BLOCKED & CHAINED:

Design of a Novel, Secure Cryptographic & Blockchain-based Voting Architecture

Arul Nigam and Malhaz Jibladze

Abstract

The United States government has found paper voting systems to be inefficient, unauditable, prone to tampering, and expensive. Electronic voting is a promising solution to these issues; however, transitioning to electronic voting systems poses two major challenges: 1) increased susceptibility to hacking, and 2) high susceptibility to voter fraud. In 2016, a third of reported cases of voter fraud were due to duplicate voting. This number is expected to increase after switching to an electronic system [8]. In this paper, we propose the implementation of a scalable, electronic, blockchain-based voting system that has the potential to reduce voter fraud while simultaneously preventing hacking and external interference in the United States' elections.

1. Introduction

Biometric techniques can be used to reliably distinguish and identify voters, detect and eliminate voter fraud, and replace the need for burdensome voter identification documents [15]. Iris recognition is a portable biometric technology that uses pattern recognition and infrared light to capture an image of a person's iris, which is a unique identifier [5] [13]. According to a 2018 report from the National Institute of Standards and Technology (NIST), current iris recognition systems are associated with false-negative identification rates of 0.0067 and false non-match rates of 0.0057, distinguishing them as state-of-the-art biometric devices [18].

Cryptographic techniques like blockchain allow for transparency, privacy, and integrity of a system. Blockchain ensures the immutability of data, removes the need for a central, trusted node, and is publicly auditable — all necessary qualities for secure electronic voting systems. According to the Observatory of Public Sector Innovation, blockchain is "a [linear] chain of blocks." Blocks are immutable and auditable records consisting of a timestamp, a unique hash, and data, which in this implementation would include the candidate chosen by the voter. Each block is added individually to the chain in a sequential manner and contains a "group of validated transactions." Blocks are linked through hashing, a process by which each block is assigned a unique hash code, thus protecting the original data. For this research, we utilized SHA-256, a 1-way cryptographic hash that can convert iris images into a concise, unique representation [16].

The mathematical algorithm used to generate the SHA-256 hash function, specified by the NIST in FIPS PUB 180-4, uses an iterative set of transformations to calculate a 256-bit hash for data in several different formats, including a digital representation of an iris scan. This hash has two important properties. First, it is impossible to recover the original data from the hash, because such a function is not resersible. Second, even a tiny change to the original data will result in the computation of a completely different hash because of the one-way alteration process that the hash undergoes for each new dataset [12].

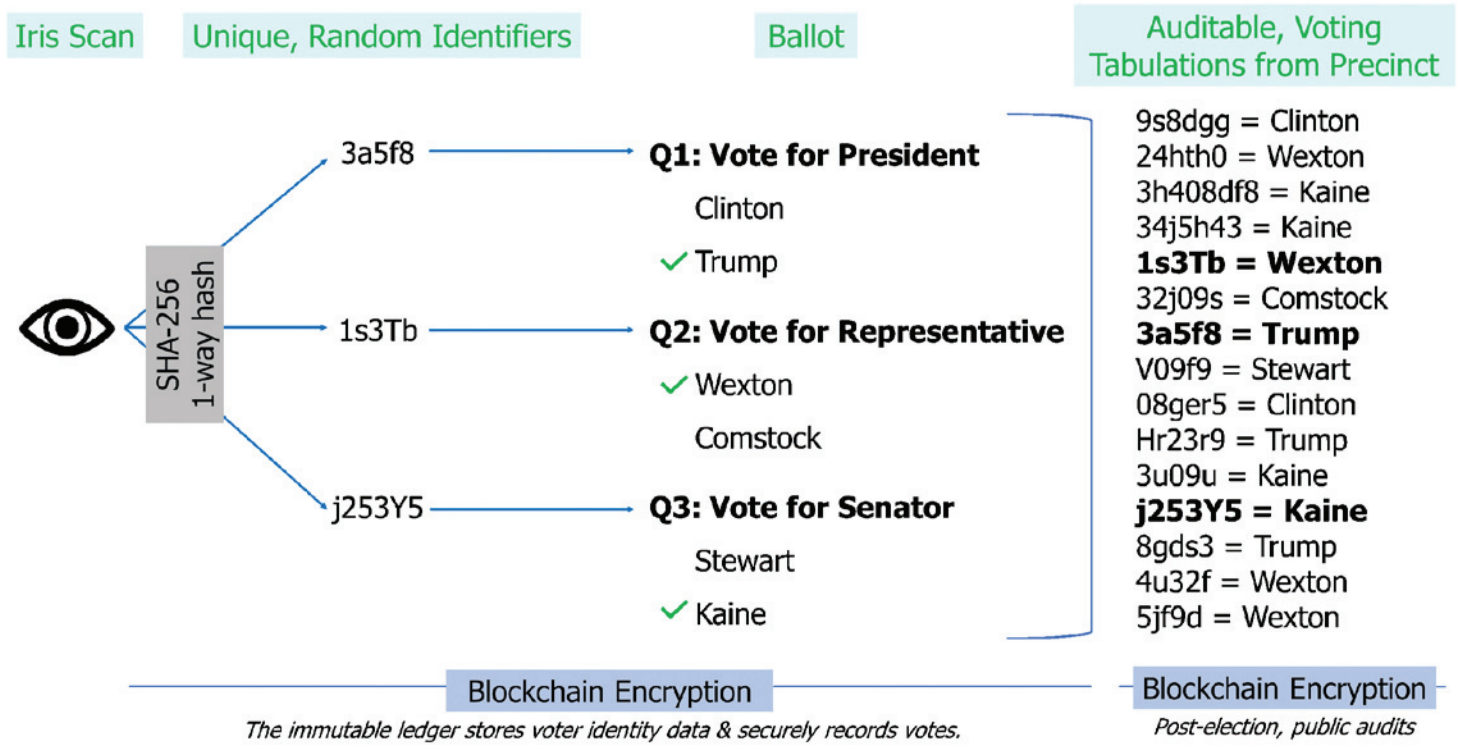

Figure 1. Novel system architecture design & sample workflow

2. Methods & Materials

We researched biometric security and cryptographic techniques and designed a secure electronic voting system architecture implementing these technologies. A scalable version of the system architecture was implemented in MATLAB.

This electronic voting system architecture consists of the following components (Figure 1):

1. Biometric security using an iris scan.
2. A repository of hashed biometrics for two purposes – first, to verify that a voter is registered to vote, and second, to ensure that a voter does not vote more than once.
3. An immutable blockchain-based register to capture each vote as a transaction. This register is public (but does not include personally identifiable information that could connect the vote back to a specific voter), and thus auditable, ensuring that a vote cannot be changed or tampered with once it has been recorded. Each vote on a ballot will be recorded independently (i.e. a given individual's vote for President, Senator, and Representative will each be recorded separately).
4. A cryptographic module that secures and transforms the identity of each voter in the blockchain-based register. This ensures that anyone can verify the votes and election results (e.g. they can independently count the votes), but it remains impossible to associate a particular vote with an individual voter, ensuring anonymity.

3. Results

Overall, the implementation of the outlined scalable design architecture allows for several improvements to the electoral system in the United States (Figure 2).

The iris scan successfully reduces voter fraud by 33% by eliminating duplicate voting, based on the Heritage Foundation's Election Fraud Database. Encryption with blockchain allows for transparency, verifies that all votes were fairly counted, guarantees that votes were not tampered with or changed, and ensures voter anonymity.

This new system architecture will eliminate 5 of the 7 methods of voter fraud as described by the Heritage Foundation's Election Fraud Database, namely: 1) impersonation, 2) false registrations, 3) ineligible voters, 4) duplicate voting, and 5) altering ballots.

4. Discussion

Our electronic voting architecture successfully demonstrates the ability of a blockchain-based system to eliminate sources of voter fraud and reduce the risk of external interference when measured against factors identified by the Heritage Foundation's Election Fraud Database and other standard fraud measurement parameters. The implementation in MATLAB serves as a proof-of-concept that the architecture design can actually be built in a functional way. It also prepares the architecture to be scaled and tested for security and integrity under high transaction rates in the future.

Our focus was to ensure that as society moves toward electronic voting systems, we solve known obstacles without introducing vulnerabilities. In addition, public confidence in a voting system is critical, especially with an increasingly polarized electorate. Therefore, our voting system is demonstrably resistant to voter fraud. We propose that the next steps focus on detailing the logistical implementation of this system. We recommend gathering iris images during the vehicle licensing process, and/or during immigration, and testing the system in a small number of districts prior to expanding nationwide.

Further research can explore mechanisms of expanding the transactional performance of blockchain networks. According to an analysis from the Brennan Center for Justice,

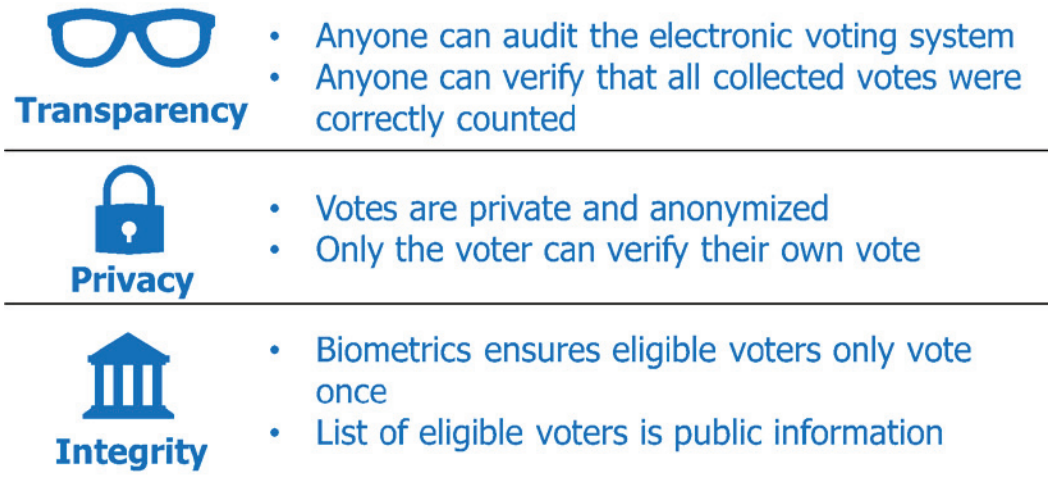

Figure 2. Notable advances found in our architecture

"In the typical state, 35 to 45 percent of voters surveyed arrived at their polling place during the peak three hours of voting" [4]. Based on a report from the California Secretary of State, 6,166,915 people voted in person during the 2016 General Election. This would imply that between 2,158,420 and 2,775,112 citizens voted during the busiest three hours (or 10,800 seconds,) meaning that a blockchain-based voting system in California would need to be able to handle a peak of 200 to 257 transactions per second [3].

Research must identify ways to increase the transaction rate so that the blockchain-based electronic voting system can handle these high voter turnouts. Additionally, part of the robustness of blockchain networks arises from a distributed consensus mechanism. This mechanism could be ineffective when a single entity (e.g. a state government or other well-funded organization) controls more than 51% of the nodes [7]. Therefore, further research should explore ways to limit the overconcentration of nodes.

Combining the proposed unique architecture developed in this study with results from the additional research recommended above would allow for a strong and practical electronic voting system.

5. Conclusion

This paper outlines the design and implementation of architecture that uniquely combines blockchain-based electronic voting and a biometric iris recognition system to ultimately improve security and transparency in voting. Such a system, when fully implemented, will offer many benefits: quantitatively reducing several types of voter fraud, preventing hacking and external interference in the United States electoral process, allowing independent third parties to verify the integrity of the voting system, and providing voters with confidence that their vote was recorded accurately.

6. References

[1] Agora (2019). Bringing our voting systems into the 21st century. [Online] Available at: https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5b6c38550e2e725e9cad3f18/1533818968655/Agora_Whitepaper.pdf

[2] Ayed, A. B. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. *International Journal of Network Security & Its Applications, 9*(3), 01–09. doi: 10.5121/ijnsa.2017.9301

[3] California Secretary of State. (2016, November 8). General Election - Statement of Vote - November 8, 2016. Retrieved from https://elections.cdn.sos.ca.gov/sov/2016-general/sov/03-voter-participation-stats-by-county.pdf

[4] Cortés, E., Ramachandran, G., Howard, L., & Norden, L. (2019, December 19). Preparing for Cyberattacks and Technical Failures. Retrieved from www.brennancenter.org/sites/default/files/2019-12/2019_12_ContingencyPlanning.pdf

[5] De, & Ghoshal, Dibyendu. (2016). Human Iris Recognition for Clean Electoral Process in India by Creating a Fraud Free Voter Registration List. *Procedia Computer Science. 89*. 850-855. 10.1016/j.procs.2016.06.071.

[6] Diamond, S. (February 2018). Are You Voting "No" to Paper Ballots? Retrieved from https://www.eballot.com/blog/voting-no-to-paper-ballots

[7] Dunietz, J. (2018). Are Blockchains the Answer for Secure Elections? Probably Not. Scientific American. Retrieved from https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probably-not/

[8] Goel, S., & Meredith, M. (2017). One Person, One Vote: Estimating the Prevalence of Double Voting in U.S. Presidential Elections.

[9] Hao, F., & Ryan, P. (2017). Real-world electronic voting: design, analysis and deployment. Boca Raton, FL: Taylor & Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa Business.

[10] How Blockchain Could Secure Elections. Retrieved from https://www.cbinsights.com/research/report/blockchain-election-security/

[11] Howell, G. (2019). NIST's Role in Election Security.

[12] Information Technology Laboratory NIST. (2015, August). FIPS PUB 180-4, Secure Hash Standard (SHS) - NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[13] Kelley, J., Sheard, N., Lynch, J., Hussain, S., Guariglia, M., & Tsukayama, H. (2019, October 26). Iris Recognition. Retrieved from https://www.eff.org/pages/iris-recognition

[14] Jaffe, J., Iii, C. S., & Coblentz, J. (2018). Modeling Voting Service Times with Machine Logs. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3216178

[15] Nnachi Lofty, Amah & Mansour, Ali & Hamisu, Muhammad. (2019). Towards A Secure E-Voting Model with Blockchain and Biometric Technology.

[16] Observatory of Public Sector Innovation. (2018). Blockchain and its Use in the Public Sector.

[17] Penn Wharton Public Policy Initiative. (2016). The Business of Voting: Market Structure and Innovation in the Election Technology Industry. Public Policy Initiative. Retrieved from https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-votin.

[18] Quinn, G. W., Grother, P., & Matey, J. (2018). IREX IX part one, performance of iris recognition algorithms. doi: 10.6028/nist.ir.8207

Spread Designers: Isabelle Deng
Editors: Junho Lee and Sahana Ramesh