

School of Applied Sciences  
Bachelor of Science in Computing

**COMP490 Final Year Project  
Project Proposal**Academic Year 2021/22

|  |  |
| --- | --- |
| Tamper-resistant Voting System over Blockchain | |
|  |  |
| Project number: | 23 |
| Student ID: | P1807139 |
| Student Name: | Owen Szeto |
|  |  |
| Supervisor: | Philip Lei |
| Assessor: | Liam Li |
|  |  |
| Submission Date: | September 9, 2021 |

Table of Contents

[1 Project Description 2](#_Toc453937400)

[2 Summary of Related Work and Key References 3](#_Toc453937401)

[3 Project Workplan 5](#_Toc453937402)

[4 Risk Assessment 7](#_Toc453937403)

[References 10](#_Toc453937404)

# Project Description

In our lives, there are large and small voting activities everywhere, from small-scale elections such as student union elections to national elections such as the US presidential election. They all have one thing in common, that is, a centralized organization controls the entire voting process. Moreover, this mode has some inevitable shortcomings. For example, ballots may be lost, or a bunch of votes may be forged maliciously when it is difficult for others to find out. This poses a high risk to the fairness of voting. Therefore, feasible solutions will be discussed and proposed in this project.

The project aims to design and build a decentralized online voting system and a distributed voting application based on the system. The major objectives of this project are as follows:

* Study the characteristics of the blockchain and find out those characteristics that facilitate the voting process and apply them to the system.
* Design and implement an online voting system with a distributed architecture, which consists of both on-chain and off-chain components. The distributed architecture should guarantee the high availability of the system.
* Design and implement a distributed application (DApp) that supports the online voting system, allows users to vote online and verifies whether users are eligible to vote and whether their votes are valid.
* Use blockchain technology like Ethereum to ensure that once a vote is submitted, no matter whether the attempt is harmless or malicious, no changes can be made. In addition, it needs to ensure that the votes are transparent and auditable.
* The system and the application are able to protect the personal information of voters and their voting choices.

The application is suitable for any voting activity, and qualified voters can vote through it. Furthermore, since the system will be developed with DApp development platform in Ethereum [1] and distributed architecture, the system will be decentralized, robust, non-repudiable and highly available.

The development platform provided by Ethereum is a blockchain paradigm that combines encryption and secure transactions in a universal way. This paradigm has proven its usefulness through many projects. The most widely known is Bitcoin. Due to the multi-layer inheritance relationship, it is ensured that the application can meet the above requirements. [1]

Since applications and systems run through blockchain technology, and transactions within the blockchain are carried out by cryptocurrency, which means that will be the cost we need to pay when the application is running. Determining how much cost is reasonable will be the primary difficulty in this project. Another major difficulty is the security of the system. All information, such as voters' personal data and their votes, need to be well protected, and measures like data encryption or access permissions will also be set. Last but not least, the application needs to verify whether voters are qualified and whether their votes are valid.

# Summary of Related Work and Key References

With the development of the Internet, numerous online voting platforms have emerged, such as “electionrunner” [2] and “eBallot” [3]. However, they have the same problems as traditional entity voting. The entire process is handled by a centralized organization, which may have many hidden vulnerabilities, such as losing votes or tampering with the number of votes without being discovered. Therefore, in order to completely solve these problems, a brand-new voting platform is built through blockchain technology, which is not common in today’s market.

Voatz [4] is currently a very rare platform for voting through the blockchain in the market, but unfortunately, in 2020, an engineering team from MIT found a series of vulnerabilities in Voatz [5]. This proves that the blockchain voting system is still not perfect.

In this project, it will refer to Voatz and try to perfect its shortcomings. The voting system implemented by blockchain technology should not only avoid the risks of all entities voting, but also must not have fatal vulnerabilities that will affect the voting process. In addition, voter information and the validity of votes will be properly stored and verified.

# Project Work Plan

Table

Description automatically generated

Table

Description automatically generated

**Table 1: Project Work Plan**

# Risk Assessment

This project may encounter four risks and the priorities of these risks is listed in Table 2. Figure 1 and Figure 2 are two probability impact matrices. Figure 1 shows the probability impact for the risks before the solution are taken and Figure 2 shows the probability impact for the risks after the solution are taken.

**Risk 1: Users rejects the product due to the unfriendly user interface**

The user interface of the application is not user-friendly, such as poor interface design, which makes users confused and difficult to vote, which may eventually cause users to refuse to use the application.

Solution: In the design phase, follow some widely used design principles, such as The Eight Golden Rules [6]. Also in the product development process, arrange some UI-related tests and find some users with IT background for the first stage of testing and use, try to find out what may be unfriendly to ordinary users and make improvements.

**Risk 2: Users cannot vote due to server crash**

There are many reasons for the server crash, such as being hacked, having too many requests at the same time or server hardware problems.

Solution: Using a distributed architecture, even if one server crashes, the system will dispatch users to another server.

**Risk 3: User data leakage**

The user data is crucial to the entire voting process. Once user data is leaked, anyone can pretend to be a voter to vote, which will seriously affect the fairness of the entire voting.

Solution: The server side and the client side can use asymmetric encryption to ensure the security of data transmission, and the data stored in the blockchain will be encrypted before uploading.

**Risk 4: Computer failure or development environment problems**

If the computer fails in the development process, the whole project may be stopped. This will seriously affect the progress of the project.

Solution: Make good use of online code repositories such as Github and make regular backups to ensure that the development progress will not be affected even if the computer fails.

**Table of Priority Risk**

|  |  |
| --- | --- |
| Priority | Risk identifier and Description |
| 1 | Risk 3: User data leakage |
| 2 | Risk 2: Users cannot vote due to server crash |
| 3 | Risk 1: Users reject the product due to the unfriendly user interface |
| 4 | Risk 4: Computer failure or development environment problems |

**Notes: Priority 1 is the highest risk**

**Table 2: Table of priority risk**

As shown in table 2, there are four related risks. The risk of user data leakage has the highest priority, because once this risk becomes a reality, it will make the whole application unusable. The second priority risk is that the server crashes, and users cannot vote. This will not only cause inconvenience, but in the worst case, users may even miss the opportunity of voting. The third priority risk is that the users reject the product because of the unfriendly user interface, and the last one is computer failure or development environment problems. Neither is fatal, but they still have considerable consequences. However, if prevention work and design are done well, the probability of these risks occurring is very low.

Table

Description automatically generated with medium confidence

**Figure 1 -Probability Impact Matrix – Initially**

A picture containing chart

Description automatically generated

**Figure 2 - Probability Impact Matrix - Solutions**

References

[1] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), 1-32. Chicago.

[2] electionrunner (n.d.). Retrieved September 7, 2020. From <https://electionrunner.com/>

[3] eBallot (n.d.). Retrieved September 7, 2020. From <https://www.eballot.com/>

[4] Voatz (n.d.). Retrieved September 7, 2020. From <https://voatz.com/>

[5] Russell Brandom. Blockchain voting app is dangerously vulnerable, researchers say. February 13, 2020. Retrieved September 7, 2020. From <https://www.theverge.com/2020/2/13/21136219/voatz-blockchain-voting-app-election-software-hacking-mit-research-cybersecurity>

[6] Ben Shneiderman, The Eight Golden Rules of Interface Design (n.d.). Retrieved September 7, 2020. From <https://www.cs.umd.edu/~ben/goldenrules.html>