Analysis of Secure Electronic Voting Using Blockchain Technology

Carter H. Corneil, Sherief Elsowiny
TSYS School of Computer Science
Columbus State University
Columbus, GA, USA
corneil_carter@columbusstate.edu, elsowiny_sherief@columbusstate.edu

Abstract-
Blockchain has become a popular revolutionary technology in recent years, especially since the creation and rapid adoption of Bitcoin. One reason it has become well known is because it provides a secure and transparent ledger of transactions. In the aftermath of the 2020 US Presidential election, questions arose surrounding the security and transparency of the entire voting process. This begs the question: Can Blockchain be used to resolve these questions, and restore confidence in all Americans regarding election integrity? One of the challenges that a solution like this may face is trust. Will everyone ever completely trust a software-based solution after the amount of software exploitations we see on an annual basis. In this paper, we will discuss how Blockchain could potentially be a viable solution due to its secure nature. We will discuss a couple approaches taken to implement secure electronic voting using Blockchain and review the results.

Keywords - Blockchain, E-Voting

I. Introduction

In 2020, the United States saw controversy over the handling of the election. Citizens of the United States were constantly being informed of registering to vote, how to mail in your vote, and that their voice matters. In a world where technology has advanced to new heights, it is unfortunate to see how antiquated our ways of voting are. The Covid-19 pandemic impacted the ways in which voters expressed their right to vote. Many Americans were left waiting in anticipation of the results that were being counted slowly. The ballots were also counted by several points of failures, where transparency was a question for some. In our current ways of voting in the United States, a voter must be registered to vote. Due to the Covid-19 pandemic, mail-in voting was adopted and expanded in most states throughout the country. This led to some questions regarding proper voter registration and identification. Many accusations arose over voter fraud because of this. With the advancement of technology, there must be a way to design a system that is secure enough to allow electronic voting either by a mobile device or computer, or at a polling station.

There is no doubt that technology has advanced at a stunning rate. In this paper we explore the integration of blockchain technology into e-voting and a couple of proposed systems.

II. Background/Motivation/Problem

A. *Blockchain*

Blockchain is a Distributed Ledger Technology (DLT). In other words, it is a decentralized database that is managed by multiple parties. It records information in a way that makes it virtually impossible to modify. Blockchain works by creating a public history of transactions and distributes it to multiple independent nodes in a network. Every time a new transaction occurs in a system, this data is stored in the form of a block. These transactions are linked together, creating a public ledger that is distributed to each node involved, making it decentralized. This provides complete transparency since all parties are aware of every transaction on the blockchain. Along with decentralization, Blockchain technology has several other properties that make it more secure and auditable. Listed below are a few of these:

- Encryption: All records on a blockchain are individually encrypted. This ensures that the only nodes that will be able to read the data are the ones it is meant for.
- Unanimity: In order for a transaction to be added to a blockchain, all parties must agree to the validity of the record. This preserves the integrity of the ledger.
- Immutable: Any records that have already been validated and added to the blockchain are permanent and cannot be changed. Blockchain does this by recording transactions with an immutable cryptographic signature called a hash. This allows for a completely accurate audit trail.

Blockchain works similarly to the way a Google Doc works. A Google Doc, when shared with a group of people, is distributed rather than copied or transferred. This decentralizes the changes made to the document and gives everyone full, real-time access to the document. No one is locked out while waiting for someone else to finish their changes. Also, modifications to the document are recorded and distributed, making them transparent and preserving the integrity of the document. If the group wanted, they could implement a way to force a unanimous vote for a change to be added to the document. It is clear to see how each of the Blockchain properties listed above are in play in the Google doc example. These properties are what would make the Google Doc the much more preferred way for collaboration over passing a single, centralized document around the group. These properties are also what make Blockchain a revolutionary technology with the potential to change the way today's systems work.

B. *Voting*

The process of electing officials to lead a country is a staple of a democracy. Traditionally, this voting process has been done by paper ballots at local polling stations. Over time, as millions and millions more people are voting in each election, this process has shown some negative aspects. People are having to wait several hours in a line to vote and counting the ballots can take up to several days. Another issue with this process is that it does not bode well during a pandemic where social distancing is required. This reared its head during the 2020 presidential election, which occurred during the Covid-19 pandemic. Obviously, measures had to be taken to ensure the health and safety of millions of voters throughout the country. One of these measures taken involved the process of counting the ballots. Historically, this is a public process in which anyone can observe. In 2020, due to social distancing, only official counters were allowed in the building in several cases. Another one of these measures included an extension of mail-in voting, which historically has been limited to active-duty military serving out-of-state, or people who are away from their home state during the election period. In 2020, many states expanded the eligibility for this, some more strict on the rules than others. Some states mailed a ballot to every eligible voter. Some states allowed mail-in ballots to be counted if they were received several days after Election Day. A lot of these changes were met with controversy, especially by the ones on the side who did not like the outcome of the election.

The 2020 presidential election raised a lot of questions about election integrity. The paper and pen voting process may have some flaws, but it seems to be the most trusted process. However, what if there was a way to implement a secure, auditable, completely electronic process? Theoretically, it would speed up the process by a lot, and reduce much of the headaches associated with voting. Given the properties of blockchain discussed earlier in this section, it seems to be a perfect solution. Especially if there was a way to do the voting remotely and keep it secure. No longer would people have to wait several hours in line, or trust the counting done by humans. Everything would be done by computers and would be completely auditable. In the next couple sections of this paper, we will discuss some of the approaches taken to achieve this, and whether they could potentially be a viable solution.

III. Approaches

As part of the research done for this paper, we reviewed several articles with approaches for using Blockchain to implement electronic voting, and a couple of them stood out. The first was dubbed "Auditable Blockchain Voting System (ABVS)" [1]. This system is made up of three components: super-node, trusted nodes, and polling stations. The super-node would be considered the main Blockchain, and the official vote count would come from it, while the trusted nodes would act as backups. All the nodes provide computing power and storage space for the blockchain. They will also all play a part in the verification of transactions done by the blockchain. ABVS also has three phases as part of the election

process: initiation, voting, counting and verification. The main point of initiation is setting up equipment and software, and generating unique Vote ID tokens for each voter which will be used to authorize votes. The voting phase is done at an official voting location; therefore, it is not remote. Each voter takes a random Vote ID token for authorization and casts a vote as is done in traditional voting. Once the vote is cast, it is added to the blockchain. When the voting deadline passes, and the last voter has voted, the counting and verification phase begins. In this phase, the votes are counted from the super-node and the trusted nodes and are compared for verification. There is also a paper trail of each vote to add an extra layer of verification. To increase security of ABVS, two agents are used in the voting phase: an authorization-configuration agent and a voting agent. Both agents are distributed from the trusted nodes to the polling stations when they are needed. The authorization-configuration agent's main role is to ensure proper authorization is given and act as a mediator between the polling station and trusted nodes. If proper authorization is given, it sends a request to the trusted nodes to send the voting agent. The voting agent's role is to provide the voter an electronic ballot and send the vote along with other necessary information from the polling station to the trusted nodes. This system works similarly to the way the current voting process works in the US today. The biggest difference is that besides the paper trail used for count verification, ABVS is completely done on computers. Additionally, since it incorporates Blockchain technology, the security and integrity of the process is ensured.

C. *Evolutions in blockchain and smart contracts.*

In the paper "Towards Secure E-Voting" [2], e-voting is explored with the use of blockchain and Ethereum. Ethereum is a type of blockchain network most notably known for it's cryptocurrency (Ether) and also it's smart contracts.(https://ethereum.org/en/) Smart contracts can be defined as mini programs within the blockchain, that are executed according to certain rules and protocols. In this article, a sample system for voting was put into place using Ethereum and it's smart contracts. The proposed system aims to tackle the problems of authentication, transparency and integrity of the system. In other words, there needs to be verification of the identity of the voter, a system that is trusted by it's users and a system that will ensure that a vote does not get created twice, or the system be manipulated.

Their reasoning for picking Ethereum, is for the smart contracts. Smart contracts can be written into the blockchain to be executed where rules and logic apply. In this system, users can validate the system by checking if the execution of the smart contract is true or not.

In their creation of this system, they created a proposed voter object in the programming language Solidity known as the language to write Ethereum smart contracts. (https://soliditylang.org/). In this voter object, it contained information relating to their right to vote, if they have voted, their Ethereum account identification, and who they voted for. There is another object in this system known as the chairperson

who would be responsible for initializing the voting process and assignment of these voter objects to actual voters. After the collection of voters has been obtained, there is the vote function that has been written for every voter. This function is part of a contract in which a voter will pass the ID of who they want to vote for, where the function will check if they are authorized to vote, and if so, will cast their vote to that particular candidate's vote count. The voter's variable indicating whether they have voted or not would then be turned true. Another function in this system would display the current winner every time it is executed. It is noted that this function would not be the one to determine the winner, but rather display it. Upon the end of the election, the user can view their Ethereum account and verify that their vote has been added to the Ethereum blockchain.

IV. Findings

In the previous section, we discussed a couple approaches found in research given to implement secure electronic voting using Blockchain technology. The first was the agent based ABVS system. Compared to traditional voting, this system offers increased security. The agents do the tasks related to processing and transmitting the votes to the blockchain, which reduces the application in the polling stations. Since these agents are distributed by trusted nodes, they would not be able to be modified outside the nodes. This solution offers an increased level of security; however, it seems there would still be problems of long lines at polling stations and absentee voting. If this system could be expanded to allow voters to vote from any polling station, as opposed to a single polling station they are registered to, then that may solve those problems. In our exploration of sample systems, the blockchain/smart contract approach that utilized the Ethereum blockchain network seemed a good step forward in this approach. A unique token that is assigned to each voter would be necessary as is similar to having a driver's license. There would need to be a verification process in the beginning, to where the necessary documents are presented to verify the voters right to vote. After this implementation has been made, when the user goes to cast their vote, they would then need to present Two Factor or such authentication to verify that they are the voter. Such systems could use either a password as is common in most applications, or biometric authentication as is seen in the article Secured E-voting System Using Two-factor Biometric Authentication. Their system proposes either facial recognition, or fingerprint recognition. [4] In this era, facial recognition has claims of errors rates being 0.08% [5] where the algorithm in place uses a database of well taken photos where someone was present when the photo was taken If in the verification of voting eligibility, there is a documentation of the persons face as in a driver's license, this would aid in the authentication for when they log in.. The idea of this being intrusive is of course taken into consideration, however this system is no different from the one we currently use.

V. Conclusion/Discussion/Future work/ Open problems

Blockchain technology is a promising technology with many implementations. The nature of the blockchain and its self-correcting algorithms as well as the extensibility of smart contracts in other blockchain networks suggests that e-voting is very feasible. Although in our findings the proposed system was made on a small scale, there have been countries that have utilized an e-voting system, albeit without blockchain technology [7]. With facial recognition algorithms showing promising accuracy, a possible voting system could be made in which a voter would be authenticated and given a unique token. In an ideal world all would be great, however there are of course limitations. The accessibility of the application must be user-friendly to ensure all voters can navigate it properly. Authentication would then have to take place prior to accessing the application and ultimately voting.

With the last election of 2020, integrity in the electoral system was questioned. In this proposed system, blockchain technology's public ledger would allow for trust in the system and receipts for each transaction or vote. Anonymity can be obtained by having a hash for each voter's identification on the blockchain. The proposal of "smart contracts" as discussed in the second article suggests that a system could be in place where the code is executed on the blockchain without a centralized node or server running the execution of the code. With all these advancements, there are more and more secure and feasible ways in which blockchain e-voting can be implemented.

VI. References

.[1] Pawlak, Michał & Guziur, Jakub & Poniszewska-Maranda, Aneta. (2019). Voting Process with Blockchain Technology: Auditable Blockchain Voting System: The 10th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2018). 10.1007/978-3-319-98557-2_21.

[2] Koç, Ali & Yavuz, Emre & Çabuk, Umut & Dalkılıç, Gökhan. (2018). Towards Secure E-Voting Using Ethereum Blockchain. 10.1109/ISDFS.2018.8355340.

[3] "What Is Ethereum?" Ethereum.org, ethereum.org/en/what-is-ethereum/.

[4] S. Komatineni and G. Lingala, "Secured E-voting System Using Two-factor Biometric Authentication," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2020, pp. 245-248, doi: 10.1109/ICCMC48092.2020.ICCMC-00046.

[5] "How Accurate Are Facial Recognition Systems – And Why Does It Matter?". Csis.Org, 2021, https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter.

[6] Grother, P. , Ngan, M. and Hanaoka, K. (2019), Face Recognition Vendor Test (FRVT) Part 2: Identification, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8271 (Accessed April 16, 2021)

[7] Halderman, J. & Teague, Vanessa. (2015). The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. 9269. 10.1007/978-3-319-22270-7_3.