# 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 Date
Department of Computer Science and Engineering
University of Moratuwa

# 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 Date
Department of Computer Science and Engineering
University of Moratuwa

# 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

# List of Tables

# List of Figures