# BLOCKCHAIN BASED E-VOTING USING SMART CONTRACT

## THESIS

## SUBMITTED BY-

| NAME | ID |
|---|---|
| Islam, Tasnova | 15-29417-1 |
| Naim, S.M. Golam Rabbani | 15-29456-1 |
| Paul, Rajib Kumar | 15-30537-3 |
| Sadia, Kazi | 16-31064-1 |

DEPARTMENT OF COMPUTER SCIENCE

FACULTY OF SCIENCE & IT

**AMERICAN INTERNATIONAL UNIVERSITY-BANGLADESH**

DECEMBER 19, 2018

# Declaration

We declare that this thesis is our original work and has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of reference is given.

**Islam, Tasnova**
**15-29417-1**
**Computer Science and Engineering**
**American International University-Bangladesh**

**Naim S.M. Golam Rabbani**
**15-29456-1**
**Computer Science and Engineering**
**American International University-Bangladesh**

**Paul, Rajib Kumar**
**15-30537-3**
**Computer Science and Engineering**
**American International University-Bangladesh**

**Sadia, Kazi**
**16-31064-1**
**Computer Science and Software Engineering**
**American International University-Bangladesh**

# Approval

The thesis titled **"BLOCKCHAIN BASED E-VOTING USING SMART CONTRACT"** has been submitted to the following respected members of the board of examiners of the department of Computer Science in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science on 19th December, 2018 and has been accepted as satisfactory.

**Md. Masuduzzaman**
**Lecturer & Supervisor**
**Department of Computer Science**
**American International University-Bangladesh**

**Md. Al-Amin**
**Lecturer & External**
**Department of Computer Science**
**American International University-Bangladesh**

**Dr. M M Mahbubul Syed**
**Associate Professor & Head**
**Department of Computer Science**
**American International University-Bangladesh**

**Professor Dr. Tafazzal Hossain**
**Dean**
**Faculty of Science & Information Technology**
**American International University-Bangladesh**

**Dr. Carmen Z. Lamagna**
**Vice Chancellor**
**American International University-Bangladesh**

# Acknowledgement

First of all, we would thank almighty God for his grace in completing our thesis successfully on time. We would like to express our cordial thanks to the Faculty of Science & Information Technology to keep thesis/project credit in the curriculum of the graduation program and give us a scope of gathering knowledge.

We are also thankful to our honorable Thesis Supervisor **MD. MASUDUZZAMAN**, from the core of our heart for his kind support, guidance, constructive, supervision, instructions, advice and for motivating us to complete this thesis.

Furthermore, we would like to show our grateful feeling to all of our teachers, who once taught us and was our course coordinator. They are always patient to help us out with any regarding our thesis.

# Abstract

A protocol that proposes a fully decentralization e-voting system based on the blockchain technology and using smart contract. This protocol integrates the blockchain paradigm and notion of the smart contract into the e-voting system to deal with security issues, accuracy and voters' participation during the vote. The protocol results in a transparent, non-editable and independently verifiable procedure that discards all the intended fraudulent activities occurring during the election process by removing the least participation of third party.

# Table of Contents

# List of Tables and Figures

# Chapter-01: Introduction

## 1.0 Introduction:

Blockchain are incredibly popular now-a-days. So what is Block chain?

## 1.1 Blockchain:

A Blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Like the name in the case A Blockchain is a chain of blocks, they contains information. This technique originally described in 1991 by a group of researcher. Blockchain is shorthand for a whole suite of distributed ledger technologies that can be programmed to record and track anything of value from Financial Transaction to Medical Records or even Land Titles. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. A Blockchain is a distributed ledger that is completely open to anyone. They have interesting property. Once some data has been inserted inside a blockchain it become very difficult to change it. [1]

Blockchain technology uses cryptography and a solidarity mechanism to verify transactions, which ensures the legitimacy of a transaction, prevents double-spending. A blockchain offers transparency and elects the need for middleman or third-party administrators.

Blockchain is a type of technology, not a single network. It can be implemented in many different ways Example:

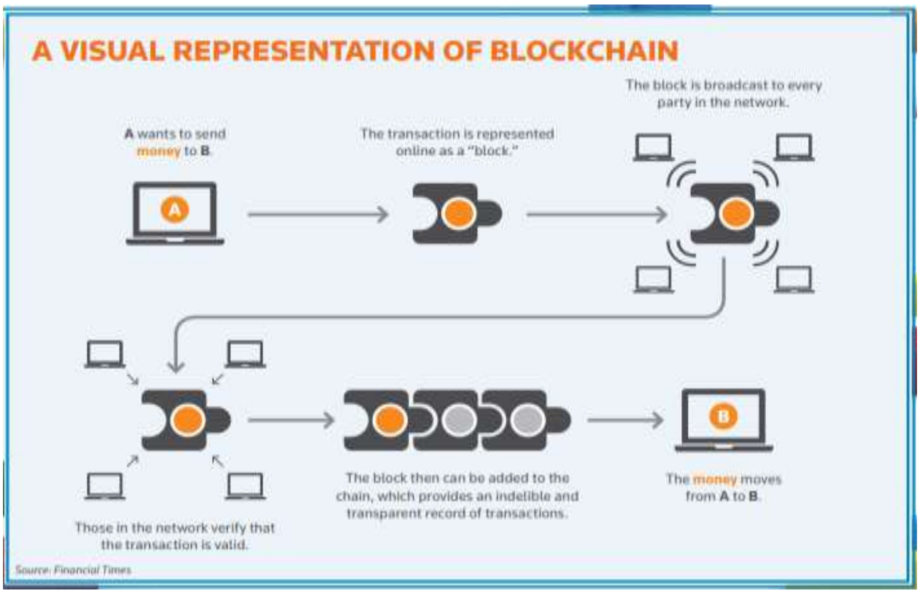

A VISUAL REPRESENTATION OF BLOCKCHAIN
A wants to send money to B.
A
The transaction is represented online as a "block."
The block is broadcast to every party in the network.
Those in the network verify that the transaction is valid.
The block then can be added to the chain, which provides an indelible and transparent record of transactions.
B
The money moves from A to B.
Source: Financial Times

**Figure: 1.1.a: Example of Blockchain Technology.**

Blockchain creates trust in the data. Let's assume A wants to send money to B. The transaction is represented online as a block. Once 'A' does the transfer, the transaction messages send to the network and passed around all the network participants which are also called nodes. In short the block is broadcast to every party in the network. Currently the transaction is in an unconfirmed state. Before a block can be added to the chain, a few things have to happen. A cryptographic puzzle must be solved thus creating the block. The computer that solves the puzzle shares the solution to all the other computer on the network. This is called proof-of-work. The network verifies the proof-of- work. If correct, the new block will be added to the chain. The combination of these complex math puzzles and verification by each and every nodes in the network ensures that can trust each and every block of the chain. Now 'A' has the opportunity to interact directly with her data and transact the money to 'B'.

## 1.2 E-voting:

In every democracy, the main important thing is to secure the election process for the national security. After studying the possibilities of electronic voting systems for a decade [2], the computer security field had a goal to minimize the cost of election as well as to emphasize more on the security conditions of an election. Ever since the candidates were needed to be elected through a democratic process, it was done by voting with pen and paper. Now replacing the vintage process of electing with pen and paper by a new innovative process might be condemnatory in stopping any sort of duplicity and imposture which is traceable and consequent [3].

By electro voting we generally mean the vote casting process with the help of any sort of computers or computerized voting equipment. Even with the use of internet we can be able to do this. Registering the voters, tally ballots and recording of votes can also be easily done by this electronic system [4].

Electro voting machine neither a complex machine nor harder to operate. It can be easily understand and operated by both election officer and the voters. EVPM has basically two units- Control Units and Ballot units. The main unit of EVPM is control unit which stores all the data and controls the basic function. Electro voting machine use dynamic coding to ensure the security of the data transmission from ballot unit to control unit [5].

## 1.3 Smart Contract:

In a localized environment the smart contracts executes, which are traceable and unalterable. For the better administration for realizing and executing digital agreements the smart contracts are helpful as it is self-confirming and self-executing [6].

The terms smart contract are first used by Nick Szabo in 1997, a long before bitcoin is created. In simple words he wanted to use a distributed ledger to store contracts. Smart contracts are just like contracts in real world. The only difference is they are totally digital. In fact a smart contract is actually a tiny computer program that is stored inside a blockchain. There are blockchain who support smart contracts. But the biggest one is Etherium. It was specifically created and designed to support smart contracts. Smart contract can be programmed and special programing language called Solidity. This language was created for Ethereum.

Smart contract is a legal application that runs on a blockchain network. Smart contracts are much like legal contract. Since smart contracts runs in the blockchain they are unstoppable. Making them ideal for financial applications. Smart contract can be used in many different things. Banks for example could use it to issue loan, worth for automatic payments. Insurance company could use it for process claims, postal company use it for payment on delivery and so on.

**Figure: 1.3.a: Example of Smart Contract.**

Smart Contract is like this:

- No trust issue in smart contract just like this vendor machine. A person itself can put the coin into this and get the desired product.
- No involvement of third party. The same as this vendor machine. When a person itself involved with this matter can directly interact with it and get the desire product. And there is not any involvement of third-party.
- As the smart contract is distributed in open ledger. There is no chance of lose or hacking of smart contract.

The e-voting system has been implemented as a system which is based on a smart contract in a approved block chain. In the block chain all the ballot smart contracts which represents the voting districts of the election administrators are set up. Each of the expected district nodes can collaborate with the appropriate ballot smart contract after the ballot smart contracts has been designed. With all the district nodes the vote data of all the individual voter casts are verifiable.

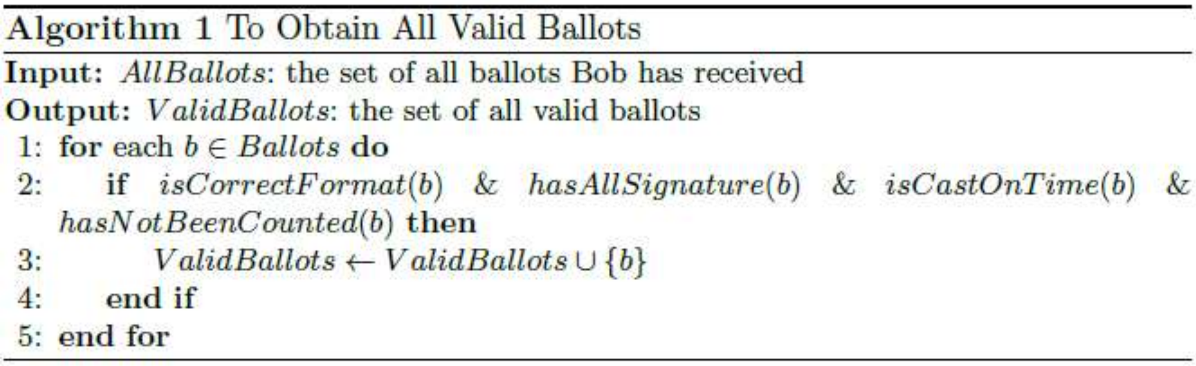
# Chapter-02: Literature Review

## 2.0 Literature Review:

In this section, we discuss the basic concept of Blockchain technology, E-voting, E-voting with Blockchain technology. Also we will discuss about the existing research of E-voting with Blockchain Technology.

A Blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among all the peer nodes. Each transaction in the public ledger is verified by consensus of a majority of the system. Once entered, information can never be erased [1]. On the other hand E-voting is when a voter cast a ballot through a digital system instead of paper ballots. It is a simple electronic device to record votes for all voters [5]. With the combination of both different author try to implement different kind of system. Blockchain technology with E-voting system is not a new thing. Many scheme have been proposed.

As we know Blockchain is decentralized open ledger system so the voting process was transparent in E-voting. And voters identity was hidden for security purpose because all the people of any particular country is involve in this system so there is a chance of life risk. Anonymity was ensured by keeping voters identity private. As Blockchain is a transparent system, the whole procedure is open to the public as a result procedure will be more fairness and validity [7]. According to E-voting protocol to provide pledge that only eligible voters are able to vote, they reckon Central Authority (CA) to be introduced for a user to be judge eligible. One must authenticate oneself to the Central Authority and also CA receives a token that proves one's eligibility to vote. The eligibility token takes the form of a digital signature over a voter [8]. Voting was divided into three phases. There are Pre-voting phase, Voting Phase, Post Voting Phase. In the Pre- voting phase the organizer Bob required to collect all valid ballots. After ending the voting time, Bob generates a set AllBallots which means that all the ballots he has received. Then Bob runs this algorithm 1 [7]:



```
Algorithm 1 To Obtain All Valid Ballots
Input: $AllBallots$: the set of all ballots Bob has received
Output: $ValidBallots$: the set of all valid ballots
for each $b \in Ballots$ do
    if $isCorrectFormat(b)$ & $hasAllSignature(b)$ & $isCastOnTime(b)$ & $hasNotBeenCounted(b)$ then
        $ValidBallots \leftarrow ValidBallots \cup \{b\}$
    end if
end for
```

This algorithm runs to gain set of ValidBallots which is set of all the valid ballots. The verification can be done by all participants, and those who have the permission to see the Blockchain. Each node will be a participating in Blockchain thus every single node represents a voter. After successful verification by all the participants, voters will added into the Blockchain. According to [9] each single block called a unique voter and all the block or node is connected with each other [7] [8].

In voting phase, for ballot preparation a correct message is formulated with voting string to keep the choice of nominee hidden to avoid expose of election progress [7].

$$\overbrace{\underbrace{\text{Choice Code}}_{x}\underbrace{0000\cdots0000}_{y}\underbrace{\text{Random String}}_{z}}^{n}.$$

Here, n = length of voter string. It varies depending on specific elections. The first x bits are the choice code, which represents the voter’s choice. Y-bit is zero-string, which is an indication of a well-formed vote. The last part is a Z-bit random string, which distinguishes different votes counting the same choice code. This voting string is needed to avoid expose of election progress. The voting time will begin and end simultaneously. When voting time was ended, each node will wait its turn to create block. The system will then broadcast the database followed by the ID of given node. Then checks whether the broadcast ID belongs to it, if yes then creates a new block and verification process is done [10].

In the genesis block of the Blockchain is used as an initial storage [11]. Where all the voters’ information as well as candidates or nominees which is selected by the election commission office is stored in this block [8]. The authors revealed the result at the end of election using the concept of value representation of the voter choice. A voter can vote multiple time and can also select multiple nominee [7] [8]. Before finishing the election time, last vote consider as a valid vote. By this process coercion will be totally removed. For the privacy of a voter, smart contract idea is introduced. In every pen and paper election scheme, voter’s privacy is very important. The law forbits any individual or entity can be able to from a single vote who gave aforementioned vote. If such information could be gathered for each vote, that particular information could be leak to the public which would allow for listing every single individual who voted for a single candidate/nominee. To satisfy this privacy of each voters no individual vote should be traceable back to voter [12]. Anyone can view the public Blockchain and there is no centralized authority. After successful voting, all the voters is added into the Blockchain. All the nodes/voters will connected to each other. Everyone can see which particular voter is voted on which candidate [9].

Blocks can remain un-broadcasted for a time being and that specific one can be broadcast again. That means block can remain private for security purpose. An organizer is needed to broadcast that private block [1].

E-voting means when voter casts a ballot through a digital system instead of paper. In Blockchain technology all the process or transaction is transparent and also much more secure system instead of any trusted third party so by the combination of that technology is better for E-voting. For that many authors try to implement this system in a secure way to remove vulnerability of E-voting system.

Initially in the genesis block all the candidate information and voters' information are stored. Central Authority or Organizer was introduced as trusted third party for process monitoring. For ballot preparation with the combine string choice code, zero string and random string, creates a voting string for avoiding expose of election progress. There is a choice of multiple voting in order to prevent coercion. After successful voting each node will be onto the Blockchain. Each single node represents a single voter. Each voter can his/her vote to know whether his/her vote is accepted or not. Authors will revealed the result at the end of election time. Block can remain private for security reason. By this related work E-voting system is more stable than before.

# Chapter-03: Problem Identification

## 3.0 Problem Identification:

- Transparency and coercion prevention cannot be obtained at the same time.
- Central Authority (CA) or Organizer which acts as a trusted third party.
- Improper involvement of voters in calculating result.
- Time consumption of Blind signature method.

Using the Blockchain technology E-voting is transparent means voter can see each other information. On the other hand to remove coercion multiple times of voting approach had been taken which is not a stable system. None of any authors can fix this two portion at the same time. So some lacking must remain of their existing methodology. Central Authority (CA) or Organizer is performing as a trusted third party which is not trusted. This Organizer is involved in making genesis block as well as verification of voters and counting process. So there is chance for corruption. So security could not perform well on the existing system. Voters cannot involve in counting the voting result so CA is involve to complete that procedure. Which is less secure in existing system. One of the author is implemented Blind signature algorithm to perform avoid any party being able to identify how to voter voted [8]. This algorithm removes CA but still its time consuming. In Blockchain Based E-voting these major problem is identified. To remove those problems a methodology is introduced in the proposed methodology section.

# Chapter-04: Proposed Methodology

## 4.1 Procedure:

The basic functionalities of the proposed protocol are illustrated accordingly in **Figure: 4.1. a.** The code is executed on the top of the blockchain therefore verifying actions that was supposed to be performed by the third party. Moreover, the peer network connected are in charge of further verification as mentioned. The figure introduces some unknown terms that are further described below.

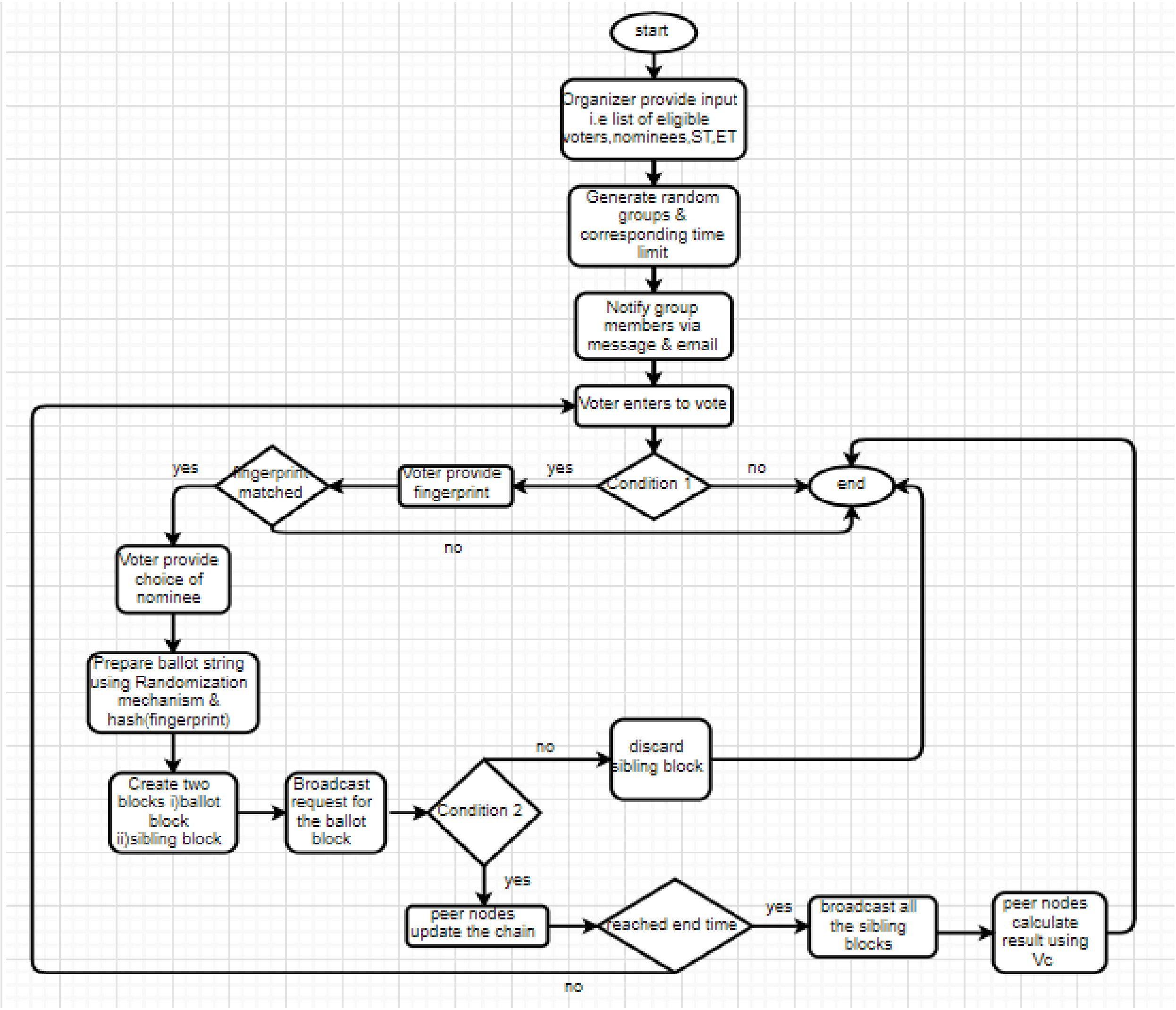

start
Organizer provide input i.e list of eligible voters,nominees,ST,ET
Generate random groups & corresponding time limit
Notify group members via message & email
Voter enters to vote
Condition 1
no
end
yes
Voter provide fingerprint
fingerprint matched
yes
no
Voter provide choice of nominee
Prepare ballot string using Randomization mechanism & hash(fingerprint)
Create two blocks i)ballot block ii)sibling block
Broadcast request for the ballot block
Condition 2
no
discard sibling block
yes
peer nodes update the chain
reached end time
yes
broadcast all the sibling blocks
peer nodes calculate result using Vc
no

**Figure: 4.1.a: Flowchart representation of the basic functionalities of the protocol.**

Condition 1-Verify whether the voter is in the group X and the flag of X is true (flag true → X is currently specified for voting). Also, check whether the voter is in the eligibility list or not.

**Condition 2-** Mathematical computation (proof of work) is done. Also, verify whether the voter has casted vote previously or not and check the ballot is in correct format or not.

**Organizer→** In this protocol, organizer is the only representative who is involved within the protocol but for a limited time. The role of the organizer is to arrange and collect the list of nominees, list of eligible voters, start date and time, end date and time. The start and end (date and time) are decided and announced by the election commission. The list of eligible voters is collected through manual registration.

**Ballot string→** The string that contains the choice of nominee hidden around random numbers to avoid recognition.

**Sibling block→** A block that contains the arrangement of choice value.

st→ ST→start time
et→ ET→end time
hash (fingerprint) →hash function used on the binary value of the voter's fingerprint

NOTE: Choice of nominee is hidden in the ballot string. The arrangement of the choice is hidden in the variable $V_c$, the arrangement is prepared by random number generation. Thus, nobody has any idea of the user's choice until the end of the election.

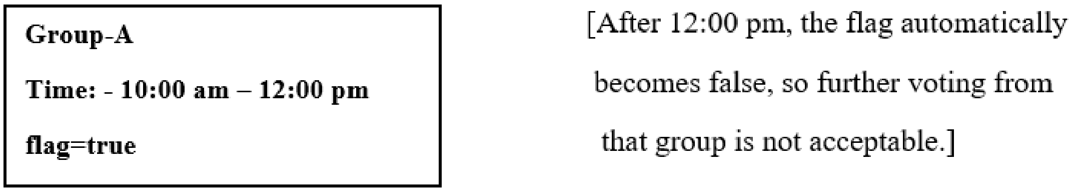
## 4.1.1 The phases of the proposed protocol

The protocol is categorized into three phases, in which each phase is dependent upon another. Following are the three phases:

I. Pre-voting phase.
II. Voting phase.
III. Post voting phase.

### 4.1.1.1 Pre-voting Phase:

The organizer is the actor responsible for collecting the list of the eligible voters and nominee based on the desired condition (if any). The list of the voters should contain voter's name, national identification number (NID), fingerprint and any other information based on the direction of the election commission. Organizer provides the list of eligible voters, their fingerprint coordinates along with the binary value, nominees, start date-time and end date-time as an input on the genesis block. Genesis block is the parent block or the first block of the blockchain. The start date-time and end date-time is mentioned earlier by the election commission. The role of the organizer ends here; as per the result of the code execution, the procedure is carried out. The program (code) is previously integrated within the blockchain. On reaching the start date-time, one of the pre-defined condition fulfills i.e. {if(DateTime.Now==st) start ();}; function is called which invokes the election procedure to start and corresponding activities are performed. Voters are grouped randomly based on the number of eligible voters and any other condition provided, and random time is generated for each groups. Each group will have distinct timing; no overlapping is taken in consideration. Voters of specific groups are notified via email and message; a time limit is set for each group.



**Group-A**
**Time: - 10:00 am – 12:00 pm**
**flag=true**

[After 12:00 pm, the flag automatically becomes false, so further voting from that group is not acceptable.]

The flag is a boolean property of a group. The flag remains true till the time limit of the group. The duration of each group is also decided by the election authority. The voting duration for each group must be adjusted in such a way that none of the voters skip to vote due to load/traffic on the network at that instant. The code works upon that to generate different timing for each group. No one is allowed to vote after the flag becomes false i.e. the time limit exceeds. The flag becomes false automatically once all the voters within the group are done with their voting (this provides further security).

### 4.1.1.2 <u>Voting Phase:</u>

**Public keys→NID & Name**
**Private key→fingerprint**

As the voter approaches to vote providing his/her public keys, it is verified (within the code) whether the voter is in the group with a flag value of true and whether the voter is in the eligibility list. As smart contract performs an executable code, it is verified through the code by the call of a function that checks whether the voter entered is eligible or not. Given that, the eligibility lists of the voters are stored on the genesis block. As the voter has proved him/her as eligible and also the voter is in the specified group (the group to serve currently), the voter is then to provide his/her private key (fingerprint) as a need of verification that no other people except the voter is casting his/her vote (this reduces the chance of anyone knowing one's public keys and using the public key to cast vote in the name of the voter, stealing votes). This is the second phase of verification of voters. The fingerprint is matched with the one provided along with the eligibility list. The fingerprint sensor is used to figure out the coordinates of particular voters, the coordinates are then matched with the coordinates provided in the genesis block, if it matches then according to the **Figure: 4.1. b**, the binary value of the coordinates is obtained from the provided list in the genesis block. Conversion of the coordinates into the binary value during the voting process will require time and memory consumption, thus this procedure is performed. The hash of the binary value is basically the unique voter identification in the ballot within the block. Direct voter's identity is avoided to ensure voters security. The hash (fingerprint_binary) value is the representation of the voter in the block. SHA-256 is used as the secured hash function, hash (fingerprint_binary) that cannot be reversed. According to some research, fingerprint is one of the most secure metadata of a person, thus fingerprint is used instead of any other metadata in this protocol.

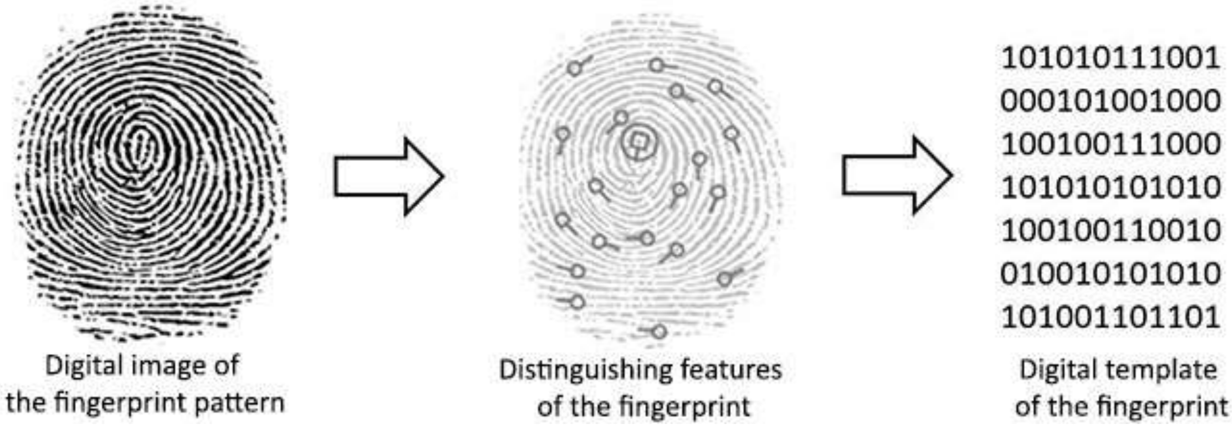

101010111001
000101001000
100100111000
101010101010
100100110010
010010101010
101001101101
Digital image of the fingerprint pattern
Distinguishing features of the fingerprint
Digital template of the fingerprint

**Figure: 4.1.b: Conversion of the fingerprint pattern to binary value.**

The voter is then provided with the list of nominees each represented by a logo. The voter then selects his/her choice of nominee. The nominees are represented by their representative logo, the logos have a binary value which is basically selected and worked with when chosen. The calculations and workings are done upon the distinct binary values. **Figure: 4.1.c** shows an example of the representation. The number of 1's and 0's in the value representing the nominees must be same otherwise it is possible to guess the choice of nominee in the ballot string. Upon several workings, it is seen that unequal number of 0's and 1's for every nominee may result in prediction of the selection of nominee, as a result the progress of the election is made visible. If the representation does not remain consistent or if it is not possible to allocate different representation of nominee within (N) bits, then increase the number of bits in order to get different representation for equal numbers of 0's and 1's. Example- Three bits with two

1's and a 0 will have representations – 110,011,101 so three logos can be represented by these in other words three nominees can be represented.

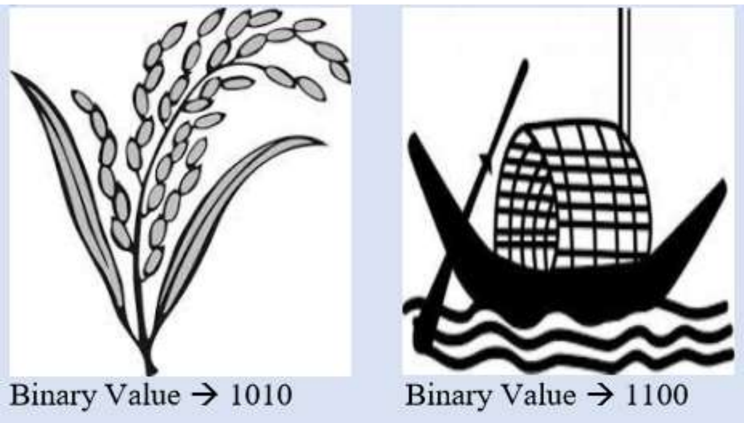


**Figure: 4.1.c: Binary representation of nominee logos.**

On choosing the nominee, the preparation of ballot takes place. A ballot is designed to have a ballot number in it in order to refer it. The ballot consists of the voter →hash (fingerprint_binary) and the ballot string. The ballot string is prepared by the execution of a function inside the code with the concept of smart contract. The ballot string must be different for every voter. The ballot string has two sub-strings, choice string and the random string. The choice string consists of the nominee choice hidden within other randomly generated values. The random string is randomly generated 0/1 values. These techniques are used in order to prevent viewers from recognising the choice of nominee. A nominee might get multiple votes therefore, to distinguish every ballot strings the concept of random string is used. Generation of the random string results unique ballot string formation. The ballot string is prepared in two phases, the following are:

NOTE: The total number of bits has no restriction. 16-bit is just an example. Greater number of bits is more secure as chances of similar generation of random number decreases. The decision of the number of bits must be taken in consideration before taking decision.

Consider a 16-bit ballot string of which 8 bits are choice string-the red ones and 8 bits are random string-the black ones. The ballot string is equally divided in these two parts.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

i) If n bits are representing each logo then n random numbers are generated from 0-7 as the choice string is between 0-7, the binary value of the logo is arranged in the generated random value indexes of the ballot string i.e.

Alice chooses the nominee with a binary value of 1100, the binary value consists of four bits thus four random numbers are generated in order to hide the choice of Alice.

Number of bits representing each logo→4

Random numbers→ 4,5,7,0 (4)→$V_c$→opening value

Nominee choice →binary value of logo→1100

Therefore, the four randomly generated number- 4,5,7,1 are the indexes to hide the binary value of the nominee’s choice. The value is assigned sequentially.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | | | 1 | 1 | | 0 | | | | | | | | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

ii) Generate another number between 1/0. Fill that number in the other four indexes. Example-1

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | | | | | | | | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

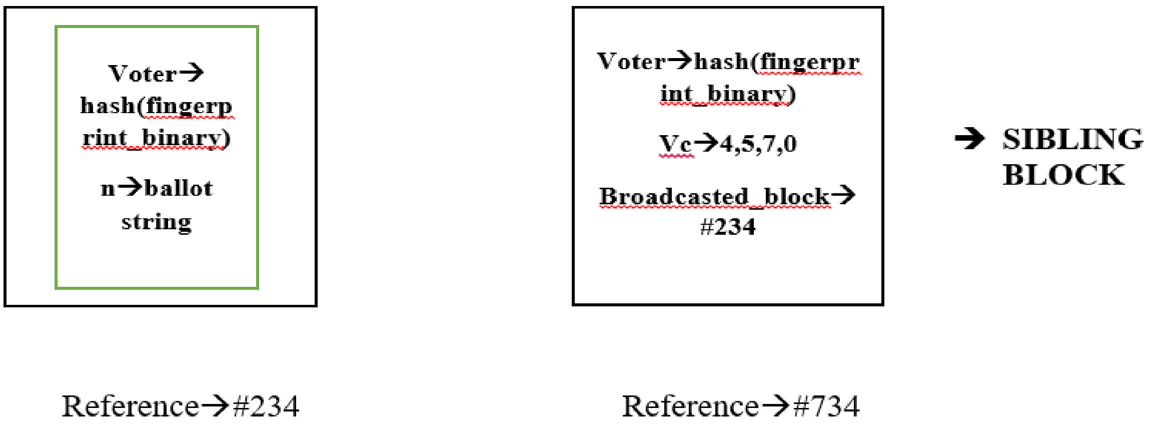
The other indexes of the choice string are assigned with either 1/0, but all the other indexes of the choice string must have the same value to avoid recognition of the choice.

iii) Generate random numbers randomly from 1/0 and put on the indexes (8-15) suppose, 11001010

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

As 8-15 is the random string part of the ballot string thus eight random numbers either 1 or 0 are generated and assigned sequentially in order to distinguish each ballot string.

The ballot string is prepared, and the choice is hidden inside the string. The choice is recognized by the $V_c$ only. Dispose of the Vc can only result in the consideration of the vote. One block is created containing the ballot and another sibling block is created that consists of the voter→hash (fingerprint_binary), the ballot number of the broadcasted one, its own reference number and the opening value of the choice, in this case- 4,5,7,0. The figure below shows the arrangement.



Voter→ hash(fingerprint_binary)

n→ballot string

Reference→#234

Voter→hash(fingerprint_binary)

Vc→4,5,7,0

Broadcasted_block→ #234

Reference→#734

→ SIBLING BLOCK

**Figure: 4.1.d: Blocks**

As the voter casts the vote i.e. the voter broadcast the ballot containing block. The ballot contained block is requested to add in the chain whereas the sibling block is remained un-broadcasted. The peer nodes start to work for the proof of work for the block. The one completing earlier then also verifies whether the voter has casted vote earlier and whether the ballot is in correct format. After all the verification, the ballot contained block is added in the blockchain and other peer nodes verifies and updates their chain. Majority is taken in consideration. If majority disagrees then the block is discarded. This not broadcasting issue is pre-defined earlier in the code to ensure the result is calculated only after the election ends.

#### 4.1.1.3 Post Voting Phase:

Once the ending time is reached, it is checked whether all the voters have voted or not. If not, then they are shortly given a notification to complete their voting within specified time. If they fail to do so then no consideration is taken to be granted otherwise their voting is performed similarly as per the voting phase. If all the voters are done with their voting then as per the contract and execution of codes, all the sibling blocks are broadcasted one by one sequentially. Once all the sibling blocks are broadcasted, the peer nodes start to calculate the result referencing the blocks and using the $V_c$ to extract the choice of nominee for every blocks. Here all the nodes are supposed to come up with the same result as no blocks are discarded unnecessarily in between and the blockchain supports no changes. Therefore, the voters in other words the peer nodes themselves count the votes and broadcast the result preventing the need of the tallier or counting using third party. The blockchain is transparent and the accuracy is ensured as everything is made visible.

# Chapter-05: Security Analysis

## 5.0 Security Goals:

When we are talking about networking. Among all the process, communications, transactions etc the security comes first. Because it’s the process to keep things running well maintained for the users who are involved. There are certain security goals which is full filled with our proposed methodology.

- Confidentiality
- Integrity
- Authenticity
- Non-repudiation

**Confidentiality:** Confidentiality is pretty equivalent to part of privacy. It’s designed to ensure the prevention sensitive information from reaching the wrong people or unauthorized users, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question. Most common method ensuring confidentiality is Data encryption.

Here we are using Block Chain for the process where if any user in a block exists then that user’s information cannot be seen by any unauthorized user who is not in Block Chain. So our process approves the confidentiality.

**Integrity:** It involves maintaining the consistency, accuracy and trustworthiness of data. It’s for entire life cycle. Data must not be changed in any transit or any authorized movement that can be changed by someone who is not authorized. Data must be in place to detect any changes. These measures include file permissions and user access controls.

Our process is when a user data stores in the block which cannot be changed or modified by any unauthorized user whether another user in block or not. The user itself has the right to change the data or information. Who is not in the block cannot store or change any data. Or any leakage of data. So here the integrity checked as well.

**Authenticity:** It’s a process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the normal process. Other options include biometric verification and security tokens, key fobs or soft tokens.

Here we are using fingerprint authentication system for the authentication of a user. In our voting system ballot string generates for individuals and as well the hash of the fingerprints. The user checks it using the fingerprint process. From the help of Genesis block if the fingerprint of that particular user exists (matches the fingerprint) then that user is allowed to do the process otherwise the user is not eligible for the process. The Genesis block is an initial block where the information of a user stores to check the authenticity of that individual.

**Non-Repudiation:** The process of non-repudiation is that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. The word repudiate means deny. In simple way it's witnessing a legal document the sign of a user that cannot deny later. An example is Digital Signature.

So here the user information is stored in genesis block. When a user performs a vote then the user cannot deny it. As the voting history is stored right after performing a vote.

# Chapter-06: Limitations

## 6.0 Limitations:

In our proposed methodology some lacking is marked in.

- If any voter doesn’t have any hand, he/she doesn’t able to vote with this system. It’s a major problem with this methodology.
- From the concept of Blockchain technology there is a system for some rewards which are actually helped all the nodes for authorization. In our system no rewards will be given for the valid voters/nodes.

# Chapter-07: Future Work

## 7.0 Future Work:

- As our future goals to improve the voting process system more easier, secure, reliable and make it available for the users as well to the developing countries.
- And when the user goes through the authentication process by fingerprint system then it will generate OTP (one-time password) for the individual and user will get notified via SMS or Email to make it more secure.
- IRIS Scanner can be introduced to instead of Finger Print Scanner verification.
- A team of controller can be involve to monitoring all process specially in voter verification which is earlier done the peer nodes.

# Chapter-08: Conclusion

## 8.0 Conclusion:

As discussed previously, E-voting is an emerging concept or solution of voting to carry out activities with accuracy and reliability. Moreover, blockchain in an interesting and attractive technology that provides transparency of data and is a topic of high demand. As the process of election must be handled with care to avoid unusual circumstances and occurring, therefore, this protocol might reduce the constraints of manual voting and other E-voting systems based on blockchain that uses least involvement of the third party. Also, the reduction of third party completely is a proof of healthy election which is enabled by the use of Smart Contract. The coercion is also prevented by the concept of random generation of groups using Smart Contract. The techniques used in the protocol is quite simpler and easily understandable and also designed to reduce memory and time consumption to make tasks faster. As a result, this protocol fulfils all the previously defined properties of the referred paper along with the prevention of coercion with transparency.  The voters are able to monitor the whole process and their privacy is also maintained to avoid any sort of issues. Furthermore, a replacement of the metadata can be taken in consideration to make this protocol widely used in all areas.

# References:

[1] M. Crosby, Nachiappan, P. Pattanayak, S. Varma, V. Kalyanaraman "Blockchain Technology: Beyond Bitcoin", 2 june 2016.

[2] Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/elections/voting-systems/ oversight/ top-bottom-review/.

[3] N. Weaver (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/ secure-vote-today.

[4] L. F. Cranor " Electronic Voting", Encyclopedia of Computers and Computer History, Fitzroy Dearborn,2001.

[5] D.A. Kumar, T.U.S. Begumn "Electronic Voting Machine – A Review", March 21-23, 2012.

[6] S. Ellis, A. Juels and S. Nazarov "ChainLink: A Decentralized Oracle Network", Available at https://link.smartcontract.com/whitepaper, 2017.

[7] Y. Liu, Q. Wang "An E-voting Protocol Based on Blockchain", October 2017.

[8] F.S. Hardwick, A. GIoulis, R.N. Akram and K. Markantonakis "E-voting with Blockchain: An E-voting Protocol with Decentralisation and Voter Privacy" 3 Jul 2018.

[9] A. Lewis "A Gentle Introduction to Blockchain Technology", 2015.

[10] R. Hanifatunnisa, B. Rahardjo "Blockchain Based E-voting Recording System Design", 2017.

[11] Zheng Z, Kies, Dai HN, Wang H "Blockchain Challenges and Opportunities"; A survey work pop; 2016.

[12] F. P. hjalmarsson, G. K. Hreioarsson "Blockchain-Based E-voting System", 2017.

[13] Md. M. Hoque "A Simplified Electronic Voting Machine System", 2014.

[14] A.K.Koc, E. Yavuz, U.C. Cabuk and G. Dalkilik "Towards Secure E-voting Using Ethereum Blockchain", 2018.

[15] R. Bohme, N. Christin, B. Edelman and T. Moore "Bitcoin: Economics, Technology, and Governance", Vol-29, No.2, Spring 2015, Pages 213-238.