A

Seminar Report

Blockchain Enabled E-Voting

Submitted in partial fulfillment of the requirements for the Award of the Degree

of

Master of Computer Applications

of

APJ Abdul Kalam Technological University

Submitted by

Nandakishore VV

RegNo: TVE16MCA33

Department of Computer Applications

COLLEGE OF ENGINEERING TRIVANDRUM

AUGUST 2018

DEPARTMENT OF COMPUTER APPLICATIONS

COLLEGE OF ENGINEERING TRIVANDRUM

CERTIFICATE

Certified that this Seminar report entitled, ***"Blockchain Enabled E-Voting "*** *is the paper presented by* ***"Nandakishore VV "(Reg No: TVE16MCA33)*** *in partial fulfillment of the requirements for the award of the degree of Master of Computer Applications of APJ Abdul Kalam Technological University during the year 2018.*

Prof. Baby Syla L.

Co-ordinator

Prof. Jose T Joseph.

Head of the Department

Acknowledgement

First and foremost I thank **GOD** almighty and my parents for the success of this seminar. I owe my sincere gratitude to everyone who shared their precious time and knowledge for the successful completion of my seminar.

I would like to thank **Dr Jiji C V**, Principal, College of Engineering Trivandrum, who helped me during the entire process of work.

I am extremely grateful to **Prof.Jose T Joseph**, HOD, Dept of Computer Applications, for providing me with best facilities and atmosphere for the creative work, guidance and encouragement.

I would like to thank my coordinator, **Prof. Baby Syla**, Dept of Computer Applications, who motivated me throughout the work of my seminar.

I profusely thank other Asst. Professors in the department and all other staff of CET, for their guidance and inspiration throughout my course of study.

I owe my thanks to my friends and all others who have directly or indirectly helped me in the successful completion of this seminar. No words can express my humble gratitude to my beloved parents and relatives who have been guiding me in all walks of my journey.

Nandakishore VV

Abstract

Blockchain is a decentralized ledger used to securely exchange digital currency, perform deals and transactions. Each member of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction. Blockchain ledger is a collection of all Bitcoin transactions executed in the past. Basically, its a distributed database which maintains a continuously growing tamper proof data structure blocks which holds batches of individual transactions. Blockchain-enabled e-voting (BEV) could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV uses an encrypted key and tamper-proof personal IDs. This article highlights some BEV implementations and the approach's potential benefits and challenges. The idea in blockchain-enabled e-voting (BEV) is simple. To use a digital-currency analogy, BEV issues each voter a wallet containing a user credential. Each voter gets a single coin representing one opportunity to vote. Casting a vote transfers the voters coin to a candidates wallet. A voter can spend his or her coin only once. However, voters can change their vote before a preset deadline. Here, we argue that blockchains might address two of the most prevalent concerns in voting today: voter access and voter fraud.

Contents

List of Figures

Chapter 1

Introduction

Election is a huge administrative process that takes up a lot of time, effort and monetary resources of a state. In a country like India, where assembly elections are not held uniformly, the entire voting process demands large scale nancial needs, workforce and infrastructure. Despite all the shortcomings it has, a lot of countries still follow the traditional paper ballot system. India has adopted Electronic Voting Machines(EVMs) from 1999 and by 2017, EVMs have replaced paper ballots all over the country. Even though EVMs are one of the most secure voting systems, they are not yet fully foolproof.

The present day voting systems, be it paper ballots or EVMs, require armed forces guarding them to ensure the security of the votes cast. Election period witnesses booth capturing to conscate ballots/EVMs, identity fraud and violence in many parts of the country. Election process demands a large number of government ofcials to work overtime for the overall management and the necessary paperwork. This indicates that elections arent carried out efciently and that their security and transparency should be improved.

1.0.1 Why use blockchain to implement E-Voting?

Blockchain is a decentralized distributed public ledgering system. It can be used for secure monetary transactions, data storage and retrieval. The problems of the now prevalent EVMs can be overcome if we implement voting using blockchain technology. It is the most secure technology available now which promises the prevention of identity fraud and multiple voting. This problem can be solved successfully only by using blockchain as all the other implementation techniques use a traditional database which could be compromised. Blockchain is a disruptive

technology and if e-voting is enabled using blockchain, it would disrupt the traditional election process and the working of the election commission in the country. The entire process would become simple and less complicated. The data saved in the blockchain is immutable, unlike the data in conventional servers. Moreover, the overall expense of the entire election process across the country could be reduced. Public holidays need not be declared in regard with elections, if this system is implemented. Votes once cast are not destroyed or mutable, even if the voting systems are damaged. Therefore, the number of security personnels at the voting centers can be reduced considerably. If a voting system is damaged, voters can make use of other voting systems in the same locality with no issues whatsoever. The counting process and result declaration is made hassle free and simple because votes are counted as they are being cast. The system also follows green protocol and is environment friendly.

Chapter 2

Future Voting Systems

E-VOTING is among the key public sectors that can be disrupted by blockchain technology. The idea in blockchain-enabled e-voting (BEV) is simple. To use a digital-currency analogy, BEV issues each voter a wallet containing a user credential. Each voter gets a single coin representing one opportunity to vote. Casting a vote transfers the voters coin to a candidates wallet. A voter can spend his or her coin only once. However, voters can change their vote before a preset deadline. Here, we argue that blockchains might address two of the most prevalent concerns in voting today: voter access and voter fraud. The idea is as follows. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV employs an encrypted key and tamper-proof personal IDs. For example, the mobile e-voting platform of the Boston-based startup Voatz employs smart biometrics and real-time ID verification. The public ledger ties each cast ballot to an individual voter and establishes a permanent, immutable record. No bad actor can engage in nefarious activities because such activities will be evident on the ledger or corrected by a peer-to-peer consensus network. To compromise the network, hackers would need to successfully hack most of the blocks (files with transaction records) before new blocks were introduced. The blockchains audit trail ensures that no vote has been changed or removed and that no fraudulent and illegitimate votes have been added. Put simply, blockchains enable the creation of tamper-proof audit trails for voting. In this article, we highlight some BEV implementations and the approachs potential benefits and challenges.

Chapter 3

Blockchain

3.1 What is blockchain

By definition, blockchain is a shared, trusted, digital transaction ledger of cryptographically secured time-stamped records that everyone can inspect, but no single user controls.Blockchain is a peer-to-peer, distributed ledger that is cryptographically-secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.

It is just like what the name says: a chain of blocks. Each block contains the data of all transactions in the system within a period of time, and it could create digital fmgerprinting which can be used to verify the validity of the infonnation and connect with the next block. There can be a huge number of such blocks in the blockchain. The blocks are linked to each other in a linear (like a chain), chronological order with every block containing a hash of the previous block.

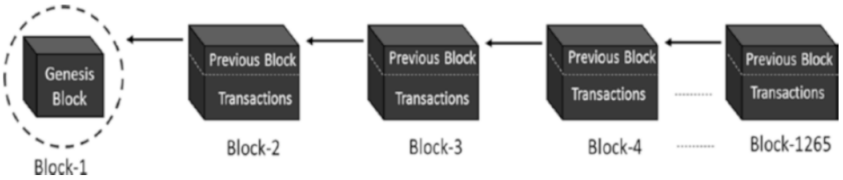

Figure 3.1: The blockchain datastructure

3.1.1 Features of blockchain

According to the definition of the blockchain above, a blockchain-based system should have several features: decentralized, trustless, collectively, reliable database and anonymity. Decentralized: there is no organization in the whole network, and even if a node is crashed, the whole system will still be up. Therefore, the blockchain system is very robust. Trustless: since the whole system is running transparently, the system is absolutely open source and there is no need for trust among every single node and any node can never cheat other nodes. Collectively Maintain: the blocks of the system are maintained by all the nodes in the whole system, and everyone can become one node of the system after registering online. Reliable Database: every node could receive a complete copy of the database from the system through the form of subdatabase. Tampering with the database by one node is invalid, and that could not influence the data of other nodes, unless one can control over 51% of the nodes in the whole system at the same time. Thus, if there are more nodes in the system, it will be more secure. Anonymity: since there is no need for trust between nodes, there is no need for nodes to reveal their identities and all the nodes in the system are anonymous.

The core problem solved by blockchain technology is how we can build a consensus foundation for secure information transaction without worrying about data tampered when any nodes can not be trusted in the whole network. Blockchain could guarantee the security of the whole network by using mathematical algorithm mechanism.

3.1.2 How blockchain accumulates blocks

Now we will look at a general scheme for creating blocks. This scheme is presented here to give you a general idea of how blocks are generated and what the relationship is between transactions and blocks. A distributed ledger is stored in a database and updated by each participant in the blockchain network. A ledger is represented in a series of units called blocks.

The blockchain network consists of a network of several independent machines named nodes.Unlike traditional databases that store entire information on a centralized database server, Blockchain nodes keep the copy of the entire database with an administrative role. Even if one node goes down, the information will remain available for the nodes.Refer figure 3.2.

- Version: It's a 4-byte field that's used to track software or protocol grades.

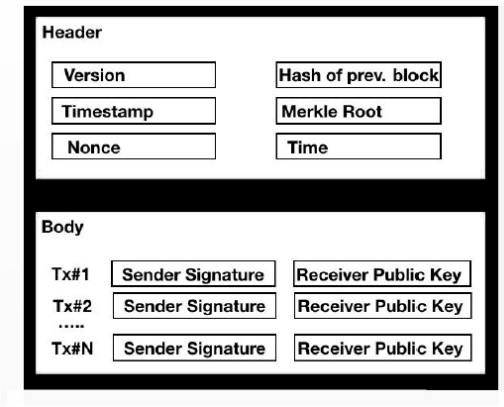

Figure 3.2: Block Structure

- Timestamp: This is a 4-byte field that indicates the creation time of the block in seconds.
- Hash of the previous block: This is a 32-byte field that indicates the hash of the previous block in the chain.
- Nonce: This is a 4-byte field that's used to track the PoW algorithm counter.
- Hash of Merkle root: This is a 32-byte field that is a hash of the root of the Merkle tree of the block transaction.
- Block body: This part of the block consists of a list of transactions.

3.1.3 Cryptography digital signature and hashing algorithm

Cryptographic hashing is a way to generate a fixed-length output against any given length of input string. The output is named hash or message digest, and is designed to protect the integrity of any kind of data, such as a file, media, or text. Only one message digest is assigned to protect a specific input or sensitive information. A small change made to the input data results in a drastic difference in the result, which makes it almost impossible to predict the data either inmotion or even at-rest. There are various ways to produce the hash or the message digest. In the world of cryptocurrency,a popular one, the SHA-265 algorithm is used to produce a fixed-length 256 bit hash or message digest against each block.

In the world of blockchain, hashing is the backbone of its immutability characteristic. The hashing process ensures that none of the blocks in the ledger are altered or tampered with.Instead

of keeping track of each transaction's details blockchain and nodes just have to remember and keep a track of its respective hash.

Let's understand how the blockchain makes use of the hashing algorithm. In blockchain, a node arranges the entire ledger in the form of chronologically connected blocks. To ensure that the ledger remains tamper-proof, each block is made dependable on the previous block. In other words, a new block can't be produced without having the hash of a previous block. Before adding a new block in the ledger, this has to be approved and verified by every node in the blockchain. This allows anyone to tamper or alter the ledger except in the case of a hacker, who is capable enough of infecting and compromising all of the millions of nodes in the blockchain at the same time. Only the first block called the genesis block is produced itself and points to itself.Every block points to the hash of previous hash block, and this becomes the backbone of the blockchain's immutable system.To avoid complex work to find one transaction, a comprehensive hash tree has been developed named the Merkle tree.

3.1.4 Working of blockchain

Now let's see how a blockchain actually works. Nodes are either miners who create new blocks and mint cryptocurrency (coins) or block signers who validates and digitally sign the transactions. A critical decision that every blockchain network has to make is to figure out that which node will append the next block to the blockchain. This decision is made using a consensus mechanism.

This scheme is presented here to give you a general idea of how blocks are generated and what the relationship is between transactions and blocks.A block is merely a selection of transactions bundled together and organized logically.Figure 3.2 show the generic structure of a block.A block is made up of transactions, and its size varies depending on the type and design of the blockchain in use.A reference to a previous block is also included in the block unless it is a genesis block. A genesis block is the first block in the blockchain that is hardcoded at the time the blockchain was first started. The structure of a block is also dependent on the type and design of a blockchain.Generally, however, there are just a few attributes that are essential to the functionality of a block: the block header, which is composed of pointer to previous block, the timestamp, nonce, Merkle root, and the block body that contains transactions.Refer figure 3.3.

When a new transaction is happen then the following operations will performed.

- New transactions are broadcast to all nodes.

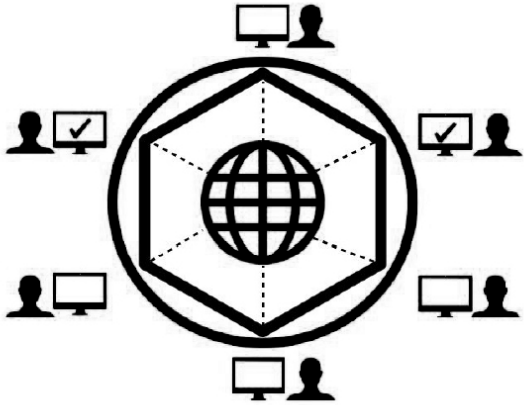

Figure 3.3: Peer to Peer Blockchain Network

- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work for its block.
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
- Nodes accept the block only if all transactions in it are valid and not already spent.
- Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

3.2 Smart Contract

A computer program that directly controls the transfer of digital currencies or assets between parties under certain conditions.These are automated, autonomous programs that reside on the blockchain network and encapsulate the business logic and code needed to execute a required function when certain conditions are met.This is indeed a revolutionary feature of blockchain, as it provides flexibility, speed, security, and automation for real-world scenarios that can lead to a completely trustworthy system with significant cost reductions. Smart contracts can be programmed to perform any actions that blockchain users need and according to their specific business requirements.

Consider the example,think about an insurance contract where a claim is paid to the traveler if the flight is canceled. In the real world, this process normally takes a significant amount of time to make the claim, verify it, and pay the insurance amount to the claimant (traveler). What

if this whole process were automated with cryptographically-enforced trust, transparency, and execution so that as soon as the smart contract received a feed that the flight in question has been canceled, it automatically triggers the insurance payment to the claimant? If the flight is on time, the smart contract pays itself.

3.3 Consensus

A blockchain is a decentralized peer-to-peer system with no central authority figure. While this creates a system that is devoid of corruption from a single source, it still creates a major problem.How are any decisions made?How does anything get done? In normal centralized organization, All the decisions are taken by the leader or a board of decision makers. This isnt possible in a blockchain because a blockchain has no leader. For the blockchain to make decisions, they need to come to a consensus using consensus mechanisms.

Consensus decision-making is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole. Consensus may be defined professionally as an acceptable resolution, one that can be supported, even if not the favourite of each individual. Consensus is defined by Merriam-Webster as, first, general agreement, and second, group solidarity of belief or sentiment. In simpler terms, consensus is a dynamic way of reaching agreement in a group. While voting just settles for a majority rule without any thought for the feelings and well-being of the minority, a consensus on the other hand makes sure that an agreement is reached which could benefit the entire group as a whole. From a more idealistic point-of-view, Consensus can be used by a group of people scattered around the world to create a more equal and fair society. A method by which consensus decision-making is achieved is called consensus mechanism. The objectives of a consensus mechanism are:

- Agreement Seeking: A consensus mechanism should bring about as much agreement from the group as possible.
- Collaborative: All the participants should aim to work together to achieve a result that puts the best interest of the group first.
- Cooperative: All the participants shouldnt put their own interests first and work as a team more than individuals.

- Egalitarian: A group trying to achieve consensus should be as egalitarian as possible.
- Inclusive: As many people as possible should be involved in the consensus process.
- Participatory: The consensus mechanism should be such that everyone should actively participate in the the overall process.

3.4 Proof of Work

A certain work is done for a block of transactions before it gets proposed to the whole network. A PoW is actually a piece of data that is difficult to produce in terms of computation and time, but easy to verify. One of the old usages of PoW was to prevent email spams. If a certain amount of work is to be done before one can send an email, then spamming a lot of people would require a lot of computation to be performed. This can help prevent email spams. Similarly, in blockchain as well, if some amount of compute-intensive work is to be performed before producing a block, then it can help in two ways: one is that it will definitely take some time and the second is, if a node is trying to inject a fraudulent transaction in a block, then rejection of that block by the rest of the nodes will be very costly for the one proposing the block. Refer figure 3.4.

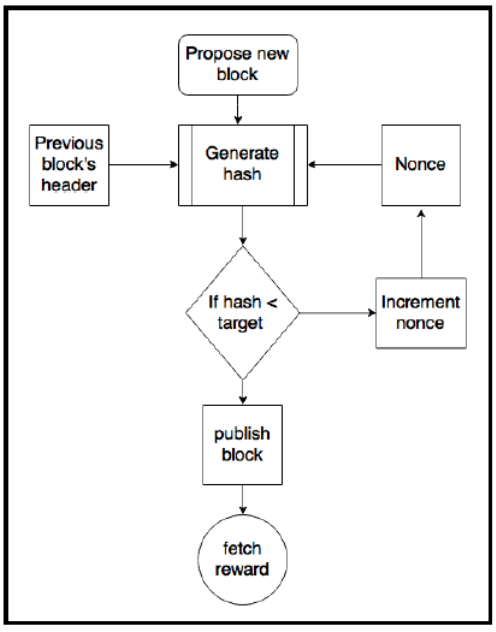

Figure 3.4: Mining process

Chapter 4

Blockchain and Voting

4.1 Implementing E voting using blockchain

It is argued that blockchains might address two of the most prevalent concerns in voting today: voter access and voter fraud. The idea is as follows. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV employs an encrypted key and tamper- proof personal IDs. For example, the mobile e-voting platform of the Boston-based startup Voatz employs smart biometrics and real-time ID verification. The public ledger ties each cast ballot to an individual voter and establishes a permanent, immutable record. No bad actor can engage in nefarious activities because such activities will be evident on the ledger or corrected by a peer-to-peer consensus network. To compromise the network, hackers would need to successfully hack most of the blocks (files with transaction records) before new blocks were introduced. The blockchains audit trail ensures that no vote has been changed or removed and that no fraudulent and illegitimate votes have been added.4 Put simply, blockchains enable the creation of tamper-proof audit trails for voting. In this article, we highlight some BEV implementations and the approachs potential benefits and challenges

4.1.1 Recent Implementations

Initial operational applications of BEV have been for informal, nonbinding, and consultative voting. For example, in early 2018, Voatz tested its mobile-phone-based system during events such as student government elections; church-group, nonprofitorganization, and union voting, and subnational political-party events. The system has also been used in town meetings in

Massachusetts.Blockchainbased solutions have been deployed for corporate, community, city, and national voting. For example, in Russia, the city of Moscows Active Citizen program was launched in 2014 and has more than two million users. Each year, Moscow neighborhoods hold up to 5,000 to 7,000 meetings. As of February 2018, 3,450 polls had been conducted using a centralized Oracle database, with 92 million votes cast on diverse subjects such as what color the seats in a new sports arena should be, whether to install driveway access gates in neighborhood yards, and whether to hire a new doorkeeper.10 Although these examples dont deal with political offices, blockchains could be tailored for that purpose. Furthermore, many Moscow residents dont have time to attend face-to-face meetings. So, meetings have moved to the Digital Home online platform. In December 2017, residents began using a blockchain to vote, and the results were publicly auditable. City officials believed that neighbors should have a convenient environment in which to influence their living conditions. The officials also believed that a blockchain would increase trust between citizens and government.12 Each question discussed by the community is moved to BEV. After the polling is finished, the results are provided.

In March 2017, the South Korean province of Gyeonggi-do employed a BEV system to vote on the Ddabok Community Support Project. Nine- thousand residents voted using a blockchain platform developed by the Korean financial-technology startup Block that included smart contracts. The votes, results, and other relevant data were stored in a blockchain. No management or central authority was involved in this process. This was the first time South Korea applied such a technology. Shareholders of the Estonian technology company LVH Group who are Estonian citizens or Estonian e-residents can now use BEV to make corporate-governance-related decisions. They can log in using their verified national online ID and vote at LVHs annual general meeting. Estonias e-residency platform authenticates e-resident shareholders. Estonia plans to adopt blockchains in a range of areas such as an e-residency project (which allows foreign citizens to establish a business within Estonian jurisdiction) and healthcare (securing health data storage and allowing real-time monitoring of patient conditions).

In Sierra Leones March 2018 general elections, Swiss blockchain startup Agora provided a partial tally of election results.11 Agora was one of the accredited observers that provided an independent count for comparison. Agora described Sierra Leones elections as a use case rather than a full implementation of BEV.18 Finally, Nasdaq has built and operated four web-based user interfaces for BEV.15 A BEV system issues voting-right assets and voting-token assets for each shareholder in a company. A user can spend voting tokens to cast votes on each meeting

agenda item if that user owns the related voting-right asset.

4.2 Main Platforms

4.2.1 Hyperledger

Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing, and Technology. Hyperledger does not support Bitcoin or any other cryptocurrency. But the platform is thrilled by blockchain technology. Not since the Web itself, the website tells, has a technology promised broader and more fundamental revolution than blockchain technology. Blockchains has the potential to build a new generation of transactional applications that establishes trust, accountability, and transparency at their core while streamlining business processes and legal constraints.

The umbrella strategy of Hyperledger incubates and promotes a range of business blockchain technologies, framework, libraries, interfaces, and application. Currently, Hyperledger is the host of the following projects:

Hyperledger Sawtooth: This is a modular blockchain suite developed by Intel, which uses a new consensus algorithm called Proof of Elapsed Time (PoeT).

Hyperledger Iroha: Iroha is a project of a couple of Japanese companies to create an easy to incorporate the framework for a blockchain.

Hyperledger Fabric: This project is lead by IBM. Fabric is a plug and plays implementation of blockchain technology designed as a foundation to develop high-scaling blockchain applications with a flexible degree of permissions.

Hyperledger Burrow: This project develops a permissible smart contract machine along the specification of Ethereum.

4.2.2 Ethereum

At its simplest, Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications. Like Bitcoin, Ethereum is a distributed public blockchain network. Although there are some significant technical differences between the two, the most important distinction to note is that Bitcoin and Ethereum differ

substantially in purpose and capability. Bitcoin offers one particular application of blockchain technology, a peer to peer electronic cash system that enables online Bitcoin payments. While the Bitcoin blockchain is used to track ownership of digital currency (bitcoins), the Ethereum blockchain focuses on running the programming code of any decentralized application. In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn Ether, a type of crypto token that fuels the network. Beyond a tradeable cryptocurrency, Ether is also used by application developers to pay for transaction fees and services on the Ethereum network.

There is a second type of token that is used to pay miners fees for including transactions in their block, it is called gas, and every smart contract execution requires a certain amount of gas to be sent along with it to entice miners to put it in the blockchain.

Ethereums core innovation, the Ethereum Virtual Machine (EVM) is a Turing complete software that runs on the Ethereum network. It enables anyone to run any program, regardless of the programming language given enough time and memory. The Ethereum Virtual Machine makes the process of creating blockchain applications much easier and efficient than ever before. Instead of having to build an entirely original blockchain for each new application, Ethereum enables the development of potentially thousands of different applications all on one platform.

4.2.3 What to use and how ?

We could use both the available platforms to develop a voting system. Many institutions would love to have some control over the election process and they might opt for the permissioned blockchain, Hyperledger. Ethereum can also be used by implememting a token based mechanism for voting.

In voting, we don't implement cryptocurrencies, hence we use a token mechanism or a simple flag system which would enable voters to cast only one vote. There is an admin(the election official) who would initiate the process and publish the result. Candidate registration is also done by this admin. The voter registration is needed but it is also possible to convert the existing database into a blockchain database inthe future.

For beter security, we can employ the use of secure biometric information for authorisation so that we can ensure two way identity checking to prevent fraudulent voters.

Chapter 5

Conclusion and Future scope

The future scope of blockchain enabled E-voting is extensive. The Blockchain voting system can be expanded to make Any Time Voting systems whoucl would alow users to cast their votes using just their mobile devices. An Adhaar model blockchain database could be created with all the personal details of a citizen, thereby making nancial transactions easy and traceable. It will also make the scrutiny of candidate nomination simple. Administrative level implementation of the blockchain would make the functioning of the governments more transparent than ever before. Any Time Voting has the potential to disrupt the whole election process and it would be challenging to implement as it could be difcult to win the condence of the authorities and general public.

In future studies, with the rapid development of blockchain, building a decentralized system in which the information can be completely trusted would be the development tendency of most of the government organizations and election comes first here. There is no doubt that with the wide application of these emerging technologies, election can be carried out seamlessly in a secure and hassle free manner. Even though it raises concern for a section of people, yet it holds the promise of making elections more transparent, secure and would encourage people to exercise their voting right

Bibliography

[1] Sachchidanand Singh and Nirmala Sing, *"Blockchain: Future of Financial and Cyber Security"*, IBM Software Lab Pune, India - 411 057 Email: sach.success@gmail.com, , Tech Mahindra, Pune, India Email: nirmala.online@gmail.com

[2] Nir Kshetri and and Jeffrey Voas, *" Blockchain-Enabled E-Voting"*, University of North Carolina at Greensboro. nbkshetr@uncg.edu, co-founder of Cigital, IEEE Fellow. j.voas@ieee.org.

[3] Satoshi Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System"*,satoshin@gmx.com, www.bitcoin.org