# EtherVotes: EleiÃğÃţes Baratas com techonologia blockchain

Matheus Faria de Alencar

ETEP - Faculdade de Tecnologia de São José dos Campos
mtsalenc@gmail.com

August 12, 2017

**Abstract**

*Databases and web application servers that hold election information or the backend for elections are extremely valuable and vulnerable to cyber attacks that aim to either practice fraud or delay the election process. Dispite the remarcable improvements in cloud computing, this still causes prices of applications where availability and data integrity to be prohibitively high and as a result many governments simply opt for slower and still vulnerable means of conducting elections. Recent developments on peer-to-peer storage and blockchain development allow for a new family of applications to be developed with the qualities that are required for systems where availability, confidentiality and integrity of data are crucial. This study documents a research on building an application that is DDoS resistant, provides fraud resistance and guarantees zero-down time at a low cost through blockchain technology and peer-to-peer storage.*

## I. Introduction

The era of cloud computing has reshaped the internet and allowed for many new classes of applications to be built. Despite these advancements, building cloud-based applications for elections on representative democracies have remained challenge. This is the case because most election processes must meet very strict requirements to remain consitutional:[1]:

1. Anonymity
2. The election process must not be postponed due to system failure.
3. Each elector has the right to a single vote.

Despite redundancy and server mirroring techniques, the traditional server-client architectures are still vulnerable to DDoS attacks, with even high-end, scalable applications either suffering major performance issues or crashing altogether during such attacks.

Consider a presidential election using a web-based application that displays election results in real time. If a given party notices that it's candidate is losing, it might initiate a distributed attack on the servers that provide the backend that is used to count and collect votes.

By moving the backend to a blockchain with enough nodes, an application becomes invunerable to such an attack since the number of addresses an attacker must target grows lineraly with the number of nodes on the network (eg. $O(n)$ where n is the number of nodes on the network). Furthermore, by programming the blockchain and turning each vote into cryptocoin, the system

[1]The reader should know that this paper will focus on the brazilian election process. However many of the issues documented here are shared by other nations with similar governance models.

immediatly gains the benefit of guaranteeing that no vote can be issued "out of thin air". Section 2 of this paper, describes how to implement issue such a token through the use of Ethereum[2] smart contracts[3].

Although blockchain smart contracts solve a specific set of problems very well, they are not suitable for every problem. On the Ethereum Virtual Machine [4], each computational step requires a certain amount of gas[5] to be paid to the miners as incentive to run the World Computer and for developers to write efficient code. Although this works well to prevent attacks on the EVM through smart contracts, it also makes the implementation of computationally intense cod such as computer graphics rendering way too expensive to be run. The solution proposed on this document, is to move all code that is not crucial to the blockchain to the client side.

Similarly it is also very expensive to data large amounts of data on the blockchain since every full node must have a copy of every state of that data.The question then becomes, how to make the frontend of the distributed application available while keeping the DDoS resistant and zero-downtime qualities provided by blockchain applications?

Section 3 of this document details how the frontend can be made into an AngularJS[6] serverless web application by moving the code and resources to an incentivized peer-to-peer storage system. This causes the it to gain DDoS resistance and zero-downtime characteristics of blockchain-only based applications while keeping operation costs low and providing the usual WWW experience users are used to. Once both the backend and frontend are moved away from centralized servers the whole application becomes truly distributed.

## II. The Problem

TODO Short introduction on the current brazilian voting machines

TODO Present security problems that UnB Professor Diego Aranha and his team documented once granted permission by the Supreme Electoral Court to audit them.

TODO Provide introduction on the problems of the client-server architecture and provide evidence of real-life cases.

TODO Detail constitutional restricions that make internet-powered solutions expensive. The consequences of cyber attacks during elections.

TODO Present introduction of blockchain-only solutions, their issues and costs.

## III. The Proposed Solution

### i. Backend side

TODO The proposed solution for the backend side. Introduce the ERC20 compliant votecoin, issuance method (one coin per elector), how it must be indivisible and only transferable to candidates.

TODO Present the theoretical operation costs of the for operating the backend and how they compare with the current costs of elections.

[2] Ethereum a blockchain technology-based platform that provides a turing complete complete language for programming distributed applications

[3]

[4] Ethereum Virtual Machine is the name given to the virtual computer that executes smart contract code. It is formed by full nodes of the network

[5] Gas is the "fuel" that is paid to the network's miners as incentive for dedicating hardware and electricity to execute smart contract code.

[6] AngularJS definition

TODO Present the concept of payment channels, the Raiden Network and it's potential to lower the costs of elections.

### ii. Frontend side

TODO Present the solution for the frontend:

- The use of Swarm to guarantee availability and DDoS resistance
- The use of Ethereum Naming Service for state-controlled address.
- the use of web3js to communicate with an ethereum client through JSON RPC API.
- The details of using angularJS to enhance UX and guarantee that the user has regular WWW experience without the need to understand underlying technologies.

TODO The need for the client to host an ethereum client on his side and how the proof-of-concept will make use of Metamask

## IV. Related Work

TODO Present Domnik's solution and how it relates to this project.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

### i. Subsection Two

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

## V. Conclusions

A statement requiring citation [Figueredo and Wolf, 2009]. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat.

Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

## References

[Figueredo and Wolf, 2009] Figueredo, A. J. and Wolf, P. S. A. (2009). Assortative pairing and life history strategy - a cross-cultural study. *Human Nature*, 20:317–330.