which included privacy, integrity, and accuracy. Elections are seen as a democratic celebration. We have a lot of challenges to overcome in order to put this festival together. Every year, we find people's names missing from the voting list owing to an election official's negligence or malfeasance. We need to eliminate manual involvement from our voting list so that it is error-free. We also observe issues such as EVM hacking accusations and booth capture. In addition, our present voting technology does not allow for remote voting. As a result, persons who live or work in various places have difficulty voting. The procedure of creating a voter ID card is similarly time-consuming. So that people may enjoy their event, we should make this procedure straightforward, secure, resilient, tamper-proof, and transparent. The group was able to adapt to the present stage of the implementation every week in regard to the specified requirements thanks to the iterative method. Due of the broad and subjective issue requirements, iterations were kept to a minimum. Any simple technical or theoretical aims are difficult to achieve without a thorough understanding of the available tools, frameworks, and ideas.

The project included both study and execution at the same time, with the two complementing one another in a cyclical fashion. The requirements were addressed and compared to the stage of execution in the weekly meeting, which led to fresh ideas on what theory or solution was needed to continue ahead.

4.1 PROPOSED SOLUTION

As a follow-up, we propose a blockchain-based election system to address all present issues.

Apply Voter Card- If a person already has an Aadhar card, a voter ID will be generated for them when they reach eighteen. If you do not have an Aadhar card, you must apply through the system by submitting your birth certificate and proof of address. Document verification and biometric (fingerprint) registration requests can be scheduled by the user.

Missing Name-The concept of a manual voting list will be abandoned. The vote list will be stored on the blockchain. When a person reaches the age of 18, the list will be automatically updated based on the information provided when applying for a voter ID.

Live in an Alternative Location- We'll have a drop box where voters may choose between current and different voter locations. If the polling officer selects a different site, the candidate information will be imported from the voter ID location.

Fake Voter and Booth Capturing- There have been several examples of people voting in their own names using another person's voting card, and some persons capturing booths for fraudulent voting. So, before voting, users must provide their finger print for verification, ensuring that no one votes twice.

Expedite Vote Counting- In order to avoid manually counting the votes, we will programme our smart contract to automatically count the votes by constituency and candidate. Without any inconsistencies, the results may be released shortly after voting.

4.2 SYSTEM ARCHITECTURE

We will use Etherium to build our blockchain back end. Our web application (client side) will interact with the blockchain system with the help of REST APIs. Client side will be build using HTML, CSS, JavaScript, Web3.js, React.js etc. Currently, we have decided to run all the nodes on a single local machine Ganache container. Our future goal is to run it on multiple machines on the same network. Our model file will contain following- participant, asset, transaction.

PARTICIPANTS

- Voter
- ID Registration Officer
- Election Officer
- Polling Officer

ASSET

- Candidate
- Constituency
- Voter

- Ballot
- Voting Status

TRANSACTIONS

- cast Vote
- Create voter card
- Update voter information
- Delete voter information
- Register candidate
- Delete candidate
- Generate voting list (add voter details from Aadhar)
- Add constituency
- Delete constituency
- Count vote
- Start Voting

4.3 DEPENDANCY

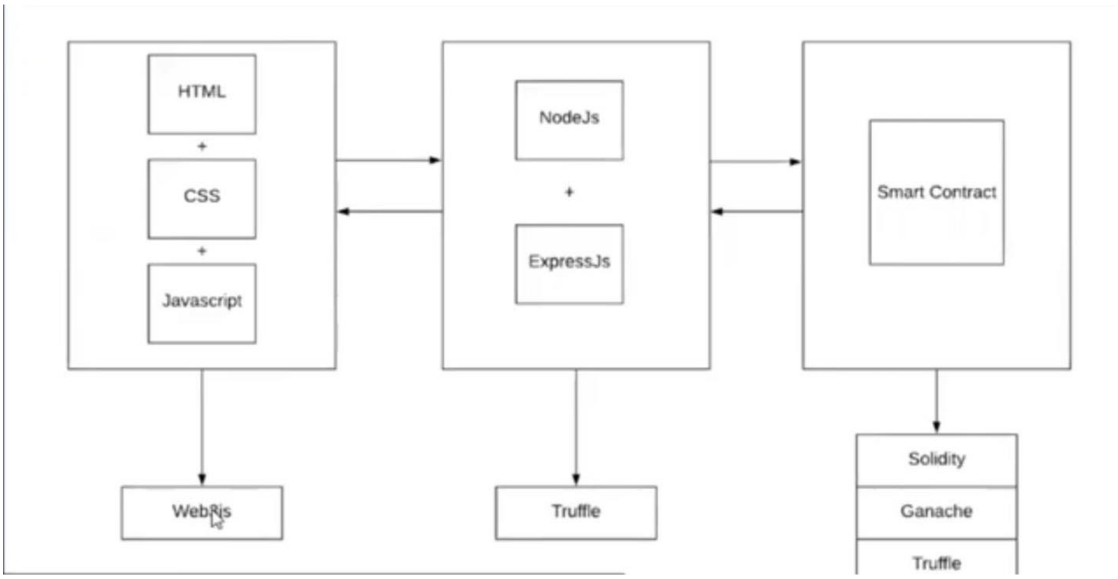


Fig 4.1 The process of building Decentralised Voting System

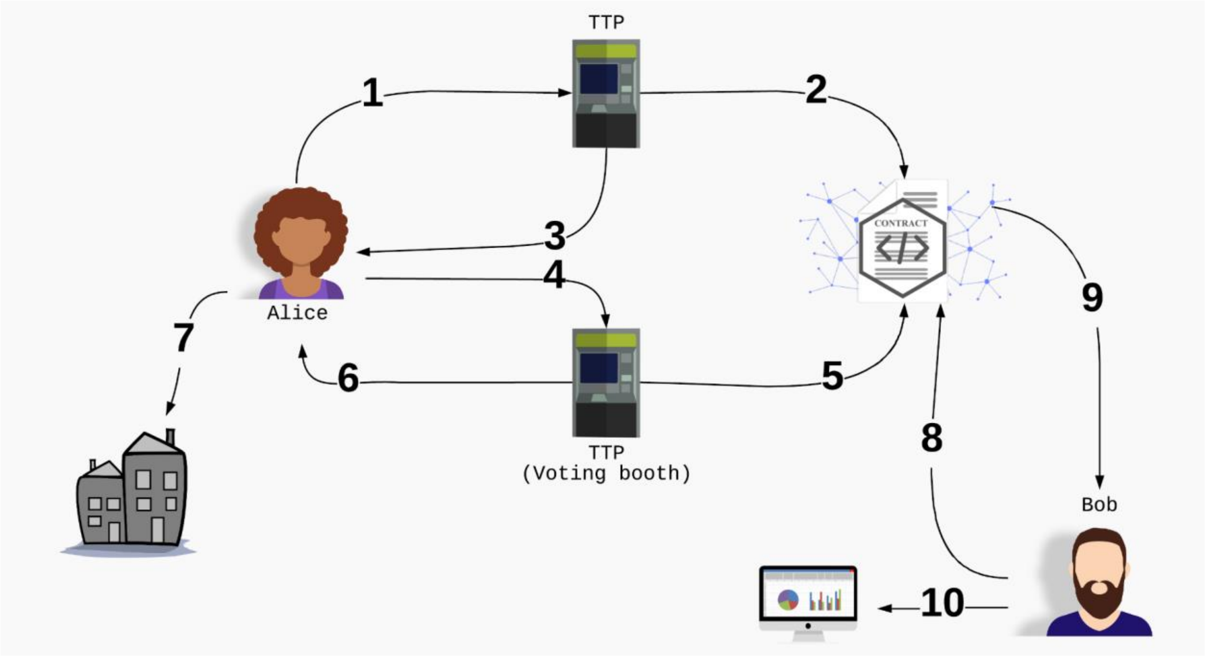


Fig4.2 Working of Decentralised Voting System

4.4 FLOW CHART

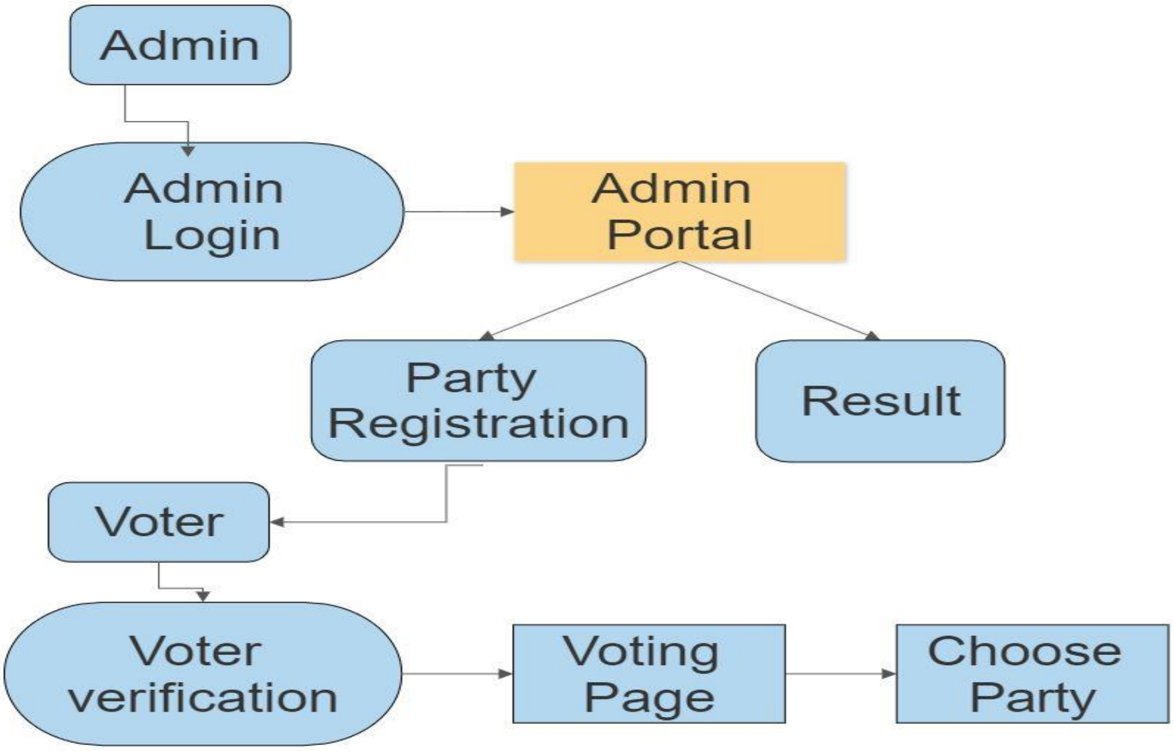


Fig 4.3 Flow chart of process

4.5 PRIVACY

To cast a vote during an election, a citizen must be eligible to vote. A TTP will ensure that they have the right to vote and will allow them to do so. Decentralised vote must ensure that individual voters' votes are anonymous during this process by making them untraceable. The TTP's goal is to secure citizens' identities by giving them an anonymous ID that is unrelated to their credentials

4.6 INTEGRITY AND CORRECTNESS

Decentralised vote must ensure that the smart contract can only be manipulated by a TTP.In order to avoid counter feiting, all IDs are produced using the same TTP. in addition to correctness is accommodated by the smart contract, which works as a set of regulations.

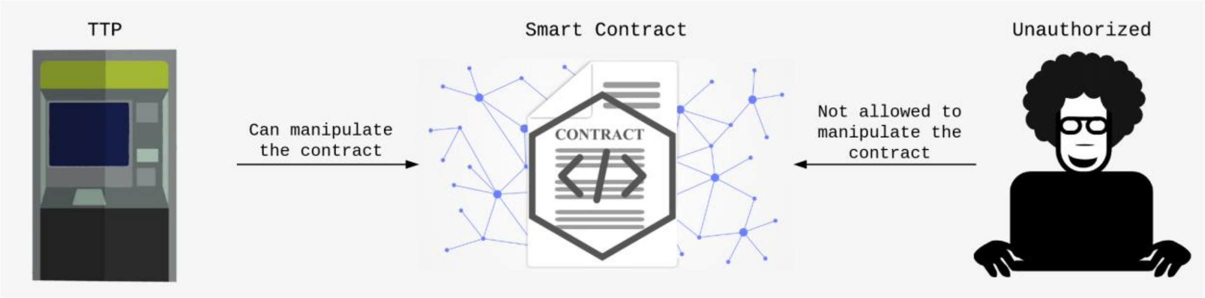

TTP
Smart Contract
Unauthorized
Can manipulate the contract
CONTRACT
Not allowed to manipulate the contract

Fig 4.4 Integrity and Correctness

4.7 TOOLS

A variety of technologies were utilised in the investigation of the feasibility of constructing a decentralised voting system. In this part, you'll learn about them. Specific technologies were utilised to facilitate cooperation and standardise the code output in order to synchronise all six participants of the project and produce code at the same time. Github was utilised to parallelize the task. A CI system, which worked in tandem with Github, tested all of the code that was written before it was accepted for inclusion in the main application. A linter was added to the project, along with a webhook, to ensure code standards. The linter was run on each submission to the main application, preventing low-quality code.

The project was split into two systems: one for smart contracts, and another for the Web application. Because the Web application relies on the developed smart contracts, both are saved together in one primary project.

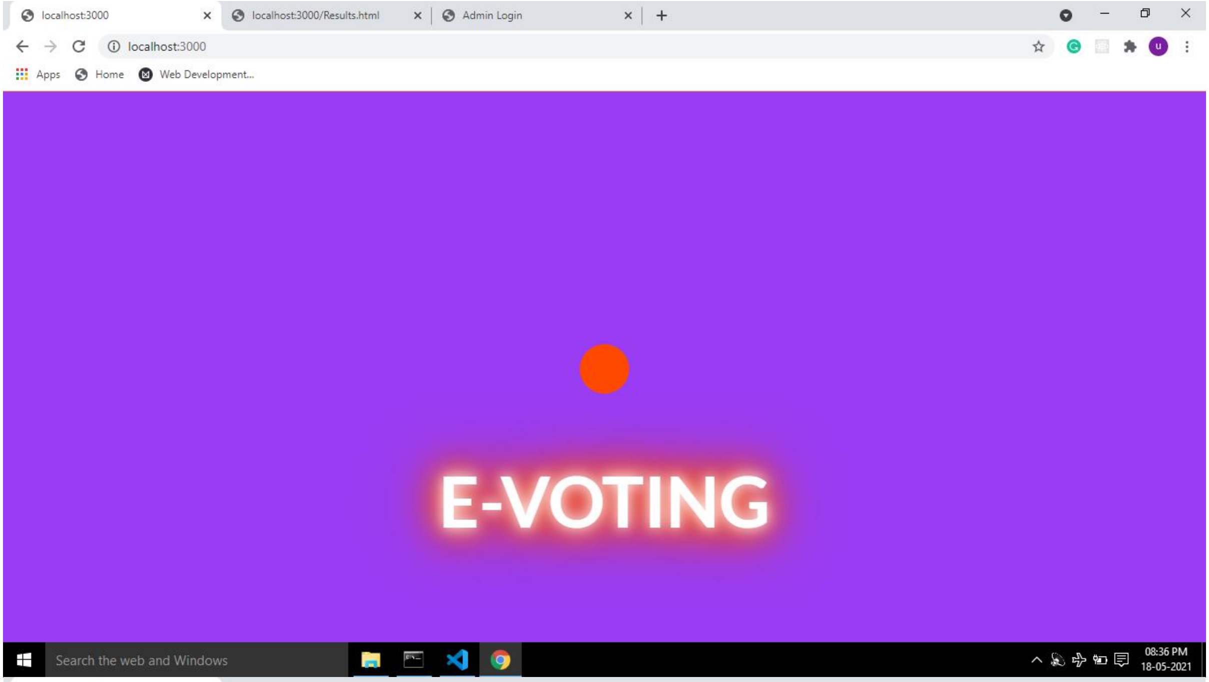
Trufle and Ganache were used to carry out Solidity code testing. Truffle provides the Mocha test framework, which allows you to build JavaScript tests. Aside from the Solidity tests, there were additional tests for the web application, mostly to guarantee adequate encryption. The Ganache CLI version was used to collect test data, and the data was later analysed and parsed is a word that is used to describe anything that

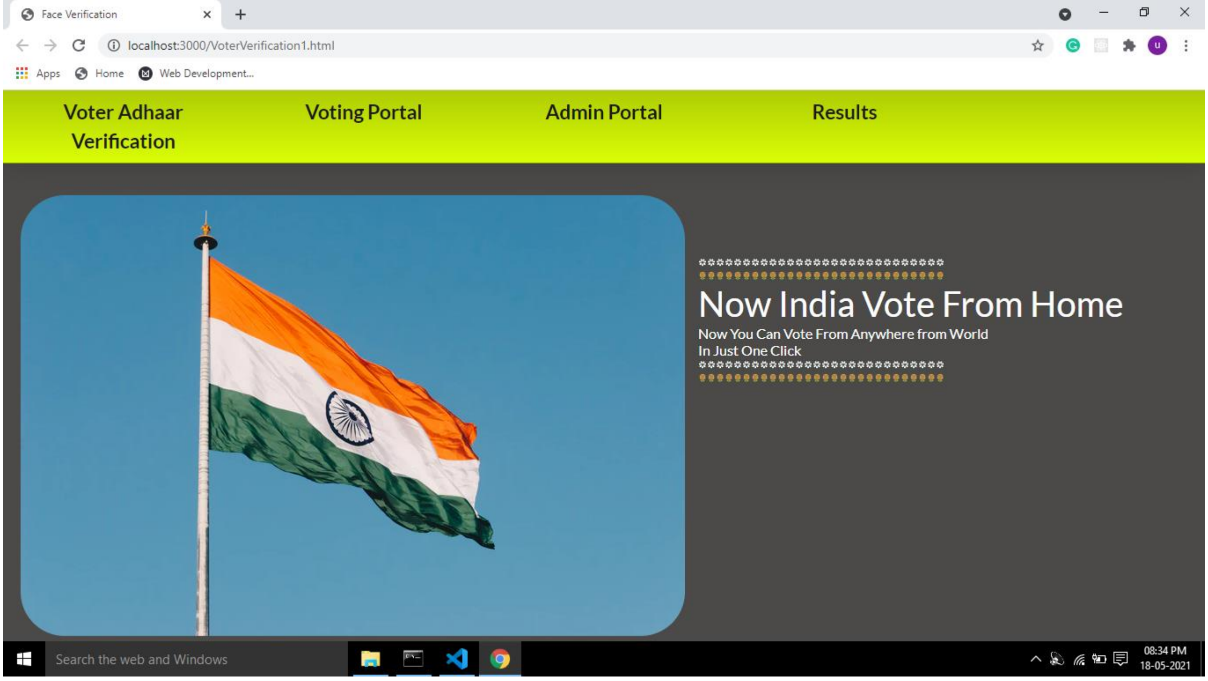
4.8 CONCLUSION

The problem of EVM hacking and booth capturing are resolved and the voter’s rights are not encapsulated. This is how we can make use of resources to make this process simple, secure, robust, tamper proof and transparent so that people can enjoy their festival.

CHAPTER 5 RESULTS

5.1 HOME PAGE

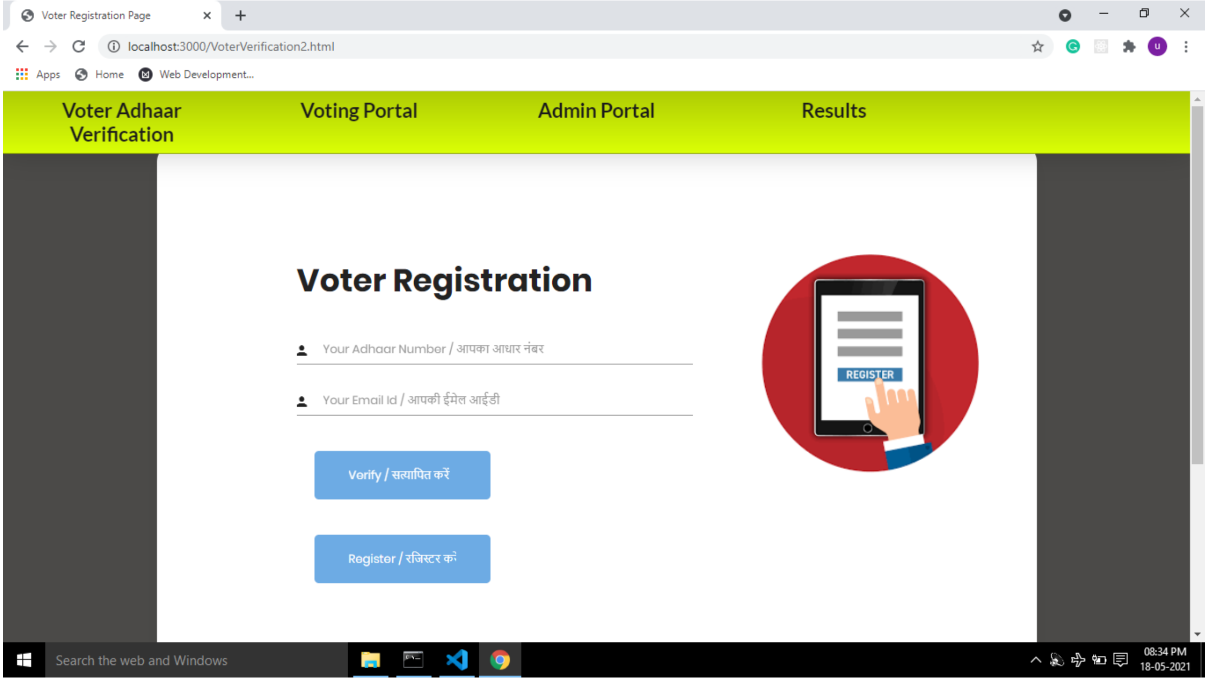




Now India Vote From Home

Now You Can Vote From Anywhere from World
In Just One Click

5.2 VOTER'S REGISTRATION



Voter Registration

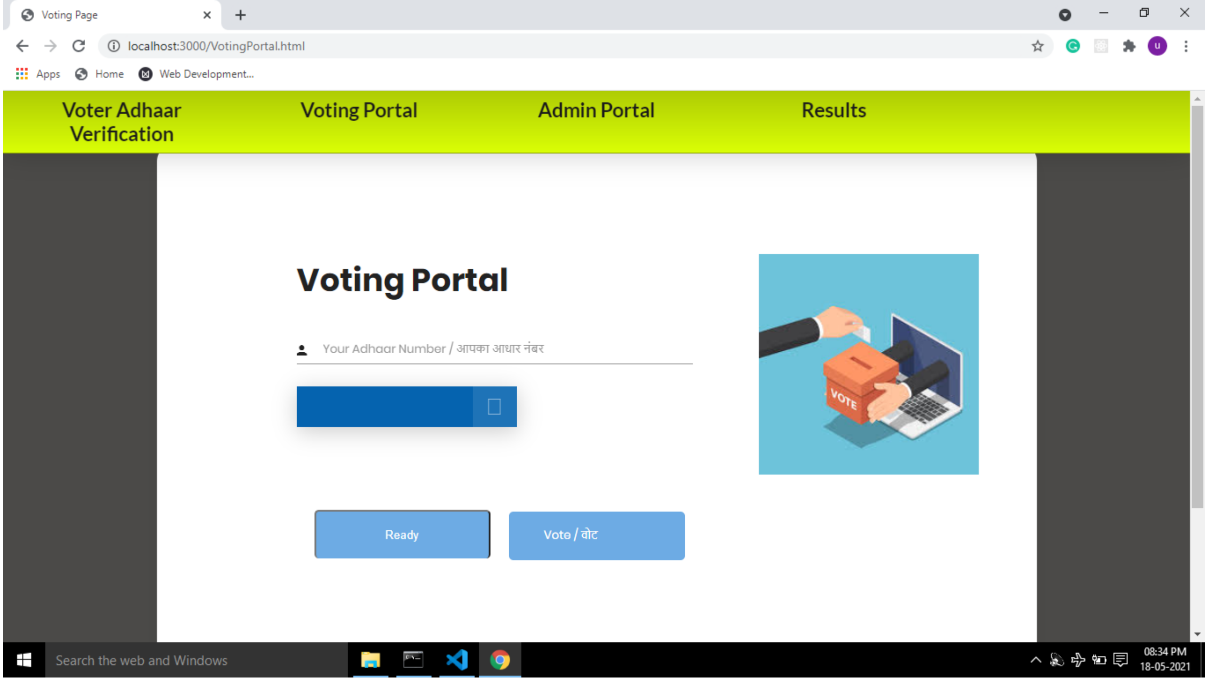
Your Adhaar Number / आपका आधार नंबर

Your Email Id / आपकी ईमेल आईडी

Verify / सत्यापित करें

Register / रजिस्टर करें

5.3 VOTER LIST



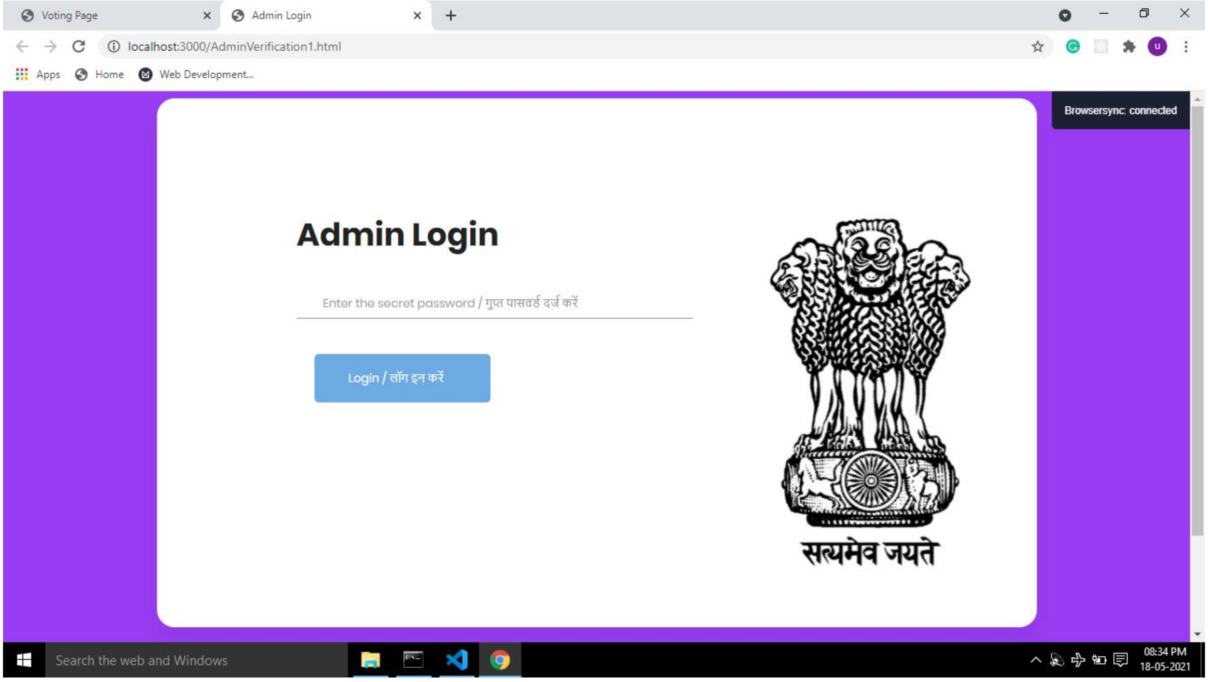
Voting Portal

Your Adhaar Number / आपका आधार नंबर

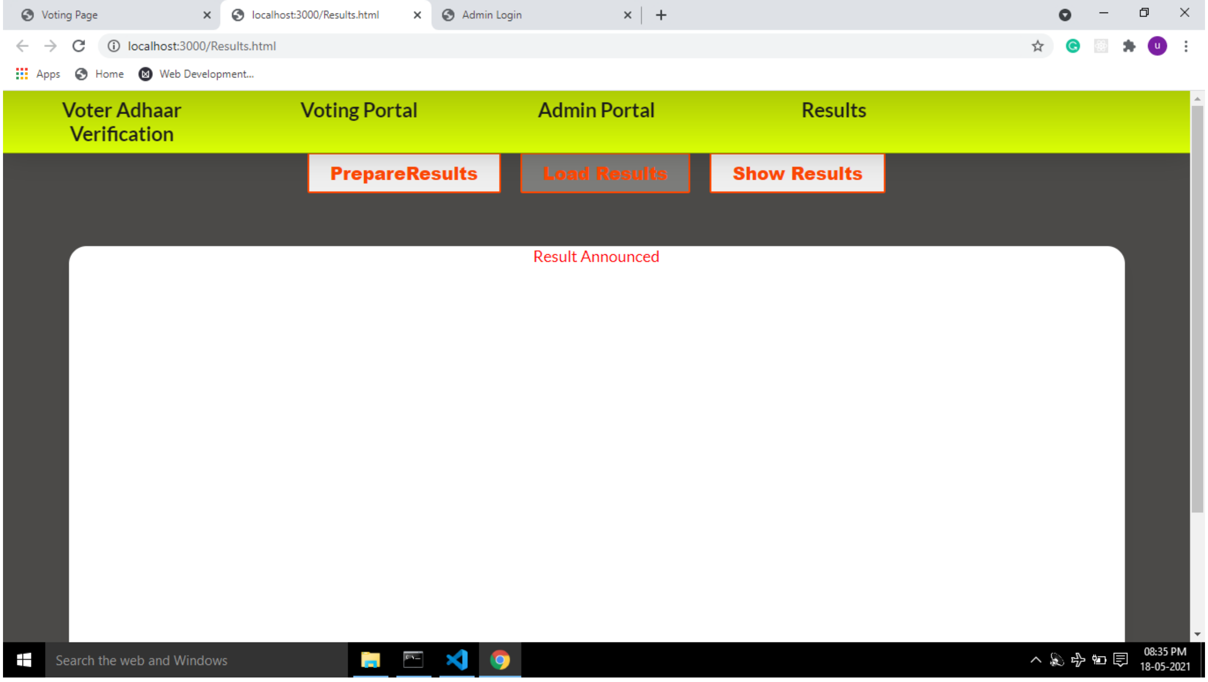
Ready

Vote / वोट

5.4 ELECTION OFFICER PORTAL



5.5 ELECTION RESULTS



Result Announced

REFERENCES

1. Electronic Voting Machine: Here's all you wanted to know about India's EVMs. Retrieved 22 8, 2018, from https://www.indiatoday.in/india/story/all-you-need-to-know-about-electronic-voting-machine-969155-2017-04- 03. 2017.
2. i-Voting—e-Estonia. Retrieved 22 8, 2018, from https://e- estonia.com/solutions/e-governance/i-voting/., 2018.
3. Hari K. Prasad, J. Alex Halderman, Rop Gonggrijp, Scott Wolchok, Eric Wustrow, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati.“Security Analysis of India’s Electronic Voting Machines. Retrieved 228, 2018”, from https://indiaevm.org/evm_tr2010-jul29.pdf., 2010.
4. McGuinness, D. “How a cyber attack transformed Estonia. Retrieved 22 8, 2018”, from https://www.bbc.com/ news/ 39655415., 2017.
5. Lafaille, C. “What is Blockchain Technology? An Easy Guide for Beginners Retrieved 228,2018”, from https://www. investinblockchain.com/what-is-blockchain-technology/., 2018.
6. Nakamoto, S. Retrieved 22 8, 2018, from https://bitcoin.or /bitcoin.pdf., 2008.
7. What is Ethereum? — Ethereum Homestead 0.1 documentation. Retrieved 22 8, 2018, from http://www.ethdocs.org/ en/latest/introduction/what-is- ethereum.html., 2016.
8. Vogelsteller ,F. ethereum/wiki. Retrieved 22 8, 2018, from https://github.com/ethereum/wiki/wiki/White-Paper., 2018.
9. Britannica, T. E. Australian ballot | politics. Retrieved 22 8, 2018, from https://www.britannica.com/topic/Australian- ballot., 2018.
10. Voting Systems & Use: 1980-2012 - Voting Machines - ProCon.org. Retrieved 228, 2018, from https://votingmachines.
11. Electronic Voting and Counting Around the World. Retrieved 22 8, 2018, from https://www.ndi.org/e-voting- guide/electronic-voting-and-counting-around-the-world., 2018.
12. Internet Voting. Retrieved 22 8, 2018, from https://www. ndi.org/e-voting-guide/internet-voting., 2018.
13. E-lected. Learning about the Du-Vote internet voting system. Retrieved 26 8, 2018, from http://e- lected.blogspot.com/2015/ 06/secure-du-vote-card-based-internet.html., 2015.

14. Verified Voting. Retrieved 22 8, 2018, from https://www. verifiedvoting.org., 2018.
15. Porup, J. Online voting is impossible to secure. So why are some governments usingit?Retrieved228,2018,from https://www.csoonline.com/article/3269297/security/online-voting-is-impossible-to-secure-so-why-are-some- governments-using-it.html., 2018
16. Marr, B. A Very Brief History Of Blockchain Technology Everyone Should Read. Retrieved 268,2018,from https://www.forbes. com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#5a98f88f7bc4., 2018.
17. CEUR-WS.org - CEUR Workshop Proceedings (free, open- access publishing, computer science/information systems/information technology). (2017). Retrieved 26 8, 2018, from http://ceur-ws.org/
18. Onecoin. Retrieved 26 8, 2018, from https://www.onecoinpk. com/blockchain-quotes., 2018.
19. Brave New Coin. Retrieved 22 8, 2018, from https:// bravenewcoin.com., 2018.
20. What Are Smart Contracts? A Beginner’s Guide to Smart Contracts. (2018). Retrieved 26 8, 2018, from https:// blockgeeks.com/guides/smart-contracts/., 2018.
21. Blockchains & Distributed Ledger Technologies. Retrieved 22 8, 2018, from https://blockchainhub.net/blockchains- and-distributed-ledger-technologies-in-general., 2018.
22. What Are Smart Contracts? A Beginner’s Guide to Smart Contracts. Retrieved 26 8, 2018, from https://blockgeeks. com/guides/smart-contracts/., 2018.
23. Smart Contracts. Retrieved 26 8, 2018, from https:// blockchainhub.net/smart-contracts/., 2018.
24. PwC. Retrieved 26 8, 2018, from https://www.pwc.com., 2018.
25. Maniuk, I. Tests in Extreme Programming. Retrieved 22 8, 2018, from https://hygger.io/blog/tests-in-extreme- programming., 2016.