Pre-Project Report

On

DIGITAL VOTING USING BLOCKCHAIN TECHNOLOGY

Submitted in partial fulfillment of the requirements

for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

INFORMATION TECHNOLOGY

Submitted by

Ashutosh Rahi (IT/31/15)

Rakshit Sharma (IT/33/15)

Baljeet Singh (IT/26/15)

Under the supervision of

Ms. Iqra Altaf Gillani

DEPARTMENT OF INFORMATION TECHNOLOGY

NATIONAL INSTITUTE OF TECHNOLOGY, SRINAGAR

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Motivation

Large sections of society today do not trust their government [1]. This makes the election a very important event in a modern democracy. The issue with the current ballot system is that it can be easily manipulated by power hungry organizations.

The traditional process of voting is prone to riggedness, and use of unfair means, as the electoral voting transactions are never made public, the whole process is not transparent. The best way to prevent rigged elections to make the whole process **transparent,** yet **immutable to undesired changes.** The best solution for this is Blockchain technology [1].

The current ballot system does offer anonymity to the voter but the counting process is not transparent. People are supposed to trust the result which is provided by an Election commission or a government body. This makes the process of counting, a major vulnerability in the current process. There are also other major electoral scams such as voter fraud, ballot stuffing and booth capturing. All these make it very difficult for organizers of an election to distinguish between the actual votes and votes added without authorization.

The system that is being proposed solves most of the issues mentioned above and can be implemented in the current world environment.

The proposed system looks to eliminate the aspect of trust from an election to make it more secure and transparent. The system uses existing technology such as a client server architecture integrated with a blockchain system to ensure aspects such as transparency, security and auditability are achieved without sacrificing privacy for

voters. The cost of building the system is substantially less as compared to the cost of running a ballot based system. There are substantial social benefits to using the system as well such an easier and quicker voting process which will lead to higher voter turnout. This system can be implemented for a larger number of countries as the internet penetration in the world increases.

1.2 Problem Statement

To design a system, which can satisfy the following requirements:

(1) Online decentralized trustless app-based voting, so that voters can vote from the comfort of their homes, or from anywhere else subject to meeting the verification requirements.

(2) Fool-proof digital identification system, which can store the verified details of the voter, and verify his identity again prior to voting.

1.3 Our Approach

The proposed system essentially uses client-server based architecture, secured with TLS v1.2, Modified Needham Schroeder and other such network security protocols, and a blockchain network based on *Ethereum™* platform. The first phase is user-authentication, for which Kerberos protocol is used, involving one authentication server, connected with voter-detail database at back-end, and an arbitration server, which acts as an interface between the blockchain system & the voter. The blockchain used will be a private one, in which only one node will be authorized to **read** the transactions, but not to modify those, & that too will be allowed only once the election gets over. Moreover, even when the election is proceeding, the voter can verify whether his vote has been counted or not, ensuring full transparency. However, the identity of the voter will not be revealed in the voting transactions, as a key will be used to address any voter, and not his name, or image.

CHAPTER 2
BLOCKCHAIN TECHNOLOGY

2.1 The need for decentralization

Traditional banking system, governance, data storage, and other such systems are essentially centralized in the current scenario, but the issue with such systems are numerous:

- Such systems store whole data at a single centralized location, so the confidentiality of data can be easily compromised as it rests on a single location.
- Centralization involves trust over a third party, but we wish to have a completely *trustless* system.

2.2 Blockchain as a solution

At its core, the blockchain is a distributed database that maintains a secure and ever-growing ledger of records (usually transactions) known as blocks. This database (the blockchain) is managed by a network of nodes that all have their own copy of the blockchain. The nodes are simply computers connected to the network that have agreed to process the validity of transactions on the blockchain based on a set of rules the network has agreed to. Once a node validates a transaction, it adds it to a chronological group known as a block that is then added to the blockchain. Valid transactions are therefore grouped together and added to the database in a block, one after the other, hence the name blockchain. When the first block of the chain is added, it is marked with a hash function.

As the second block is added, it is also marked with a hash function that contains part of the first block's hash function. Therefore, when a node submits a new block for addition to the chain, if the node has changed any of the database transactions included within the previous blocks, the hash function of that block would also need

to be changed. When that altered block is added to the blockchain, all other nodes will realize its hash function is incorrect (so a change must have been made on previous blocks) and the update will be rejected. This fundamental aspect of blockchain is what makes the technology tamper-proof and secure.

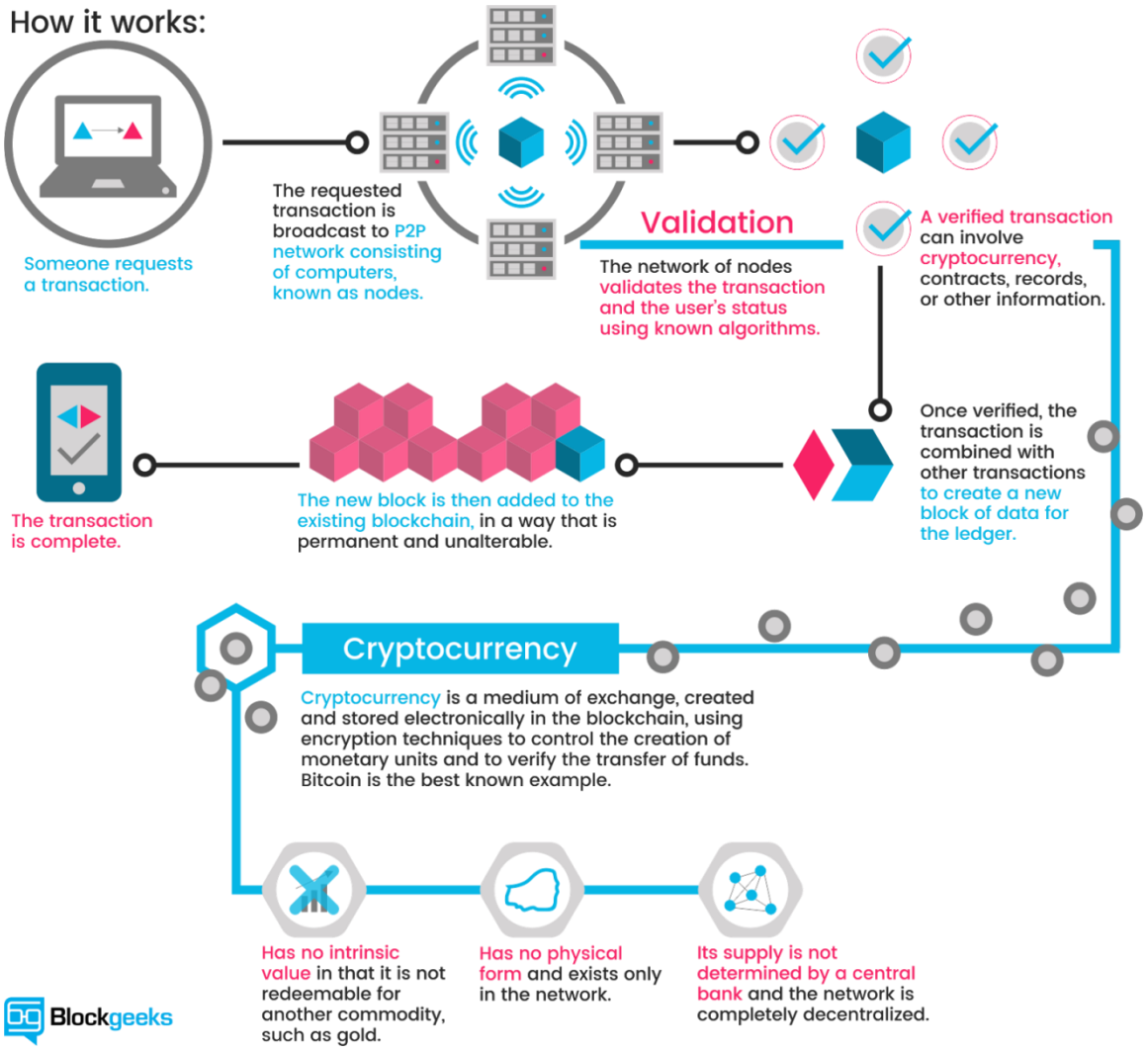

Fig. 1: How Blockchain Works [4]

2.3 Smart Contracts

A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies, and enforces the negotiation or performance of an agreement or transaction. It is the simplest form of decentralized automation.

It is a mechanism involving digital assets and two or more parties, where some or all of the parties deposit assets into the smart contract and the assets automatically get redistributed among those parties according to a formula based on certain data, which is not known at the time of contract initiation.

2.4 Blockchain Consensus Algorithms

Consensus decision-making is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole. Consensus may be defined professionally as an acceptable resolution, one that can be supported, even if not the "favourite" of each individual [3]. Consensus is defined by Merriam-Webster as, first, general agreement, and second, group solidarity of belief or sentiment [3].

Proof of Work is one such algorithm, in which an expensive computer calculation, also known as mining, needs to be performed to create new blocks on blockchain. It serves two main purposes:

(1) To verify the legitimacy of a transaction, or avoiding the so-called double-spending;

(2) To create new digital currencies by rewarding miners for performing the previous task.

CHAPTER 3
LITERATURE SURVEY

3.1 FollowMyVote [2]

In Follow My Vote's approach, the voter has to install the "voting booth" on a computer, tablet or smartphone. The voter then needs to verify its identity by submitting legal documents (like a passport) to an Identity Identifier that would have been already approved by the organization holding the election. Once its identity verified, the voter could request an online ballot and submit their vote to the blockchain. Follow My Vote's system also allows for voters to vote early or even have the ability to change their mind and vote for another candidate as long as its before a cutoff on election day. Once the polls closed, voters' most recent vote would be the only one counted. Finally, voters would be able to follow their vote from the ballot box to make sure their vote counted.
In 2016, Follow My Vote tried to run a parallel presidential election to demonstrate the effectiveness of its system. However, the team failed to meet the election day deadline for development and failed on its mission. There are too many security flaws associated with the method: authentication of the user is quite hard, remote voters can easily be intimidated, and voter's personal computer could be compromised.[2]

Those factors alone make this an unrealistic choice for an effective governmental voting system although it could still be used for private elections with less at stake.

3.2 Blockchain E-Voting System [1]

The proposed system involves a client server architecture integrated with a block chain system. The minimum requirements needed by a voter is a smartphone or a computer with a webcam and an internet connection. If these are not met alternate arrangements such as pop up cyber cafes and computers at public buildings must provide access to disadvantaged voters.

The system uses an authentication server for verification of the user details, an arbitration server for the interface between the blockchain & the user, the blockchain system and the user.

CHAPTER 4
METHODOLOGY

4.1 System Architecture

There are four main parts of the system:

(1) User

The user must have a smartphone, laptop or any device with a browser and a front facing camera. The user must also have an internet connection to register and vote as well.

If the user does not have a computer or an internet connection, he/she could go to a public building such as a library or a school which does have computers to register to vote. These could be kept open all day during voting registration and voting days to ensure people with low sources of income do not get left out.

(2) Authentication Server

The Authentication Server is a traditional centralized web server. It has a backend database connected to it which has the information of all the citizens in the country. This system is used by people to register to vote for their elections. People create login accounts when they register. It also creates accounts on the blockchain system for the users when they vote. The blockchain account is used by the Arbitration Server to vote for a candidate of the users' choice. The AS also authenticates the token provided to the Authorization Server by the user while voting.

(3) Arbitration Server

The Arbitration Server acts as an intermediary between a user and the Blockchain voting system. It verifies the user while voting using the Authentication Server. The AR is a blockchain thin client that sends the users' vote to a blockchain node. It also sends the user the key to encrypt their vote. The AR sends the users' vote

to the appropriate node to be added to the blockchain. The user can verify their vote using the AR as an intermediary.

(4) Blockchain System

The blockchain system is the system on which the actual voting takes place. The users' vote is sent to the one of the nodes on the system depending on the load on each node. The node then adds the transaction to the blockchain depending on the smart contracts that exist on each node. The smart contracts are the rules that the nodes follow to not only verify but also add the vote in the system. Each node follows the smart contract to verify the vote. The blockchain is a private system and is not accessible to the public directly.

4.2 Procedure

(1) User first registers for the vote, & for doing so he interacts with the Authentication Server, via a website, & scans supporting documents to verify his identity to the server. He enters a username & password for login which are stored separately from these details for **user privacy & anonymity.** All the information between the user and the AS is sent using **TLS v1.2** protocol to ensure it is all secure.

(2) During voting day, the user logs in to the authentication server using the username and password created in the previous step. An image of the user is taken to ensure that the user is the owner of the account. This image is compared with the image taken during registration.

(3) A small video of the user is taken before they log in and is sent to the Authentication Server. Using the Affectiva API the AS can identify user emotions based on machine learning technology [4]. If the system detects fear, the users' session is stopped and told to retry after 5 minutes. While logging in for the second time if the system detects fear again, the user must go to their local polling center such as a library to vote.

(4) Once the user logs in, their system would create a public key which they would send to the Authentication Server. The AS would add associate the key with the username. The key would be used to create an account for the user on the blockchain system to vote. A specific amount of ether (currency the user can use to vote) is added to the users' account which enables them to vote. The AS would then send a session token back to the user.

(5) The user would be redirected to the AR. The user would provide the AR with the session token, would verify it with AS. A video of the user is again recorded to detect fear. The verification and generation of token between the AR, user and AS is done using the Modified Needham-Schroeder protocol. This protects the system from impersonation and man in the middle attacks.

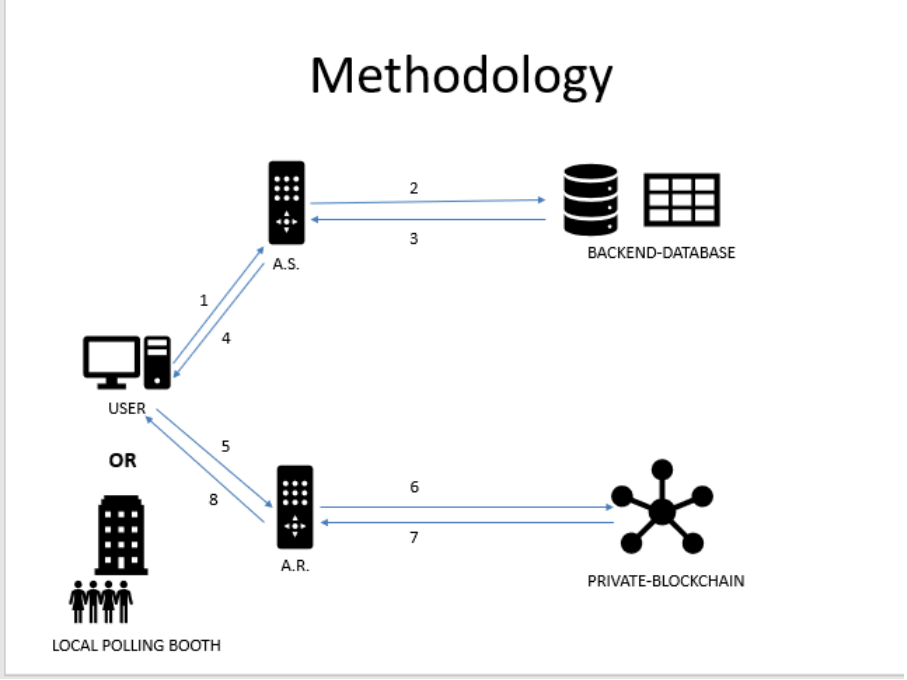

Fig. 2: The Methodology

(6) The AR would send a verification message to the user along with the public key of the blockchain node to which his/her vote would be sent. The user would encrypt their vote with the public key and send it to AR. This would ensure that

the AR cannot read the users' vote and hence the vote would remain a secret. The AR would send the encrypted vote to the appropriate node.

(7) The node would decrypt the message with their private key and send a specific amount of ether from the users' account to the candidates' (or to the Abstain account if they would like to forfeit their vote) blockchain account. Each node would verify the transaction according to the smart contracts. These contracts would verify a particular transaction was a duplicate one or no and check its validity. After this process the node would pass this transaction to other nodes in the blockchain system.

(8) The process of counting votes of a candidate can be very simple. Each voter has a fixed amount of ether or currency value that they use to vote for a candidate of their choice. The candidate with the highest amount of ether in their account wins the election. For users who abstained from voting, their ether will be sent to an Abstain Account. This ensures their vote does not get misused.

CHAPTER 5
PROJECT OUTCOMES

On successful completion of the project as per the discussed strategy, the following outcomes will be there:

(1) If implemented, the voting process for the state elections will become quite less tedious & **more economical**.

(2) The voters will be able to vote even if they are travelling abroad.

(3) Physically challenged voters will be able to vote from the comfort of their homes.

(4) The issues of rigged elections, fake voters in electoral rolls, will be eradicated.

REFERENCES

[1] Shah, S., Kanchwala, Q. and Mi, H. (2018). *Blockchain Voting System*.

[2] Osgood, R. (2018). *The Future of Democracy: Blockchain Voting*.

[3] Blockgeeks. (2018). *What Are Smart Contracts? A Beginner's Guide to Smart Contracts*. [online] Available at: https://blockgeeks.com/guides/smart-contracts/ [Accessed 7 Nov. 2018].

[4] Blockgeeks. (2018). *Basic Primer: Blockchain Consensus Protocol - Blockgeeks*. [online] Available at: https://blockgeeks.com/guides/blockchain-consensus/ [Accessed 7 Nov. 2018].