An Online Voting System Using Blockchain

Shalva Kushashvili
M.S. Cybersecurity
The City University of New York, City College
New York, USA
skushas000@citymail.cuny.edu

Abstract — **Nowadays, traditional voting is stuck in the last century, and those that want to vote must leave their home and submit paper ballots to a local authority. Why not just make this process online? Some countries have tried this, but it has proven difficult due to large security gaps. Thus, electronic voting has not yet been adopted on a national scale, considering all its possible advantages. Modern voting systems suffer from various security threats such as DDoS attacks, vote alteration, manipulation, and so on. Also, it requires huge amounts of paperwork, human resources, and time. Blockchain technology can overcome the risks of electronic voting, and fix shortcomings in today's method of elections. It can make the polling mechanism clear and accessible, stop illegal voting, strengthen data protection, and check the outcome of the polling. This paper presents an effort to leverage the benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for e-voting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves verifiability and security. Blockchain's a digital, decentralized, encrypted, transparent ledger, and if we use this technology correctly, we can withstand manipulation and fraud in voting systems.**

Keywords — *Blockchain, electronic voting, e-voting, blockchain-based electronic voting, security, voting, verifiable voting, trust*

I. Introduction

An election is a way for the people to choose who will represent them in government. It happens once every few years. They are a fundamental pillar of a democratic system enabling the general public to express their views in the form of a vote. The election process is also used in many other private and business organizations, from clubs to voluntary associations and corporations. A ballot is a form that is used to cast votes in an election, classically in a polling precinct, which is a central location set up for voting. A ballot includes a list of candidates and ballot measures being voted on, along with spaces for voters to indicate their preferences. Balloting systems can vary from physical papers to computerized machines. The issue with the current ballot system is that the votes can be manipulated or faked, thus the election process won't be trustworthy. A lot of organizations and people are taking advantage of the problems the ballot system has. For instance, In the 1883 election for the district of Cook, in Queensland, Australia, arrests were made in connection with accusations of ballot stuffing, and the election committee subsequently changed the result of the election. Also, during the 2018 Russian Presidential Election [1], there were multiple instances, some caught on camera, throughout Russia of voters and polling staff alike stuffing numerous votes in the ballot box. Furthermore, during the 2003 Georgian parliamentary election [2], the elections were won by a combination of parties supporting President Eduard Shevardnadze. However, the results were annulled by the Georgia Supreme Court after the Rose Revolution on 25 November, following allegations of widespread electoral fraud and large public protests which led to the resignation of Shevardnadze. After that, a fresh election was held on 28 March 2004. There are also other disadvantages to the current voting system, such as – a lot of paperwork involved, hence less eco-friendly and time-consuming, long queues during elections, the difficulty for differently-abled voters to reach polling booths, and the cost of expenditure on elections being high.

These issues with the current ballot voting system can be solved with electronic voting. It is a voting technique in which votes are recorded through electronic equipment. It's usually defined as voting that is supported by some electronic hardware and software. The implementation of the electronic voting method is very significant, however, electronic voting carries risks such as if the electronic voting system is compromised, all votes can be misused and manipulated. If an electronic voting system is hacked, the consequences can be far-reaching. Thus, electronic voting has not yet been adopted on a national scale, considering all its possible advantages.

Blockchain technology can overcome the risks of electronic voting, and fix shortcomings in today's method of elections. It can make the polling mechanism clear and accessible, stop illegal voting, strengthen data protection, and check the outcome of the polling. Suppose we are a voter who goes to the polling booth and casts a vote using an Electronic Voting Machine. But since someone might tamper with a microchip, we may never know if our vote was submitted or not. But, if we use blockchain, it stores everything as a transaction, then it will be broadcasted to every node in the network, which is then verified. If the network approves the transaction, it is stored in a block and added to the chain. Once a block is added to the chain, it stays there forever and can't be updated. Users can now see results and also trace back transactions if they want. So it will give us a receipt of our vote in the form of a transaction ID, and we can use it to ensure that our vote has been counted securely. Now, let’s suppose that a digital voting system (either a website or an application) has been launched to digitize the process, and all confidential data is stored on a single server/machine. If someone tries to hack it, they can change the candidate’s vote count. We may never know that a hacker installs malware or performs clickjacking attacks to steal or negate the votes or simply attacks the central server. But, if the system is integrated with blockchain, a special property called immutability protects the system. In typical database systems like SQL and PHP, we can insert, update, or delete data. But in a blockchain, we can only insert data but cannot update or delete it. Hence when you insert something, it stays there forever and no one can manipulate it. That is why blockchain is called an immutable ledger. Also, the system should be decentralized, so if one server goes down or something happens to a particular node, other nodes can function normally and do not have to wait for the victim node’s recovery. In short, this kind of system infrastructure is extremely useful for voting.

The remainder of this paper is organized as follows: Section II discusses the background and related works on blockchain and applications for voting systems. Section III describes the requirements to build a secure voting system. Section IV presents the methodology for a blockchain-based online voting system. Section V explains the voting process. Section VI discusses the metrics, and finally, Section VII presents the conclusions of this paper.

II. Background and related works

Blockchain is one of the biggest emerging technologies with a powerful cryptographic foundation enabling applications to leverage these abilities to achieve strong security solutions. The first thing that comes to mind about blockchain is famous cryptocurrencies – Bitcoin and Ethereum. Bitcoin was the first cryptocurrency solution that used a blockchain data structure, created and developed by Satoshi Nakamoto in 2009 [3]. Ethereum introduces smart contracts which use the power of blockchain immutability and distributed consensus as well as offering a cryptocurrency solution similar to Bitcoin. Nowadays, we call Blockchain a set of technologies that combines – the distributed consensus algorithm, public key cryptography, smart contracts, and of course, the blockchain data structure itself.

Blockchain creates a set of blocks replicated on a peer-to-peer network. Each block has a cryptographic hash and a timestamp added to the previous block. A block also contains a merkle tree block header and several transactions. It is a secure networking method that combines computer science and math to hide information from others. It allows data to be transmitted safely across insecure networks, in encrypted as well as decrypted forms[4]. One of the main reasons for using this kind of technology is to achieve immutability. If a piece of data is changed, the blocks containing this piece must be recalculated. Not only that, but the hashes of all subsequent blocks also need to be recalculated [5]. Furthermore, data stored in the blockchain are formed from all the validated transactions during their creation. This means that no one can insert, update or delete transactions in a validated block without being noticed [6].

In the blockchain, nodes contain identical data and form a peer-to-peer network without any kind of central authority. To reach an agreement on blockchain data, a consensus algorithm is used, which is fault-tolerant in the presence of malicious actors. This type of consensus is called Byzantine fault tolerance, which is also known as Byzantine Generals’ Problem [7]. Blockchain solutions can use different kinds of consensus algorithms, such as proof-of-stake, proof-of-work, proof-of-vote, proof-of-capacity, proof-of-activity, and so on [8].

Public key cryptography is used for two purposes. First and foremost, all validators own their keypairs used to sign consensus messages. Also, all incoming transactions must be signed to determine the requester. There's also anonymity on the blockchain network, so anyone who wants to use cryptocurrencies needs to generate a random keypair and use it to control a wallet linked to a public key. Blockchain guarantees that the only keypair owner can manage the funds in their wallet, and this property is verifiable.

A smart contract is also very interesting since it brings a new life into the blockchain. The concept of smart contracts was introduced by Nick Szabo in the 90s. It was described as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises” [9]. In Ethereum, a smart contract is a piece of code deployed to the network so that everyone can have access to it. The results of executing this code are verified by a consensus mechanism and by every member of the network [10]. Once it is written, it can’t be changed, and all network participants need to verify it.

As for electronic voting, it has been a research topic for quite some years. The development of electronic voting systems is becoming a major activity. Official government policies in many countries aim at introducing e-voting at a fast pace. For instance, in the UK, the first experiments have been done with elections on the local level. Furthermore, Estonia was the first country to offer Internet voting to the entire electorate nationwide in 2005 [11]. The officials from Estonia stated that the electronic voting system was a success and found that it withstood the test of real-world use.

Recently, distributed ledger technologies such as blockchain in e-voting also have been a big topic at it’s being used to create e-voting systems mostly due to their advantages in terms of end-to-end verifiability. With characteristics such as anonymity, privacy protection, and non-repudiation, blockchain is a very attractive alternative to contemporary e-voting systems. The research presented in this paper also attempts to leverage these properties of blockchain to achieve an efficient e-voting system.

A lot of organizations are developing blockchain-based online voting systems. One of them is Polyas, which was founded in Finland in 1996. This company employs blockchain technology to provide the public and private sectors with an electronic voting system [12]. Polyas has been recognized as a secure app by the German Federal Office for Information Security for electronic voting applications in 2016. Many companies in Germany use Polyas to perform electronic voting. Polyas is also used in other countries such as the United States and countries in Europe. Another one is Agora, which is a group that introduced a blockchain digital voting platform in 2015 and partially implemented it in the presidential election in Sierra Leone in March 2018. Agora's architecture is built on several technological innovations, being: a custom blockchain, unique participatory security, and a legitimate consensus mechanism [13]. There's also *Voatz.* This company established a smartphone-based voting system on blockchain to vote remotely and anonymously, and verify that the vote was counted correctly. Voters confirm their applicants and themselves on the application and give proof by an image and their identification including biometric confirmation that either a distinctive signature such as fingerprints or retinal scans [14].

III. E-voting Requirements

Let's take a look at what are the important requirements to build an electronic voting system, and how a blockchain-based online voting system should implement it.

1. Privacy

   This requirement keeps an individual's vote a secret. The system would leverage the cryptographic properties of blockchain to achieve the privacy of a voter. Categorically, when a voter is registered into the system, a voter hash is going to be generated by the blockchain, which is a unique identifier of a voter into the blockchain. Of course, it is protected from misuse due to the collision resistance property of the cryptographic hash. Due to this, the traceability of a vote will be non-trivial, and this will protect the voter from threats.

2. Eligibility

   This requirement allows only registered voters to vote, with each such voter voting only once. All eligible users are required to register on the system using their unique identifiers such as government-issued documents to state their eligibility. Additionally, the system shall implement a strong authentication mechanism using either fingerprinting technology or face recognition to assert that only authorized voters can access the system. Furthermore, the use of biometrics also enables the system to protect against double voting.

3. Verifiability

   When voters cast their vote successfully, they will be provided with their unique transaction ID in the form of a cryptographic hash. They can use this transaction ID to track if their vote was included in the tallying process or not.

4. Convenience

   Voters must be able to vote easily, and everyone eligible must be able to vote without any problems. The system shall be implemented in a user-friendly web-based interface with the voting process requiring minimal input/work from the user.

IV. Methodology

The following system involves a client/server architecture that also uses a blockchain system. Let's describe each member of this architecture

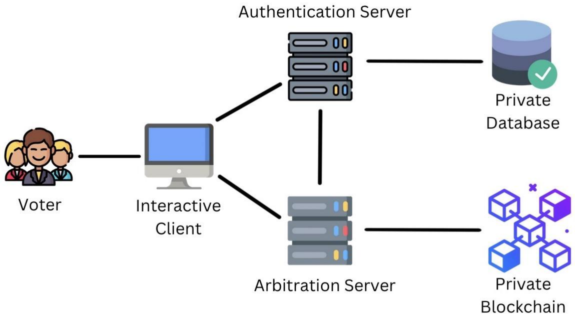

Figure 1: The proposed architecture of the online voting system with blockchain

User/Voter & Administrator

First off we have the user and the administrator. Admin is there to support administering the election process. The user must have a smartphone, laptop, PC, or any device with a browser, and for biometrics, a front-facing camera or a sensor that can scan fingerprints. Of course, The user must have an internet connection to register and vote.

Interactive Client

The interactive client is going to be responsible for interacting with a voter (and the administrator). It's just going to be a typical website where users can vote for candidates.

Authentication Server

The Authentication Server is a traditional centralized web server. It encapsulates two key functions which are authentication and authorization of the users to ensure that access to the system is not restricted to legitimate users. Several different methods can be used to achieve this function, ranging from basic username/password to more advanced such as fingerprint or face recognition. It also has a backend database connected to it which has the information of all the citizens in the country. In short, this system is used by people to register to vote for their elections. Of course, when people create accounts, It also creates accounts on the blockchain system for the users when they vote. The blockchain account is used by the Arbitration Server to vote for a candidate of the users' choice.

Arbitration Server

The Arbitration Server will act as an intermediary between a user and the Blockchain voting system. It verifies the user while voting using the Authentication Server. The Arbitration server sends the users' votes to a blockchain node. It will also send the user the key to encrypt their vote. The Arbitration server sends the users' vote to the appropriate node to be added to the blockchain.

Blockchain System

Last but not least, the Blockchain System is the system on which the actual voting will take place. The users' vote will be sent to one of the nodes on the system depending on the load on each node. The node then adds the transaction to the blockchain depending on the smart contracts that would exist on each node. The smart contracts are the rules that the nodes will follow to not only verify but also add the vote in the system. So, each and every node will follow the smart contract to verify the vote. The blockchain is a private system and is not accessible to the public directly.

V. The voting process

Now that we described each part of the proposed architecture, let's talk about how the voting process will be done. The voting process involves verifying the user's identity with the Authentication Server and then voting using Arbitration Server. As previously mentioned, when users register, the system will also create a blockchain account for them, so they can vote. The candidates will also get their very own blockchain account, so they can get votes.

When the user logs in to the system with the use of their username & password, the system would ask for either a fingerprint scan or for them to turn on the camera for face recognition. If everything matches the data they used for registration, the system will let the user through. Once the user logs in, the system would create a public key which it would send to the Authentication Server. The Authentication server would add the key to the specified username. This key would be used to create an account for the user on the blockchain system to vote. A specific amount of currency is also going to be added to the users' accounts, so they can vote for their desired candidate.

The Authentication Server would then send a session token back to the user. The user would be redirected to the Arbitration server. The user would provide the Arbitration Server with the session token and would verify it with the Authentication Server. The verification and generation of the tokens (between the Arbitration Server, user, and Authentication Server) is going to be done using the Needham-Schroeder protocol. The Needham-Schroeder protocol is a security protocol in which two parties authenticate one another by exchanging large and recently created random numbers called nonces that nobody else should be able to read [15]. This protocol will protect the system from impersonation and man-in-the-middle attacks.

The Arbitration Server would send a verification message to the user along with the public key of the blockchain node to which their vote would be sent. The user would encrypt their vote with the public key and send it to the Arbitration Server. This would ensure that the Arbitration Server cannot read the users' votes, so their votes would remain a secret. The encrypted vote would be sent to the appropriate node. The node would decrypt the message with their private key and send a specific amount of currency from the users' account to the candidates' blockchain account. Each node would verify the transaction according to the smart contracts. These contracts would verify whether a particular transaction was a duplicate or not and check its validity.

After this process, the node would pass this transaction to other nodes in the blockchain system. For the vote verification, we can do that by creating a separate page similar to blockchain.info, where the user would use their Transaction ID to see if their vote successfully went through or not. As for vote counting, this process is very simple. Each voter has a fixed amount of currency value that they use to vote for a candidate of their choice. The candidate with the highest amount of currency on their account wins the election.

VI. Metrics

As for the metrics, we are going to measure the success of this system by comparing it with the modern voting system (ballot voting/E-voting). Specifically, the metrics are going to be:

- Accuracy
- Availability (Less Time-consuming)
- Cost Of Election
- Robustness/Security

The system of remote blockchain voting will impact society in a very positive way. The system will increase convenience for voters since they can vote from **anywhere**. This will make it very easy for people with disabilities or who have trouble moving around to vote. It is a speedy and private way to vote. This will also increase the number of voters since the process does not take too much time off their day. It will help increase the trustworthiness of the people in the government since it is more transparent and **accurate** than the current ballot system and electronic voting systems. The system is better for the environment as compared to the paper voting system. It eliminates the need for paper voting. Also, the **cost** of the elections would be much less than the traditional voting systems. Last but not least, the **security** of this system should be top-notch as it will not be a victim of any security threats like a man in the middle, DDoS, vote alteration, and so on.

VII. Conclusion

In conclusion, The current ballot system is shown to have a large number of issues that can lead to widespread political unrest in a country. Even electronic voting systems prove to be difficult to deal with due to large security gaps because they can be a victim of threats such as DDoS attacks, vote alteration, and manipulation. Therefore, the use of blockchain technology in voting systems is perfect, since it adds an extra layer of security and encourages people to vote from anywhere, any time without any hassle, making the voting process more cost-effective and time-saving.

References

[1] Bodner, Matthew (March 19, 2018). "Analysis | Videos online show blatant ballot-stuffing in Russia". *The Washington Post*. Archived from the original on July 13, 2020. Retrieved July 6, 2020.

[2] Georgian Supreme Court Rejects Shevardnadze Poll Results The Guardian. 25 November 2003

[3] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf.

[4] Garg, K.; Saraswat, P.; Bisht, S.; Aggarwal, S.K.; Kothuri, S.K.; Gupta, S. A Comparative Analysis on E-Voting System Using Blockchain. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019.

[5] Nofer, M.; Gomber, P.; Hinz, O.; Schiereck, D. Blockchain. *Bus. Inf. Syst. Eng.* **2017**, *59*, 183–187.

[6] Zhang, L.; Peng, M.; Wang, W.; Jin, Z.; Su, Y.; Chen, Secure and efficient data storage and sharing scheme for blockchain—Based mobile—Edge computing. *Trans. Emerg. Telecommun. Technol.* **2021**.

[7] Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. Available online: https://www.usenix.org/legacy/publications/library/proceedings/osdi99/full_papers/castro/castro_html/castro.html.

[8] WisdomTree - Consensus Mechanism Overview: https://www.wisdomtree.eu/en-en/-/media/eu-media-files/other-documents/research/market-insights/wisdomtree_market_insight_consensusmech_en.pdf

[9] Szabo, N. Formalizing and securing relationships on public networks. *First Monday* **1997**, *2*, 9.

[10] Wood, G. Ethereum: A secure decentralized generalized transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.

[11] Electronic voting in Estonia - https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia

[12] Polyas. Polyas. 2015. Available online: https://www.polyas.com

[13] Agora. Agora. 2020. Available online: https://www.agora.vote

[14] Voatz. Voatz—Voting Redefined ®®. 2020. Available online: https://voatz.com

[15] Needham-Schroeder Authentication Protocol https://harmony.cs.cornell.edu/docs/textbook/ns/

[16] Blockchain for Electronic Voting System—Review and Open Research Challenges - https://www.mdpi.com/1424-8220/21/17/5874

[17] Secure Digital Voting System based on Blockchain Technology - https://core.ac.uk/download/pdf/155779036.pdf