# **A Block-Chain Implemented Voting System**

The Benefits and Risks of Block-Chain Voting

Francesca Caiazzo Computer System Security Professor Ming Chow December 14, 2016

# **Table of Contents**

Abstract	2
Introduction	2
To The Community	3
The U.S. Voting System	3
Fear and the 2016 Election	4
Blockchain: An Overview	5
Blockchain: A Technical Overview	6
Current Block-chain Voting Implementations  FollowMyVote Implementation	7
Risks and Concerns	9
Call to Action	10
Conclusion	11
Bibliography	

#### Abstract

The United States of America was founded on principles of democracy, making our voting systems a critical aspect of our government infrastructure. In recent years, concern about the integrity and security of our voting systems has become prevalent, particularly in regards to the 2016 Presidential Election. Doubts and worries about our current voting technology include heightened risk of foreign attack to our democratic system, voter fraud, and "rigged" elections. While concerns grow about outdated or insecure voting systems, it is necessary to consider and evaluate new and technologically advanced voting systems. Blockchain technology has evolved in recent years as a secure system for storing data and could be implemented as a secure platform for American elections. This paper explores the current security shortcomings of the U.S. voting system, as well as the feasibility of an online voting system implemented using blockchain technology. Despite security risks and concerns, block-chain data storage in combination with electronic voting is a progressive and secure option for our voting systems.

#### Introduction

In order to understand the potential of an American voting system implemented on the blockchain, there must first be a discussion about the current failings of our voting systems. This paper will first explore current voting systems being utilized in the United States, as well as the weaknesses associated with them. This serves as a starting point for a conversation about fear and vulnerabilities in the election infrastructure and the necessity for considering new options. There are a few currently proposed implementations, each with their own risks and shortcomings. However, despite the valid concerns regarding the blockchain, this voting system remains a viable and exciting prospect for improving our nation's election infrastructure.

### To The Community

As 2016 draws to a close, we must reflect on the state of our government and society as a technological community. In the past year, we have witnessed countless breaches of personal and government security, with repercussions ranging from irksome to catastrophic. We must confront these attacks, as well as yet un-exploited vulnerabilities, with the utmost seriousness. While this certainly means making strides to protect our personal and business-related data, it also means working to protect what makes America, America. Despite the fact our voting system carried us through the 2016 Presidential Election, fear about credulity of the result as well as the possibility of foreign hackers attacking our election were prevalent across the nation. The growth of technical knowledge in regards to exploiting security vulnerabilities vastly outstrips the capacity of our voting system to hold it's own. It is necessary to seriously consider methods by which to centralize and fortify our voting system. This paper asserts that, given necessary time and research, a blockchain implementation of American voting could be the change that this nation needs to see.

# The U.S. Voting System

No singular protocol for managing votes exists in the United States. Voting equipment varies across jurisdiction. Several different voting systems are commonly employed, including paper ballots and Directly Recording Electronic (DRE) systems. Punch card voting systems are also used, as well as ballot marking devices to assist disabled voters. In addition to votes being cast in a multitude of way, that information is also recorded and stored non-uniformly. Paper ballots are typically scanned into a computer system, either at the polling place or a centralized location for that jurisdiction. DRE systems store vote information in the machine's hard drive

and some systems have the capacity to generate a paper audit trail, but not all jurisdictions maintain an audit trail.

A number of concerns have been raised about the current tabulation processes for votes. In 2010, the Brennan Center for Justice published a study containing research specifically focused on the failures and shortcomings of American voting machines. In the study's exploration of the nation's voting systems, it revealed that 43 states still rely on voting equipment that is over ten years old. Among the findings of this study was the fact that sellers and producers of electronic voting machines were legally not obligated to notify anyone about problems cropping up in regards to their machines. Similarly, there exists no resource for public officials to learn about potential problems with their voting machines ahead of time. <sup>1</sup>

The study issues a call for action, asserting that a new system for regulating and correcting defects of the voting system. More explicitly, there is a plea for a "publicly available, searchable centralized database." A blockchain implemented voting system would allow just this.

#### Fear and the 2016 Election

The most recent presidential election was a groundbreaking and historical event in American history for a number of reasons. However, it also marks one of the most widespread panics about the security of the election and voter fraud. President-Elect Donald Trump was principal in this fear-mongering, making off-handed remarks that he ""[was] afraid the election' [was] going to be rigged," but he was not alone. From the time that the news broke about the Democratic National Committee email hack, suspicions and anxieties were mounting. Research

<sup>&</sup>lt;sup>1</sup> Brennan Center for Justice, "Voting System Failures: A Database Solution," accessed December 16, 2016

<sup>&</sup>lt;sup>2</sup> Diamond, Jeremy. "Trump: 'I'm Afraid the Election's Going to Be Rigged'" CNN.

and media demonstrated that the most vulnerable aspect of our election infrastructure was the voting machines themselves.

In August of 2016, a story broke confirming that voting machines in Arizona and Illinois had been compromised by overseas hackers.<sup>3</sup> A number of different groups of ethical hackers took steps to hack into voting machines to demonstrate their vulnerabilities. A group of researchers at Symantec generated a list of many vulnerabilities, and another group from Princteon re-programmed a voting machine in order to demonstrate their blatant security shortcomings.<sup>4</sup> Voting machines were shown to be losing votes and malfunctioning in many different jurisdictions. Perhaps most concerning of all, however, was the shocking number of jurisdictions utilizing voting systems with no paper audit trails. With no audit trail, there is no way to verify that a vote has been cast and no way to detect fraudulent activity.

### Blockchain: An Overview

In order to understand how our voting systems could be implemented using blockchain technology, it is important first to understand how blockchain works and what makes it a secure option for data storage. The most common application of blockchain technology is book-keeping associated with Bitcoin transactions. While Bitcoin is a form of digital currency and much discussion surrounding blockchain focuses on financial applications, any sort of transaction-based data can be stored with blockchain. For our purposes, we will consider a voter casting a vote to be a "transaction."

<sup>&</sup>lt;sup>3</sup> Bruer, Wesley, and Evan Perez. "Officials: Hackers Breach Election Systems in Illinois, Arizona." *CNN*, accessed December 14, 2016

<sup>&</sup>lt;sup>4</sup> Smiley, Lauren. "America's Voting Machines Are a Disaster in the Making." *New Republic*, accessed December 14, 2016

Traditionally, the owner of a database can modify the contents of the database with no repercussions. This isn't a problem – of course a database should be modifiable by its owner. However, in the case of transactions managed by blockchain databases, such as bitcoin or other financial assets, the repercussions of tampering with the transaction data stored in the database are too high for even the database owner to be able to tamper with the database. Consider this in terms of financial assets and votes. The windfall that could arise from meddling in a database could be life-changing, not only for an individual but also for a nation. Such extraordinarily sensitive data demands that *no one*, not even the database manager, should have the capacity to modify data once it has been sent to the database.

Blockchain databases solve this meddling problem, thereby protecting our overly sensitive votery data. On a surface level, the easiest way to conceptualize blockchain is to consider it as a decentralized database. No singular server is responsible for the management and persistence of all of the data. Instead, this responsibility is dispersed across a network of systems, or nodes. This decreases the vulnerability that comes with having a single server. Every single node has access to the database and a "consensus protocol". The consensus protocol contains a set of rules with instructions about which nodes are allowed to modify the database and in what order. As it is named, the consensus protocol allows for all nodes to be in *consensus* at all times.

#### Blockchain: A Technical Overview

On the most basic level, we can think about a blockchain as a file that contains a reference to another file, like a linked structure (hence the name "block-chain"). A blockchain has two major components, the first being the transaction itself, and the second being a reference to the previous block, called a "fingerprint". These fingerprints are the pivotal secure aspect of this type of data storage. A fingerprint can be generated via different cryptographic algorithms,

but the fingerprint of a block is always generated from the fingerprint of the previous block, meaning that the transactions are "chained" together.<sup>5</sup> It follows that if the transaction data of any block were changed, the fingerprint of all of the subsequent blocks would also have to change. This strategy of generating fingerprints protects against malicious tampering.

The fingerprint, or hash, is typically generated using the transaction data contained within the block and a random number, or nonce, associated with the block.<sup>6</sup> The arbitrary nonce value makes it more difficult to contextualize how the block's hash is generated, and thus more difficult for an attacker to solve.

# Current Block-chain Voting Implementations

### FollowMyVote Implementation

The most prevalent initiative to implement blockchain voting is spearheaded by an organization known as FollowMyVote. FollowMyVote preaches a philosophy that they "want every voter to have faith in the democratic process, trust in their government, and feel like their voice matters." FollowMyVote proposes a voting platform that exists entirely online. In this system, a voter would cast their ballot via a downloaded application. United States law requires valid identification in order to vote in public elections. Therefore, the voter would submit their relevant identification to the application to verify their identity as a United States citizen. The voter would have the option to print a receipt of their transaction and ultimately to audit the ballots cast. An additional feature of the FollowMyVote platform is the ability for a voter to vote

<sup>&</sup>lt;sup>5</sup> Kibin, Ejeta, and Kim. "Electronic Voting Service Using Block-Chain.", accessed December 14, 2016

<sup>&</sup>lt;sup>6</sup> Kibin, Ejeta, and Kim. "Electronic Voting Service Using Block-Chain.", accessed December 14, 2016

<sup>&</sup>lt;sup>7</sup> "Blockchain Voting: The End-to-End Process." Follow My Vote, accessed December 14, 2016

early and modify their vote should they change their mind in the days leading up to the election.

Hypothetically, with use of this system, tallying votes would be instantaneous as well.

As anonymity is a crucial staple of the American voting system, and block-chain style databases hinge on creating a publicly auditable database, it is imperative for any block-chain voting implementation to account for both identity verification and the ability to vote anonymously. FollowMyVote proposes the use of a form of cryptography known as elliptic curve cryptography, or ECC, to maintain voter anonymity. ECC is a form of asymmetric cryptography, and FollowMyVote utilizes it to two key-pairs per voter, one for verifying identity, and one for voting. The use of these two different key-pairs allows a voter to verify their vote without sacrificing their right to vote anonymously.

FollowMyVote utilizes Bitshares as their blockchain platform, although they acknowledge a hope that one day FollowMyVote will be compatible with many different blockchain implementations.

#### **BitCongress**

A second currently proposed blockchain voting platform is called BitCongress.

BitCongress gives a nod to Bitcoin in the introduction of their proposal, acknowledging that "The advantages of this system shows how a peer to peer system running a decentralized node network can become the most powerful computer network on the planet in under a decade." <sup>9</sup>

BitCongress relies on the amalgamation of four existing platforms: Bitcoin, Smart Contracts, Counterparty and Blockchain technology.

<sup>&</sup>lt;sup>8</sup> "Elliptic Curve Cryptography." Follow My Vote. accessed December 14, 2016

<sup>&</sup>lt;sup>9</sup> "BitCongress Whitepaper." BitCongress Whitepaper, accessed December 14, 2016

Like FollowMyVote, BitCongress proposes a system in which every vote is hashed into the blockchain (in this case, the Bitcoin Blockchain as opposed to Bitshares). However, in some ways, BitCongress looks to extend its impact beyond just a voting system, describing the platform as tool for governance and legislation, and stating that they hope to re-structure the governing bodies that use the platform.

The BitCongress platform centers on the integration of an application called AXIOMITY. AXIOMITY is the BitCongress wallet that allows users to participate in every aspect of the democratic process. While FollowMyVote uses EEC to generate private keys, BitCongress utilizes individual tokens, called VOTE tokens. These tokens are used to vote for candidates and legislation, and are returned to the individual when the election has ended, limiting unnecessary inflation of private tokens.<sup>10</sup>

### Risks and Concerns

No large-scale technical changes exist without concerns, and blockchain voting is no exception. The most prominent concern about a widespread implementation of blockchain voting is lack of experimental evidence that such a system could hold up in a large-scale use case, say, a national election. Counterintuitive as it may be, the wide variety of voting systems used in the U.S. actually serves to make our election infrastructure a little more resilient. Despite the fact that much of the voting equipment is outdated or potentially insecure, there is next to no potential for a hack to universally compromise a national election *because* we don't have centralized voting infrastructure. It would be dangerous to implement an end-to-end online voting application without first performing large-scale, intensive experimentation.

<sup>&</sup>lt;sup>10</sup> "BitCongress: The Decentralized Blockchain Voting Platform", EconoTimes, accessed December 14, 2016

An additional concern surrounding blockchain voting is in regards to private security keys. As described above, FollowMyVote makes use of a cryptographic key by which a verified voter can cast their ballot. Some critics of blockchain voting argue that this technology will simply force malicious attackers to change the focus of their attacks, focusing instead on compromising voter keys. In an analysis of blockchain voting, Forbes reported that cryptographic voting specialist Dr. Jeremy Clark remarked that "requiring users to manage cryptographic keys has been shown through usability experiments to be difficult." He recommended against the FollowMyVote method of allowing voters to use personal pphoens and instead advised a system that still utilizes blockchains but mandates that voters show up to vote in person on Election Day. <sup>11</sup>

#### Call to Action

While the security risks and concerns associated with cryptographic voting are valid, they are also addressable and solvable. FollowMyVote, the primary initiative in creating this technology, is not a perfect solution by any means. However, the risks and problems with their implementation can be solved. While FollowMyVote hopes to create an end-to-end online voting system fueled by an application, a more sensible solution for American voting would be that suggested by Dr. Jeremy Clark, in-person voting that utilizes blockchain technology.

For blockchain voting to be seriously considered as a solution to our nation's crumbling election infrastructure, we need to simultaneously see an explosion in wide-spread experimentation with this technology and further attempts to shed light upon the failures and dangers of our outdated and non-homogenous voting systems.

Koven, Jackie Burns. "Block The Vote: Could Blockchain Technology Cybersecure Elections?" Forbes Magazine, accessed December 14, 2016

### Conclusion

The voting system in the United States is in dire need of an overhaul. Current voting systems are simultaneously outdated, subject to machine malfunction, and vulnerable to security attacks and voter fraud. Fear and concern surrounding the 2016 General Election highlight the pressing need to institute change. The decentralized nature of our voting systems as well as alarming inconsistency in the generation of paper audit trails necessitates the creation of a centralized, public voting system that virtually always creates an easy-to-audit paper trail.

Despite valid concerns about the efficacy and security of a widespread utilization of this type of voting platform, the benefits of having a publically auditable and tamper free way of keeping track of votes outweigh the risks. A block-chain implementation of electronic voting is a viable and secure solution to the problems the nation faces as a result of our current voting systems.

# Bibliography

- "A Gentle Introduction to Blockchain Technology." *Bits on Blocks*. N.p., 24 Nov. 2016. Web. 14 Dec. 2016.
- "BitCongress: The Decentralized Blockchain Voting Platform EconoTimes." *EconoTimes*. N.p., 23 Mar. 2016. Web. 14 Dec. 2016.
- "BitCongress Whitepaper." BitCongress Whitepaper. N.p., n.d. Web. 14 Dec. 2016.
- "Blockchain Voting: The End To End Process." Follow My Vote. N.p., n.d. Web. 14 Dec. 2016.
- Bruer, Wesley, and Evan Perez. "Officials: Hackers Breach Election Systems in Illinois, Arizona." *CNN*. Cable News Network, n.d. Web. 14 Dec. 2016.
- "Cryptographically Secure Voting." Follow My Vote. N.p., n.d. Web. 14 Dec. 2016.
- Diamond, Jeremy. "Trump: 'I'm Afraid the Election's Going to Be Rigged'" *CNN*. Cable News Network, n.d. Web. 14 Dec. 2016.
- "Elliptic Curve Cryptography." Follow My Vote. N.p., n.d. Web. 14 Dec. 2016.
- "How Vulnerable to Hacking Is the U.S. Election Cyber Infrastructure?" *U.S. News*. U.S. News, 1 Aug. 2016. Web. 14 Dec. 2016.
- Koven, Jackie Burns. "Block The Vote: Could Blockchain Technology Cybersecure Elections?" *Forbes*. Forbes Magazine, 30 Aug. 2016. Web. 14 Dec. 2016.
- Kibin, James Joshua I, Tekachew Gobena Ejeta, and Hyoungjoong Kim. "Electronic Voting Service Using Block-Chain." *The Journal of Digital Forensics, Security and Law* 11.2 (2016): 123-35. *ProQuest*. Web. 14 Dec. 2016.
- Newman, Lily Hay. "Officials Are Scrambling to Protect the Election From Hackers." *Wired*. Conde Nast, 21 Sept. 2016. Web. 14 Dec. 2016.
- Norden, Lawrence. "Voting System Failures: A Database Solution." *Brennan Center for Justice*. Brennan Center for Justice, 13 Sept. 2010. Web. 14 Dec. 2016.
- Smiley, Lauren. "America's Voting Machines Are a Disaster in the Making." *New Republic*. N.p., 19 Oct. 2016. Web. 14 Dec. 2016.
- "Voting Equipment in the United States." *Verified Voting*. N.p., 06 Nov. 2016. Web. 14 Dec. 2016.
- "Voting Methods and Equipment by State." Ballotpedia. Ballotpedia, n.d. Web. 14 Dec. 2016.