KANTIPUR ENGINEERING COLLEGE

(Affiliated to Tribhuvan University)

Dhapakhel, Lalitpur

[Subject Code: CT755]

A MAJOR PROJECT PROPOSAL ON

DIGITAL VOTING SYSTEM USING BLOCKCHAIN

Submitted by:

Digbijaya Shakya	[16/BCT/2071]
Manjik Shrestha	[58/BCT/2071]
Rahul Deshar	[65/BCT/2071]
Siddhi Kiran Bajracharya	[78/BCT/2071]

Submitted to:

Department of Computer and Electronics Engineering

December, 2017

DIGITAL VOTING SYSTEM USING BLOCKCHAIN

Submitted by:

Digbijaya Shakya	**[16/BCT/2071]**
Manjik Shrestha	**[58/BCT/2071]**
Rahul Deshar	**[65/BCT/2071]**
Siddhi Kiran Bajracharya	**[78/BCT/2071]**

Submitted to:

Department of Computer and Electronics Engineering

Kantipur Engineering College

Dhapakhel, Lalitpur

December, 2017

COPYRIGHT

ABSTRACT

Voting is one of the important right that helps to present our opinion in our society. When it comes to the countrys election the issue of security on counting those votes is paramount. Therefore, our project intends to aid in security of the voting system by bringing in an blockchain technology to secure those votes. By design, a blockchain is a decentralized and distributed digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network. In our system voters are supposed to enter their unique voter id to issue their vote and they can observe instant result of their voting.

Keywords– Immutable Voting System, Block Chain, Secure Voting, Decentralized network

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Background

Paper-based voting has been around for a long time. The voters then use paper ballot to mark out their preference. In the time where technology is overtaking everything, it was obvious that there might be a time when we would use digital voting technology or electronic voting. Digital voting technology is far better in comparison than the traditional paper-based voting systems. Its not only transparent, accurate and secure, but it also generates faster results as computer is used instead of humans to count votes. For digital voting, a number of machines are placed which are connected to a server. The server usually maintains a database to store the vote counts. This data then can be retrieved in order to count the number of votes. Since, the counting is done by machines, there is zero percent chance that the votes will be miscounted. This is only possible because of advancement in the field of computer science and technology. Digital voting is arguably the most difficult upgrade, as this technology involves the core of the entire electoral process: the casting and counting of votes. Digital voting greatly reduces direct human control and influence in this process, and provides an opportunity to solve some old electoral problems, but it also introduces a whole range of new concerns.

Estonia was the first in the world to adopt an electronic voting system for its national elections. Soon after, electronic voting was adopted by Switzerland for its state-wide elections, and by Norway for its council election. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity.

An e-Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voters ballot from being tampered with. A core concept of bitcoin, known blockchain, has allowed us to make the digital voting procedure more secure. Blockchain is a continuously growing list of records, called blocks, that are made secure using cryptography.

Blockchains offers a way for people who do not know or trust each other to create a record of who owns what that will compel the assent of everyone concerned. It is a way of making and preserving truths[1].

1.2 Problem Statement

As we have seen in this previous election, the voting system was a mess. The unreliability to properly count the votes is not only shameful, but also unprofessional. The vote counting procedure is always in debate because of this. We need some reliable way to count the votes.

Introduction of Digital Voting System introduces new issues, there is always a risk that someone might hack the database and turn the results to the benefit of his/her favored party. Because of such risks (and some other reasons), the e-Voting system was boycotted almost everywhere.One of the main critics of both Estonian and Norwegian electronic voting systems is the secrecy of critical parts of the code. The script to post the vote on the Estonian I-Voting system is made close what raise questions about transparency. An open source e-voting system is a must for a trusted election.

The system we are proposing could resolve these problems. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data.By design, blockchains are inherently resistant to modification of the data[2].

1.3 Objectives

The main objectives for developing our project are :

- To provide the result of the election faster.
- To reduce the chance of external influence on voting data.
- To achieve higher amount of security than digital voting system.

1.4 Project Features

Some features of our projects are :

- Instant Poll result.
- Higher level of security than any existing voting system.
- Immutable i.e. votes cannot be altered.
- Ledger of the votes is distributed and synchronized across network.

1.5 Feasibility Analysis

The feasibility analysis of our project is divided into three category :

1.5.1 Economic Analysis

Election is one of the most important event of the country. For paper-based voting system government has to waste a lot of money for creating paper ballot for every election and pay hefty sum to count those votes. Our project needs new hardware but doesnt require any any third party softwares. The government can invest in this project only once and will only require some maintenance charges which will be worth it considering the level of security it provides.

1.5.2 Technical Analysis

Our project does not require high end computers. Equipments available currently in the market is adequate for the use in our system and for wide implementation of our project. Our project needs new hardware but doesnt require any any third party softwares.

1.5.3 Operational Analysis

Only basic knowledge about computers is necessary to vote for the favored candidate. A brief training on how to use the system before the voting is enough.

1.6 System Requirement

1.6.1 System Requirement

Software required to cast a vote are :

- Python 2.7 or above.
- Any Operating system (preferably windows 7 or later).

Software required to build our proposed system are:

- Javascript.
- Anaconda (IDE for python).

1.6.2 Hardware Requirement

Basic hardware requirement required for our proposed system are:

- Touch Display unit.
- 2GB of RAM or more.
- Atleast 20GB harddisk (32 GB SSD for best performance).
- Core 2 duo @1.8MHz or above.
- Motherboard supporting above processor.
- Power Supply (approximately 300-500W).
- CPU case.
- Case for whole machine.

CHAPTER 2
LITERATURE REVIEW

2.1 Concept of e-Voting System

E-Voting refers to voting using the electronic means to aid in counting or casting votes. Electronic voting uses a standalone machines or computers connected to the internet.

The first-ever electronic voting system was introduced in the early eighties by David Shaum. The system used a public key cryptography, which was used to cast votes and keep voters anonymous. To make sure there were no links between voters and ballots, the Blind Signature Theorem was used. Most of the research done on the field has focused on the Direct Recording Electronic System and the Internet Voting Systems. The first system is used in polling stations instead of paper ballots and the later one is for mobile, that allows casting votes from everywhere[3]. It is obvious that e-Voting is far more secure than traditional voting systems, but it is not completely secure from attacks by hackers.

2.2 Research Review

In the paper Real-World Electronic Voting:Design,Analysis and Deployment , the authors claim E-voting faces a wide variety of potential attackers beyond those considered in traditional elections. These include insider attacks from system administrators, cybercriminals working for dishonest candidates, hacktivists seeking to disrupt elections as a form of political protest, and even sophisticated nation-states applying offensive cyber warfare capabilities. We can roughly divide these attackers goals into three categories: (1) Tampering with the election outcome, e.g., to favor particular candidates; (2) Discovering how people voted, e.g., to retaliate against those who voted against the attackers preferred candidates, as a means of enforcing vote buying or coercion; and (3) Disrupting or discrediting the election process,e.g.,through denial of service, conspicuous tampering, or the false appearance of such problems[4].

Critics of most voting system is the secrecy of the critical parts of the codes. Such secrecy arises questions towards the transparency of voting systems. Another problem with traditional e-Voting is its centralization. The centralization of database makes it vulnerable towards DDOS attacks that could make the voters unable to cast votes. Intelligence agencies have enough resources to analyse voting data for possible alteration. Even with enhanced security, State level attacks are possible. In the paper, A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC VOTING SYSTEM[3] by Ahmed Ben Ayed, he suggests that all these security issues could be solved by using open source code to develop e-Voting systems. He then suggests the use of blockchain technology to secure votes and decentralize the system.

2.3 e-Voting in Nepal

The Election Commission had ruled out the possibility of using electronic voting machines (EVMs) for the provincial and federal parliamentary elections after it failed to convince three major parties. The argument was that there wasnt enough time to teach all the voters on how to use these EVMs[5].

CHAPTER 3
METHODOLOGY

3.1 Introduction

For our project we searched for different research papers and books written on blockchain technology and decentralized systems on the internet. We searched for articles related to our project and viewed videos that would aid us to develop our applications.

3.2 Research Methods

Most of our research materials were gathered from the internet. We studied different research papers on blockchain technology and downloaded books provided by different authors in their site. We watched a lot of videos to get more idea about decentralized applications(dapps) and also researched about the implementation and development of such applications. We searched for articles on different site to find out more about the programming languages used to develop dapps.

3.3 System Design

Multiple languages can be used to create our voting system. However, we must consider a lot of challenges that we could face while coding such a software. The programming language that we choose must provide:

- Security: vulnerability must be minimized so that hackers cannot get the upper hand and change outcome in their favour.
- Resource Management: system should be well equipped to handle local and remote queries.
- Performance: we must verify if the tasks are parallel or not and deal with them accordingly.
- Isolation: transactions must be deterministic i.e. they cannot work in 2 different ways in 2 different time and machines.

Javascript and Python are 2 possible programming languages that can be used for blockchain coding. In order to code using either of these languages we must focus more on gaining proper knowledge and construction of the genesis block, cryptographic hash functions as well as proof of work.

3.4 Software Development Model

We follow the Prototyping Model for our system development. The prototyping Model is a system development method (SDM) in which a prototype, an early approximation of a final system or product, is built, tested, and then reworked as necessary until an acceptable prototype is finally achieved from which the complete system or product can be developed. It is an iterative, trial-and-error process that takes place between the developers and the users.

Prototyping model is an evolutionary process model which tends to refine the software requirements by release and evaluation of prototypes. Especially in case of poorly defined or fuzzy requirements and uncertain adaptability of the system, a prototype can be used for evaluation purpose by the customer and developer both. Prototypes offer limited aspects of features of the final product, sufficient enough to convey the developers proposal for the design of ultimate product. Major benefits of the prototyping model is that it allows earlier assessment of the proposed solution. It also allows the software engineer some insight into the accuracy of initial project estimates and whether the deadlines and milestones proposed can be successfully met[6].

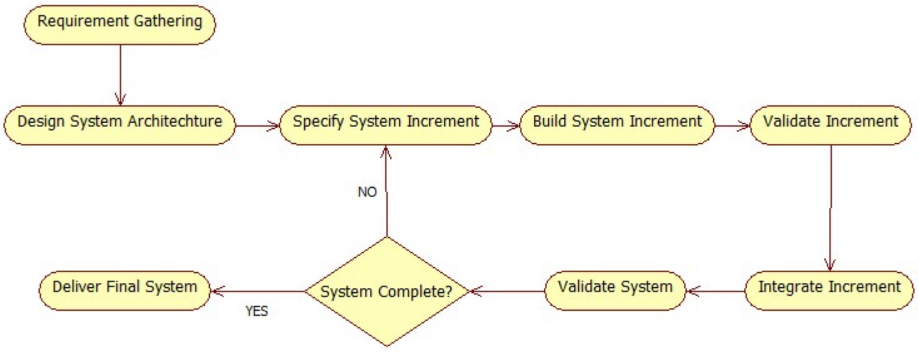

Figure 3.1: Software Development Model

3.5 Use Case Diagram

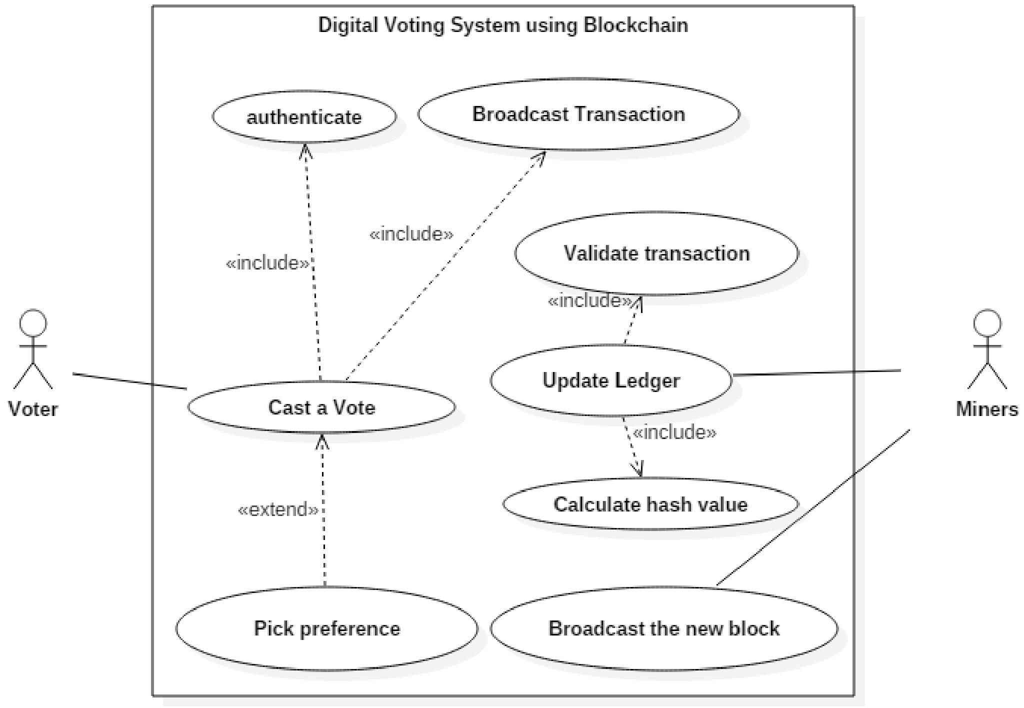

Figure 3.2: Use Case Diagram

3.6 Blockchain

A blockchain originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hashpointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. The Harvard Business Review describes it as ”an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.” For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

A block is the current part of a blockchain, which records some or all of the recent transactions. Once completed, a block goes into the blockchain as a permanent database. Each time a block gets completed, a new one is generated. There is a countless number of such blocks in the blockchain, connected to each other (like links in a chain) in proper linear, chronological order. Every block contains a hash of the previous block. The blockchain has complete information about different user addresses and their balances right from the genesis block to the most recently completed block.

The blockchain was designed so these transactions are immutable, meaning they cannot be deleted. The blocks are added through cryptography, ensuring that they remain meddle-proof: The data can be distributed, but not copied. However, the ever-growing size of the blockchain is considered by some to be a problem, creating issues of storage and synchronization.

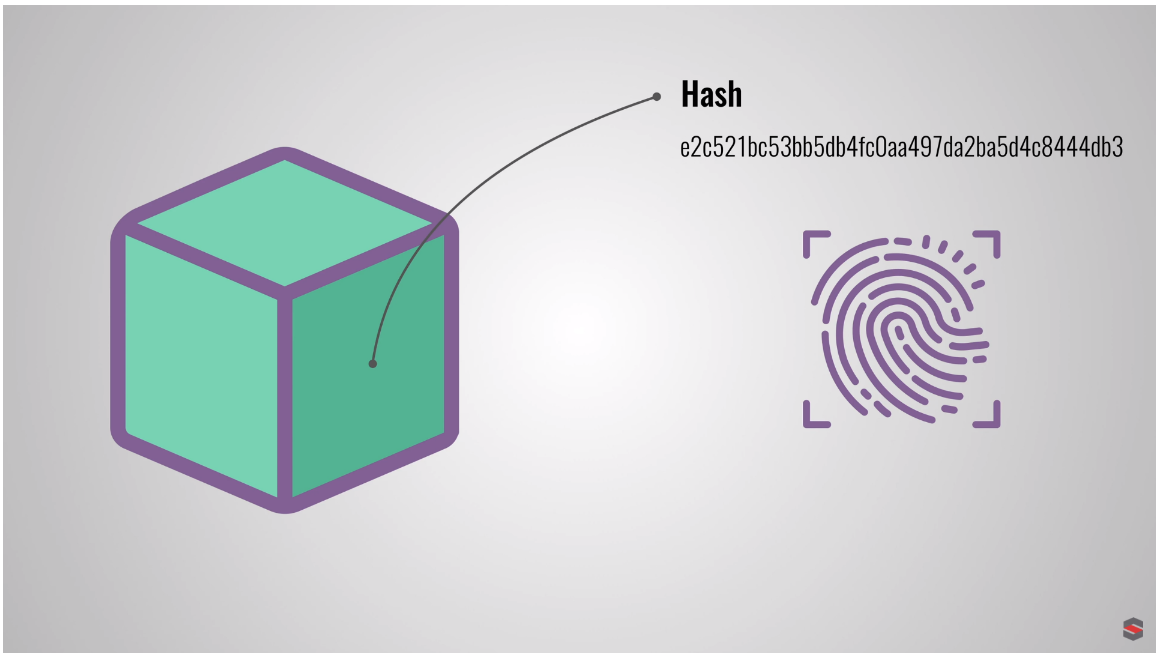

Figure 3.3: Hashing the Block

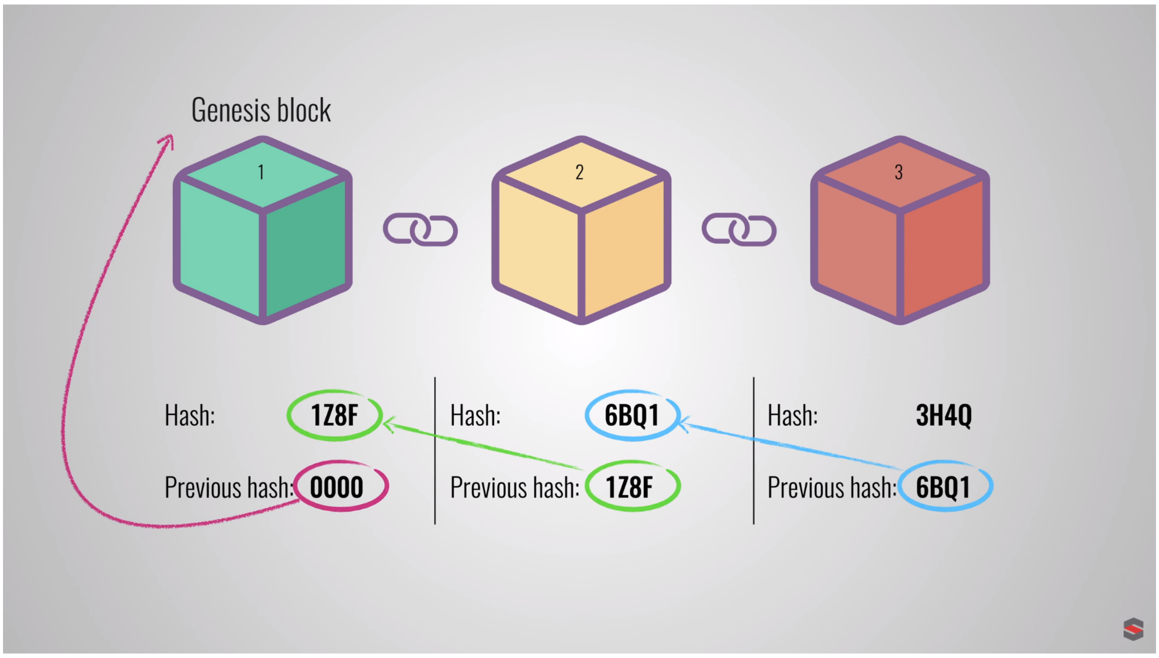

Figure 3.4: Chain of Blocks

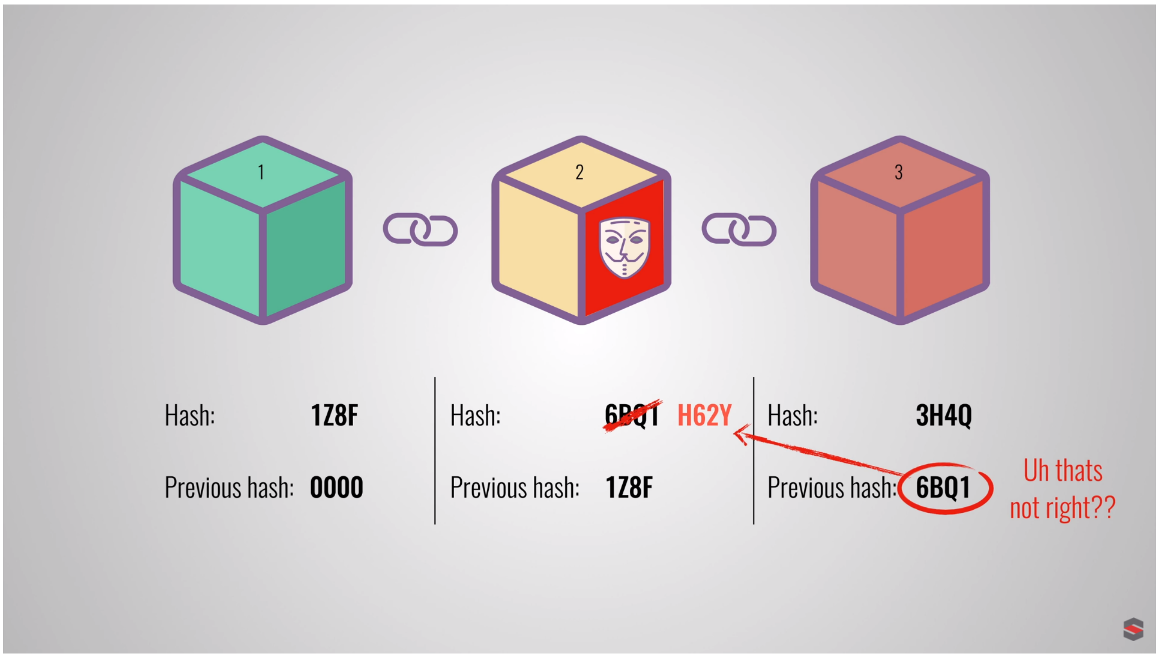

Figure 3.5: External Interference

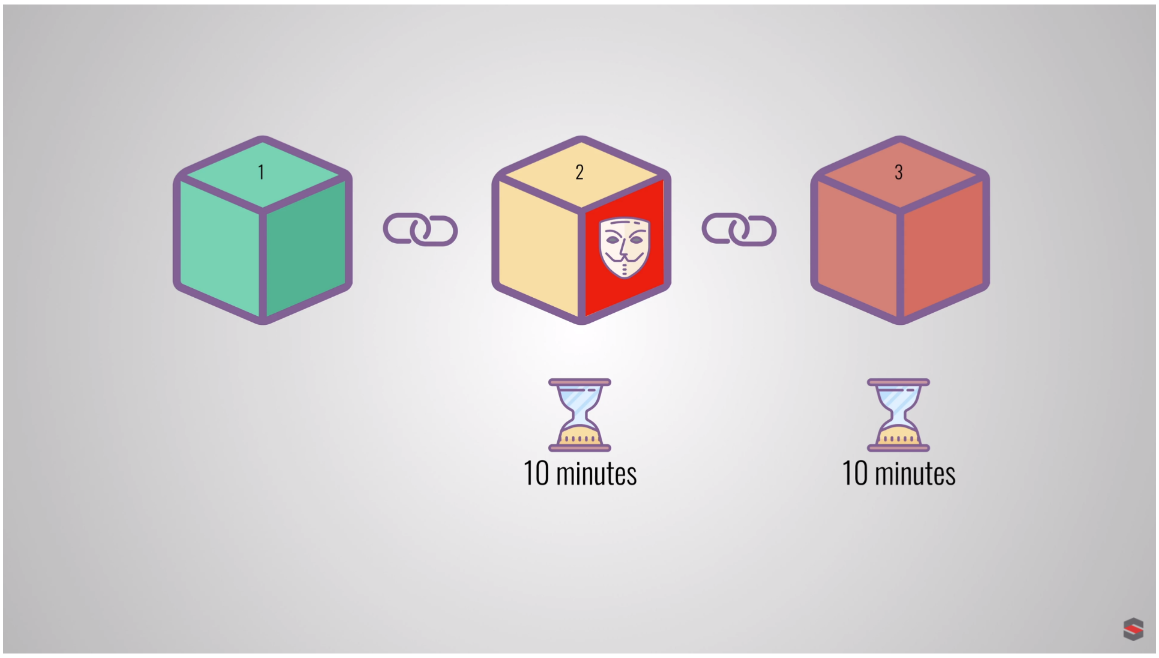

Figure 3.6: Delay because of ”Proof of Work”

3.6.1 Security Issues of Blockchain

51% attack

51% attack refers to an attack on a blockchain usually bitcoins, for which such an attack is still hypothetical by a group of miners controlling more than 50% of the network’s mining hashrate, or computing power. The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network.

The estimated rate of hashes of the Bitcoin network peaked at 13,523,350 Th/s. So for 51% attack, theoretically attacker must own about 7,000,000 Th/s, which is ludacris to even think of. The most used mining tool is antminer d3 which is a Application Specific Integrated Circuit, it cost about $2000 and has hash rate of 19.3 GH/s consuming 1300 W power. On stock settings, the nvidia GTX 1080 Ti FE outputs 32.04 MH/s.

For successful 51% attack attacker will need approximately 371,400,000 antminer d3.

CHAPTER 4
EPILOGUE

4.1 Expected output

The final output of our project will be a webapp that can run on the voting machines/computers. The users will be provided a purely graphical interface, through which they can vote for their preferred candidates. The main objective is to provide a user friendly interface, which is easy to learn for people having very less or no technical experiences.

4.2 Work Schedule

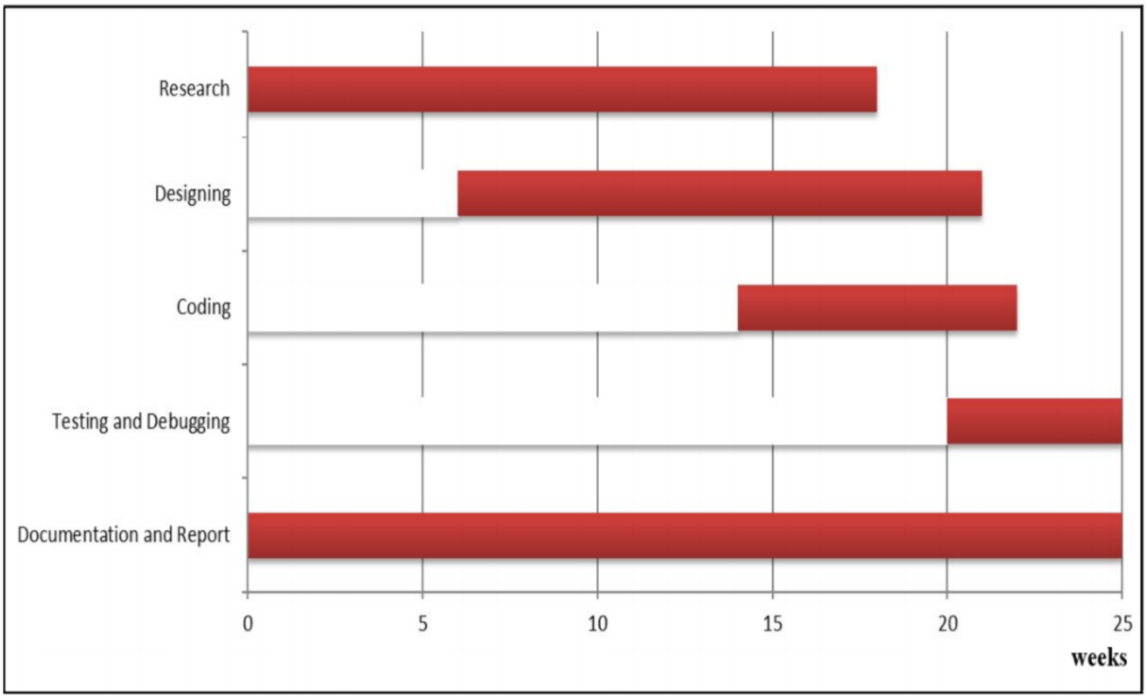

Figure 4.1: Gantt Chart

REFERENCES

[1]”Cite a Website - Cite This For Me”, Economist.com, 2017. [Online]. Available: https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable. [Accessed: 30- Dec-2017].

[2]En.wikipedia.org, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Blockchain. [Accessed: 30- Dec- 2017].

[3]International Journal Of Network Security & Its Applications (Ijnsa) Vol.9, No.3, May 2017, ”A CONCEPTUAL SECURE BLOCKCHAIN - BASED”, 2017. [Online]. Available: http://aircconline.com/ijnsa/V9N3/9317ijnsa01.pdf. [Accessed: 30- Dec-2017].

[4]”Cite a Website - Cite This For Me”, Jhalderm.com, 2017. [Online]. Available: https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf. [Accessed: 30- Dec-2017].

[5]”EVM use ruled out in upcoming polls”, Kathmandupost.ekantipur.com, 2017. [Online]. Available: http://kathmandupost.ekantipur.com/news/2017-08-19/evm-use-ruled-out-in-upcoming-polls.html. [Accessed: 30- Dec- 2017].

[6]”What is Prototyping Model? - Definition from WhatIs.com”, SearchCIO, 2017. [Online]. Available: http://searchcio.techtarget.com/definition/Prototyping-Model. [Accessed: 30- Dec- 2017].

[7]C. Prableen Bajpai, ”Blockchain”, Investopedia, 2017. [Online].
Available: https://www.investopedia.com/terms/b/blockchain.asp#ixzz52iqmCUPd. [Accessed: 30- Dec- 2017].