Block Chain

Research

Project

# 

Student Number: B00131083

Name: David Long

Lecturer: Mark Cummins

Module: Secure Communications & Cryptography

Submission Date: 19th Dec 2020

Table of Contents

[Introduction 1](#_Toc57838984)

[What is Blockchain 1](#_Toc57838985)

[Base Requirements for a voting system 2](#_Toc57838986)

[Literature Review 2](#_Toc57838987)

[Appendix A 3](#_Toc57838988)

[Appendix B 3](#_Toc57838989)

[Appendix C 3](#_Toc57838990)

# Introduction

This paper is going to explore the application of Blockchain technology to the very controversial area of voting. The reason for this is sparked by current world issues, voting has been at the forefront of current global news in recent years with a number of different scandals Cambridge Analytica/ Facebook for one[1]. This led to many questions around the security of elections. It has also led to a lot of research into different systems and even Blockchain been adapted for online voting[2], but has it been done in a controlled and secure manner. This paper seeks to see if this is could be implemented in a way that can either reduce or eliminate security flaws in an online voting systems, while providing voter anonymity mitigating common attacks.

As we know Blockchain is rather secure thanks to the style of encryption and method used to create a chain, this will be explained further in the following section. The concept is to use Blockchain and the security that comes with it to provide safer way to vote online, while mitigating the more common attacks like DoS, vote tampering or buying. Blockchain is perfectly suited to such an application as, not only is it secure but it can also provide voter anonymity. With the peer-to-peer shared ledger providing a perfect way to mitigate DoS attacks and the immutableness of a created block eliminates the chances of vote tampering. This however is an area that has been addressed and researched in recent years, but has sparked very different opinions[3].

## What is Blockchain

Blockchain or what we know now to Blockchain all started with, Stefan Konst[4]. He was the man that spawned the concept of Blockchain. He first published a paper that delivered his theory of cryptographically secured chains[5]. This was later picked up by either an individual or a group of developers, under the guise of Satoshi Nakamoto. Though his name completely ubiquitous with Bitcoin, the physical entity eludes us and has never been found. Leading people to believe that it is a pseudonym for a different person or group of people[6].

Since its birth late in the year 2000[2], adapted and implemented with the crypto currency Bitcoin[7] in the year 2008[7]. It has been adapted into many areas, everything from crypto currencies[8], supply chain management[9] right through to health care[10]. What Blockchain is then, it’s an immutable backword linked chain of encrypted blocks where each block is encrypted using the last block[11]. Blockchain is a system of recording information in a way that makes it difficult or impossible to alter, corrupt or steal the data[12]. A Blockchain is essentially a ledger, just digital and far more secure than a regular ledger[13].

There are three types of Blockchain, public, such as Bitcoin and Ethereum[14]. This means that the code is open source and it is duplicated and distributed across the entire network of devices on that Blockchain[15]. Then there is private Blockchain, with the most widely known being Ripple[16] and Hyperledger[17]. These restrict who has access to the Blockchain and who can add data to it, most commonly used in business [18]. Every block within a chain contains a number of transactions[11], every time a new transaction takes place on the Blockchain, a record of that specific transaction is added to every ledger on the distributed system[13]. The decentralised database managed by multiple participants is known as Distributed Ledger Technology[13]. Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash[19].

## Base Requirements for a voting system

The core fundamentals of any election is clear from the research conducted and outlined in[20], they are as follows.

* Ballot secrecy
* Software independence
* Voter-verifiable ballots
* Contestability
* Auditing.

What this means is that votes must be cast as intended, counted as cast and verified as counted. There are a number of ways that we can address the aforementioned issues, but there will always be an attack surface when dealing with such a desirable target for sophisticated adversaries. This paper will not address all of the issues as it is beyond the scope, it will focus on the most prevalent issues that have arisen to date.

# Literature Review

There are many instances where Blockchain has been implemented with massive success[21], electronic voting is one however that has sparked a lot of debate as to whether or not it is safe[3]. A paper released back in May of 2017 by the International Journal of Network Security and it’s Apps(IJNSA) stated that Blockchain is perfectly suited to an electronic or internet voting system[22]. There have been quite a few attempts at an implementation of a safe system, one of the first to do so was Estonia[23], this instance was not using Blockchain technology[15].

Previous systems have used other methods for encryption, like that used in the Norwegian system[24]. Developed by Scytl[25], the system while it worked as intended the ever looming threat or possibility of nation-state sized attacks or other external threats led to the Norwegian Government discontinuing the project due to similar concerns[26]. Roll forward a couple of years and we have the adoption of Blockchain for electronic/internet voting proposed and implemented in a number of different ways[27]–[32]. According to a draft paper published just last week[20], none address the main underlying concerns with the security of online or electronic voting[20]. The paper published was titled *“Going from Bad to Worse: From Internet Voting to Blockchain Voting”* , given that there are a number of points of concern outlined in the paper, there are a number of security concerns to consider. This being highlighted, the conclusion of the aforementioned paper while stating there is no current implementation that satisfies all the constraints/requirements for an election. It does pose a number points to address, for a better understanding of this we need to consider the base requirements of an election as outlined in the previous section.

In the different application researched for this paper, none of the applications of Blockchain recognised or address the issues that any instance of a block chain voting system is still open to a number of vulnerabilities as outlined in[20]. The main issues that has yet to be addressed is the inherent risk of allowing voters to use their own end device, there also no guarantee that the end device is secure.

This issue is addressed in the aforementioned document and it is a valid argument, one that could be overcome with the correct implementation of the system. The main points that were outlined as the points of failure for the previously proposed systems, all can be addressed. To address all the issues that are outlined in [20] is beyond the scope of this paper, instead this paper will look to provide a safe implementation of Blockchain as a means of voting, while highlight possible solutions to the other areas that are deemed a security pitfall with electronic voting.

The first issue is user authentication, this is something that should not be handled by anyone other an impartial or unbiased body, the next issue is making sure that voters can cast a vote and remain anonymous, while being able to see if the vote was counted as cast and verifiable. There needs to be some sort of user handling, Let us assume, that the user has selected the wrong candidate by mistake

# Appendix A

# Appendix B

# Appendix C