Metropolitan State University

Blockchain Technology: Towards a Cryptographic Democracy

Pitch Deck Part Two: White Paper

Oluwaseyi Ola

ICS 698-01 Blockchain Technology

Spring 2022

Dr. Craig Calcaterra

April. 12, 2022

**Introduction**

I became interested in the capabilities of Blockchain Technology after the first lecture in ICS 690-Blockchain Technology class. This class explored a variety of theoretical and practical topics about blockchain technology. These topics included the Ethereum blockchain architecture, Ethereum Virtual Machine, and my favorite, Game Theory. The area of application that piqued my interest is electronic voting. My research revolved around how blockchain technology could be used to enable voting in small- and large-scale elections. The rest of these white paper includes the background, my research findings, and my conclusion.

**Background**

Before we dive deeper into the findings of my research, it is imperative that we understand the definition, scope, and the status of the problem. The underlying issue this research aims to tackle is the to understand why electronic voting systems have not been adopted as a standard for general real-world elections. Furthermore, how can the new emerging and effective technological of blockchain be applied to the electronic voting systems to make them more secure. To achieve this goal of cognizance, we must explore the rudimentary characteristics of traditional e-voting systems and blockchain technology. As part of the aforementioned process, this white paper would 1. explore how blockchain technology works, 2. how it’s implementation (specifically Ethereum) works, 3. How electronic voting built on top of end-to-end-encryption works 4. The current e-voting systems that have been built on top of blockchain technology and finally, 5. Exploring the limitations of the existing systems.

Ethereum is a famous platform built on top of the blockchain architecture. Ethereum emerged after Bitcoin as a solution to move beyond the limitations of Bitcoin. After the success of bitcoin and its proven solution for decentralization, people needed a way to apply blockchain to other areas aside cryptocurrency. Fortunately, Ethereum achieved this by creating a platform where Decentralized Applications could be programmed. The goal of Ethereum’s invention was to give developers the ability to build arbitrary applications that is supported by consensus protocols that possesses features such as scalability, ease of development and integrative ability offered by the previous systems. Ethereum was able to realize this goal by creating an abstracted base layer which consists of a blockchain architecture with a built-in Turing complete programming language. This allows developers to program smart contracts and decentralized applications (DApps). The major programming language for creating DApps is Solidity.

E-voting is a very pertinent area of research in both theoretical and practical contexts. To understand how e-voting can be fully functional and implemented, the theoretical concept behind end-to-end encryption needs to be explored. The structure of an effective electronic voting system involves many different components. These components include security and auditability. The most important of these components is security. This research explores the question of how we can carry out a secure and discreet election. There are important characteristics to consider when assessing the security features of voting E2E voting systems. While some of these properties are co-harmonious, others do conflict with one another. The first is voter privacy which deals with how a voter should not be linked to whatever vote they cast. Another crucial feature of end-to-end encryption is vote verifiability which deals with how votes can be verified on an individual and a universal level. On the individual level, a voter will be able verify that their vote is included in the set of all cast votes. Other properties include eligibility verifiability, accountability, robustness, usability, and accessibility.

As Ethereum is a robust platform for programming decentralized smart contracts, it is a suitable platform to implement an electronic voting system. E-voting is quite beneficial in various ways as it can solve issues such as low voter turnout, support voters with special needs, and decrease election tampering via human interference. However, it could also be argued that electronic elections are open to hacking. In this research, we explore how the various blockchain platforms can be utilized to build an electronic voting system as well as the drawbacks associated with such as systems. The most common implementation of a blockchain e-voting system was BitCongress (no longer available). This system used bitcoin-colored tokens to verify voters as well as cast votes, and the used Ethereum smart contracts to sum up the results. Another interesting system was Follow-MyVote which was from a non-profit organization. This system permits three different types which includes Proportional Representation, Mixed member, and Majority. However, this system still requires a central governing body. Finally, an existing Ethereum based e-voting implementation called Open Vote Network is a fully decentralized e-voting system that does not require any human tallying the votes.

**Research Findings**

There are number of features that make the blockchain technology applicable to e-voting systems. In my research however, I found that the bulletin board advantage as the most significant as the Ethereum blockchain technology implements it perfectly. Storing messages into a popular blockchain such as Ethereum will prevent a singular entity from serving as a gatekeeper. This advantage is enabled by the immutability feature of the Ethereum blockchain. Everyone in possession of the longest chain will see the same data as part of the chain.

The underlying issue found in my preliminary research is majorly based on scalability. There are major drawbacks that concern the usage of the system for real governmental elections. Due to the computational methodology employed by the Ethereum network, gas fees are necessary for all DAOs applications. Now when the Open Vote Network (existing blockchain e-voting system) was created in 2016, there were major limitations that prevents it from being scalable. First, it could not perform the voting process for more than 40 people. Second, the conversion rate of Ethereum to dollar at the time (November 2016) was 1 ether = $11. In 2022, 1 ether is currently around 2500. Finally, the other major drawback is the readiness of the government themselves to accept such a system.

Even though electronic voting is implementable from a theoretical and practical standpoint, we have not seen any real applications of such a system in general elections. The major insight as to why this occurs is because of the low-level trust that the public has for these technologies. In this section, we would be exploring the major factors affecting the public perception. To evaluate how prepared the public is for a blockchain enabled voting system, National Aeronautics and Space Administration (NASA) suggests a nine-degree scale known as Technological Readiness Level to categorize the readiness and the maturity of a technology. This assessment was used to carry out an evaluation on blockchain enabled voting. The two major questions addressed with the TRL are 1. How technologically ready is Blockchain Enabled voting for use in general elections a 2. What further research and developments are required for BEV to move forward in technological readiness**?** The conclusion extracted from the assessment was that blockchain enabled voting technology does not prove at its current state because most implementations based on Ethereum smart contracts have problem with scalability and useability of such systems. This is due to the high gas fees associated with the computation of smart contracts.

**Conclusions**

For blockchain enabled e-voting systems to support nationwide governmental elections, novel methods of scalability for Blockchain based technologies must be introduced. An idea to build up on will be to create an architecture where a centralized government owned server will be charged gas fees (unit being Ether) for every vote casted as opposed to voters paying gas fees themselves. The problem of social acceptability and adoption deals with people’s trust in the blockchain enabled voting. An idea is to solve the social acceptability problem is to create a User Experience that will draw users in.

References

*Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services. 14. 352. 10.1504/IJWGS.2018.095647.*

*Maesa, Damiano & Mori, Paolo. (2020). Blockchain 3.0 applications survey. Journal of Parallel and Distributed Computing. 138. 10.1016/j.jpdc.2019.12.019.*

*“Ethereum Whitepaper.” Ethereum.org,* [*https://ethereum.org/en/whitepaper/*](https://ethereum.org/en/whitepaper/).

*Bin Sharudin, Mohd Shahrul Zharif. “Implementation of Open Vote Network in Blockchain Signaling System Using Decentralized Autonomous Organization SMART Contract in Ethereum Blockchain.” DASH Home, 1 Jan. 1970,* [*https://dash.harvard.edu/handle/1/37365632*](https://dash.harvard.edu/handle/1/37365632)*.*

*Ali, Syed & Murray, Judy. (2016). An Overview of End-to-End Verifiable Voting Systems. Real-World Electronic Voting: Design, Analysis and Deployment*