Final Year Project Report



Blockchain based E-Voting System

Bachelor of Science

Computer Science

Submitted by

Muhammad Anus Khan 61842002251

Muhammad Usama Alam 61842002307

Muhammad Ammar Alam 61842002256

Supervised by

Abdullah Raza Lakhan

DEPARTMENT OF COMPUTER SCIENCE

Newport Institute Communications & Economics.

North Campus Karachi

2020

Abstract

Electronic voting (e-voting) is a symbol of modern democracy activities. Due to the high ballot privacy and verifiability, e-voting system has been booming in the recent years.

Particularly, Bitcoin, a digital currency system based on the cryptography, is highly open and transparent for the individual transaction. In other words, anyone can access to the transaction contents via blockchain. Besides, regarding to anonymous way it trades, the transaction of Bitcoin is untraceable.

On account of the pseudonymous of BitCoin address and the openness of the

blockchain, which is consistent with part of e-voting requirement. This paper proposed an e-voting protocol based on blockchain by using the ring signature algorithm. The requirements can be satisfied with ballot-privacy, individual verifiability, eligibility, completeness, uniqueness, robustness, and coercion-resistance.

In order to prove the feasibility of protocol. This design implemented a \_ne web voting

system software through PHP and JavaScript programming languages.

A security analysis, software performance analysis and evaluation are presented in the

last section.

# CERTIFICATE OF COMPLETION

This is to certify that the following students

Muhammad Anus Khan 61842002251

Muhammad Usama Alam 61842002307

Muhammad Ammar Alam 61842002256

Have successfully completed their final year project named

Blockchain based E-Voting System

In the partial fulfillment of the Degree of Bachelor of Science in Computer Science

Signature & Seal of Supervisor

|  |  |
| --- | --- |
| Name: |  |
|  |  |
| Department |  |
|  |  |
| Email |  |
|  |  |
| Mobile No. |  |
|  |  |
| Date |  |

# ACKNOWLEDGEMENT

I would like to thank my supervisor Dr.David Galindo who gave me great help when

doing the dissertation. David help me doing this challenging dissertation with his expert

advice and his patient guidance. He listened to my thoughts and made suggestions and

improvements to my protocol, and \_nally \_nished the dissertation. I would also like to

thank my inspectors David Oswald and Per Kristian Lehre. They gave me great suggestions

to write this paper.

I would like to express my gratitude to my best friend Rujia Li who gave me suggestions

and encouragement to \_nish this dissertation and the software BlockVotes. I would also like

to thank Ruoyu He, Xi Jin and Amy Li who help me to solve the grammar issues of the

whole paper.

Finally, I would like to thank my parents who were always supporting me with their best

wishes.

Table of Contents

[Abstract ii](#_Toc521097670)

[CERTIFICATE OF COMPLETION iii](#_Toc521097671)

[ACKNOWLEDGEMENT iv](#_Toc521097672)

[List of Figures viii](#_Toc521097673)

[List of Tables ix](#_Toc521097674)

[List of Keywords 1](#_Toc521097675)

[1 Introduction 1](#_Toc521097676)

[1.1 Motivation 1](#_Toc521097677)

[1.2 Aim and Objective 1](#_Toc521097678)

[1.3 Outline of the Project 1](#_Toc521097679)

[2 Prototyping 3](#_Toc521097680)

[2.1 Sub Heading 1 3](#_Toc521097681)

[2.2 Sub Heading 2 3](#_Toc521097682)

[2.3 Sub Heading 3 4](#_Toc521097683)

[2.3.1 Sub Sub Heading. 4](#_Toc521097684)

[2.4 Sub Heading4 4](#_Toc521097685)

[2.5 Chapter Summary 6](#_Toc521097686)

[3 Implementation 7](#_Toc521097687)

[3.1 Sub Heading 1 7](#_Toc521097688)

[3.2 Sub Heading 2 7](#_Toc521097689)

[3.3 Sub Heading 3 8](#_Toc521097690)

[3.3.1 Sub Sub Heading. 8](#_Toc521097691)

[3.4 Sub Heading4 8](#_Toc521097692)

[3.5 Chapter Summary 8](#_Toc521097693)

[4 Tools and Environment 9](#_Toc521097694)

[4.1 Sub Heading 1 9](#_Toc521097695)

[4.2 Sub Heading 2 9](#_Toc521097696)

[4.3 Sub Heading 3 10](#_Toc521097697)

[4.3.1 Sub Sub Heading. 10](#_Toc521097698)

[4.4 Sub Heading4 10](#_Toc521097699)

[4.5 Chapter Summary 10](#_Toc521097700)

[5 Conclusion and Future Enhancement 13](#_Toc521097709)

[5.1 Conclusion 13](#_Toc521097710)

[5.2 Future Enhancement 13](#_Toc521097711)

[References 14](#_Toc521097712)

[Appendix – A: User Manual 15](#_Toc521097713)

[Appendix – B: Coding 16](#_Toc521097714)

List of Figures

[**Figure 2.1:** Title of Figure A 4](#_Toc521097715)

List of Tables

[Table 2.1: Title of the table 5](#_Toc521097716)

[Table 2.2: Title of the table 5](#_Toc521097717)

# List of Keywords

AES – Advanced Encryption Standard

CSA - Cloud Security Alliance

Trusted Computing

IoT – Internet of Think

TPM – Trusted Platform Module

AEGIS – A Fast Authenticated Encryption Algorithm

# Introduction

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.

E-voting, a new substantial online voting system which is structured on cryptography

technique, has been gradually implemented and emphasised by people. The system supports full-function online voting by general household devices, and the entire polling results will be counted automatically and anonymously. Compared with traditional voting, electronic voting is a more economic system addresses on transparency and impartiality.

As e-voting system mainly relies on the internet platform. The crucial challenge for

e-voting is the significant security risks it might cause. In order to reduce risks, in the past

40 years, various protocols related to the ballot-privacy, individual verifiability, eligibility,

completeness, fairness, uniqueness, robustness, universal verifiability and receipt-freeness

have been widely proposed. Besides, the published protocols have implemented a variety

of technologies, such as blind signature, ring signature, homomorphic encryption, Mix-Net,

zero knowledge proof, etc. In particular, the application of e-voting in digital currency

has become gradually maturity nowadays.

Based on the common security requirements of participants, this paper proposed a

blockchain-based protocol associated with the priorities of the voter-privacy, verifiability,

eligibility, completeness, uniqueness, robustness, and coercion- resistance.

A Blockchain Voting software has also been made to verify the feasibility of this protocol, by implementing a real-life online voting website, which allows participants to vote and view the results easily.

## Motivation

In 2008, the founder of Bitcoin S.Nakamoto published a paper to specify a cryptocurrency system based on the peer-to-peer network. The Bitcoin has changed the traditional

way of the cash payment system. With the development of the Bitcoin. Blockchain is a hashing algorithm technology has aroused the attention of people. The blockchain is a public ledger, all individuals can synchronize the latest ledger into local and they have no permission to tamper the content of the public ledger.

To distinct various blockchain, there are two categorizations of the blockchain. One

is classi\_ed by the requirement of the network nodes to the veri\_cation process.

\_ Permissionless blockchain: No central service or authority is required to compute

during the veri\_cation process. Usually, this computational process happens in the

device of anyone.

\_ Permissioned blockchain : There is a central network used for con\_rming the

veri\_cation nodes.

Another one is classified by the publicity of the blockchain.

Public blockchain: Anyone in the world can read, download, broadcast the trans-

action of the blockchain.

Private blockchain: The blockchain only belongs to the individual, government or an organization which is not public. Since the birth of the blockchain, the blockchain has the properties of decentralization,

decentralized trust, common maintenance, data reliability, privacy protection. It has been unprecedented attention and its development is very rapid. The blockchain will use consensus algorithm to create a new transaction unique identifier. A new block is

generated by the consensus algorithm, which generates a new block by calculating the hash

value of the block header it will be added to the

blockchain database.

## Aim and Objective

Our e-Voting or Blockchain Voting solution will include four main requirements that can be illustrated as shown below:

**Authentication:** Only registered people to vote can cast a vote. Our system will not support a registration process. Registration usually requires verification of certain information and documents to comply with current laws, which could not be done online in a secure manner.

**Anonymity:** The e-Voting system should not allow any links between voters’ identities and ballots. The voter has to remain anonymous during and after the election.

**Accuracy:** Votes must be accurate every vote should be counted and can’t be changed duplicated or removed.

**Verifiability:** The system should be verifiable to make sure all votes are counted correctly. Beside the main requirement, our solution supports mobility, flexibility, and efficiency.

## Outline of the Project

This report contains 5 chapters.

Chapter 1 is the introduction of the problem of its related technologies.

Chapter 2 is the prototyping of the project. This chapter detailed the properties and

requirements of the e-voting scheme and other technique or algorithm used in the protocol.

Chapter 3 is the most important part of this report. This chapter indicates the

whole design scheme of the implementation.

Chapter 4 is the tools and environment of the protocol. By creating an application named the tools and technology to use in this project.

Chapter 5 is the conclusion of the proposed protocol and discussed the future work.

# Prototyping

This chapter …. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …...

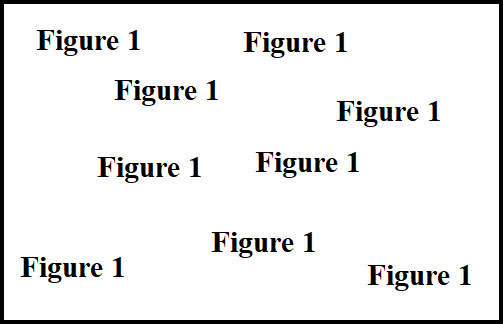
## Sub Heading 1

In the …. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …...

## Sub Heading 2

In the …. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. ….. are mention in Figure 2.1.

The …. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …...

**Figure 2.1:** Title of Figure A

## Sub Heading 3

Let …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. .

### Sub Sub Heading.

In …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. .

## Sub Heading4

As ….. …. …… …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. ……, mention in Table 2.1. Beside ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. ……on in Table 2.2.

Table 2.1: Title of the table

|  |  |
| --- | --- |
| **Option** | **Description** |
| Option 1 | … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … |
| Option 2 | … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … |
| Option 3 | … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … |

Table 2.2: Title of the table

|  |  |
| --- | --- |
| **New Security Risks** | **Description** |
| Option 1 | … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … |
| Option 2 | … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … … … … … …. …. …. .. … … |

## Chapter Summary

Chapter 2 ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. ……

# Implementation

The e-voting system or online voting has been designed using the above protocol named Blockchain Voting. The system will have the properties of ballot privacy, individual verifiability, eligibility and etc. When developing this project the system should consider the basic models and the properties of the e-voting.

In general, Blockchain Voting allows voters and candidates to register in the system. The voter can vote in the system and verify the result of voting using CNIC. The administration of Blockchain Voting is Election Authority.

The Blockchain Voting system should have the models as follows.

1. User Model is the logic of logging in.

2. Election Model is a model for Election Authority.

3. Candidate is a model for the candidate registration.

4. Voter is a model for voter registration.

5. Vote is a model for voter cast own vote.

6. Result is model for tallying a candidate votes.

## Blockchain Voting Model

The Blockchain Voting has been developed by the PHP programming language. To make the logic clearly, the MVC framework named Laravel has been used to route the page. The Laravel/Illuminate used to Data Access Object (DAO) and the Blade templating engine used to connect the front-end page with the back-end. To manage the dependencies, the Composer has been used as the dependency management tool. The system is developed with the database MYSQL and the Git is used to version control of the whole project.

## User Model

In the …. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. ….. are mention in Figure 2.1.

The …. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …...

## Sub Heading 3

Let …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. .

### Sub Sub Heading.

In …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. .

## Sub Heading4

As ….. …. …… …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. ……,

## Chapter Summary

Chapter 3 ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… …..

.

# Main Heading 4

This chapter … …. … … …. . … …. … … …. . … …. … … …. . … …. … … …. . … …. … … …. . … …. … … …. . … …. … … …. . … …. … … …. . … …. … … …. . … …. … … …. . … …. … … …. ..

## Sub Heading 1

In the …. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …...

## Sub Heading 2

In the …. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. ….. are mention in Figure 2.1.

The …. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …...

## Sub Heading 3

Let …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. .

### Sub Sub Heading.

In …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. .

## Sub Heading4

As ….. …. …… …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. ……,

## Chapter Summary

## Chapter 4 ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… …..….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. …… ….. …..…. …. ….. …. ……

# Conclusion and Future Enhancement

This paper has mainly explored the basic concept of e-voting and blockchain by specifying blockchain encryption algorithm.

The entire protocol development process has also been described from the transitional

software development perspective, such as how the blockchain transaction happens and some mechanism analysis of the voting system.

Finally, the paper evaluates the performance and potential security risk for the protocol,

further limitations have been discussed at the end.

## Conclusion

Even though the generated protocol satisfied with the properties of ballot-privacy, individual, verifiability, eligibility, completeness, uniqueness, robustness, and coercion-resistance. However, it does not fulfill the needs of complete fairness and receipt-freeness.

The primary advantage of this protocol is to guarantee the authenticity of electronic

voting. As every ballot will be broadcasted to the blockchain once voting starts. Moreover,

as blockchain is a decentralized public ledger, ballots result is represented in a real time

and cannot be modified by an individual, which satisfied the design of open-auditing.

Blockchain Voting confirmed the feasibility of the proposed protocol in disguise. The purpose of selecting local databse table as the blockchain network, primarily rests with its free of charge and ease when comparing with Bitcoin and Ethereum. Beyond that, the high similarity degree to BitCoin network structure is another principal reason to appointed to broadcast voting result.

## Future Enhancement

Blockchain based e-voting protocol still have a large room for improvement, such as improving its transparency, fulfill unconsummated functions within current status.

As for Blockchain Voting, functions switching to networks like BitCoins and LiteCoin can be appended. In addition, accomplishment multiple voting within one vote can be an ideal topic for further study.

# References

[1] Baudron, O., Fouque, P.-A., Pointcheval, D., Stern, J., and Poupard, G.

Practical multi-candidate election system. In Proceedings of the twentieth annual ACM

symposium on Principles of distributed computing (2001), ACM, pp. 274{283.

[2] Benaloh, J., and Tuinstra, D. Receipt-free secret-ballot elections. In Proceedings

of the twenty-sixth annual ACM symposium on Theory of computing (1994), ACM,

pp. 544{553.

[3] Bitcoin-Wiki. Conation - bitcoin wiki. https://en.bitcoin.it/wiki/

Confirmation.

[4] bitcoinfees.21.co. Predicting bitcoin fees for transactions. https://bitcoinfees.

21.co/.

[5] Card, D., and Moretti, E. Does voting technology a\_ect election outcomes? touch-

screen voting and the 2004 presidential election. The Review of Economics and Statistics

89, 4 (2007), 660{673.

[6] Cetinkaya, O., and Cetinkaya, D. Towards secure e-elections in turkey: require-

ments and principles. In Availability, Reliability and Security, 2007. ARES 2007. The

Second International Conference on (2007), IEEE, pp. 903{907.

[7] Chaum, D. L. Untraceable electronic mail, return addresses, and digital pseudonyms.

Communications of the ACM 24, 2 (1981), 84{90.

[8] Christian Schaupp, L., and Carter, L. E-voting: from apathy to adoption. Jour-

nal of Enterprise Information Management 18, 5 (2005), 586{601.

[9] Cohen, J. D., and Fischer, M. J. A robust and verifiable cryptographically secure

election scheme. Yale University. Department of Computer Science, 1985.

[10] Cranor, L. F., and Cytron, R. K. Sensus: A security-conscious electronic polling

system for the internet. In System Sciences, 1997, Proceedings of the Thirtieth Hawaii

International Conference on (1997), vol. 3, IEEE, pp. 561

[11] Czepluch, J. S., Lollike, N. Z., and Malone, S. O. The use of block chain tech-

nology in di\_erent application domains. The IT University of Copenhagen, Copenhagen

(2015).

[12] DeMillo, R. A., Lynch, N. A., and Merritt, M. J. Cryptographic protocols. In

Proceedings of the fourteenth annual ACM symposium on Theory of computing (1982),

ACM, pp. 383{400.

[13] Fraunholz, B., and Unnithan, C. E-governance: enabling the french web 2.0

revolution? In Foundations of e-government (2007), [International Conference on E-

Governance] Academic Publishing, pp. 344{359.

[14] Fujioka, A., Okamoto, T., and Ohta, K. A practical secret voting scheme for

large scale elections. In International Workshop on the Theory and Application of

Cryptographic Techniques (1992), Springer, pp. 244{251.

[15] Hirt, M., and Sako, K. Ecient receipt-free voting based on homomorphic encryp-

tion. In Advances in CryptologyEUROCRYPT 2000 (2000), Springer, pp. 539{556.

[16] Jason, P. C., and Yuichi, K. E-voting system based on the bitcoin protocol and

blind signatures. TOM 10, 1 (2017), 14{22.

[17] Jonker, H., Mauw, S., and Pang, J. Privacy and veri\_ability in voting systems:

Methods, developments and trends. Computer Science Review 10 (2013), 1{30.

[18] Juels, A., Catalano, D., and Jakobsson, M. Coercion-resistant electronic elec-

tions. Towards Trustworthy Elections 6000 (2010), 37{63.

[19] kiwi. Bitcoin testnet sandbox. https://testnet.manu.backend.hamburg/faucet.

[20] Lee, K., James, J. I., Ejeta, T. G., and Kim, H. Electronic voting service using

block-chain. The Journal of Digital Forensics, Security and Law: JDFSL 11, 2 (2016)

# Appendix – A: User Manual

To build and run the project, the running environment is required as follows.

* Mac OS X or Linux or Windows
* Apache 2.4.27 or Nginx 1.12.1
* MySQL 5.7.19 (at least 5.4)
* PHP 7.2
* Composer
* Laravel 7.x (PHP framework)
* Mailtrap (mailing service for email testing purpose)

The project has been uploaded to the git repository. To download the project,

please run the following command.

git clone <https://github.com/AmmarAlam/OnlineVoting.git>

composer install

php artisan key:generate

php artisan serve (for running app to local server)

To run the system, some critical but private information are not uploaded by gitignore

file. Please add the .env file into the root of this project directory.

DB\_CONNECTION=mysql

DB\_HOST=127.0.0.1

DB\_PORT=3306

DB\_DATABASE=online\_voting

DB\_USERNAME=root

DB\_PASSWORD=

MAIL\_MAILER=smtp

MAIL\_HOST=smtp.mailtrap.io

MAIL\_PORT=2525

MAIL\_USERNAME=username

MAIL\_PASSWORD=password

MAIL\_ENCRYPTION=tls

MAIL\_FROM\_ADDRESS=your email address

MAIL\_FROM\_NAME="${APP\_NAME}"

# Appendix – B: Coding