Blockchain based E-Voting System

Jerome Mizzi, Frankie Inguanez

MCAST, Institute of Information & Communication Technology, University College

Objectives

The main goal of this project is to see if blockchain technology can be used for a system which requires a very high level of security. This means that a system needs to be created which covers multiple points:

- A system which is secure
- A system makes sure that the voter remains completely anonymous
- A system that is easy to use, even by people with no experience using a computer
- A system which is cost effective

Introduction

The main goal of this research is to see if blockchain technology can be used for a system which requires a very high level of security and privacy. Blockchain technology has been created for the recording of cryptocurrency transactions, and new innovative uses are being explored at a fast rate [1]. Considering the security a blockchain can offer, mostly against internal tampering since it is a decentralised system, a high security application like e-voting would be a perfect example of how blockchain technology can be used for something other than cryptocurrencies. It must be noted that the technology is still in its infancy and one of the major limitations is the transaction rate. We have therefore set out the following hypothesis: The blockchain is an ideal store to securely offer an e-voting system. This research is being split into two stages:

1. **Stage 01: Initial Prototype:** where a proof of concept is created to familiarise ourselves with the technology and identify whether the hypothesis can be accepted.
2. **Stage 02: Securing and Scaling:** where the prototype is revised to focus on the security of the voter and scaling it to support a large number of concurrent voters.

Technologies

The following technologies were used to create the prototype:

- Ethereum Blockchain
- Solidity
- Ganache
- Apache Web Server
- MySQL

Challenges

While creating this prototype I encountered several challenges. The largest one being the time constraint. As I was very limited when it came to time, since I had four other subjects and their assignments alongside an internship during the short time period, I had to limit my prototype and research to a point which I feel is not sufficient. Also learning how to program onto the Ethereum blockchain took its time. Since I was using, Solidity which does not yet have all the features other high-level languages have as it is still in development. An example of a problem I encountered is that you cannot make a method which returns a structure, as this is not yet supported. To solve this, I had to create multiple methods which return each value within the structure. Another limitation of such is that there is no List datatype, although Ethereum has mappings, which allow you to link a datatype with the other, for example linking a string containing the id number, with the voter structure which holds the voters information. Other challenges included setting up a local testing blockchain, which at first I found complicated tutorials require everything to work through the Node.js command line, only to later find that there is a much simpler user interface version of the same local blockchain. There were other smaller challenges encountered as well, although I managed to overcome these challenges trough research.

Methods

For the prototype application I made a three-step plan which explains how the entire system will work, the diagram below shows a basic idea of these three steps.

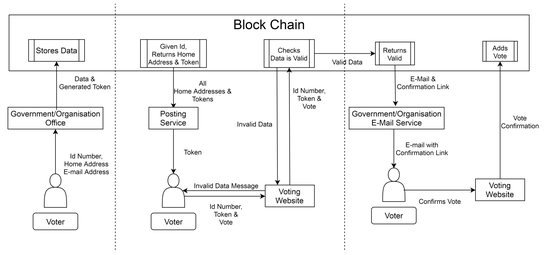

Figure 1: Three Phase Plan

In the first phase a voter who wishes to use the system must go to a government/organisation office to register. The voter will show his/her national identification document, where a public officer will assure that the documents belongs to the applicant, after which the home address and e-mail address are noted. These registrations will be open for a certain time period before the voting start, when it is time we move on to the next step. In the second step all the home addresses of the voters that have registered are passed on to a posting service. From here every voter will receive a unique token. When a voter receives the token, he/she can go onto the voting website, where the voter must input his/her id card number, token and his/her vote. From there, the data is validated to make sure that the id card number and token match and that that voter has not yet voted. If everything is valid we move to the third phase. Where the voter will receive an e-mail on the address that the voter registered with. The e-mail will contain a confirmation link. If the user was to receive such e-mail before voting it means that someone managed to get his/her id card number and token, and thus he/she should delete the e-mail and contact the government/organisation that his/her information was stolen and someone voted for him. However, if it was the voter who voted, then he/she needs to click a link within the e-mail to confirm his/her vote, after which the vote would be added.

Conclusion

Throughout the project, we have managed to find interesting literature which gave a good idea of the blockchain technology and on how to use it for creating an e-voting system. A sample prototype with the main features has been created, analysed and has proven that this hypothesis is accepted. For this reason we shall extend this research to cater for the entire process flow of a voting system, securing it further and to support large scale usage. This research will also gather user feedback to determine user acceptance.

References

[1] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander.
Where is current research on blockchain technology?âĂŤa systematic review.
PloS one, 11(10):e0163477, 2016.

[2] Yifan Wu.
An e-voting system based on blockchain and ring signature.
Master. University of Birmingham, 2017.

[3] Pavel Tarasov and Hitesh Tewari.
The future of e-voting.
IADIS International Journal on Computer Science & Information Systems, 12(2), 2017.

[4] Satoshi Nakamoto.
Bitcoin: A peer-to-peer electronic cash system.
2008.

Contact Information

- Email: jerome.mizzi.a100453@mcast.edu.mt
- Phone: (+356) 79809391