Blockchain based E-Voting System

Jerome Mizzi, Frankie Inguanez
Institute of Information and Communication Technology
Malta College of Arts, Science & Technology
Paola PLA9032, Malta
fjerome.mizzi.a100453
frankie.inguanezg@mcast.edu.mt

ABSTRACT: *In the rst part of our research we investigate the use of blockchain technology as a viable solution for a national e-voting system. To achieve this a small prototype was made, whilst still a work in progress, the main features of the prototype are there. For the prototype a web-site was created and the smart contract on the blockchain was written in Solidity. The data was saved on Ganache. We believe that blockchain is the right tool to guarantee the integrity of vote counting, yet more research is needed to safeguard the privacy aspect of a democratic vote.*

Keywords: E-voting, Blockchain, Ethereum, Security

DOI: 10.6025/jet/2018/9/2/44-48

Received: 20 January 2018, Revised 24 February 2018, Accepted 3 March 2018

1. 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 [11]. Considering the security a blockchain can oer, 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 oer 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.

In this paper we document the rst stage of our research undertaken as a second year undergraduate research project, with the second stage to be undertaken during the nal year. In Section 2 we go through some current notable research about the subject, followed by our research approach in Section 3. In Section 4 we evaluate the research with some concluding arguments found in Section 5.

2. Literature Review

"Electronic voting (e-voting) is a symbol of modern democracy activities. Due to the high ballot privacy and variability" [9]. Unfortunately, such a system is not easy to implement due to the high risks of security problems. Not only is there the risk of hackers penetrating the defences of the application and altering the votes, there is also the risk that someone from within can alter the data into their favour, especially if the people taking care of the voting system work for one party of who the votes are going for. So what kind of technology can we use to secure such an application? Satoshi Nakamoto [5] wrote about the idea of cryptocurrency, the idea of using a peer-to-peer network to store currencies and transactions, this writing lead to the Bitcoin. The Bitcoin created a new method for online money transfer, one which is not reliant on banks. As Bitcoin gained popularity, so did the technology behind it, the blockchain. Blockchains use the idea of a decentralised system where unlike a regular online data system, in which one computer referred as the server holds all the data and anyone who needs to use such data connects to that server. In blockchains, the data is stored on many computers connected using a peer-to-peer network. To access the data, you have to move from one computer to another to get to the data you need [9, 7].

The Bitcoin blockchain works through six steps, which in this system [9] decided to add fingerprint data, so that each voter can be identied as unique. To use the Bitcoin blockchain you rst have to generate a private key, in this case using the parameters of the Elliptic Curve Digital Signature Algorithm (ECDSA) referred to as Secp256k1. Then generate the Bitcoin public key from the Bitcoin private key with the DER format. After which you need to hash the Bitcoin public key, using SHA256. Continue by adding the prex of the version at the head and dene the intermediate hash value of public key while using fingerprint data. Then dene Sha256, using the fingerprint yet again as the check digit. Finally, generate the nal Bitcoin address by encoding the fingerprint data with the Base65 encoding algorithm [9, 5].

In an e-voting system certain key steps must be followed as documented in [1]. The researchers suggest to have a pipeline starting from the identity verification, then proceeding to getting a turn to vote, updating the database, creating a new block, then broadcasting. Their research has demonstrated, as in other research, that blockchain can be used for small scale voting, yet the technology is still limited for large scale voting.

The adoption of blockchain technology for voting is generally considered benecial on two aspects, that to address voter fraud and to voter access [4] and has been explored in South Korea, Sierra Leone, Russia and Estonian. An implementation of an e-voting system with blockchains uses Zcash, which is another blockchain designed to be used for payments. Its main goal is to provide anonymity and privacy of transactions. A very large difference between Zcash and Bitcoin is that the Zcash blockchain has a proof of work system, in which Zcash relies on zero knowledge proofs. In addition to this the Zcash blockchain supports anonymous and transparent transactions, making it more ideal for something like an e-voting system [7]. Results do show that blockchain technology offers an inherently more secure platform when compared to centralized systems, and that Zcash makes it very easy so that the voters remain anonymous. Although since Z-cash uses a proof-of-work system, mining expenses are still there, thus being costly to use just like blockchain [7].

Testing an e-voting system using the Bitcoin blockchain had positive results however in the performance evaluation when testing on a large number of votes, which is normally the case in a voting system, it started to slow down a lot for generating and verifying cryptographic algorithms, thus needing miners to run the system on a large scale, signicantly increasing the cost of such a system. It was not all bad however, the Bitcoin blockchain did manage to guarantee the authenticity of each vote. It was also able to represent the votes in real time, allowing people to see the votes going up as soon as people cast their vote [9].

In [10] the researchers have made a similar proof of concept based on the Ethereum network and using an Android application. They have benchmarked the creation of a smart contract, which is the equivalent of a vote, and have demonstrated that this is possible on small scale voting with an average time of around 30seconds to register a vote.

The use of blockchain technology does come with its own risks. One of the most common threats is the so called 51% attack where an entity manages to grab hold of the majority of the blockchain and double spend transaction coin in a specic wallet [2] such as what happened on the Bitcoin Gold network [3]. This is a serious threat for private and hybrid blockchain networks commonly used for government entity purposes such as, case in point voting systems. A delay in the verification process is one way of mitigating this threat.

The blockchain technology traces a transaction directly to a singular wallet, yet in a voting system the privacy of the voters preference must be conserved. [6] have proposed a one-time ring signature technique where the voter generates a ring from a fracture, using a public key produced by other signers, and the fracture from a private key. This technique has been adopted for large scale voting using the Ethereum Blockchain with positive results [8].

If a state or nation is considering introducing the use of blockchain for voting then one of the major concerns is to provide a good and reliable infrastructure such as access to a reliable broadband service and good quality software [4]. The choice of which network to use is also key, [9] mentioned the idea of combining multiple blockchain technologies together to take the advantages from different networks and diminish the limitations of each.

3. Research Methodology

The hypothesis of this research is: The blockchain is an ideal store to securely oer an e-voting system. The following research questions were established:

1. Can an e-voting system be more efficient than the traditional manual and postal voting?
2. Can it really oer a higher security than a centralised system?
3. Will voters and it easier to use when compared to the traditional manual and postal voting, or is it just more complicated?
4. How safe is it for a government or an organisation to replace their old voting system for this?
5. Is it even worth replacing the old voting systems for this? Especially since blockchains are known to be costly to use?

To be able to answer these questions, there rst needs to be a prototype of a blockchain based e-voting system, so that than questionnaires and interviews can be carried out to see what people think about it. The prototype was developed using the Ethereum blockchain, which differs from Bitcoin and Zcash as it serves as a generic platform for creation of custom functionality, rather than it being designed for money transactions. This means that it should be easier to develop an e-voting system on Ethereum offering more flexibility as it is designed to support any custom application, known as \smart contracts", rather than it being designed for monetary transactions. According to [7] the Ethereum blockchain lacks the much-needed anonymity factor, which has not yet been present within the protocol. For the prototype Ganache was used, which is a virtual Ethereum blockchain which runs locally, so that one can test his/her application without deploying it on the actual Ethereum blockchain.

So, for the prototype itself a three-step plan which explains how the entire system will work, (see g. 1). In the rst phase a voter who wishes to use the e-voting system must go to a government/organisation office to register. Therefore 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 for the voting to start we move on to the next step. In the second step all the home addresses and tokens of the voters that have registered for the e-voting system 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 himself it means that someone managed to get his/her id card number and

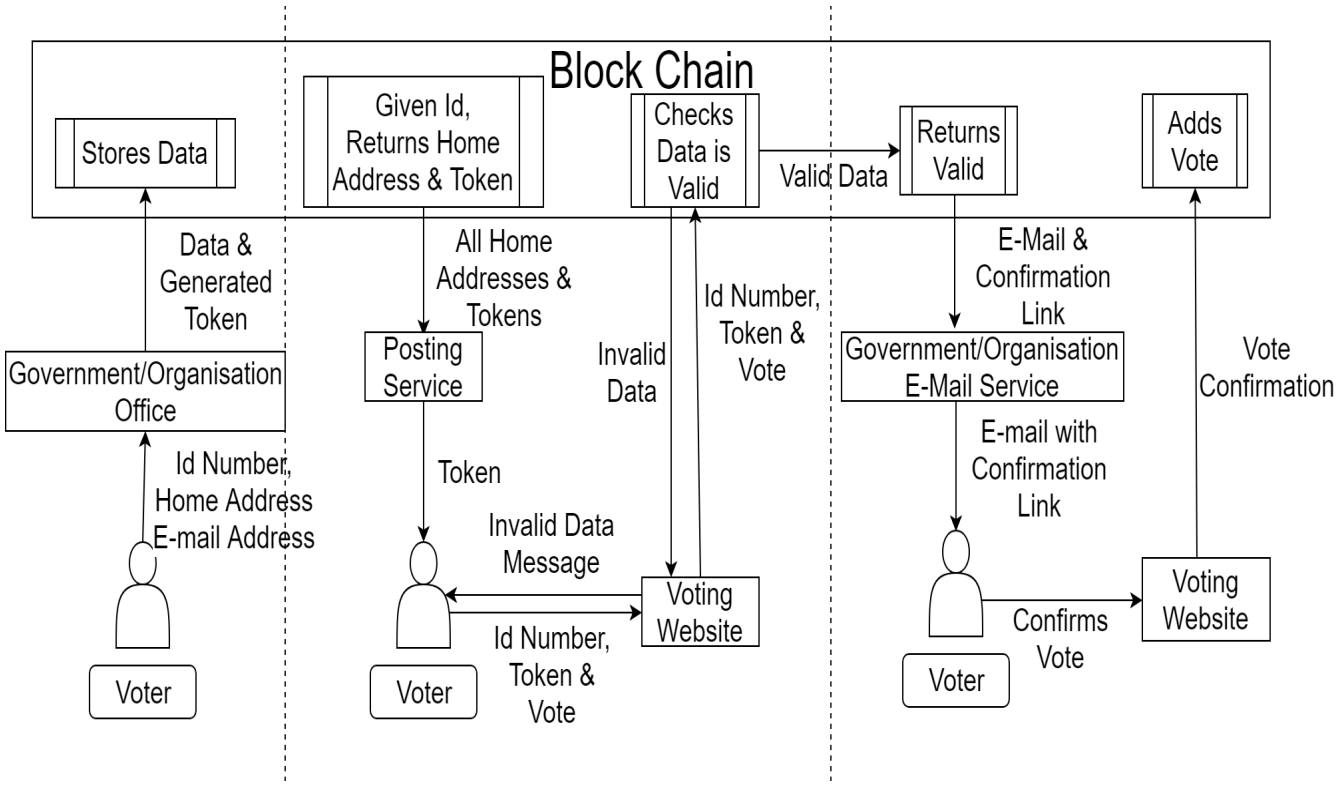

Figure 1. 3 Phase Plan

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. If the voter is to click the link more than once, he/she will receive an error pointing out that the vote has already been confirmed.

4. Project Evaluation

The registration system works, even if for now there is no clerk nor office it is the user that has to input his/her information into the website. As for posting the token by mail, currently the home addresses and tokens are displayed onto a web page. The voting is there however the voting options are hard coded, meaning that they cannot be changed without changing the code. The user still has to input his/her id and the token related to that id, where validation is working properly. However, instead of sending the confirmation link by email, for now the application prints the user's email address and confirmation link into the console of the web browser. Currently the confirmation link shows some sensitive data, this must be encrypted so such data cannot be seen, however this is not yet being done either. If the link is navigated to, there is validation of whether the voter has voted yet, and if he/she has not yet voted, the vote is added and a success message is shown to the voter, else a message stating that the voter has already voted is shown to the voted. As for answering the research questions, when a fully functioning prototype has been developed two type of data collection methods have to be carried out: a questionnaire to a large quantity of voters of varying ages and varying knowledge of using computers, and an interview or interviews, with people in governmental/ organisations which take care of the current voting system.

Through our research we have noted, similar to literature found, that in Ethereum there is no real block size limit but rather a gas limit per transaction. Our tests were not able to reach this limit, yet we do not that our tests were very limited in numbers. A limitation of the current technology is the lack of support for complex structures. To solve this, multiple methods had to return each value within the structure. Whilst we do recognise that this prototype is still in its initial phases it has given us the confidence in the knowledge that blockchain can be used for voting. In the next phase we plan to revise the prototype to allow more flexibility and the scaling of the voting system. We are not confident that a public blockchain would be ideal for this

scenario and thus plan to explore private and hybrid blockchains such as HyperFabric.

The research performed so far is limited to a few tests using a small number of voters, in the next phase we plan to apply it on a larger scale such as the voting for the student union representatives which should be a real world representation. We would also like to gather the marker acceptance of this proposal and thus a number of surveys will be held with participants of the voting system.

5. Conclusion

Throughout the project, we have managed to nd 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 ow 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] Hanifatunnisa, R., Rahardjo, B. (2017). Blockchain based e-voting recording system design. *In*: 2017 11th International Conference on *Telecommunication Systems Services and Applications* (TSSA). p. 1-6 (October). https://doi.org/10.1109/TSSA.2017.8272896

[2] Harris, C.G. (2018). The risks and dangers of relying on blockchain technology in underdeveloped countries. *In*: NOMS 2018 - 2018 IEEE/IFIP *Network Operations and Management Symposium*. p. 1-4 (April). https://doi.org/10.1109/NOMS.2018.8406330

[3] Iskra, E. (2018). Double spend attacks on exchanges (2018), https://forum.bitcoingold.org/t/double-spend-attacks-on-exchanges/1362

[4] Kshetri, N., Voas, J. (2018). Blockchain-enabled e-voting. IEEE Software 35(4), 95-99 (July). https://doi.org/10.1109/MS.2018.2801546

[5] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[6] Rivest, R. L., Shamir, A., Tauman, Y. (2006). How to leak a secret: Theory and applications of ring signatures. *In*: Theoretical Computer Science, p. 164-186. Springer.

[7] Tarasov, P., Tewari, H. (2017). The future of e-voting. *IADIS International Journal on Computer Science & Information Systems*, 12(2).

[8] Wang, B., Sun, J., He, Y., Pang, D., Lu, N. (2018). Large-scale election based on blockchain. Procedia Computer Science 129, 234 - 237.

[9] Wu, Y. (2017). An e-voting system based on blockchain and ring signature. Master. University of Birmingham.

[10] Yavuz, E., Ko, A. K., abuk, U. C., Dalkl, G. (2018). Towards secure e-voting using ethereum blockchain. *In*: 2018 6th *International Symposium on Digital Forensic and Security* (ISDFS). p. 1{7 (March). https://doi.org/10.1109/ISDFS.2018.8355340

[11] Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K. (2016). Where is current research on blockchain technology?a systematic review. PloS one 11(10), e0163477.