



# A Bitcoin Based Secure Electronic Voting System

by

*DMGK Wimalarathne (168278C)*

A thesis submitted to University of Moratuwa in partial fulfilment of the requirements for  
the  
Master of Computer Science, *Specialized in Security Engineering*

Department of Computer Science & Engineering  
University of Moratuwa, Sri Lanka

*February 2020*



# A Bitcoin Based Secure Electronic Voting System

by

*DMGK Wimalarathne (168278C)*

A thesis submitted to University of Moratuwa in partial fulfilment of the requirements for  
the  
Master of Computer Science, *Specialized in Security Engineering*

Department of Computer Science & Engineering  
University of Moratuwa, Sri Lanka

*February 2020*

# Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text. Also, I hereby grant to University of Moratuwa the nonexclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

---

DMGK Wimalarathne:

---

Date

Approved by:

---

Lt Col Dr Chandana D. Gamage  
Department of Computer Science and Engineering  
University of Moratuwa

---

Date

# Copyright Statement

I hereby grant the University of Moratuwa the right to archive and to make available my thesis or dissertation in whole or part in the University Libraries in all forms of media, subject to the provisions of the current copyright act of Sri Lanka. I retrain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

---

DMGK Wimalarathne:

---

Date

I have supervised and accepted this thesis/dissertation for the award of the degree.

---

Lt Col Dr Chandana D. Gamage  
Department of Computer Science and Engineering  
University of Moratuwa

---

Date

# Abstract

Over the last few decades, several electronic systems have been proposed and implemented to as attempt to replace the traditional paper-based voting systems. Even though the e-voting system are more efficient and convenient than the traditional voting systems, it was identified that they should meet the specific security goals, such as authentication, anonymity, availability, and integrity up to the same level that is provided by manual systems.

If the voting system is centralized and controlled by one party, they may have the opportunity to manipulate the votes thereby compromise the integrity. In this paper we propose a Bitcoin based online transaction system to provide a solution to the identified integrity related threats in an electronic voting system.

We have taken an existing, well-proven, robust, scalable e-cash system as the basis for implementing the e-voting system. A comprehensive list of properties and features expected of an e-cash system and e-voting system have been analysed in the paper to show how different properties/features of an e-voting system map to an e-cash system. We have shown how various functionalities of a bitcoin-like system directly provide the required features/properties of an e-voting system. Also, we have shown how various functionalities of a bitcoin-like system can be modified and/or adapted to provide some of the other required features/properties of an e-voting system.

Based on the outcomes of the methodology, we discuss how the complete e-voting system is going to be built on blockchain technology. Further, we discuss how strongly various security and performance requirements are being met in the research work related to the proposed e-voting system.

# Acknowledgements

I would like to express profound gratitude to my supervisor, Dr. Chandana Gamage, for his invaluable support by providing relevant knowledge, materials, advice, supervision, and useful suggestions throughout this research work. His expertise and continuous guidance enabled me to complete my work successfully.

I am grateful for the support and advice given by the CSE Lecturer panel and the MSc course coordinators, by encouraging continuing this research till the end. Further I would like to thank all my colleagues for their help on finding relevant research material, sharing knowledge and experience and for their encouragement.

I am as ever, especially indebted to my parents and sister for their love and support throughout my life.

# Abbreviations

ATM - Automated Teller Machine  
BIP - Bitcoin Improvement Proposal  
CPU - Central Processing Unit  
DRE - Direct Recording Electronic  
DVBM - Digital Vote-by-Mail  
E2E - End-to-end  
ECC - Elliptic Curve Cryptography  
ECDSA - Elliptic Curve Digital Signature Algorithm  
NFC - Near-field communication  
P2PKH - Pay-To-Public-Key-Hash  
PIN - Personal Identification Number  
PKI - Public Key Infrastructure  
PRNG - Pseudo Random Number Generator  
QR code - Quick Response code  
SHA - Secure Hash Algorithm  
TLS - Transport Layer Security  
URI - Uniform Resource Identifier  
VVPAT - Voter Verified Paper Audit Trail

# Table of Contents

<b>Declaration</b>	<b>v</b>
<b>Copyright Statement</b>	<b>vi</b>
<b>Abstract</b>	<b>vii</b>
<b>Acknowledgements</b>	<b>viii</b>
<b>Abbreviations</b>	<b>ix</b>
<b>Table of Contents</b>	<b>x</b>
<b>List of Tables</b>	<b>xiii</b>
<b>List of Figures</b>	<b>xiv</b>
<b>1. Introduction</b>	<b>1</b>
1.1. Background.....	1
1.2. Research Problem .....	2
1.3. Objective.....	3
1.4. Organization of the Thesis .....	3
<b>2. Literature Review on e-Voting and e-Cash Systems</b>	<b>5</b>
2.1. Existing Voting Systems .....	5
2.1.1 Paper Ballots.....	5
2.1.2 Electronic Voting Systems .....	6
2.1.3 Internet Voting.....	6
2.2. Related Work.....	7
2.2.1. Voting: What Has Changed, What Hasn't, & What Needs Improvement .....	7
2.2.2. Security considerations for remote electronic voting .....	8
2.2.3. On the notion of 'software independence' in voting systems .....	9
2.2.4. Voting Systems Audit Log Study.....	9
2.2.5. An Introduction to Electronic Voting .....	9
2.2.6. Security Analysis of the Estonian Internet Voting System.....	10



2.2.7.	Attacking the Washington, D.C. Internet Voting System.....	13
2.2.8.	End-to-end voting systems.....	15
2.2.9.	Blockchain based e-voting systems.....	15
2.2.10.	Summary .....	16
<b>3.</b>	<b>Methodology for Designing Bitcoin Based Electronic Voting System</b>	<b>18</b>
3.1.	Introduction.....	18
3.2.	List of Properties and Features Expected of an e-cash System.....	19
3.3.	Properties and features of Bitcoin.....	20
3.3.1.	Transferability .....	20
3.3.2.	Anonymity.....	23
3.3.3.	Authenticity and Tamper-Resistance.....	23
3.3.4.	Unforgeability.....	24
3.3.5.	Double spending avoidance/detection.....	24
3.3.6.	Date/Time attachability.....	25
3.3.7.	Divisibility.....	25
3.3.8.	Portability .....	26
3.4.	List of Properties and Features Expected of an e-voting System.....	27
3.5.	Mapping the properties/features of an e-voting system to an e-cash system.....	28
3.6.	Adopting Functionalities of a Bitcoin-like System.....	29
<b>4.</b>	<b>System Design and Implementation</b>	<b>33</b>
4.1.	Introduction.....	33
4.2.	General Assumptions .....	33
4.3.	Pre-election setup.....	34
4.4.	Election.....	38
4.5.	Tabulation .....	39
4.6.	System Architecture.....	40
4.7.	Proof of Work Implementation .....	41
4.8.	Summary .....	43
<b>5.</b>	<b>System Evaluation and Performance Review</b>	<b>44</b>
5.1.	Introduction.....	44
5.2.	Evaluation of Security Requirements of an e-Voting System.....	44
5.2.1.	Authorization.....	44
5.2.2.	Anonymity.....	44
5.2.3.	Tamper-resistance.....	45
5.2.4.	Restriction of attempts .....	45
5.2.5.	Prevention of impersonation .....	46
5.2.6.	Individual Verifiability.....	46
5.2.7.	Universal Verifiability.....	46
5.3.	Evaluation of the Protocols and Algorithms.....	46

5.3.1.	Random Number Generation .....	46
5.3.2	Elliptic Curve Digital Signature Algorithm and secp256k1 Curve	47
5.3.3	Private Key Management .....	47
5.4.	Evaluation of the Performance.....	48
5.5.	Summary .....	48
<b>6.</b>	<b>Conclusions</b>	<b>50</b>
	<b>References</b>	<b>51</b>

# List of Tables

2.1 Attacks on the Diebold AccuVote-TS 4.3.1 system.....	16
3.1 Similar Features in e-cash and e-voting systems.....	28
5.1 Performance Data of the e-Voting System.....	48

# List of Figures

2.1	AccuVote TS and TSX touch screen DRE voting machines.....	6
2.2	I-voting client used by Estonians to cast votes online [8] .....	7
2.3	The overview of the i-voting system.....	11
2.4	(a, b, c) i-Voting system protocols .....	12
2.5	Network architecture of the Washington, D.C. Internet Voting System .....	13
2.6	Screenshots of the Washington, D.C. Internet Voting System.....	14
2.7	Zcash based e-voting system .....	16
3.1	Creating a P2PKH Public Key Hash to Receive Payment [21].....	20
3.2	Example Base 58 Encoding Algorithm [24].....	22
3.3	QR Codes Containing a Bitcoin URI .....	22
3.4	Only the Bitcoin Address is Required to Make a Payment.....	23
3.5	Transaction Data is Signed with Bob's Private Key.....	24
3.6	Bitcoin Transactions .....	25
3.7	Each Transaction Spends Previously Received Satoshis .....	26
3.8	Bitcoin Payment Protocol Proposed in BIP 70.....	31
4.1	Pre-election Setup.....	34
4.2	Conversion from ECDSA Public key to Address. Source: bitcoin.it.....	36
4.3	Pre-election Transactions .....	37
4.4	The e-Voting Blockchain.....	37
4.5	The Election.....	38
4.6	The Voting Transactions.....	39
4.7	Sample Vote Balance Recorded to a Candidate's Address.....	39
4.8	Bitcoin Based e-Voting System Architecture.....	40
4.9	App syncs with the network(left) The initial vote balance is 0 (right) .....	41
4.10	Voter can request votes from the Election Committee.....	42
4.11	The spendable vote balance is reflected in the voter's wallet .....	42
4.12	Confirmed vote total recorded to candidate's address.....	43
5.1	Anonymity Verification.....	45