E-voting system based on blockchain

Project for Advanced topics in online privacy (67515) taught by Mr. Yossi Gilad, 2023

Adi Meroz (adi.meroz@mail.huji.ac.il)

Eden Arni (eden.arni@mail.huji.ac.il)

The Rachel and Benin School of Computer Science and Engineering

The Hebrew University of Jerusalem

1. Introduction

Elections are a cornerstone of democratic societies, but most of the nations still rely on in-person voting, which can be inconvenient, time consuming, expensive and might have some security risks.

In recent years, the development of e-voting systems, which allow voters to cast their ballots remotely using electronic devices, has been seen as a potential replacement for in-person voting.

Although much study has been done in this area, since this is a difficult challenge, there are concerns about the security and privacy of electronic voting systems, as well as the potential for technical glitches and errors that could affect the credibility of the election.

In this paper, we will propose a solution for the problem using blockchain technology, in order to accomplish both security and anonymity. While security has been the main focus of the majority of research in this field. In this paper, we'll place a particular focus on the difficulty of maintaining voter anonymity in such a system.

2. E-voting system V.S. in-person voting system

While casting ballots in person has traditionally been the preferred method for casting votes during elections, there are several advantages of e-voting compared to in-person voting. The first benefit of e-voting systems is that they provide greater accessibility and convenience, which can lead to higher voter turnout. Additionally, e-voting systems are also much more efficient and could reduce the possibility of errors in vote counting, and are more cost-effective in the long run.

In addition to these advantages, e-voting systems may also include special capabilities that are not available in in-person voting, such as the capacity to review and change votes. In this paper we'll introduce a blockchain-based e-voting system, which gives voters greater control over the voting process.

E-voting systems, however, face several challenges, including security and privacy concerns, they are susceptible to potential manipulation. Furthermore, concerns regarding the anonymity of voters are another issue. In this paper, we will present a possible solution that uses blockchain technology to overcome these concerns.

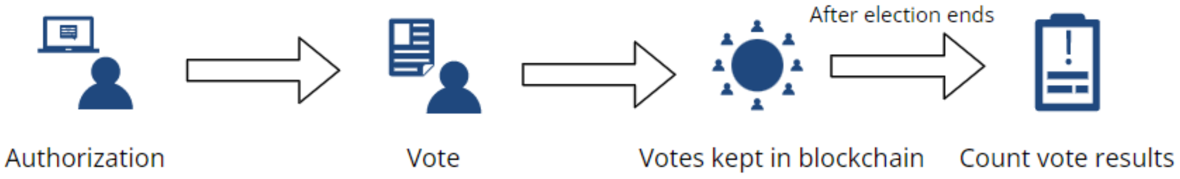

Figure 1. The process of a e-voting election with blockchain

3. Structure and Algorithms

The e-voting system uses two distinct functions to ensure security and anonymity. The Voter Authentication Function (VAF) is responsible for verifying voter eligibility and generating cryptographic keys for secure communication between the voter and the Encrypted Voted Blockchain (EVB). The Encrypted Voted Blockchain (EVB) is responsible for storing the votes until the end of the elections, maintaining anonymity and preventing unauthorized access to the votes.

The VAF class contains a public and a private key, and has accessibility to the data of those who have the right to vote. After receiving the id and name of the voter, the VAF determines if the voter is eligible to cast a ballot. If the eligibility is confirmed, the VAF generates a key pair and sends them to the voter. The VAF includes this information into data updates as well.

Once the voter receives the key pair from the VAF, they can send their encrypted ballot to EVB. This function is connected to a blockchain ,and holds a private and public key. After determining the voter's eligibility with the help of the EVB (more details about this process in Chapter.4), the EVB stores the vote in the blockchain until the election is over.

4. Implementation

The implementation of the e-voting system involves three phases: the authentication phase, the voting phase, and the counting results phase. The complete swimlane schematic of the entire procedure can be found in figure 4. Each of these phases will be thoroughly explained in this chapter.

4.1 Authentication Phase

To vote, the voter must first pass the authentication phase, which involves verifying the voter's eligibility through the Authentication Function(VAF). During this process, the voter submits their personal information, which is verified by the VAF. If the information is valid, VAF generates a pair of keys, consisting of a public key (PubVo) and a private key (priVo), and registers this information in its data.

It is important to note that the term “public key” in this context does not mean that the key is accessible to everyone. Rather,it refers to the fact that a message that has been encrypted by the public key can only be decrypted by the corresponding private key, and vice versa.

4.2 Voting Phase

In the voting phase, the first step follows a similar approach as Reference [1]. Once the voter receives the key pair, they can select their preferred candidate to vote for. The voter will first encrypt their vote along with a randomly generated nonce using VAF’s public key (PubVAF). The nonce that is added to the encryption ensures that any pattern is not recognized, as the same public key (VAF’s public key) is used for encrypting the same vote. Then, the voter will combine the encrypted vote with a random block nonce, the block nonce is used for the blockchain, and encrypt the combinated result again using their public key (PubVo). Finally, the encrypted result along with the voter’s private key are encrypted again with EVB’s public key (PubEVB), creating a message with the following format:

$$Message\ = Enc_{PubEVB}[PriVo + Enc_{PubVo}[Enc_{PubVAF}[Vote + nonce] + blocknonce]]$$

The voter will also sign the message with their private key (PriVo):

$$signature = sign_{PriVo}[message]$$

In addition to the message, the voter will also send a verification of their identity to the EVB. The verification includes the voter’s ID and public key, and is encrypted using the public key of the VAF, so that the EVB cannot access it and discover the voter’s identity.

$$Verification = Enc_{PubVAF}[voter's\ id,\ voter's\ public\ key]$$

Upon receiving the verification and encrypted message, the EVB sends the verification to the VAF for decryption, since it can be only decrypted by VAF. VAF decrypts the verification using its private key and verifies that the public key provided by the voter matches their ID. If the verification is successful, VAF sends a positive answer to the EVB.

Once the EVB receives a positive answer from VAF, it checks the signature on the message to verify its authenticity. If the signature is valid, the EVB uses its private key (PriEVB) to decrypt the message and obtain the voter's private key, along with the encrypted vote plus nonce, and the block nonce for the blockchain. This is done through the following decryption process:

$$Dec_{PriEVB}[message] = PriVo + Enc_{PubVo}[Enc_{PubVAF}[Vote + nonce] + blocknonce]$$

After decrypting the message, the EVB can access the voter's private key. Then, the EVB decrypts the second part of the message with the voter's private key, which comprises the block nonce and the encrypted vote plus nonce. However, since the vote is encrypted using VAF's public key (PubVAF), the EVB cannot determine which candidate the voter voted for. Additionally, the random nonce that is added to the encryption ensures that no pattern can be recognized, further enhancing the security of the voting process.

After decrypting the above message, the EVB will extract the encrypted vote and the block nonce, and temporarily store them in a local dictionary. Once the dictionary contains a certain amount of votes, the EVB will randomly select a vote and add it as a new block to the blockchain. This approach helps to maintain randomness in the blockchain, preventing the VAF from guessing the voter's vote based on the position of the votes in the blockchain. In contrast, other approaches rely on timestamp-based additions to the blockchain, which may lead to bottlenecks or other issues. Therefore, the technique of transaction shuffling is used in this case.

At the end of the election, the EVB will store all of the remaining votes in the blockchain in a random order.

At this point, the vote is still encrypted and cannot be counted yet [Figure.3] .

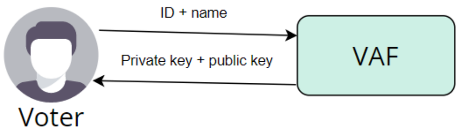

Figure 2. Authentication Phase

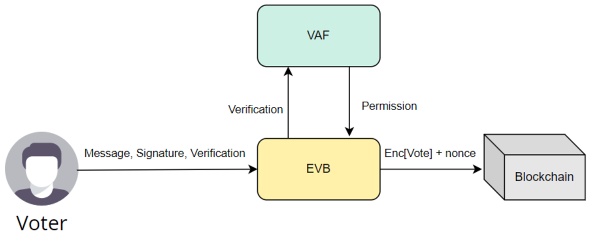

Figure 3. Voting Phase

4.3 Counting results phase

After the voting process is over, the EVB will send the blockchain to VAF for tallying. Using its private key, the VAF can decrypt the votes, it ignores the nonces that were encrypted along with the vote, and counts all the votes. After the VAF finishes counting all the votes, it will announce the election results. Since the blockchain is immutable, it provides a tamper-proof record of the election results. Additionally, since the votes are encrypted, the privacy and anonymity of the voter is maintained throughout the voting process.

5. Security Property Analysis

Ensuring the security of the electronic voting system is a critical challenge that requires maintaining various essential properties. as highlighted in Reference [2]. In this chapter, we will name a few of the main security properties, and analyze how the system we provided above fulfills those security properties.

5.1 Authentication

Authentication is critical in the e-voting system, it ensures that only eligible voters are allowed to cast their votes. In the e-voting system that was provided above, only voters that successfully pass authentication will be given a pair of keys that enables them to cast a ballot in the e-voting system described above. The use of cryptography ensures that the voter's personal information and private key are kept secure and out of the hands of unauthorized parties.

5.2 Integrity

Integrity is essential for maintaining the voting system's precision and dependability. The use of blockchain technology provides an immutable record of the voting process, as well as using encryption and digital signatures that ensure that votes cannot be tampered with or be changed during transmission.

5.3 Privacy

Privacy is important in every voting system to protect the voter's personal information. During the authentication phase, the e-voting system encrypts and preserves the voter's personal information securely. Additionally, throughout the voting process, the voter's identification is validated without revealing their personal information to unauthorized parties.

5.4 Anonymity

Anonymity is a critical aspect of any voting system as it helps protect the voter's choice from being intimidated. While several e-voting systems use blockchain and nonce techniques to prevent third parties from connecting the vote back to the voter, these systems can still have leaks when it comes to anonymity from the system itself.

In the e-voting system described in this paper, anonymity is maintained from both the VAF and EVB. When a voter submits their vote to the EVB, it is encrypted with VAF’s public key, ensuring that the EVB cannot access the voter’s choice or identity. The VAF only receives the results at the end of the election, and goes through the entire blockchain. Since no personal information is stored in the blockchain, the VAF has no way of knowing who voted for which candidate. Additionally, the votes are also randomly ordered in the blockchain, further preventing any attempt to deduce a pattern from the sequence of the votes.

6. Conclusion

In conclusion, e-voting has the potential to overcome many of the limitations of traditional in-person voting, including accessibility, convenience, efficiency, and cost-effectiveness. However, the security, privacy, and anonymity of electronic voting systems remain concerns, which have prevented their widespread adoption. In this paper, we have proposed a blockchain-based e-voting system that employs the Voter Authentication Function and Encrypted Voted Blockchain to ensure both security and anonymity. Notwithstanding the potential advantages of this solution, there are still a lot of challenges and improvements that need to be addressed before the e-voting system can be implemented. Further research will be needed to evaluate the feasibility and effectiveness of blockchain-based e-voting systems. However, we truly believe that blockchain technology has the potential to revolutionize the way we conduct elections in the future.

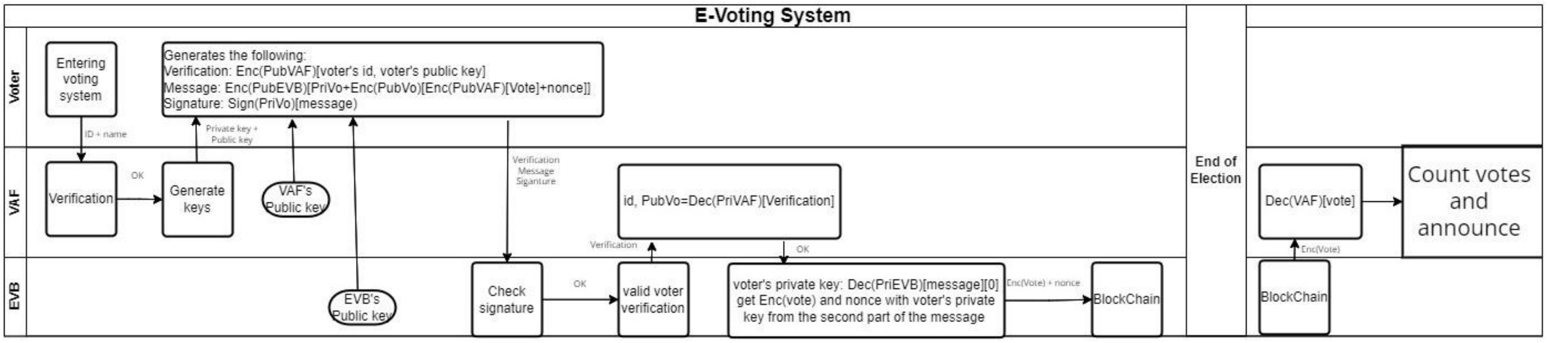
E-Voting System
Voter
VAF
EVB
Entering voting system
ID + name
Verification
OK
Generate keys
Private key + Public key
VAF's Public key
EVB's Public key
Generates the following:
Verification: Enc(PubVAF)[voter's id, voter's public key]
Message: Enc(PubEVB)[PriVo+Enc(PubVo)[Enc(PubVAF)[Vote]+nonce]]
Signature: Sign(PriVo)[message)
Verification Message Siganture
Check signature
OK
valid voter verification
Verification
id, PubVo=Dec(PriVAF)[Verification]
OK
voter's private key: Dec(PriEVB)[message][0] get Enc(vote) and nonce with voter's private key from the second part of the message
Enc(Vote) + nonce
BlockChain
End of Election
BlockChain
Enc(Vote)
Dec(VAF)[vote]
Count votes and announce

Figure 4. Swimlane of the voting process

Reference

[1]Vehbi Neziri, Isak Shabani, Ramadan Dervishi, Blerim Rexha, “Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain”, Appl. Sci. 2022

[2]SHIYAO GAO , DONG ZHENG , RUI GUO , CHUNMING JING , CHENCHENG HU, “An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function ”, Aug, 2019

[3]Hong-Ning Dai, Academic Editor, Jiajing Wu, Academic Editor, and Hao Wang, “Blockchain for Electronic Voting System—Review and Open Research Challenges”, Aug, 2021

[4]Syada Tasmia Alvi , Mohammed Nasir Uddin, Linta Islam, Sajib Ahamed , “DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system”, Oct, 2022

[5]Muhammad Shoaib Farooq, Usman Iftikhar, Adel Khelifi, A Framework to Make Voting System Transparent Using Blockchain Technology, June, 2022