Modified E-voting System Using Blockchain Technology

By

Md. Tanvir Rahman

(151-35-881)

Samen Anjum Arani
(151-35-1008)

A thesis submitted in partial fulfillment of the requirement for the degree of Bachelor of Science in Software Engineering

Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY

Fall – 2018

APPROVAL

APPROVAL

This thesis titled on "**Modified E-voting System Using Blockchain Technology**", submitted by **Md. Tanvir Rahman**, 151-35-881 and **Samen Anjum Arani**, 151-35-1008 to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Dr. Touhid Bhuiyan
Professor and Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Chairman

Dr. Md. Asraf Ali
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1

Md. Maruf Hassan
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Prof Dr. Mohammad Abul Kashem
Professor
Department of Computer Science and Engineering
Faculty of Electrical and Electronic Engineering
Dhaka University of Engineering & Technology, Gazipur

External Examiner

DECLARATION

It hereby declares that this thesis has been done by us under the supervision of **Ms. Syeda Sumbul Hossain**, Lecturer, Department of Software Engineering, Daffodil International University. It is also declared that neither this thesis nor any part of this has been submitted elsewhere for award of any degree.

Tanvir Rahman

Md. Tanvir Rahman
Student ID: 151-35-881
Batch: 16th
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Samen Anjum Arani

Samen Anjum Arani
Student ID: 151-35-1008
Batch: 16th
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Certified by:

24.12.2018

Ms. Syeda Sumbul Hossain
Lecturer
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

ACKNOWLEDGEMENT

First of all, we are grateful to the Almighty Allah for giving us the ability to complete the final thesis.

We would like to express our gratitude to our supervisor **Ms. Syeda Sumbul Hossain** for the consistent help of my thesis and research work, through his understanding, inspiration, energy, and knowledge sharing. Her direction helped us to finding the solutions of research work and reach to our final theory.

We would like to express my extreme sincere gratitude and appreciation to all of our teachers of **Software Engineering** department for their kind help, generous advice and support during the study.

We are also express our gratitude to all of our friend's, senior, junior who, directly or indirectly, have lent their helping hand in this venture.

Last but not the least, we would like to thank our family for giving birth to us at the first place and supporting me spiritually throughout my life.

Md. Tanvir Rahman
ID: 151-35-881

Samen Anjum Arani
ID: 151-35-1008

DEDICATION

We dedicate this thesis to our family for their love; affection and the dedication to us support us for the success of our life. We also dedicated this thesis to our teachers and especially to our supervisor, because without their guidance, inspiration, and dedication it was not possible.

TABLE OF CONTENT

APPROVAL.....ii
DECLARATION.....iii
ACKNOWLEDGEMENT iv
DEDICATION..... v
LIST OF FIGURE viii
LIST OF TABLE ix
LIST OF ABBREVIATION ix
Abstract x
1. Introduction 1
1.1 Problem Outline 1
1.2 Motivation 2
1.2.1 What are we studying 2
1.2.2 Why are we interested in it 2
1.2.3 Why should this be interesting to others 3
1.3 Research Question (RQ) 3
1.4 Research Design 3
2. Literature Review..... 4
2.1 Research Method 4
2.2 Search strategy 5
2.2.1 Search string 5
2.2.2 Search scope 6
2.2.3 Search period 6
2.2.4 Search method..... 6
2.2.5 Inclusion/exclusion criteria 7
2.3 Classification Schema 8
2.4 Descriptive analysis 8
2.4.1 Search scope results 9
2.4.2 Time period results 9
2.4.3 Publication type results 9
3. Background Study 11
3.1 Electronic voting 11
3.2 Working Method 11
3.3 Analogy of e-voting system 12
3.4 Why blockchain in e voting 14
4. Gap analysis 16
4.1 Drawback of Electronic voting machine 16
4.1.1 Substituting Look-Alike CPUs 16

4.1.2 Messing with Software before CPU Manufacture **16**
4.1.3 Substituting Look-Alike Circuit Boards **17**
4.1.4 Substituting Look-Alike Units **17**
4.1.5 Messing with Machine State **17**
4.2 Manifestation Attack **17**
4.2.1 Deceptive display assault **18**
4.2.2 Clip-on Memory Manipulator Attack **18**
4.3 Similar models **19**
5. Proposed Model **20**
5.1 Model Structure **20**
5.2 Model Process **22**
5.2.1 Registration **22**
5.2.1.1 Voter registration **22**
5.2.1.2 Candidate Registration **23**
5.2.2 Request for Vote **24**
5.2.3 Peer to peer network **24**
5.2.4 Create a block **24**
5.2.5 Counting vote **25**
6. Contribution **26**
Future Work **28**
References **30**

LIST OF FIGURE

Figure 1. 1: Study Design 3

Figure 2. 1: Flowchart of the search and separating process 8
Figure 2. 2: Distribution of related papers over time period per publication type 10

Figure 5. 1: Our Proposed Model 20
Figure 5. 2: Voter giving single vote 21
Figure 5. 3: Voter giving multiple votes 22
Figure 5. 4: Voter Registration Process 23
Figure 5. 5: Candidate Registration Process 24
Figure 5. 6 : Voting process 25

LIST OF TABLE

Table 1. 1: Related works summary 5

Table 2. 1 : Distribution of selected studies 10

Table 3. 1: Comparison among the countries of e-voting system 13

LIST OF ABBREVIATION

Terms	Abbreviation
E-voting	Electronic Voting
EVM	Electronic Voting Machine
RQ	Research Question
DRE	Direct Recording Electronic Voting
EPROM	Erasable Programmable Read Only Memory
BHEL	Bharat Heavy Electricals Limited
FPP	First Past The Post
OPEN PR-LIST	Open Party List
DEVS	Discrete Event System Specification
GEMS	Global Election Management System
SVS	Stored Value Solution
PR-STP	Proportional Representation Single Transferable Vote
AVC	Advantage Direct Recording Electronic Voting
CPU	Control Processing Unit
LED	Light Emitting Diode
EEPROM	Electrically Erasable Programmable Read Only Memory
NID	National Identity Card
P2P	Peer To Peer

Abstract

From the beginning of society, voting is an important event. That time people had been made the decision by throwing the different colored ball or by showing a simple hand gesture. With the development of society and the increment of the population, the voting process became more complex. At first, those simple processes were replaced by the ballot paper system. However, it has some technical, social and financial issues. The electronic voting can solve these issues, but it has come with some drawback of its own like software errors, security issues. The development of technology has been continuously influencing modern society to create a more accessible and secure process for voting. In this flow, the invention of the blockchain is a turning point because of its transparency, immutability and decentralize properties. This paper underlines the lacking of the current e-voting system. In this paper, we proposed a more secure e-voting system that uses blockchain technology. In here, we use blockchain network to check the validity of voter and candidates. Concluding this paper is a view of how blockchain can solve the problems with the current e-voting system.

1. Introduction

1.1 Problem Outline

Voting plays an important role in constructing a democratic society. The traditional voting requires voters to cast in appointed polling stations, which usually involves enormous expenditure on time and cost budget [7]. In generally paper ballots, voters choose their favorite choices by marking on ballots and place them in boxes, which are sealed and officially opened under special conditions to warrant transparency[15],[16]. The current ballot system can be easily manipulated by the power-hungry organization.

Electronic voting (e-voting) is a promising platform that aims to provide a secure, convenient, and efficient voting environment over the Internet [3]. Electronic voting (e-voting) is a symbol of modern democracy activities. E-voting system has been booming in recent years because of its high ballot privacy and verifiability, [7]. It is pushed as a potential solution to attract young voters [8], [9]. It has been a challenge for a long time to building an electronic voting system that satisfies the legal requirements[2]. Digital voting is the use of electronic devices, such as voting machines or an internet browser, to cast votes [6]. Electronic voting machines have been viewed as flawed, by the security community, primarily based on physical security concerns. Anyone with physical access to such machine can sabotage the machine, thereby affecting all votes cast on the aforementioned machine [2]. With the use of blockchain, a secure and robust system for digital voting can be devised [6].

A blockchain is a public ledger which distributed, immutable, incontrovertible, public ledger [2]. It is designed to be accessed across a peer-to-peer network. Each node/peer communicates with other nodes for block and transaction exchange [6]. Obvious advantages of e-voting using blockchain include i) greater transparency due to open and distributed ledgers, ii) inherent anonymity, iii) security an authenticity and iv) Unalterableness [1].

1.2 Motivation

The overall perspective of this research is:
To provide a more secure e-voting system by using blockchain technology. We formulated the following questions, to identify specific studies and research questions from the overall research topic and goal.

1.2.1 What are we studying

- We studied about e-voting systems. Our main focus was on the current e-voting system. We also studied blockchain technology and about it is features for securing e-voting system.

1.2.2 Why are we interested in it

- In recent time e-voting system is a highlight topic. Many countries are using e-voting system in their government election. But people have some compound experience about using EVM (Electronic voting machine) and its security system.
As blockchain is a decentralized, distributed and immutable database, we thought we could find a solution of a security issue by using blockchain technology as the foundation of the e-voting system.

1.2.3 Why should this be interesting to others

- Both voting authority and both voting authority and voter benefit from this research. Both will gains deeper understanding about security and transparency of blockchain based e-voting system. The voter might get help by giving vote without any worry.

1.3 Research Question (RQ)

Based on our research goal, we have defined our Research Question (RQ) as followings:

RQ1: What are the e-voting systems already implemented in different counties?
RQ2: What are the lacking of existing e-voting systems?
RQ3: How the proposed model will solve existing problems of e-voting system?

1.4 Research Design

This research has been divided into two segments (see in Figure 1.1). Background study has been used as input of segment 1 and segment 1 has been used to answer **RQ1** and **RQ2**. Similarly, segment 1 has been used as input of segment 2, which answered **RQ3**.

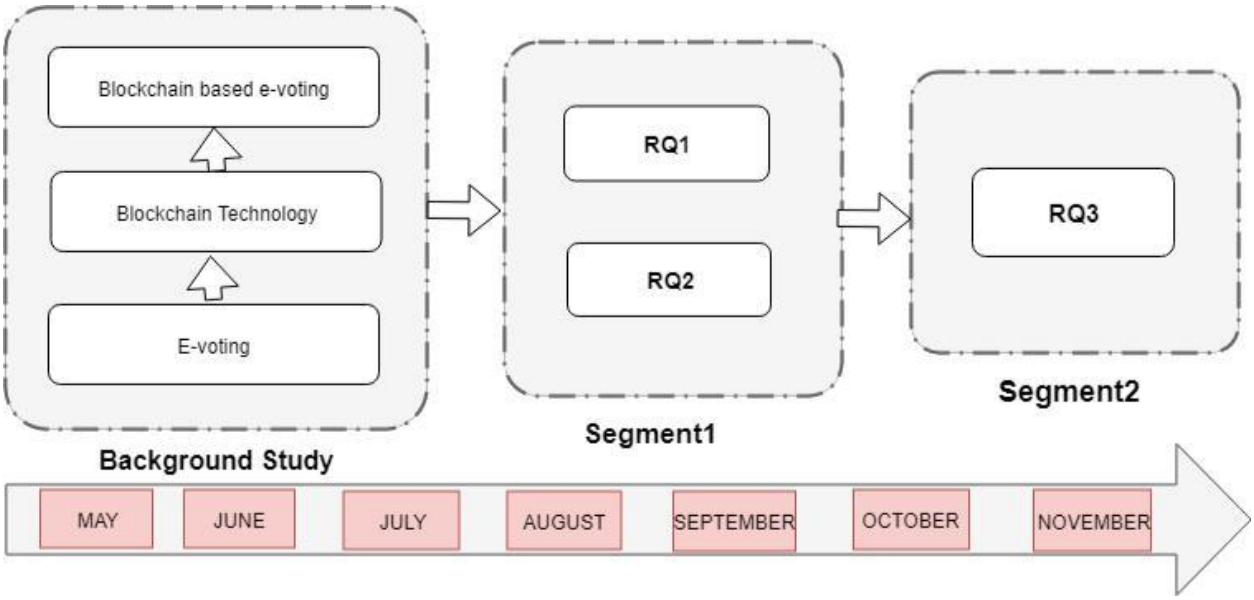

Figure 1. 1: Study Design

2. Literature Review

Researchers had performed various methods for literature reviews, such as case studies, experiments, surveys, and systematic reviews. In our study, to find out the current status of electronic voting (e-voting) and blockchain, we directed a comprehensive systematic mapping study. We describe the phases of the method we use and how the mapping study has been planned in this section.

The methodology contains identifying and answering the research questions pertaining our topic of research, defining the research strategy (search string, search scope, search period, search method, inclusion and exclusion criteria), classification of included works and the composition of the results. Figure 1 presents the flowchart of our systematic mapping process. In the following subsections, the full details of the steps are described in the chart.

2.1 Research Method

The point of this examination is to arrange the information on e-voting system using blockchain. Several concepts should be identified before formulating the research questions to clarify the scope of knowledge. The concept is mainly focused on the electronic voting system, the different types of electronic voting system, blockchain technology, the verification for the proposed approach, and the influence on security factors. The goal of the study is then broken down into three research questions (RQs)

Table 1. 1: Related works summary

Reference	Goal	Period of study
Hardwick et al. (2018)	An E-Voting Protocol with Decentralization and Voter Privacy	2002 to 2017
Ayed, Ahmed Ben (2017)	Provide a secure blockchain based electronic voting system	1981 to 2017
Jason et al. (2017)	Develop a e-voting protocol using Bitcoin technology	1982 to 2016
Hjalmarsson et al.(2018)	Research about existing blockchain frameworks and propose a blockchain-based e-voting system using permissioned blockchain	1986 to 2018
Wolchok et al. (2010)	Security Analysis of India's Electronic Voting Machines	1990 to 2010
Our work	Research about current e-voting system and propose a more secure e-voting system using blockchain technology	1978 to 2018

2.2 Search strategy

The research strategy addresses our proposed search string, search scope, search period, search method, and our inclusion/exclusion criteria. The search string should be gingerly outlined to have a broad coverage of the state of the art.

2.2.1 Search string

According to the main goal and the research question, we formed the search string. The strings should be simple to achieve multiple results and cover the topics exactly. To link the main terms and their synonyms we use the OR Boolean The final search string is: ("Block Chain" OR "block-

chain" OR "blockchain" OR "EVM" OR "e-voting" OR "e voting" OR "e voting" OR "electronic voting" OR "blockchain technology" OR "block chain technology" OR "electronic voting machine" OR "voting") and ("using" OR "system" OR "technology") With the end goal to utilize the string formed with the AND/OR Boolean operators, we utilized the available advanced search in every database.

2.2.2 Search scope

To achieve a high coverage of finding the relevant studies and publications, we included electronic databases in the search scope. ACM Digital Library (www.acm.org), IEEEXplore (https://ieeexplore.ieee.org/Xplore/), Springer(www.springerlink.com), is the most popular electronic databases and efficient to conduct systematic studies in the context of software engineering and re-engineering[11],[33],[34]. These are robustly recommended websites for widely searching. We included the Science Hub (https://scihub.org/), Google Scholar (https://scholar.google.com/) database for finding more effective studies that do not appear in the standard search process, regardless of the way that the search results will, in general, be iterative with the search results of the chose databases.

2.2.3 Search period

All related papers published in journals, books, conferences covered the time period from January 2000 to the end of July 2018. The beginning of 2015 blockchain technology became popular and e-voting system also become popular 2003. Early may in 2018 we started working on this e-voting using blockchain technology.

2.2.4 Search method

We used both automatic and manual searches. In the automatic search, each electronic database which provided by a search engine, checks the search terms against the metadata, including the title, abstract, and keywords of each paper in the database. In the manual search, we looked inside each conference, article and workshop report listed in the database that was related to the search string for the papers closely related to our e-voting and blockchain technology, but which did not appear in the automatic search. On the other side, we studied the snow-balling technique [13],[14],

which permits the reference list of the final determined studies from the automatic side we search (electronic databases) to be analyzed. Hence, we could add them to our blockchain technology study.

2.2.5 Inclusion/exclusion criteria

The selection criteria aim to find all relevant papers in our topic of systematic mapping as follows.

Inclusion criteria:

- Papers published from January 2000 to July 2018
- The whole paper published in conference, journal, and chapter in a book.
- Papers with the search string appear in title, abstract, and keywords

Exclusion criteria:

- Papers that are unrelated to search strings once their text was explored manually
- Ph.D. theses, reports, position papers, research proposals, projects
- Duplicated papers of the same study in different versions, journals, conferences, and Workshops
- Papers that do not have their full text available.
- Papers were written in other languages

All selected study must contain all inclusion criteria and must dissatisfy all of the exclusion criteria. In spite of the inclusion/exclusion criteria, we still found papers that do not answer the research questions. A quick perusing is required to get the final relevant papers. The separating procedure after searching in the electronic databases and obtaining the primary studies can be seen in Figure 2.1. The first search process returned 2965 papers, discarding duplicate papers reduced the list to 1852.After set inclusion and exclusion criteria to 281 by discarding non-English, non-full text paper reports, position papers, Ph.D. theses, and proposals. We think to identify the current knowledge of the e-voting system with blockchain; the final number of selected studies is enough. Finally, we acquired 328 selected papers after exploring the text manually based on title, abstract and keywords, to discard papers that non-related to any of the research questions and after the snow-balling, we wound up with 24 applicable papers, which represent 1.412% of the initial 2965.

2.3 Classification Schema

Classifying the papers in facets is a nice base for answering research questions. As a result of the cursory reading, a set of facets can be determined, into which the papers can be classified.

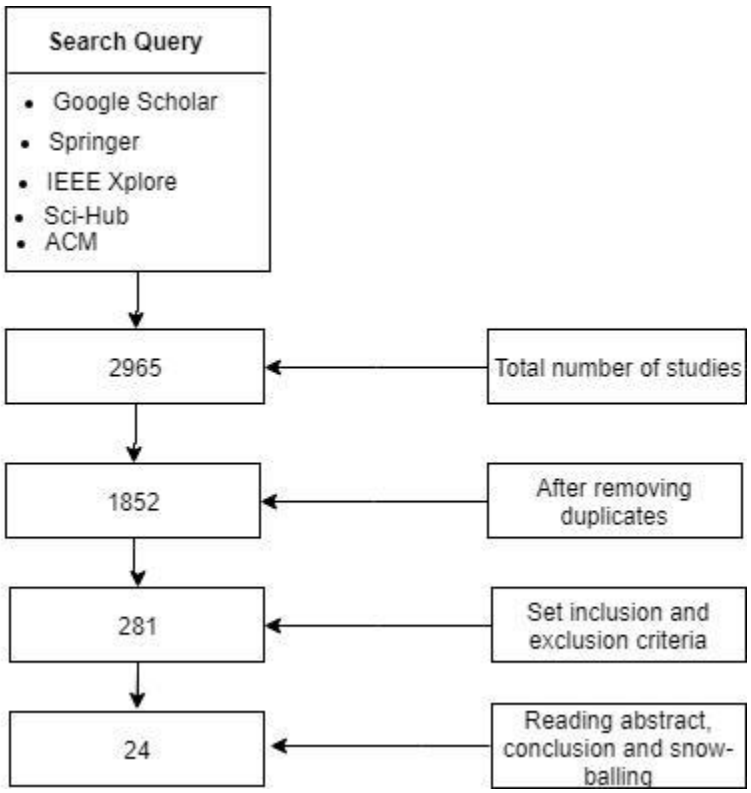

Figure 2. 1: Flowchart of the search and separating process

2.4 Descriptive analysis

We continued the mapping study according to the steps which we get in upper section . After completing all the steps like search, filtering, selection, and data extraction procedures, we got a vision on this field. Firstly, we get an overview of the results based on different features of the mapping study. Regarding descriptive analysis in this section we focused on e-voting system based on blockchain.

We narrate the results with respect to think about study scope, study selection, time period and publication type in the following sections.

2.4.1 Search scope results

As the result of the first search process table 3 shows a total of 2965 papers, the number of papers per electronic database and it represents the percentage. It can be noticed that Google Scholar returned the vast sets of papers and most of them are related to our study. Therefore, as the result this database is more effective for our study as compared to the remaining databases. In Science-hud, we found many papers from other areas but those were not related to our study.

2.4.2 Time period results

Figure 2.2 presents the distribution of related papers over the time period from 2000 to 2018. During the year 2002, only a journal was published. In the year 2003 and 2004, no papers were published. Two book chapters published in 2007 and 2013. The book chapter is the result of the manual search. Those chapters were added as references. As Figure 2.2 In 2007 and 2017, the number of published papers is most.

2.4.3 Publication type results

The selected 24 papers were published as a journal, article, conferences, workshops, or book chapters. Figure 2.2 views the distribution of selected papers over the publication types and years. Approximately 62.5% (24 studies) of the selected papers were published in proceedings as follows:

Table 2. 1 : Distribution of selected studies

DB source	Paper No.	Ratio	Related papers
ACM DL	746	25.16%	35
IEEE Xplore	676	22.80%	43
Google Scholar	930	31.366%	90
Springer	410	13.828%	21
Science Hub	203	6.84%	12
Total	2965	100%	

(9) conferences, (3) workshops, and (4)article, and 20% (5 studies) of the selected papers were published in leading journals, while only 24% (2 studies) were publications in book chapters.

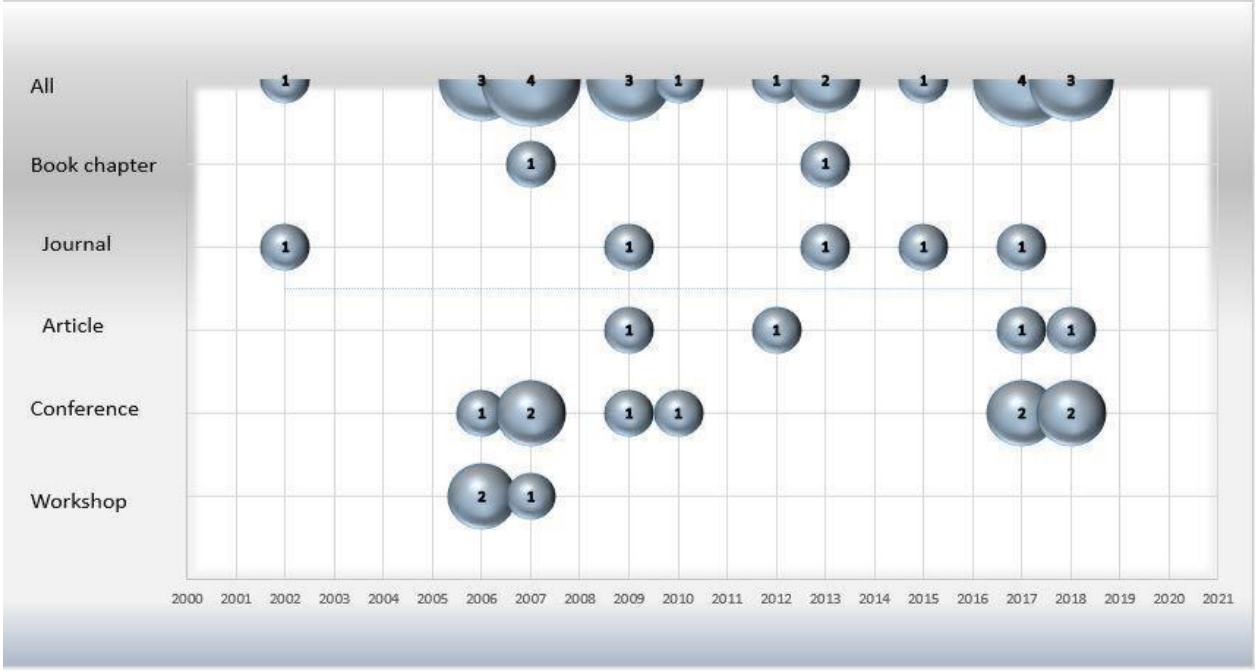

Figure 2. 2: Distribution of related papers over time period per publication type

3. Background Study

3.1 Electronic voting

Electronic voting is an indicator of a modern democratic society. Electronic voting offers to vote through electronic means to administer the chores of casting and counting votes. On the basis of particular implementation, electronic voting may use electronic voting machines (EVM) or computers that connected to the Internet. The main purpose of electronic voting (e-voting) is to create a promising platform that provides a secure, convenient, and efficient voting environment over the internet [3]. Electronic voting is a more economic system addresses on transparency and impartiality than traditional voting [7]. For a vigorous e-voting, the quantity of practical and security necessities are determined including straightforwardness, precision, auditability, framework and information trustworthiness, protection, accessibility, and circulation of power [17], [18], [19]. For being used in a national election, an e-voting system needs to fulfill essential requirement [2]:

(i) An election system should not enable pressured casting a vote.

(ii) An election system should not enable detectability of a vote to a voter's to recognize qualification.

(iii) An election system should ensure and proof to a voter, that the voter's vote, was counted and counted correctly.

(iv) An election system should not enable control to a third party to alter any vote.

(v) An election system should not enable a solitary substance power over counting cast a ballot and deciding a race's outcome.

(vi) An election system should just enable qualified people to cast a vote in an election.

3.2 Working Method

Electronic voting innovation can incorporate punched cards, optical scan voting systems, and direct-recording electronic voting (DRE) [20]. It can likewise include transmission of tallies and votes through phones, private computer systems, or the internet. As the electronic voting machine, all countries, for the most part, utilize the direct-recording electronic (DRE) voting machine. In

this procedure, voters see ballots on a screen and make their vote utilizing an input device, for example, a bank of buttons or a touchscreen. Some DRE frameworks additionally utilize a card swipe or cartridge framework that must be actuated before a ballot can be cast. Votes are stored on a memory card, compact disc or other memory devices. At that point race, election authorities transport these memory devices to a unified area for tabulation, similarly as they would with paper-based ballots. A few machines have the ability to broadcast results over a modem-to-modem line.

3.3 Analogy of e-voting system

Electronic voting in favor of electorates has been being utilized since the 1960s [21] when punched card frameworks appear. Their first far-reaching use was in the USA where 7 regions changed to this technique for the 1964 presidential race [21]. Estonia was the first on the world to receive an electronic voting for its national elections [22]. Before long, electronic voting was received by Switzerland for its all-statewide elections [23] and by Norway for its council election [24]. Table 1 shows the details information of different countries using e-voting system.

Table 3. 1: Comparison among the countries of e-voting system

[27]

Country	E-voting	Company	Election Type	Electoral System	Introduced Year	Year Used	Software Used	Hardware Used
India	814.5 million	BHEL	state	FPP	2001	2009 /2004 /2003 /2001	EPROM	EVM
Belgium	3.2 million	Steria	General & Municipal	Open PR-List	1994	1999	Digivote, Jites, Stesud	DEVS
Brazil	66 million	UniSys & Diebold	All Govt. Level		1996	1996 /1998 /2000 /2002	GEMS	GX-1 Integrated processor
UK	1.5 million	SVS	Local Govt	PR-STV	2000	2000 /2003	AVC	DRE
Spain	3000	Indra	Municipal	FPP	2002	2003	SIRE	SIRE System
Canada	98000	Can Vote	Municipal	FPP	2002	2003	Can Vote On Linux	Can Vote On Internet

3.4 Why blockchain in e voting

EVM technology though has not been observed to be totally secure, tamper-proof or fraud-proof [25]. From Australia to India to Norway to Venezuela, in excess of 20 nations on the world have canoodled with electronic voting systems over the most recent 20 years with changing degrees of reception or dismissal [25]. A noteworthy contention against internet e-voting states that the internet is an innately unreliable platform. To be sure, different assaults including worms, viruses, spyware, spoofing, denial of service and others can be utilized to bargain the casting ballot results, to break the voter's secrecy, or to interrupt the elections. The vulnerabilities behind these assaults emerge from the major properties of the architecture of the internet and current individual computers. It has additionally been noticed that successful e-voting trials do not generally demonstrate the security of internet voting. Firstly, it is extremely hard to demonstrate that no security break has happened; and secondly, successful trials cannot dispense with security dangers for future decisions [22]. Frequently the character of the voter is not checked, voting material may not be anchored and the principles for secret voting may have been loose even in surveying stations
[26].

3.5 Blockchain as a Base of E-voting

A distributed network comprising of a huge number of interconnected nodes bolsters blockchain innovation. Every one of these nodes has their own copy of the distributed ledger that contains the full history of all transactions the system has processed. There is no authority for controlling the organize. They accept a transaction when most of the nodes concur. This system enables clients to stay anonymous [1]. The blockchain is simply that a chain of multiple blocks. Each block has transaction data that is permanently recorded which is added to the blockchain [35]. The first block of a blockchain, known as a genesis contains its transactions that, when combined and validated, produce a unique hash. Then the hash and all the new transactions that are being processed are used as input to create a brand new hash and it is used in the next block in the chain. Forming a chain back to the genesis block, each block links back to its previous block through its hash. Hashing is the way toward taking an input of any length and transforming it into a cryptographic settled yield through a mathematical algorithm. Anyone who might attempt decrypt the data by taking a gander at the hash will not have the capacity to work out the length of the encrypted data

dependent on the hash [36]. An essential analysis of the blockchain innovation recommends that it is a suitable basis for e-voting a ballot and, in addition, it could possibly make e-voting a ballot more worthy and solid [1].

4. Gap analysis

4.1 Drawback of Electronic voting machine

Essentially, we find that while the basic plan of the EVMs makes certain software-based assaults more improbable than in different DREs, it makes assaults including physical altering far simpler [20].

4.1.1 Substituting Look-Alike CPUs

Assailants may attempt to substitute look-alike CPUs containing software that checks the votes dishonestly. The EVM architects could have made such assaults more troublesome by building a cryptographic mechanism for recognizing the original CPUs, for example, a challenge-response protocol based on a secret contained in the original firmware. In expansion to the fundamental CPU utilized in the control unit, the programmable rationale devices in the ballot unit may likewise be focused in such an attack [20].

4.1.2 Messing with Software before CPU Manufacture

The EVM firmware is stored in masked read-only memory inside the microcontroller chips, and there is no arrangement for removing it or confirming its integrity. This implies that if the product was altered before it was manufactured into the CPUs; the progressions would be exceptionally hard to detect. Consider the designer in charge of aggregating the source code and transmitting it to the CPU maker. He or she could substitute an adaptation containing an indirect access with minimal possibility of being gotten. This reality alone would be incredible allurement for fraud. Similarly, representatives at the chipmakers could adjust the aggregated program picture before consuming it into the chips [20],[27],[28],[29].

4.1.3 Substituting Look-Alike Circuit Boards

Attackers may think that it is quicker to develop an electrically compatible dishonest main board and substitute it for the original. An attacker could steal votes by supplanting the circuit board in the ballot unit with one that falsely responds to key press events, or by replacing the display board in the control unit with one that reports inaccurate vote totals. The associations between these parts are trusted as well, so an attacker could attempt to embed a device between the ballot unit and control unit with the end goal to capture the keypress flags and supplant them with votes in favor of various applicants [20].

4.1.4 Substituting Look-Alike Units

Voters and poll workers have no down to earth approach to confirm that the EVMs they utilize are valid, so attackers may attempt to construct identical looking yet dishonest control units or ballot units and substitute them before an election. Since the units we analyzed have no compelling method to check the genuineness of the units they are matched to, supplanting either unit with a deceptive one would enable the assailant to change decision results [20].

4.1.5 Messing with Machine State

Regardless of whether each segment of the framework acts truly, attackers could in any case endeavor to control the framework by specifically getting to or controlling the inward condition of the machine in manners not contemplated by its designers [20].

4.2 Manifestation Attack

They actualized two manifestation Attack to delineate and tentatively affirm a portion of the EVM security issues. A criminal who utilized strategies like these could modify vote adds up to in genuine decisions or undermine tally mystery to decide how every voter casted a ballot.

4.2.1 Deceptive display assault

The deceptive display includes a different, concealed microcontroller that blocks the vote aggregates and substitutes fake results. To achieve this, the unscrupulous display reads the electrical signs from the control unit that would regularly control the 7-section LED digits. This enables it to recognize when the control unit is endeavoring to show decision results. It additionally translates the "add up to cast a ballot" yield to decide the real overall number of votes so it can make the unscrupulous votes include effectively. At last, it ascertains and indicates conceivable, however, the deceitful vote means every hopeful. When the unscrupulous display is introduced in an EVM (perhaps months or years before the decision), the assailant must convey which candidate is to be favored, and by what edge. There is a wide range of ways that aggressors could send such a signal—with different sorts of radios, using secret combinations of key presses, or even by utilizing the number of candidates on the vote [20]

4.2.2 Clip-on Memory Manipulator Attack

Unlike the deceptive display assault, which included supplanting equipment segments with dishonest look-alikes, this second assault includes just the impermanent utilization of new hardware. They developed a device that cuts directly to the electronically erasable programmable read-only memory (EEPROM) [20]. Chips that record the votes inside the EVM. This little device fits prudently in a shirt pocket. It encourages two sorts of attacks: stealing cast a ballot and abusing vote secrecy. To take cast a ballot, the assailant demonstrates his favored candidate utilizing the rotary switch. The rotary switch chooses a number from 0 to 9, and the assailant can utilize it to pick a favored applicant in any of the initial nine eballot positions, which ordinarily incorporate the real national parties. When the change is set to positions 1– 9, the clasp on gadget executes a vote-taking system [20].

An aggressor could likewise utilize our clasp on the gadget to abuse the mystery vote. The device can be associated with a computer phone a sequential link, and, when the rotary switch is set to position 0, it anticipates directions to read or write the EEPROM [20]. This enables the aggressor to download the machine's arranged vote records to the laptop. After separating the vote records,

the assailant would just need to decide the request in which voters utilized the machine to realize which candidate each picked [20].

4.3 Similar models

This proposed model [7] utilize an RSA algorithm, a cryptographic algorithm that used to encrypt and decrypt the messages and ring signature to keep all voters anonymous and equal. This framework comprises of three elements: Voters, Registration Authority, Election Authority, and Bitcoin Address Pool. The entire convention improvement comprises of seven successive stages, various performers Preparation Phase First Registration Phase, Second Registration Phase, Publish Phase, Voting Phase, Tallying Phase and Verification Phase execute each stage.

A non-conventional e-voting system is proposed [3] that use bitcoin Protocol and blind Signature Protocol. The framework includes three element types: voters, a director, and a counter. If an activity of casting a vote is performed outside time frame the set for a phase, at that point a vote can wind up invalid.

The proposed voting [1] protocol exploits the blockchain as a transparent ballot box and to store the cast ballots. In this protocol, allow a voter to cancel his or her vote, replacing it with another if their mind changes each voter will be in charge of ensuring that deceitful votes are rejected, thus that agreement is kept up as per the election rules.

In this proposed model [5] when the first transaction added to the block will be a special transaction that represents the candidate. This transaction is will include the candidate's name and will serve as the foundation block, with every vote for that specific candidate placed on top of it. The foundation will not count as a vote like the other transactions and it will only contain the name of the candidate. In this system, a voter can give a blank vote, as a protest vote the framework utilize the Longest Chain Rule in the case of concusses.

5. Proposed Model

5.1 Model Structure

Voting is the foundation of a nation's governmental system. It gives the citizens of the nation a right to choose their own government. Electronic voting system allows votes be cast and tabulated through electronic. The electronic voting system replaced the paper ballot by the electronic voting machine and provide a way to count votes using computation. We did not try to replace the current e-voting system completely but rather we tried to integrate blockchain technology within the current system. Based on previous gap analysis we have proposed this model,

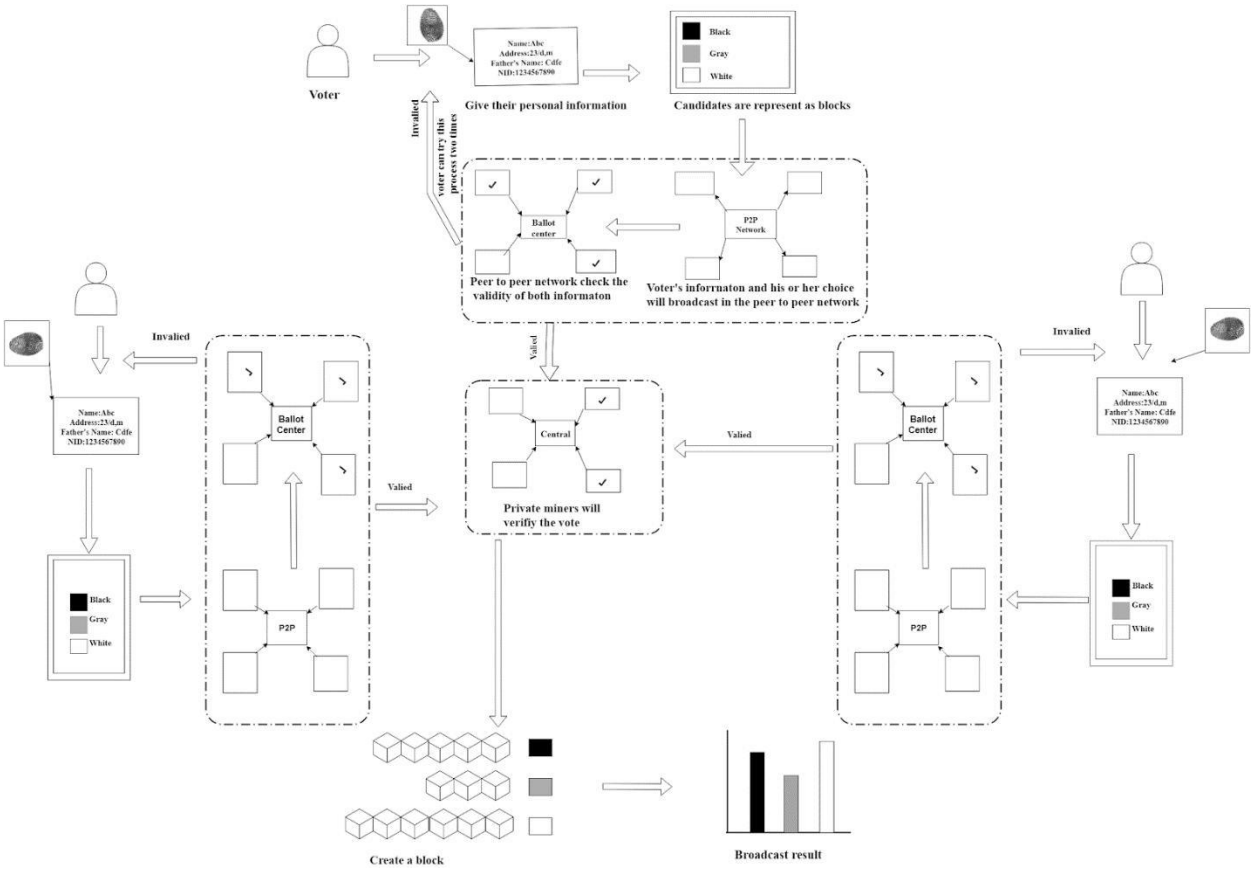

Figure 5. 1: Our Proposed Model

Our proposed model is the familiar e-voting system with blockchain technology. The eligible voters and candidates will be registered before by the government and private miners will create a

genesis block for each voter and candidate. This genesis block will contain their personal information. On the voting day, the voters will come to their corresponding ballot center. They will give their fingerprint in the fingerprint scanner for biometric verification. Then get the candidate choice list as blocks. The voters will choose their favorite candidate and give their vote. The information of the voter and their choice will then be broadcast on the peer-to-peer network. The private miners of corresponding ballot center will check the validity of both information. If both information is valid, the true information will be sent the central network. If the information is invalid the process will be back to the beginning .The voter can try the process two times then the voter will be considered a fraud .The private miner assign in central network will verify the vote .They generate a transaction for vote and create a block in the blockchain. After the voting process, come to the end the result will broadcast based on the candidate blockchain.

At the beginning, the number of vote that a voter can cast will be declared depending on the election type. Each voter can give one or multiple votes, depending on the type of the election. If the voter has one vote to cast, he/she could only give one vote to any candidate. In this case, only one vote transaction will be valid and other transaction will be invalid. When voters have right to vote multiple the candidate choice will be divided in sections. The voter could give multiple vote but not in the same section or not for the same candidate.

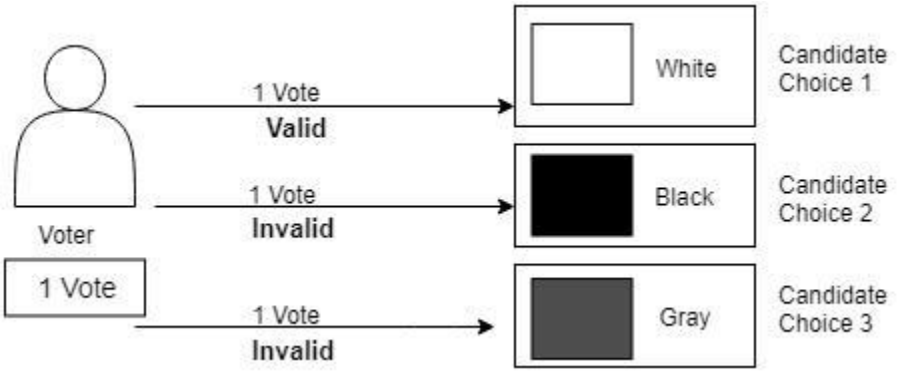

Figure 5. 2: Voter giving single vote

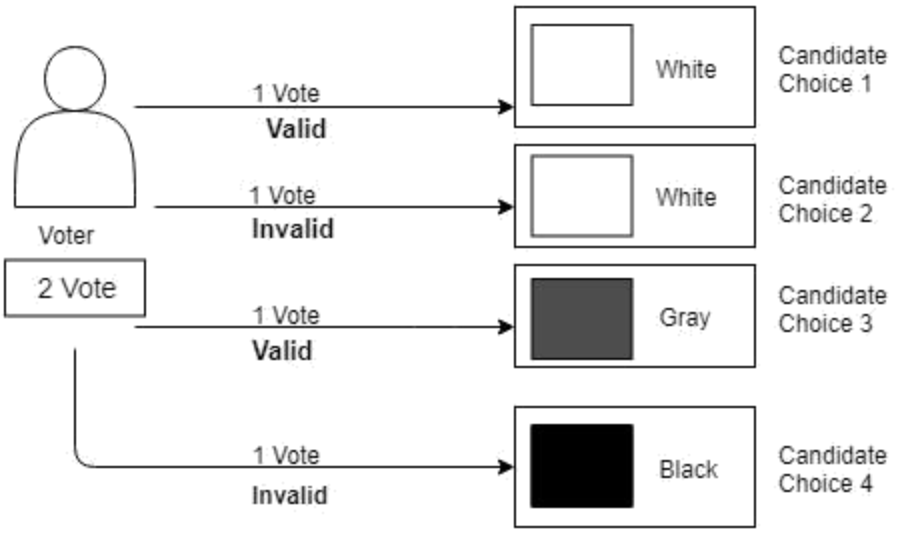

Figure 5. 3: Voter giving multiple votes

5.2 Model Process

5.2.1 Registration

The primary phase of the e-voting system is to register the voter and candidate. The registration process will be authorized and maintained by the government.

5.2.1.1 Voter registration

When a person wants to be registered as a voter, he/she has to give his/her personal information (National Identity card number, Name, Age, Address, and Father's Name). The government miners will receive the information and create a genesis block with the information. Then the person will become eligible for voting and get confirmation. If any person is already registered as a voter in the government database, the government miner will create genesis block for them.

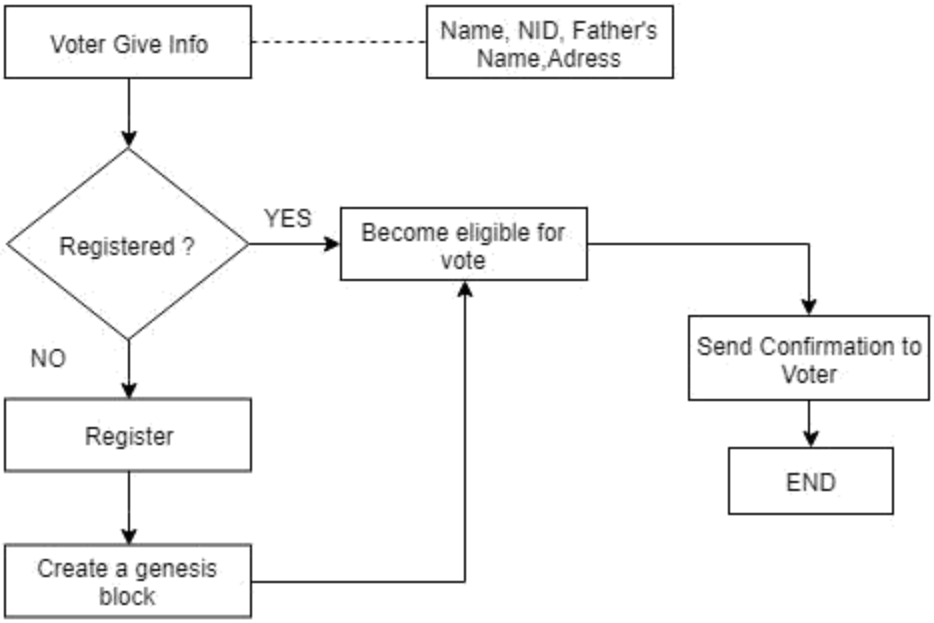

Figure 5. 4: Voter Registration Process

5.2.1.2 Candidate Registration

When a person request to be registered as a candidate he/she has to give his/her personal information(NID number, Name, Age, Address, Party Name, symbol).If the government accept her/his request, the government miner will create a genesis block. Then the person will become a candidate and get confirmation.

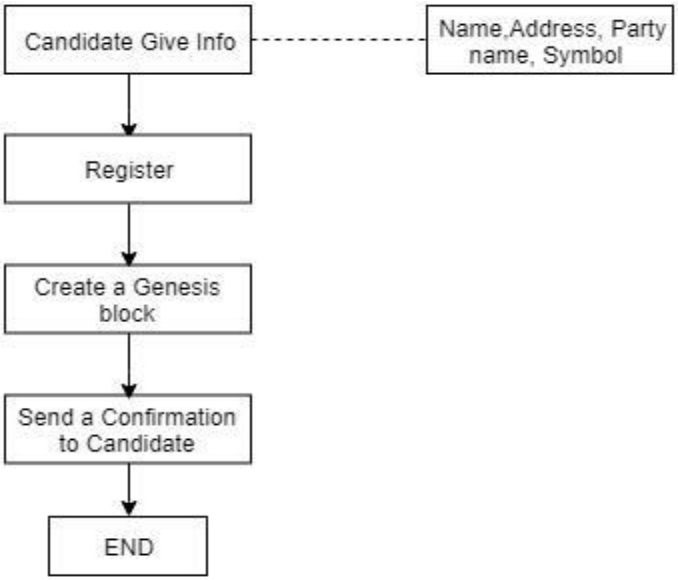

Figure 5. 5: Candidate Registration Process

5.2.2 Request for Vote

On the voting day, when voters will come to the voting station they will give their fingerprint in the fingerprint scanner. Then will get the candidate list represented as a block. Then he or she has to submit their personal details such as NID and their choice from candidates to a peer-to-peer network.

5.2.3 Peer to peer network

In this peer-to-peer network, when miners will get the voter information and their chosen candidate information, they will check if the voter and candidate information is valid or not. If all information is valid send all information to the private miners and if any information is invalid, it will return to the beginning. A voter can try this maximum three times then the voter will be blocked as a fraud voter.

5.2.4 Create a block

When the private miners get all valid information of the voter and candidate then process the vote for the count. They will mine a transaction from voter genesis block to a candidate block and create a hash. After a block is created and depending on the candidate selected, the information is recorded in the corresponding Blockchain. Each block is linked to previously cast vote by hash.

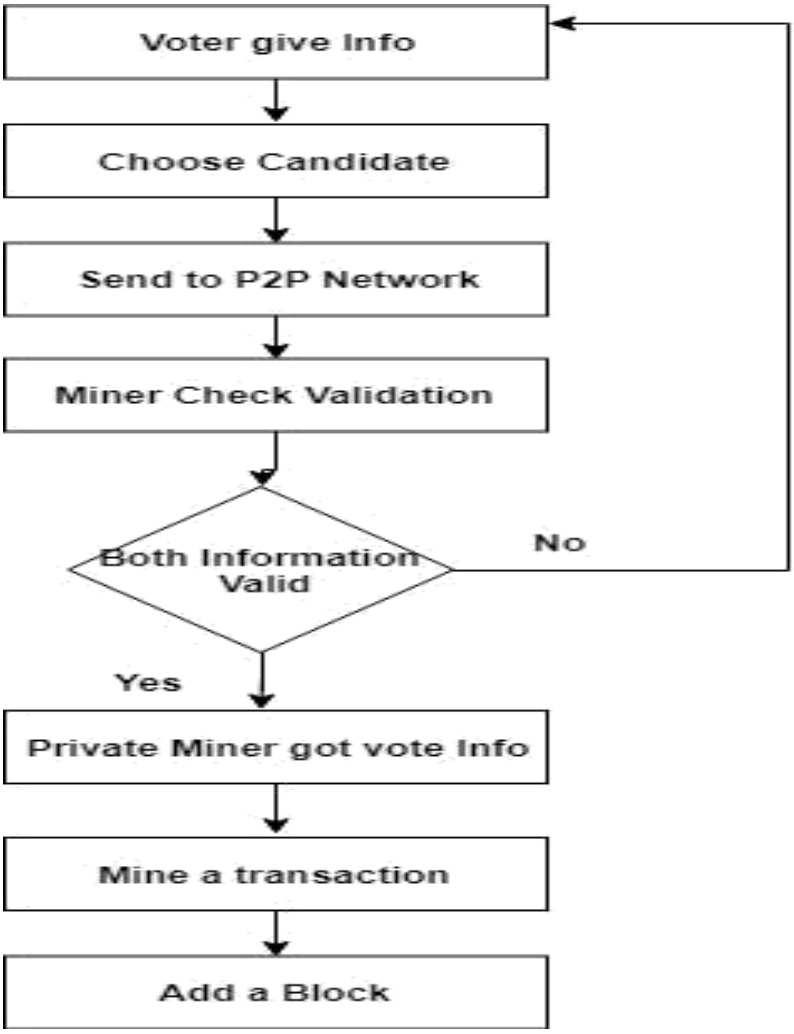

Figure 5. 6 : Voting process

5.2.5 Counting vote

After the voting process ended, the government authority will broadcast vote result based on candidate blockchain. In this counting process, using the public ledger show all the candidate get how many votes and who wins the election.

6. Contribution

In our proposed model, the whole peer to peer network is divided into many ballot center nodes and a central node. There will be a number of private miners assigned on each ballot center. They will have the right to validate the voter information and their candidate choice of that corresponding ballot center. Then they will send the vote to the central node. Whenever any dishonest voter tries to give fraud vote or many votes it will be identified in the in the ballot center. If a fraud vote would directly be sent to the central, it will take lots of time to identify it. So , it will affect the whole voting process.

Notation:

New Difficulty = ND
Old Difficulty = OD
New Target = NT
Old Target = OT

Difficulty is the measure of how difficult it is to find a hash below a given target. For the very first block the difficulty is 1. If, we assume that total number of block is 100 .When miner will first start mine a vote it will take 8 sec. With the increment of the blocks the time will increase a little bit like 10 sec.

So,
Total/Sample Block = 100
New Mining time = 10 Sec
Old Mining time = 8 Sec
Exponent = 1D

Formula 1:

ND = OD × (Total Block × New Mining time) / Sample Block × Old Mining time

=1×(100×10)/(8×100)

=1.25

Formula 2:

NT = OT / ND

=2.69×10^67/1.25

Formula 3:

OT= Coffient × 2^ (8× (exponent – 3))

=2.69×10^67

Because of assigning more miner and divided them into ballot centers and central the time of process a vote will decrease.

Formula 4:

ND = OD × New Block / Sample Block

Formula 5:

Time = (Current Time × Sample Block × Expected Block)/ Expected Miner

However, when the number of expected miners will increase it will decrease the time of processing vote but it will also increase the cost.

Formula 6:

Expected Miner = (Current Time*Sample Block * Expected Block)/

Time [Cost = Expect Miner*Reward]

Future Work

We have proposed a modified e-voting system using blockchain technology. In future, we will implement it.

Conclusion

Electronic voting is a platform that provides a secure and reliable environment for casting vote via the internet network. However the security of the electronic voting system, not enough trustworthy. Blockchain is a distributed public ledger that uses a decentralized peer-to-peer network. We proposed an e-voting system using blockchain that eliminates voter and candidate fraud, serving a transparent record of the votes cast and prevents the fraudulent election. Votes stored on the blockchain is immutable, immediately available and transparent. Therefore, because of using blockchain our e-voting system is more efficient and secure.

References

[1]Hardwick, F. S., Akram, R. N., & Markantonakis, K. (2018). E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. *arXiv preprint arXiv:1805.10258*.

[2]Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018, July). Blockchain-Based E-Voting System. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (pp. 983-986). IEEE.

[3]Jason, P. C., & Yuichi, K. (2017). E-voting system based on the bitcoin protocol and blind signatures. *Information Processing Society (TOM)*, *10*(1), 14-22.

[4]Ellis, S. A Decentralized Oracle Network Steve Ellis, Ari Juels, and Sergey Nazarov.

[5]Ayed, A. B. (2017). A conceptual secure Blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, *93*.

[6]Barnes, A., Brake, C., & Perry, T. (2015). Digital Voting with the use of Blockchain Technology. *Team Plymouth Pioneers–Plymouth University*.

[7]Wu, Y. (2017). An E-voting System based on Blockchain and Ring Signature. *Master. University of Birmingham*.

[8]Eggers, W. D. (2007). *Government 2.0: Using technology to improve education, cut red tape, reduce gridlock, and enhance democracy*. Rowman & Littlefield.

[9]Harrison, T. M., Pardo, T. A., & Cook, M. (2012). Creating open government ecosystems: A research and development agenda. *Future Internet*, *4*(4), 900-928.

[10]Moura, T., & Gomes, A. (2017, June). Blockchain Voting and its effects on Election Transparency and Voter Confidence. In *Proceedings of the 18th Annual International Conference on Digital Government Research* (pp. 574-575). ACM.

[11]Dyba, T., Dingsoyr, T., & Hanssen, G. K. (2007, September). Applying systematic reviews to diverse study types: An experience report. In *Empirical Software Engineering and Measurement, 2007. ESEM 2007. First International Symposium on* (pp. 225-234). IEEE.

[12]McCorry, P., Shahandashti, S. F., & Hao, F. (2017, April). A smart contract for boardroom voting with maximum voter privacy. In *International Conference on Financial Cryptography and Data Security* (pp. 357-375). Springer, Cham.

[13]Wohlin, C. (2014, May). Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th international conference on evaluation and assessment in software engineering* (p. 38). ACM.

[14]Alkharabsheh, K., Crespo, Y., Manso, E., & Taboada, J. A. (2018). Software Design Smell Detection: a systematic mapping study. *Software Quality Journal*, 1-80.

[15]Okediran Oladotun, O., Omidiora Elijah, O., Olabiyisi Stephen, O., Ganiyu Rafiu, A., & Sijuade Adeyemi, A. Towards Remote Electronic Voting Systems.

[16]Okediran, O. O., & Ganiyu, R. A. (2015). A Framework for Electronic Voting in Nigeria. *International Journal of Computer Applications*, *129*(3).

[17]Wang, K. H., Mondal, S. K., Chan, K., & Xie, X. (2017). A review of contemporary e-voting: Requirements, technology, systems and usability. *Data Science and Pattern Recognition*, *1*(1), 31-47.

[18]Gritzalis, D. A. (2002). Principles and requirements for a secure e-voting system. *Computers & Security*, *21*(6), 539-556.

[19]Anane, R., Freeland, R., & Theodoropoulos, G. (2007, July). E-voting requirements and implementation. In *null* (pp. 382-392). IEEE.

[20]Wolchok, S., Wustrow, E., Halderman, J. A., Prasad, H. K., Kankipati, A., Sakhamuri, S. K., ... & Gonggrijp, R. (2010, October). Security analysis of India's electronic voting machines. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 1-14). ACM.

[21]Saltman, R. G. (1978). *Effective use of computing technology in vote-tallying* (No. 500-530). US Dept. of Commerce, National Bureau of Standards: for sale by the Supt. of Docs., US Govt. Print. Off..

[22]Madise, Ü., & Martens, T. (2006). E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. *Electronic voting*, *86*(2006).

[23]Gerlach, J., & Gasser, U. (2009). Three case studies from switzerland: E-voting. *Berkman Center Research Publication No*, *3*, 2009.

[24]Stenerud, I. S. G., & Bull, C. (2012). When reality comes knocking Norwegian experiences with verifiable electronic voting. *Electronic Voting*, *205*, 21-33.

[25]https://www.thedailystar.net/opinion/cybernautic-ruminations/news/the-pros-and-cons-evms-1637551

[26]Vollan, K. (2006). Voting in Uncontrolled Environment and the Secrecy of the Vote. *Electronic Voting*, *2006*, 2nd.

[27]Checkoway, S., Feldman, A. J., Kantor, B., Halderman, J. A., Felten, E. W., & Shacham, H.

(2009). Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage. *EVT/WOTE, 2009*.

[28]Feldman, A. J., Halderman, J. A., & Felten, E. W. (2006). Security analysis of the Diebold AccuVote-TS voting machine.

[29]Gonggrijp, R., & Hengeveld, W. J. (2007). Studying the Nedap/Groenendaal ES3B voting computer.

[30]PRE POLL PREPARATION.https://www.youtube.com/watch?v=WshVmhzTifE

[31]Polling day Preparation.https://www.youtube.com/watch?v=ktMRr79K0JQ

[32]Close Of Poll.https://www.youtube.com/watch?v=KBPAGaEygQo

[33]Laguna, M. A., & Crespo, Y. (2013). A systematic mapping study on software product line evolution: From legacy system reengineering to product line refactoring. *Science of Computer Programming*, *78*(8), 1010-1034.

[34]Novais, R. L., Torres, A., Mendes, T. S., Mendonça, M., & Zazworka, N. (2013). Software evolution visualization: A systematic mapping study. *Information and Software Technology*, *55*(11), 1860-1883.

[35]Abhishek Chakravarty.The Product Manager's guide to the Blockchain—Part 1, 29 November,2018.

https://hackernoon.com/the-product-managers-guide-to-the-blockchain-part-1-fb95dfb7af31

[36]Hashing, 30 November, 2018,

https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/what-is-hashing

