Fostering Trust and Trustworthiness in Election Infrastructure Using Trustless Technologies

Eric Landquist, Ph.D. Linda Hutchinson
Voatz, Inc.
el@voatz.com linda@voatz.com

November 29, 2021

1 Introduction

A fundamental issue in elections management is the oversight of voter registration databases. Since registration records are digital, there is an increasing burden on IT staff to maintain and safeguard these systems and to securely interface them with other networks across the various states, territories, and counties. Increasing trust and trustworthiness in these systems is therefore critical, as inaccurate or insecure registration records increase the risk of an election being compromised by a malicious actor. In addition, IT staff can play an important and valued role in making registration databases more complete by identifying and contacting eligible, unregistered citizens.

In Section 2, we discuss the two applicable issues at hand: election access and registration database integrity. Section 3 describes fundamental blockchain concepts and Section 4 provides further details on how blockchain technology can be used to identify eligible voters and also to assess the integrity of sensitive data, such as voter registration records, without compromising privacy. We give some security recommendations on the implementation of such a solution in Section 5 and make concluding remarks in Section 6.

2 Election Access and Voter Registration Integrity

A 2012 report by Pew Trusts estimated that over 2.75 million voters were registered in more than one state and nearly 13% of all voter registration records were significantly inaccurate or invalid. [4] They also noted that in 2008, voters cast nearly two million provisional ballots, possibly due in part to the issues noted above. [4] Though this report is nearly a decade old, these issues remain in many locations. Remote voters in particular need to verify their identity. If a record is flawed to the point that an identity verification attempt fails to match a voter's credentials and identification documents with official records, then the vote of an eligible, registered voter could be delayed or even denied.

A recognized leader in updating its state-wide voter records is West Virginia Secretary of State Mac Warner. Over the last four years, Secretary Warner's office has worked with the state's county clerks to identify and eliminate "364,301 deceased, outdated, duplicate, out-of-state, and convicted felon voter files." [5] Further, they used technological means to identify and contact unregistered residents who were eligible to vote. Over this same period of time, they registered 255,888 new voters. [5]

A 2019 report by Pennsylvania Auditor General Eugene DePasquale commissioned by the Pennsylvania Secretary of State noted issues similar to those that were discovered and rectified in West

Virginia. [1] Mr. DePasquale's report contains a number of recommendations to improve the security, completeness, accuracy, and auditability of voter registration records. Further, a recent lawsuit filed by the Public Interest Legal Foundation alleges that roughly 34,000 active voters registered in Michigan are deceased. [2] This lawsuit indicates growing scrutiny of voter registration systems' data by the general public. This further implies an increasing expectation of transparency in election management.

3 Blockchain Technology: Background

An idea to increase voter registration database integrity is to store a digitally signed, cryptographic hash of each voter record on a blockchain using a smart contract. Before describing this idea in more depth, we define the terms for clarity. If one has a cryptographic signing key, then that individual can create a **digital signature** on any digital document to prove that he or she had access to the document; the signature can be verified by anyone. A **cryptographic hash function**, such as SHA-256, creates an irreversible digital fingerprint of any digital document that uniquely identifies that data; it is computationally infeasible to find two documents that hash to the same value. A hash function may also input a random string called a **salt** to reduce the chance that input data is guessed by brute force.

A **blockchain** is a database that is distributed among multiple servers or computers (typically called **nodes** in this context) in a way that one can append data to the database, but one cannot erase any data. Blockchains are structured like linked lists; a hash of one set of data (called a **block**) is included in the subsequent block to establish a link between the two blocks. A blockchain can be **permissioned**, in which only certain nodes are authorized to propose a new block, or **permissionless**, in which any node can propose a new block. For example, Hyperledger Fabric is a permissioned blockchain, but the Bitcoin blockchain is permissionless. A **consensus mechanism** describes the method in which the nodes agree on whether or not a proposed block satisfies the conditions necessary to be added to the blockchain. Consensus allows for nodes that may not trust each other to agree on the data stored on the blockchain. In this way, a blockchain is an example of a **trustless** technology. A **smart contract** is a program that runs on a blockchain and executes when certain conditions are met.

4 Blockchain Solution

To expand on the idea, one could create a unique digital identifier for each resident and/or registered voter based on certain immutable characteristics, such as birth name, date of birth, and social security number. Each resident's record can then be salted, hashed, and digitally signed by at least two authorized officials, then stored on a blockchain via a smart contract under the unique digital identifier. The smart contract manages the location of each record on the blockchain, along with its hash value and signatures. In this way, resident and voter registration information can be posted publicly without any concern that private information is exposed. A comparison of the hash on the blockchain with the hash in the voter registration database will allow any official or auditor to readily distinguish an authorized creation, alteration, or deletion of a record from the actions of a malicious attacker.

There are additional benefits to such a system. Residents and voters could determine if their information has been entered correctly by computing the hash of their records and looking it up on the blockchain, without having to access their records directly. Errors would prompt the resident to submit corrections to the appropriate county office. Restricted access to the database naturally adds a layer of security as well. For example, duplicate records would be easy to identify and delete when duplicate digital identifiers are found. If information about every resident of a state is stored in a database and privacy-masked on a blockchain as well, the database can be queried to quickly and efficiently identify and contact unregistered residents who are eligible to vote.

5 Conditions

In order for these database and blockchain solutions to work, certain reasonable conditions would have to apply. Certainly sufficient resources such as personnel, budget, and time are necessary and may be strained in many offices. A **zero trust** architecture would be recommended in order to safeguard database and blockchain access and to carefully authorize certain individuals and organizations to create, modify, delete, and read these databases, with proper oversight in place for accountability. [3] To underscore the last point, zero trust architecture specifically guards against insider attacks. For example, a county records office could be allowed to flag the registration records of deceased voters for deletion, and may be allowed access to delete records for that very purpose. As another example, the U.S. Postal Service and Department of Motor Vehicles could be given access to flag the registration records of voters who have moved and may be allowed access to create, modify, or delete records as appropriate. Internal logic could also be established in these databases to check that information, such as street address, county, state, and ZIP code are correct, valid, and consistent. In all situations, zero trust architecture establishes proper oversight and accountability on all database and blockchain operations. As previously noted, a blockchain facilitates this necessary transparency, so issues ranging from benign human errors to malicious insider attacks can be identified.

Since they are impartial third parties, we recommend that auditor general offices and any other auditor so authorized by the appropriate state or territorial office be given sufficient access to all records, information, and documents in order to assess the completeness, accuracy, and security of voter registration databases and processes.

6 Conclusion

In conclusion, the public has increasing demands of election access, as well as transparency, accuracy, and security of voter registration records. Much of the burden to carry out this work falls upon IT staff. As a company that understands blockchain technology, we see the relevance of this technology to the situation at hand. Properly executed, blockchain technology and smart contracts can be applied to provide completeness, transparency, integrity, and auditability to any database, especially voter registration records.

References

[1] Eugene DePasquale. A performance audit: Pennsylvania Department of State Statewide Uniform Registry of Electors. Technical report, Commonwealth of Pennsylvania Department of the Auditor General, Harrisburg, PA, December 2019. https://www.paauditor.gov/Media/Default/Reports/Department%20of%20State_SURE%20Audit%20Report%2012-19-19.pdf.

[2] Public Interest Legal Foundation. Public Interest Legal Foundation v. Jocelyn Benson, Michigan Secretary of State. https://publicinterestlegal.org/wp-content/uploads/2021/11/Doc-1-PILF-v.-Benson-Complaint.pdf, November 2021.

[3] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. Zero trust architecture. SP 800-207, NIST, Gaithersburg, MD, August 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final.

[4] Pew Trusts. Inaccurate, costly, and inefficient evidence that America's voter registration system needs an upgrade. Technical report, The Pew Center on the States, Washington, DC, February 2012. https://www.pewtrusts.org/~/media/legacy/uploadedfiles/pcs_assets/2012/pewupgradingvoterregistrationpdf.pdf.

[5] Mac Warner. West Virginia deploys cell phone technology to all citizens to report election fraud. *WV News*, November 15, 2021. https://www.wvnews.com/west-virginia-deploys-cell-phone-technology-to-all-citizens-to-report-election-fraud/article_bae5aeb0-435b-11ec-b089-df97dfede358.html.