UNIVERSITY OF PLYMOUTH

School of Computing, Electronics and Mathematics

BSc (Hons) Computer and Information Security

PRCO304HK Computing Project
2021 / 2022

University of Plymouth Student ID: 10706828

HKUSPACE Student ID: 20082596

eVoting System by using Blockchain Technology

UK Supervisor: Dr. Hai-Van Dang
HK Supervisor: Dr. Ivy Wong

Abstract

This report studies encryption technology and methodologies. One of the main targets is Blockchain. Around the world, blockchain has been widely applied in different aspects, such as financial, healthcare, etc. It has high protection for data saving and processing. Bitcoin is one of the examples of the technology of blockchain. And the other main target is the eVoting system. Around the world, the election is one of the things that is very important in a democracy. It is because an election can affect many situations in the future, for example, the rules of the organizations, and the people who can control the organizations. However, existing eVoting systems have some vulnerabilities to let the people reduce their confidence in the election system.

This report aims to study applying the technology of blockchain to elections and creates an eVoting system. Bringing the features and benefits of blockchain to the voting system and combining them into a new eVoting system. The system can show that blockchain technology can protect the data of the ballot. Therefore, if Blockchain can be applied to the election as an eVoting system, the system can provide a fair, secrecy, and secure voting environment for election campaigns. Also, the system can improve the confidence of people, increase the performance and decrease the cost to host a large election activity.

Acknowledgments

First of all, I would like to thank my project supervisor, Dr. Hai-Van Dang, and Dr. Ivy Wong. They give me large freedom to develop the project. When there are some difficulties that I faced, they would give me some advice and guidelines. That can make me a clear direction to finish my project.

Then, I would like to thank the developer of Visual Studio Code, Mongo Database. They have done a great job to develop an excellent platform for the user to develop their application. And I am one of the users. It let me have a good environment to develop my project smoothly.

Last, I would like to thank my family, classmate, colleagues, and friends. During the project, I have faced many issues, such as health issues, job issues, etc. Therefore, I would face many pressure and difficulties. Luckily, they give me much support and help, letting me have the motivation to finish the project.

Keywords

Blockchain; eVoting; Cryptographic Algorithms; Asymmetric-key Cryptography; Decentralized; Mongo Database.

Contents

Abstract 1
Acknowledgments 1
Keywords 1
Statement of Word Count 3
Code Submission - GitHub Link 3
Code Submission – Plymouth OneDrive filespace Link 3
Project Management – Trello Link 3
1. Introduction 4
2. Background and Objectives 5
Background 5
Objectives 5
Project Vision 6
Project Risk Plan 6
Motivation 7
Deliverables 7
3. Literature Survey 8
Blockchain 8
Smart Contract 8
Hash Function 8
Use of cryptography in the blockchain 9
Distributed Ledger 10
eVoting System 11
Existing eVoting System 11
Limitations of the existing system 12
4. Legal, Social, Ethical, and Professional Issues 12
Legal 12
Social 13
Ethical 13
Professional 13
5. Method of Approach 14
6. Project Management 14
7. Architecture & Design 16
Initial design: 16
Data Storing and processing: 17
Use Case Diagram 18
Database 18
Security issue for the system 18
User interface 19

8. Testing 21

Function Test 21

Scenario Test 22

9. Verification and validation 22

10. Evaluation 23

11. Conclusions 23

12. References 24

13. Appendix 26

Project Management – Screen Captures of Trello 26

Statement of Word Count

Word count: **8,251 words**

Code Submission - GitHub Link

https://github.com/LIUCHIMAN/eVoting-System.git

Code Submission – Plymouth OneDrive filespace Link

https://liveplymouthac-my.sharepoint.com/:f:/g/personal/chi_liu_students_plymouth_ac_uk/Ev_d4Yt2S9tFrfA_o5M-MaABqXSdJhmsWrUal3To5BZrwg?e=dhC3BO

Project Management – Trello Link

https://trello.com/invite/b/eoF0mJQr/a287f98ac7acdf88fb74fca7cc862508/prco304hk2122liu-chi-man

1. Introduction

Since ancient times, most people have pursued democracy. In a democratic society, voting is an indispensable matter. It is because voting can give people the right to choose their intentions and decide their future. Therefore, democratic election activities must be fair, secure, and reliable.

With the progress of the times and the rapid development of science and technology, some places have electronic voting activities and eliminated paper voting activities. In addition to hoping to speed up the voting process, it also hopes to reduce the huge expenses brought about by the voting activities. Although electronic technology can bring many benefits to electoral work, it also brings many problems, such as security and confidentiality. There is "no known technology that can guarantee the secrecy, security, and verifiability of a marked ballot transmitted over the Internet."(The National Academies Press, 2018) These problems will make people lose confidence in electronic voting, and even lose confidence in democracy. A secure and reliable voting system that ensures the anonymity of the voter, transparency, and functioning.(Emre Yavuz et al., 2018)

Nowadays, Blockchain has been widely used in different aspects. It is a digital platform for storing or processing digital data. It consists of a continuously growing list of records known as blocks that are linked and secured using cryptography. It is mainly to be used in all cryptocurrency transactions, especially Bitcoin. (Albin Benny, 2020)

Therefore, in order to strengthen people's trust in electronic voting, this paper will study whether the addition of Blockchain to the electronic voting system can enhance security issues. In addition to this, the eVoting system also needs to make sure that it can fulfill some requirements.

"The right to vote freely for the candidate of one's choice is of the essence of a democratic society . . ."(Reynolds v. Sims, 1964)
"Every voter's vote is entitled to be counted once. It must be correctly counted and reported."(Gray v. Sanders, 1963)
That means the eVoting system needs to be anonymous and secret. Each authorized people can have the right to vote. Also, the system needs easy to use and manage by users. Finally, it needs to be rapid and accurate to present the result of the election.

This report starts with a brief introduction to eVoting and the technology of blockchain. Then, the report moves into the parts of the aims, objectives, and deliverables of this project. In addition, the literature review of blockchain is also included in this report. On the other hand, Legal, social, ethical, and professional issues of the eVoting system have been studied in this report.
Lastly, The report also records the detail of the development of an eVoting system and the project management. To show how blockchain technology can blend into the eVoting system.

2. Background and Objectives

Background

In a democratic society, voting is an indispensable issue. As large as national leaders, as small as household affairs, as long as it is a democratic group, there will be elections. From the beginning with simple rules and outdated equipment, gradually began to move towards electronic. How to go electronic? The basic requirement is that electronic voting refers to the use of electronic devices, such as electronic vote-counting machines, to assist in the election process. The first eVoting machine was patented by Anthony Beranek in 1881. It was considered suitable to be used in elections in the United States. (Hosam Alamleh et al.,2021)

Since that, many organizations recognize that the electronic voting system can bring many benefits. For example, increasing the voting rate, speeding up the progress of election activities, reducing the cost of election activities, and obtaining voting results quickly. Therefore some countries have accepted to use of electronic voting, even remote eVoting. For example, in Estonia, a remote eVoting system was first tested in late 2004 and 2005 during local referendums and elections. In March 2007, Estonia held the world's first national internet-based election, where 30,275 citizens (3.4 percent of Estonia's eligible voters) used remote eVoting which was available to Estonian voters in Estonia as well as abroad. (Hosam Alamleh et al.,2021) Although there are many advantages, there is no complete eVoting system at present. For example, the eVoting system would be hacking, vote-rigging, election manipulation, etc. Therefore, many countries or institutions conduct research and development on the technology of electronic voting systems.

In recent years, the digital coin is all over the world. The technology under the digital coin is using Blockchain. The blockchain contains different cryptographic, and high protection in data storing and processing. Also, blockchain can offer a decentralized platform to increase safety and usability. Therefore, many organizations would apply blockchain to different aspects, such as Blockchain Internet-of-Things (IoT), Insurance, etc. In order to develop a complete eVoting system, this project needs to study the technology of blockchain and design an eVoting system by using Blockchain.

Objectives

The aim of the project is to develop an election system by using blockchain technology. In real life, there are many elections conducted of different sizes, such as the Legislative Council elections or voting activities in the owners' corporations. After each election activity is completed, there will be some negative news, such as a slow vote-counting process, the security of ballot storing, privacy problem, vote-rigging, etc. Therefore, the system is designed to improve the related problems. The vision of the system is to confirm and protect an election activity under a secure situation smoothly and rapidly. Before designing the system, the project has some requirements or objectives that need to be fulfilled by the eVoting system:

1. Eligibility: Need to ensure only valid voters can vote
2. Uniqueness: One voter only can vote one time
3. Fairness: Before the end of the election, no one can know the result

4. Anonymity: All the votes need to be anonymity
5. Privacy: No one can know the voters' intention and their personal information
6. Accuracy: The result needs to be present accuracy after the end of the election
7. Security: The ballots need to be stored safely

Project Vision

The vision of the system is to confirm and protect an election activity under a secure situation smoothly and rapidly. In this system:

1. The initiator of an election needs to establish an election activity and input the information of the election, such as the information of the candidates and voters.
2. The system needs to authenticate all the voters so that during the election, the voters can be identified, and the ballots can be sent to the voters quickly and easily.
3. The system needs to ensure that voters' voting intentions can be stored securely and anonymous under integrity and confidential situations after voters have finished voting.
4. After the election is completed, the results of the election can be fully presented without interference from any person or hacking program.
5. The election is an anonymous activity. The system would use blockchain technology to encode the tension of each voter.
6. All the processes are under the electronic mechanism. The system would not use paper ballots. Therefore, need to confirm the equipment, power supply, communication service, etc. are ready for the system.

For designing and studying the project, there are many things to be considered and analyzed:

1. Need to consider how to store all the data, in a safe and confidential manner. Therefore, there is a consideration for what type of database language and database server would be better for the system.
2. In order to ensure that the election activity can be conducted in a transparent, fair, and impartial manner. After voters have finished voting, their selection could be stored safely and confidentially. Therefore, there is a consideration for what encryption method could be used in this step.

Project Risk Plan

- There are some existing eVoting systems, maybe the project would follow their design to go wrong with the project. Therefore, during the project design, it needs to clearly understand the purpose and the step of the system which is a secure electronic election system.
- The project is formed as a small team. Maybe one person needs to act in different roles. Also, that would affect the progress of the project. Therefore, the project should have a good plan for time management and finish the task before the deadline.
- Because of the team size, the group mate may be weak in programming, therefore, before starting to design the system, it would face a problem with the knowledge of coding. Therefore, it needs to spend more time choosing and learning the programming language first.

Motivation

Digital currency is all over the world. The technology (Blockchain) under the digital currency also is a hot topic. Many people would study its feature and apply them to different aspects. The main features are immutability, decentralized, and enhanced security. Based on these features, Blockchain can improve the problem of the eVoting system. Therefore, this project also needs to study the topic of Blockchain.

Furthermore, in order to protect the democracy, and save the confidence of the people. The project would study the eVoting system by using the Blockchain.

Deliverables

Before planning the project, the project deliverables need to be set up and allocate resources and documented within a governing project charter so that can be referenced throughout the duration of the project. In this project, there are two parts have been divided:

Primary:

1. Blockchain Technology

   Using the technology of blockchain to store details of a valid ballot. Before the end of the election, the data could not be amended. The data, that have been stored, is the highest priority to protect.
2. Encryption

   The information of a valid ballot is important data in an election. the system would combinate two cryptographic algorithms, which are Symmetric and Asymmetric algorithms, to encrypt and protect the data.
3. Database

   For the whole project, there are different types of data that need to be stored, such as the information of the administrator or the data of the ballot. The project would use the mongo database which is a famous database and could handle a large volume of data.
4. User

   The main users in this system are the administrator, who manages and monitors the whole election activity, and the voters, who are valid and can vote in the election activity.
5. Interface

   The interface is the front-end page, which is designed for the user who can easy to control or use the system. Also, all the information can show to the users clearly.

Secondary:

1. Decryption

   All the ballots have been encrypted two times. The administrator needs to decrypt all the data to show the result of the election.
2. Result Presentation

   After all the data have been decrypted, the system needs to count the ballot accurately and show the result to the administrator clearly.
3. Decentralization

   Setting the system to a decentralized system, can improve the security of the system and increase its usability. To ensure the system can be more safe and usable.

3. Literature Survey

Blockchain

Smart Contract

Satoshi Nakamoto identified the need to create a secure and reliable payment based on proof of trust in cryptography and dispensing through third parties for the operations of value transfer directly between the principles without the need of an intermediary. Bitcoin was launched in 2009 as an open-source technology that allows transfers through bitcoin cryptocurrency generated by a blockchain technology that stores and manages transactions. Blockchain technology aims to reduce transaction fees and facilitate international negotiations. Bitcoin was the first cryptocurrency to be created with its nodes connected to a blockchain using a proof of work algorithm formed by rules defining how the blocks containing the transactions are added to the blockchain.

Blockchains allow various functionalities due to their additional versatility besides transactions in cryptocurrency. The blockchain network provides for storage of data, decentralized registration of real estate's order tracking, and other functions such as smart contracts. Blockchains serve the purpose of safe and reliable storage of digital assets. The means these assets can occur through computer programs is smart contracts that seek to execute specific commands based on prior established instructions. Nevertheless, despite having the term contract in their title, smart contracts are not regarded as legal contracts and serve only as instruments for executing clauses in the contracts (Perugini & Checco, 2015).

Nick Szabo first utilized a smart contract in 1994 as he defined it as computer transactions that execute contractual terms. However, other authors have defined smart contracts as the software specially designed to utilize blockchain technology to impellent conditions previously agreed upon by parties when they sign a contract in an unknown environment. Additionally, Bartoletti & Pompianu (2017) defines smart contracts as computer programs that can be executed in a network of mutually trusted node like the blockchain without the mediation of another party. Because of their resistance to manipulation, smart contracts are utilized in varying scenarios, such as money transfers among parties based on specific rules agreed by the people individually.

Smart contracts are also considered digital contracts that allow people to create clauses depending on the decentralized consensus, which is tamper-proof but has no legal enforceability like the traditional contracts. The contracts can be created and maintained in varying blockchain implementations. Bitcoin allows the utilization of a scripting language with fewer resources. However, its open model and immutability of data have led to creating other better versions of smart contracts. Ethereum is another platform that utilizes the same blockchain technology as bitcoin and its enforceability of smart contracts through solidity. The smart contracts are triggered when the transactions are sent to the Ethereum blockchain, and the network validates the results. The blockchains that support smart contracts are also referred to as programmable blockchains, and Ethereum is the program with the smartest contracts in the blockchain.

Hash Function

Hash functions are the most utilized cryptographic algorithms in blockchain technologies. They are mainly cryptographic and designed to protect the integrity of data. The hash functions can map arbitrary-sized inputs to a fixed size. In simpler terms, a hash algorithm is a mathematical function that transforms any input into a predetermined output. According to a study by Smriti Gupta (2015), the cryptographic hash functions field has been evolving for the past 30 years and will continue evolving into the future. The lack of formality in hash functions terminology has led to a lack of an objective way to evaluate the security of new hash functions. The study has emphasized the importance of identifying formal terminology as the meaning of hash function with a clear set of objectives.

For cryptography security and usability in the blockchain, the hash function needs to be resistant to collisions indicating that it is difficult to input variables and produce the same output. To accomplish these functions, a hash function needs to be one way that is it is only possible to move from input to output in a hash function but no other way around, making it hard to engineer a collision from the desired output. Also, the only way of finding a hash collision is through a brute force search which requires checking multiple inputs as the hash functions have various possible outputs. A hash algorithm is considered secure until it is possible to identify a collision for it. According to Dang (2015), SHA-2 is a standardized hash family approved by NIST. SHA_2 contains varying algorithms with integrative one-way functions that process an input message to create a confessed representation termed digest. Each process passes through two stages, preprocessing and then hash computation.

Preprocessing involves parsing a message into its m-bit blocks and then setting the initialization values utilized later in the hash computation process. In contrast, the hash computation produces the message schedule filled with functions, constants, and old functions to produce hash values. The final value from the hash process can be utilized in defining the message digests. The algorithms vary depending on block sizes, message digest sizes, or a wide range of enough security levels (cheng et al., 2018). Furthermore, SHA-256 is a popular hash function in cryptocurrency utilized in the Bitcoin system for block mining (Wang et al., 2019). However, according to Courtois et al. (2014), in their study on cryptography and security systems, the bitcoin SHA-256 is considered insufficiently secure for the long term by the NIST as it results in a certain hashing problem identified as constrained input-output problems appearing in the mining process. This issue affects the cost and speed of running the hash, as Thuy & Khai (2020) identified in their study on a fast approach for bitcoin blockchains mining system integration.

Use of cryptography in the blockchain

Blockchain introduced the utilization of cryptography through both symmetrical and asymmetrical cryptography. Symmetrical encryption performs varying functions, which are similar to symmetric cryptography. Asymmetric cryptography utilizes such cases as asymmetric encryption and digital signatures. Asymmetric cryptography, identified as public-key cryptography, is one of the major branches of blockchain technology that allows the verification of transaction authenticity and protects funds from hackers. Cryptography is a method that utilizes advanced mathematical principles in storing and transmitting data in a specific form. It can only be read by the person the data intended. Encryption is a major concept in cryptography where a message is encoded in a form that a spy cannot read. Asymmetric cryptography utilizes two keys to encrypt and decrypt data, a private and public key. A public key can be in the form of a username and is available to all and can be shared with everyone and view the history of the account with that username (Zhai et al.,2019). The username is linked to the password, but there is no way of deriving the password from the username. A private key is a password to an account with a specific username. The username is not public and cannot be viewed by anyone. The private key is only utilized in authorizing transactions in the account. Because of asymmetric cryptography, it is safer to encrypt data and ensure that only the recipient will receive the information (Guegan, 2017). The key pairs allow for its utilization in authentication processes.

Digital signatures are signatures providing integrity through the utilization of asymmetric cryptography. They are utilized for a wide array of authentication purposes and have proven very secure. Digital signatures cannot be corrupted and are easier to verify due to their utilization of asymmetric cryptography (Guegan, 2017). Both asymmetric cryptography and digital signatures are prominent for their utilization in blockchain technologies. Blockchains are a system of widely distributed ledgers; thus, it is important to utilize cryptography as a reliable and secure function. Most cryptocurrencies utilize key pairs like asymmetric cryptography in managing the blockchain. The public key is the address that everyone can view, while the private key is utilized in accessing the address and authorizing address actions.

Distributed Ledger

A distributed ledger refers to a system that is digital that tracks and records assets transaction whereby these transactions are recorded in different multiple places but at the same time. A distributed ledger is therefore an essential tool in data recording and storage and the merit is that multiple transactions data can be recorded at the same time. In technology, distributed ledgers play a significant role in securing the functioning of a decentralized database that is digital. Therefore, distributed ledgers are essential in the different fields where they are applied such as the business and technological fields. In business, distributed ledgers are used to record transactions that are multiple as this is facilitated by their capability to record multiple transactions from different places at the same time.

According to Burkhardt et al., (2018) distributed ledger has gained popularity and is listed among the world’s best transactions recorders because of its outstanding ability to record transactions taking place from several places. In this article, the authors dig deeper into a distributed ledger and establish an argument that the transactions recorded by the ledger are only made available to the owner and hence are private and not everybody can access them unless they prove ownership of the information. While explaining the workability of the distributed ledger the article identifies and defines some terms such as cryptography, game theory, and graph theory among others which necessitate transparency in a distributed ledger. Additionally, the authors go ahead and describe how a distributed ledger can record the transactions and describes a blockchain where the combination of the principles into a blockchain occurs to record the transaction. Under blockchain, the article has discussed several factors such as transactions, processes, roles, blocks, cryptography, and Algorithms respectively.

El Loini & Pahl (2018) published an article that addressed the distributed ledger by comparing four distributed ledger technologies and highlighting the strengths and weaknesses of each one of them. The authors argue that since the invention of cryptocurrency and bitcoin among others, a distributed ledger has gained popularity as these technologies desire to outdo the other. In addition, these sites such as cryptocurrency require distributed ledger to help them track down and record transactions from different places while ensuring that the information is only accessible to the owner. The article employs the SWOT analysis to calculate, identify and establish the strengths, weaknesses, opportunities, and threats of the DLTs. However, they have established that the DLTs have not attained the maturity level that facilitates this evaluation. Therefore, they relied on the data collected under each distributed ledger technology and used it to determine the strengths and weaknesses of these subcategories of DLTs.

eVoting System

eVoting system is described as electronic voting where technology accounts for the casted votes in the ballot and counts them. The existing system is the traditional eVoting system which researchers are seeking to improve so that it can be effective. Electronic voting facilitates fast counting of votes, reduces costs that would have been incurred when hiring staff, and facilitates voting for the disabled. However, this system is only reliable in places of high technology where electricity, internet, and computers are available. Researchers have identified this method of voting as one of the best because people can cast their votes while at home or at work hence reducing overcrowding and the spread of covid-19. Many countries especially the developed countries such as China and America have found this type of voting reliable. India has also adopted this mode of voting especially due to its large population to reduce overcrowding. Researchers argue that in the future, almost all the developed countries will be using eVoting systems to cast and count their votes which is a fast, safe and reliable method.

Existing eVoting System

In the research conducted by Tas & Tanriover (2020) they established that the traditional eVoting systems can be improved by introducing the blockchain. They based their argument on the reliability of a blockchain as they argued that it is secure, digitized, and consensus-based and hence is quite reliable when it comes to eVoting systems. Furthermore, they explored both symmetrical and asymmetrical cryptography and agreed that these can be used in blockchain to improve the traditional eVoting systems into a fast and reliable eVoting system. The article proves that the eVoting system that is supported by blockchain provides better results because of its unique characteristics such as generativity, integrity, coin-based, consensus, and privacy. These factors improve the traditional eVoting system when they are combined. Although blockchain has unique features, it does not guarantee security and speed and hence is not quite reliable unless the issues are addressed. Therefore, this article argues that blockchain can be used to improve traditional eVoting and make it a reliable session but does not guarantee safety.

According to Ksheitri & Voas (2018), eVoting can be used alongside blockchains where citizens ask questions that are fed to the system by the blockchain. Based on the authors' arguments, blockchain plays a significant role in ensuring that the eVoting system is successfully achieved. Once the citizens are done with the voting, a distributed ledger is used to record the data since distributed ledgers are capable of recording multiple transactions taking place at the same time but from different places. The main idea of this article is to reduce fraud during voting and enhance eligibility by ensuring that elections are conducted properly without any irregularities. Later, the article discusses potential benefits and challenges regarding this technology by highlighting that this combination will lead to effective voting but has some challenges such as technological challenges. In addition, this technology is only reliable in places where literacy levels are high. To sum it all up, this article has established that distributed ledger technology can be effective in improving and facilitating the eVoting system as they conclude that the new technology will reduce fraud and irregularities.

Limitations of the existing system

The existing system is the traditional eVoting system which has had several challenges making it unreliable for use during voting because it is associated with fraud. Due to this reason, researchers have been in the field carrying out research on how to improve the system from a poor system to a reliable voting system that is free from fraud. In relation to this research problem, various limitations of the traditional voting system have been identified as the researchers are using the findings to come up with solutions regarding the matter. Therefore, some of the limitations that have been established include, exposure to hacking since the distributed ledger technology had not been incorporated which secures recorded data and only allows access to the owner upon verification. Multiple fraud cases were reported regarding the traditional voting system where people would change the votes easily.

Abuidris et al., (2019) identify that there are several risks associated with the existing eVoting system that hinder it from producing reliable information. The authors argue that the system exposes the votes to hackers hence leading to fraud and swearing-in of unwanted leaders. The article explores how these challenges have affected the citizens whose leaders of choice are announced as losers and bad leaders are announced as the winners. This is against the freedom of democracy as the citizens are unable to practice democracy. Hence, this article highlights the main limitation of this system as exposure to hackers and fraud.

According to Hjálmarsson et al., (2018) eVoting system has had numerous challenges that have triggered the improvement of the traditional system by introducing blockchain which is a safe and reliable measure to control limitations associated with it. Some of the mentioned limitations include the lack of track for the recorded data and the inability to record data from multiple places at the same time. This leads to fraud during elections and may stir up post-election violence which causes great loss and harm.

4. Legal, Social, Ethical, and Professional Issues

Legal

A legal election should contain a bunch of regulations. The regulations should clearly state the voting process, the requirement of the voters, and how the voting result would be generalized. The existing voting ways still suffer from a blemished system. Vote rigging, hacking of the EVM (Electronic vote machine), and election manipulation are still counted as the major problems to the fairness of the election. This project aims to deeply investigate the risks of using an electronic voting system and the significance of using blockchain technology to tackle the risks of the existing voting system. To fulfill the legal regulation of implementing a fair election, it is important to have a transparent and stable norm to store and count the votes. In addition, making hacking activities impossible is also critical under a fair election process. To make the electronic voting system popular on a national scale, using blockchain technology could be an effective step.

Social

Every democratic society needs a secure election system to ensure the whole political environment is operating properly under fair conditions. A fair condition needs to attain a high voting participation rate and a high level of security. In a democratic system, every vote is being counted but the participation rate is not so high mainly due to the place to vote is not convenient for the voters and some may think that their votes will not be counted as the election results are not fair. The most critical benefit of conducting an eVoting system is the possibility to make the vote remotely (Adeshina et al., 2014). eVoting system is an effective means to increase the voting participation rate and reduce the mistakes of counting votes.

In the current election system, voting is generally done by either writing the voters' preferences on a piece of paper or by electronic voting machines. To replace the traditional systems, it is necessary to limit the voting frauds and to make the voting as well as the counting process more transparent. Conducting an eVoting system has a higher risk of hacking activities by hackers who could hack the servers and make the voting systems becomes unfair. Entering blockchain technology could be a means to deal with the possibility of being hacked. Blockchain can help to manipulate an electronic voting system that is immutable, transparent, and cannot be hacked into in order to change the voting results. Therefore, to conduct a fair election in democratic societies, getting used to the eVoting system with the help of blockchain technology can effectively increase the voting participation rate to make the whole society could be operated under a fair election.

Ethical

The ethical concern is a major item when the process of the development of an application, eVoting system is being considered. It is significant to ensure that the electronic voting system is secure, legal, and convenient when used for elections. Nowadays, the electronic voting system has not yet been adopted on a national scale as this voting system carries possible risks such as all votes might be misused or generalized a wrong result when the voting system is confused or compromised. To make the eVoting system ethical, we need to take into account that it should be fair and safe, and therefore we can minimize the possible risk of manipulating the eVoting system and make this voting method sustainable. To solution to overcome the risks is using blockchain technology.

Professional

A professional electronic voting system should meet some requirements such as accuracy, singularity, transparency, and fairness. Blockchain technology makes the electronic voting system professional and reliable as it is different from the traditional voting systems which have a central authority to cast a vote. It is easy to change the result from the traditional voting system. The consequences will be far-reaching if an electronic voting system is hacked. (Jafar et al., 2021) Under blockchain technology, there is no central authority under the implementation of blockchain technology, the data are stored in multiple nodes. It is unlikely for hackers to hack all nodes and change the data. Thus, in this way, we can ensure that voters can cast the vote once only and all the data has been stored safely. Compared with the traditional voting system, the electronic voting system with blockchain technology can generalize the voting results faster and in a more accurate way, and therefore, make the election fairer and more professional.

5. Method of Approach

Before starting to develop the project, an iterative approach should be selected. This is because the approach can be a guide for the project, it can help the project can be developed smoothly. The project would be divided into different stages. It is the outline of the Project Initiation Document (PID). Every stage has its task to achieve in a period. Although each stage is independent and has its task, it also needs to be finished before the following stage start. Otherwise, the following stage would be affected. This project needs to be finished within 14 weeks. From project topic designing to finishing the system and reporting, it has been divided into different stages and the detail will show in the next part, Project Management.

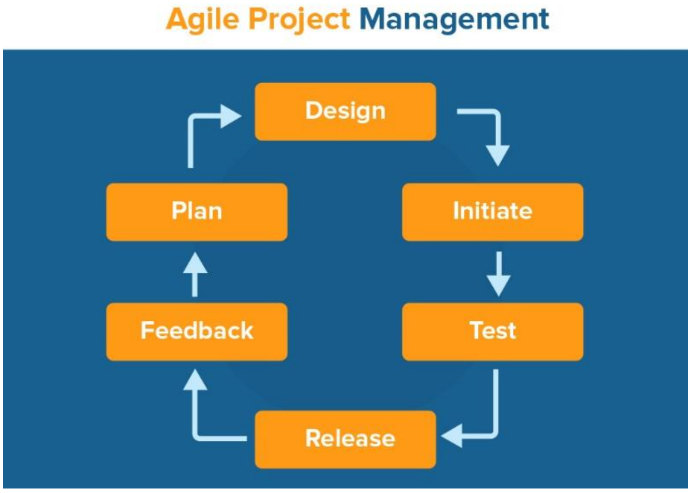


Figure 1: Agile Project Management

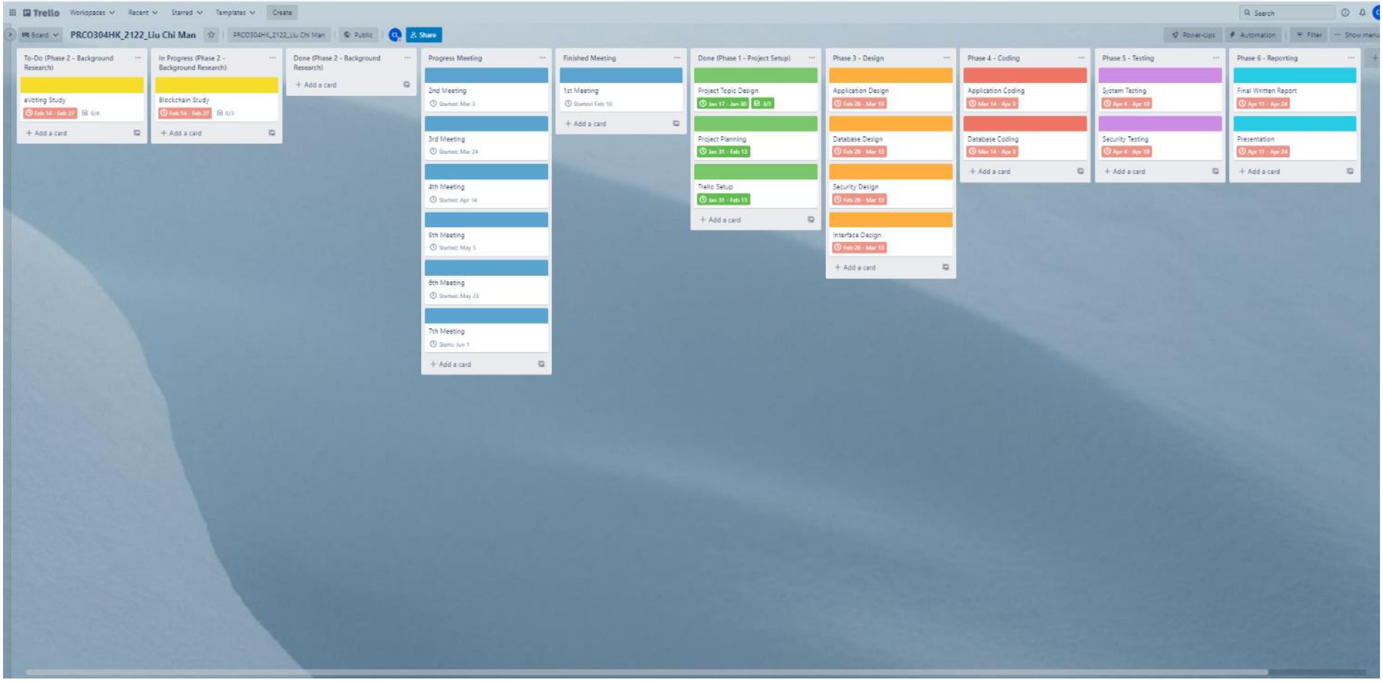
For this project, the iterative approach that has been used is the Agile Methodology approach (Seen Figure 1: Agile Project Management). The reason for choosing this methodology for this project is the size of the project team and the time management for the project. If there is any problem that would affect the following stage, it needs a natural mechanism for responding to change quickly. It is a set of values that guide the project toward the correct path.

For project time management, it is using the Trello to control and record the progress of the project. Trello is a flexible work management tool where teams can ideate plans, collaborate on projects, organize workflows, and track progress in a visual, productive, and rewarding way. The project team can create their task boards with different columns and move the tasks between them. The detail will present in the following part, Project Management.

6. Project Management

This project is an individual project. A man needs to act in different roles in a project team. For example: As a project manager who needs to manage the task of the project can achieve it on time, arrange the task for team members, and draw up the main topic of the project to guild the team member in the correct direction. As an analyst who needs to assist in defining the project, gather the requirements from the client, and verify that project deliverables meet the requirements. As a programmer or a tester who needs to develop the system to achieve the requirements and confirm the system is complete. Therefore, a brilliant management plan is important in this project.

In this project, Trello has been used to manage all tasks for the project. It can be used for personal and business purposes including real estate management, software project management, etc. Therefore, the project manager can create the task boards with different columns, which is mean the status columns such as To Do, In Progress, and Done, and move the tasks between them. The following Figure 2 can show the corresponding project management plan.



To-Do (Phase 2 - Background Research)
eVoting Study
Feb 14 - Feb 27 0/4

In Progress (Phase 2 - Background Research)
Blockchain Study
Feb 14 - Feb 27 0/3

Done (Phase 2 - Background Research)

Progress Meeting
2nd Meeting
Started: Mar 3
3rd Meeting
Started: Mar 24
4th Meeting
Started: Apr 14
5th Meeting
Started: May 5
6th Meeting
Started: May 23
7th Meeting
Starts: Jun 1

Finished Meeting
1st Meeting
Started: Feb 10

Done (Phase 1 - Project Setup)
Project Topic Design
Jan 17 - Jan 30 3/3
Project Planning
Jan 31 - Feb 13
Trello Setup
Jan 31 - Feb 13

Phase 3 - Design
Application Design
Feb 28 - Mar 13
Database Design
Feb 28 - Mar 13
Security Design
Feb 28 - Mar 13
Interface Design
Feb 28 - Mar 13

Phase 4 - Coding
Application Coding
Mar 14 - Apr 3
Database Coding
Mar 14 - Apr 3

Phase 5 - Testing
System Testing
Apr 4 - Apr 10
Security Testing
Apr 4 - Apr 10

Phase 6 - Reporting
Final Written Report
Apr 11 - Apr 24
Presentation
Apr 11 - Apr 24

Figure 2: Plan management by using Trello

Since this project is using an iterative approach. So, the completion and progress of each stage are important. This is because each stage depends on the completion of the previous stage and before the next stage can begin. In good project management, the project manager needs to set a time limit for each stage, and the project members should complete the relevant tasks at the designated time. The specified time is adjusted according to the difficulty of the task. Of course, with the development of the project, some changes may occur in the tasks of each stage, and the project manager can show the relevant changes to the members through the system. Also, the system can record different milestones and tasks to be done, and even discuss issues.

For this project, the project manager has divided the whole plan into 6 stages and each stage has a reasonable time frame. The stages are:

1. Project Setup: Setting up the project topic and aim. This stage is like discussing the system requirements with the project owner and project manager.
2. Background Research: According to the project setup, the analyst needs to have some research on the relevant topic, and draw up the direction of the system.
3. System Design: According to the previous stage, the system developer needs to design the whole system plan, such as the function of the system, interface of the system, database of the system, security of the system, etc.
4. System Coding: According to the function and the security that is drawn up in the previous stage, the programmer needs to follow the requirement to create the system.
5. System Testing: When the system is finished, the tester needs to test and try the finished system.
6. Reporting: If all the previous stages are finished, the project manager needs to round up all the things and report to the project owner.

The detail of each stage would present in Trello. The screen captures are shown in Appendix.

7. Architecture & Design

In this report, the eVoting system has been designed as a common and straightforward voting system. The main focus of the system is how to store and process the ballot to avoid hackers stealing data or tampering with data during the whole process, thereby affecting the voting results. Besides, this is an anonymous voting activity. Therefore, when designing the system, the following requirement have been mentioned in the objective: 1. Eligibility 2. Uniqueness 3. Fairness 4. Anonymity 5. Privacy 6. Accuracy 7. Security

Initial design:

From the beginning, the initial design is shown in Figure 3. There are two users, Admin and Voter. First of all, the system also will generate a ballot tracker for the valid voter. The voter after verification can get a ballot tracker. The ballot tracker is a random digital hash. It would be used to encrypt the ballot after the voter vote and avoid recording the personal detail of the voter, as anonymity.
Second, the system will generate a pair of keys, a public key and a private key, which are used to encrypt the ballot before storing it in the ballot database.
Lastly, blockchain technology would be applied to the ballot database.

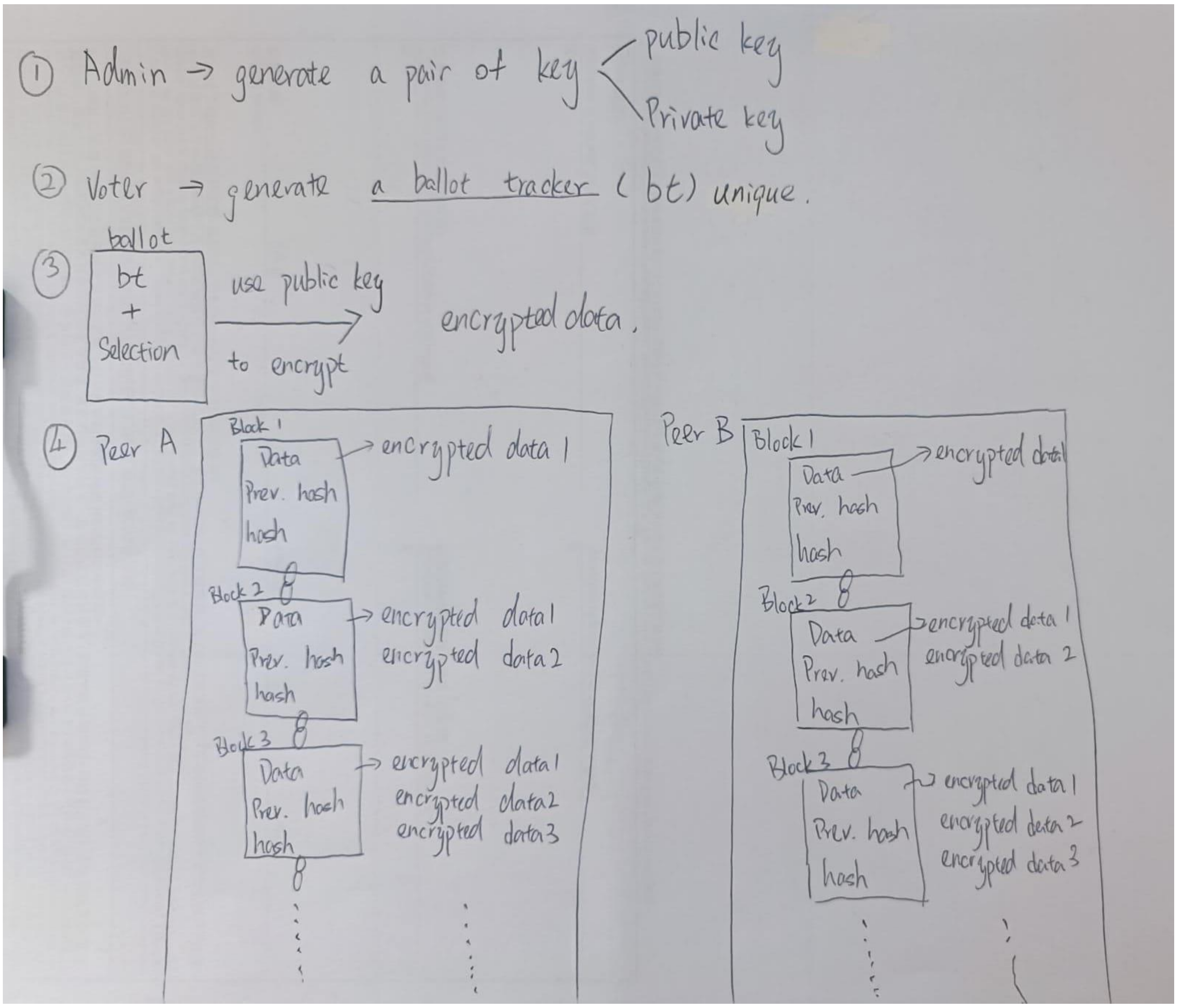


Figure 3 : Initial Design

Data Storing and processing:

Before the data of the ballot can be stored in the database, there are three steps to be processed.

1. The symmetric encryption algorithms has been used in step 1 (Shown in Figure 4: Symmetric Encryption Algorithms). The vaild voter would get a ballot tracker. It also is a key which is used to encrypt the selection of the voter.

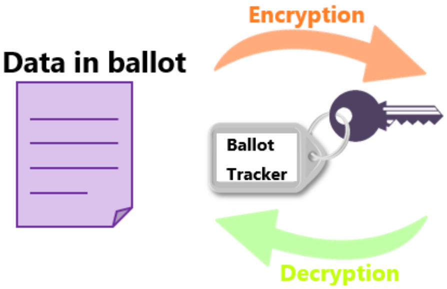


Figure 4: Symmetric Encryption Algorithms

2. The asymmetric encryption algorithms has been used in step 2 (Shown in Figure 5: Asymmetric Encryption Algorithms). The ciphertext 1 which is encrypted after first step would be processing to the second encryption. This time would used the public key of the admin to encrypt the data again.

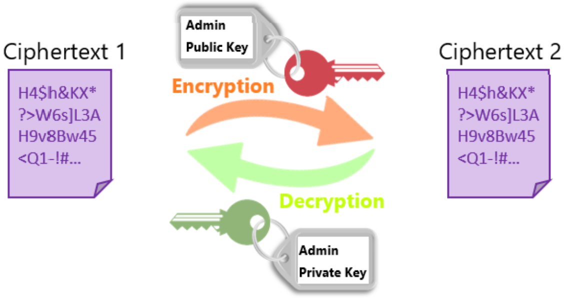


Figure 5: Asymmetric Encryption Algorithms

3. Blockchain technology would be applied in last step. The ciphertext 2 would be represented as Block Data and stored in the block. Before the new block is created, it needs to check the existing block data first. If the block data has been amemded, the hash would not same with the existing hash.

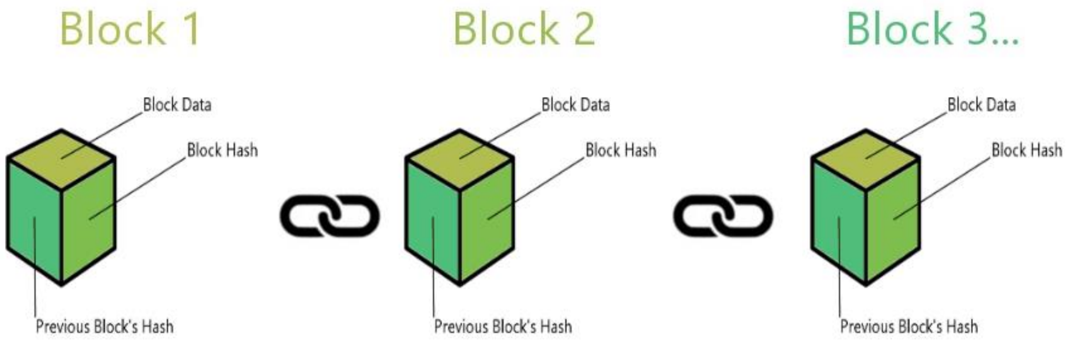


Figure 6: Blockchain

Use Case Diagram

The Figure 7 explains the flow of the project from user end and back end.

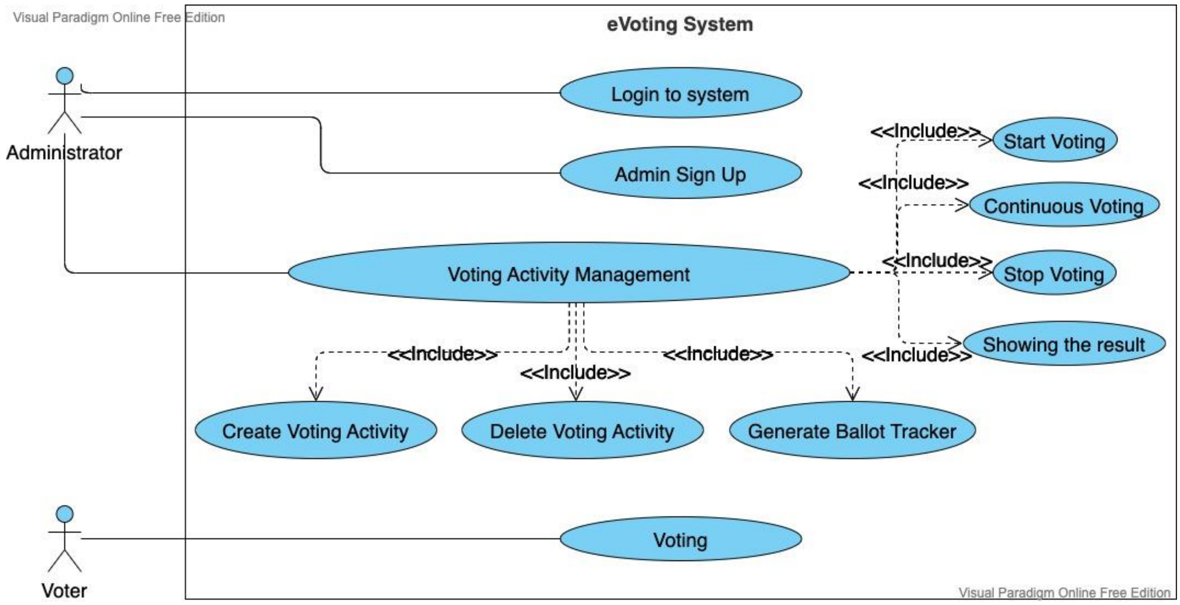


Figure 7: Use Case Diagram

Only the user – Admin, need to register to the system. Then the admin can go to the admin page, which can manage the the voting activity, such as creating voting activity, deleting voting activity, controlling the status of voting activity, generating the ballot tracker to the voters, and showing the result of the voting activity. The user – Voters, only can vote after the admin open the voting page to them.

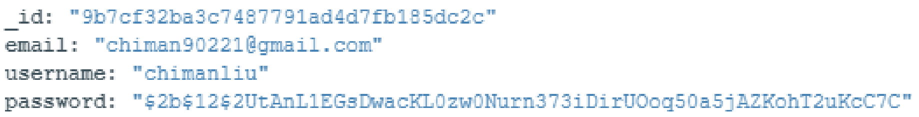
Database

In this project, the database sever has been selected as MongoDB. It is a NoSQL database and it can provide a high performance, high availability, and easy scalability. It is suitable for manage a large amount of data. In the system, there are 4 collections:

1. userDB: To store the information of the admin user.
2. votingDB: To store the information of voting activity that created by admin user.
3. ballottrackerDB: To store the ballot tracker only.
4. BallotDB: To store the data of the ballot what is transformed as a block.

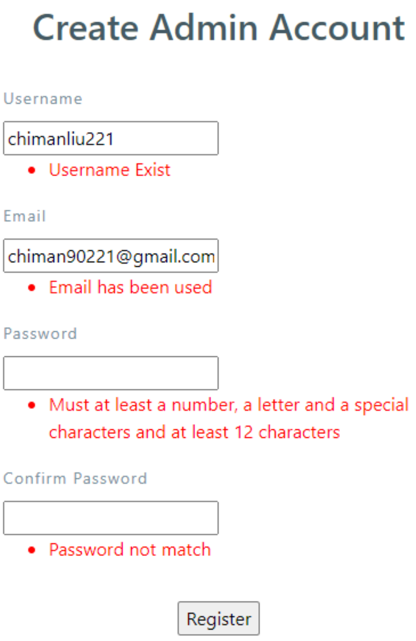
Security issue for the system

- Password hashed with SHA256 before sending to the database. (Figure 8)
- Specified a format for some of the data such as email, and password for mitigating the potential error or damage. (Figure 9)
- Used Regex to limit the user input to mitigate the potential error or damage. (Figure 10)
- Used CSRF token to mitigate CSRF attack. (Figure 11)



```
_id: "9b7cf32ba3c7487791ad4d7fb185dc2c"
email: "chiman90221@gmail.com"
username: "chimanliu"
password: "$2b$12$2UtAnL1EGsDwacKL0zw0Nurn373iDirUOoq50a5jAZKohT2uKcC7C"
```

Figure 8: Password hashed



Create Admin Account

Username

chimanliu221

- Username Exist

Email

chiman90221@gmail.com

- Email has been used

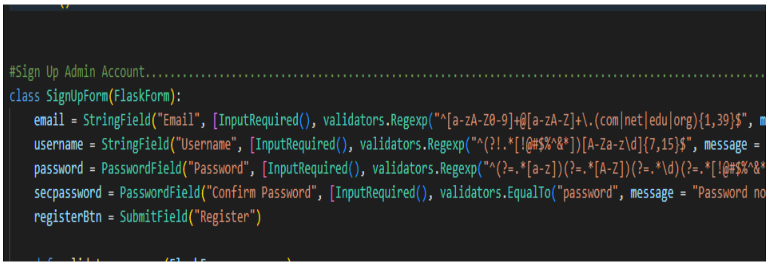
Password

- Must at least a number, a letter and a special characters and at least 12 characters

Confirm Password

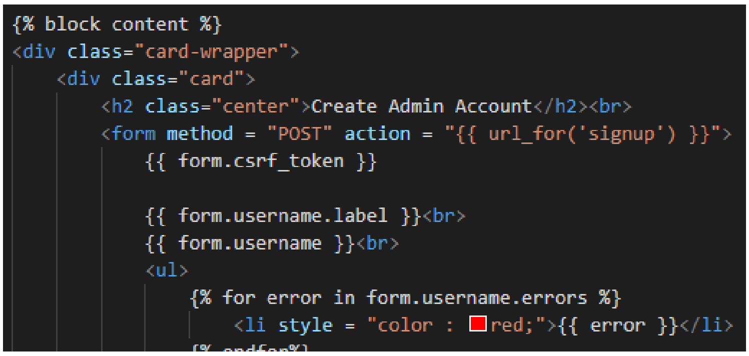
- Password not match

Figure 9: Specified a format



```
#Sign Up Admin Account..........................................................................................
class SignUpForm(FlaskForm):
    email = StringField("Email", [InputRequired(), validators.Regexp("^[a-zA-Z0-9]+@[a-zA-Z]+\.(com|net|edu|org){1,39}$", m
    username = StringField("Username", [InputRequired(), validators.Regexp("^(?!.*[!@#$%^&*])[A-Za-z\d]{7,15}$", message =
    password = PasswordField("Password", [InputRequired(), validators.Regexp("^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[!@#$%^&*
    secpassword = PasswordField("Confirm Password", [InputRequired(), validators.EqualTo("password", message = "Password no
    registerBtn = SubmitField("Register")
```

Figure 10: Used Regex



```
{% block content %}
<div class="card-wrapper">
    <div class="card">
        <h2 class="center">Create Admin Account</h2><br>
        <form method = "POST" action = "{{ url_for('signup') }}">
            {{ form.csrf_token }}

            {{ form.username.label }}<br>
            {{ form.username }}<br>
            <ul>
                {% for error in form.username.errors %}
                    <li style = "color : red;">{{ error }}</li>
```

Figure 11: Used CSRF

User interface

First of all, this is a simple voting system with few users, so it doesn't take too much time to design it. In addition, another goal of this voting system is to design an easy-to-use program for users. Therefore the design of the interface would be simple. The following Figures 12-18 will show the interface of this system.

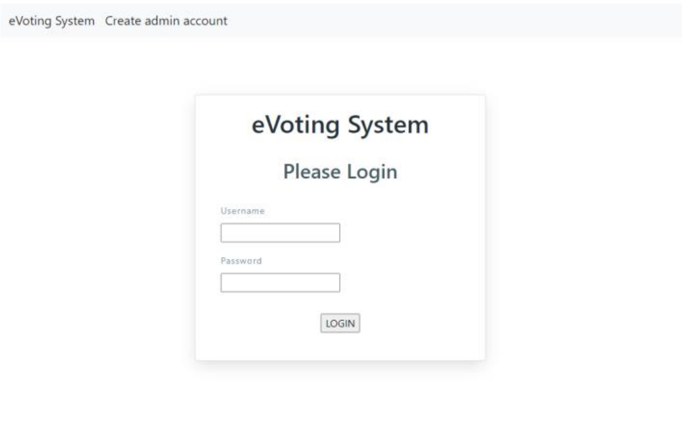


Figure 12: Login Page

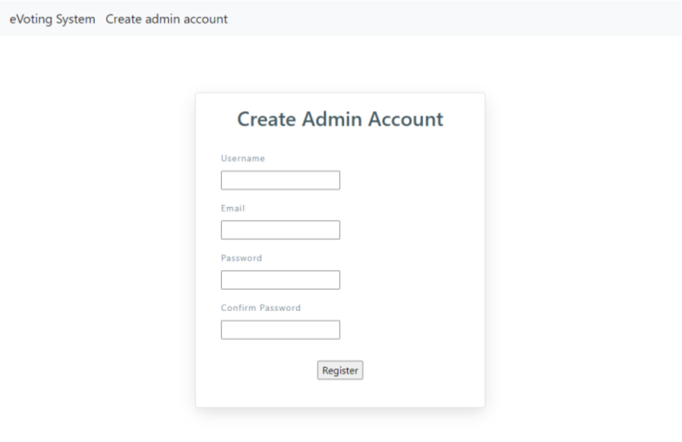
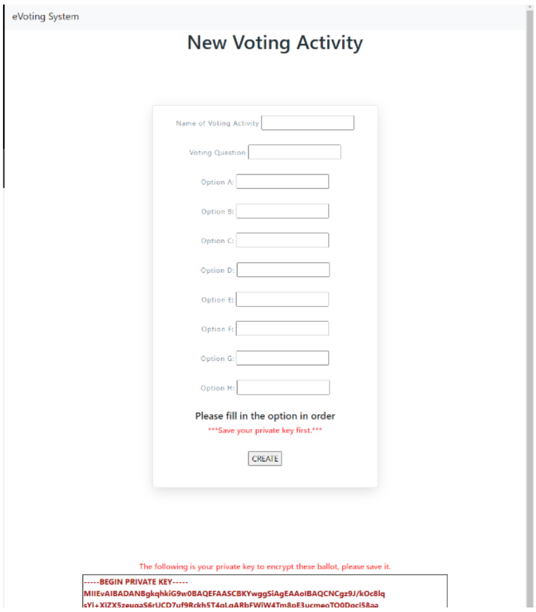


Figure 13: Sign Up Page



eVoting System

New Voting Activity

Name of Voting Activity

Voting Question

Option A:

Option B:

Option C:

Option D:

Option E:

Option F:

Option G:

Option H:

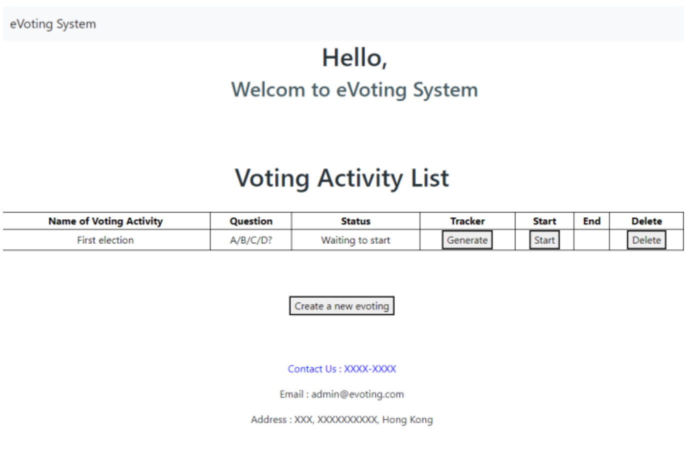
Please fill in the option in order

Save your private key first.

The following is your private key to encrypt these ballot, please save it.

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCNCgz9J/kOc8lq
sYi+XiZX5zeugaS6rUCD7uf9Rckh5T4qLqARbFWiW4Tm8pE3ucmeoTO0Dqci58aa
```

Figure 14: Create Voting Activity Page



eVoting System

Hello,

Welcom to eVoting System

Voting Activity List

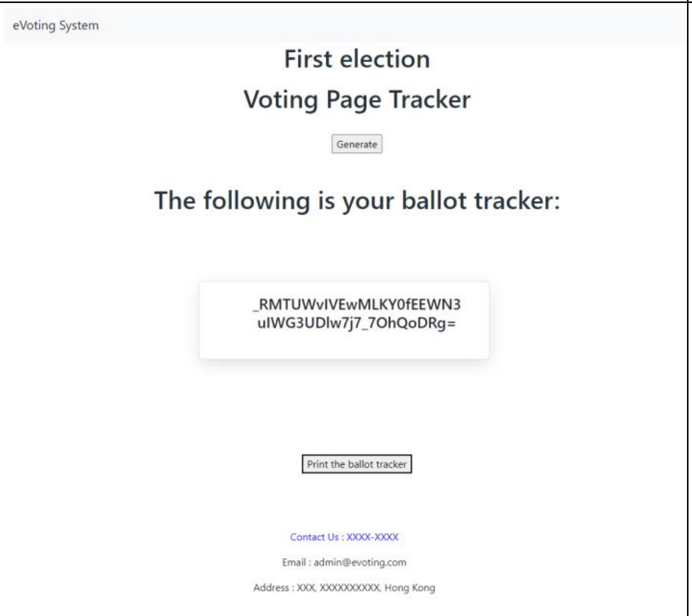
Name of Voting Activity	Question	Status	Tracker	Start	End	Delete
First election	A/B/C/D?	Waiting to start	Generate	Start		Delete

Contact Us : XXXX-XXXX

Email : admin@evoting.com

Address : XXX, XXXXXXXXXX, Hong Kong

Figure 15: Admin Main Page – Manage the voting activity



eVoting System

First election

Voting Page Tracker

The following is your ballot tracker:

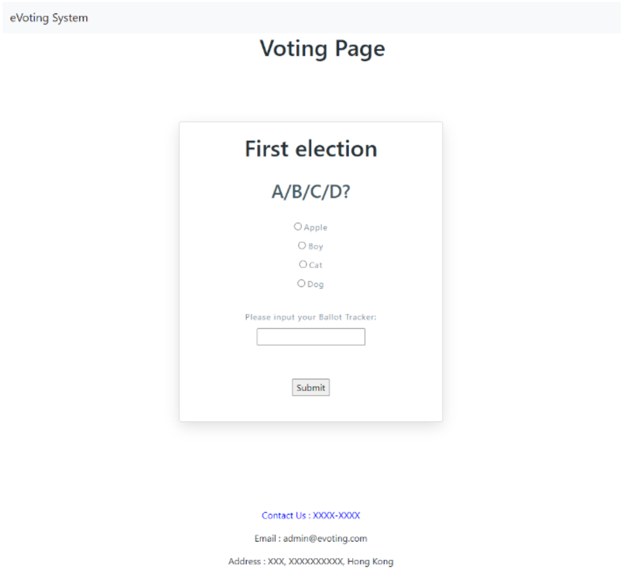
_RMTUWvIVEwMLKY0fEEWN3
uIWG3UDlw7j7_7OhQoDRg=

Contact Us : XXXX-XXXX

Email : admin@evoting.com

Address : XXX, XXXXXXXXXX, Hong Kong

Figure 16: Generate Ballot tracker Page



eVoting System

Voting Page

First election

A/B/C/D?

○ Apple
○ Boy
○ Cat
○ Dog

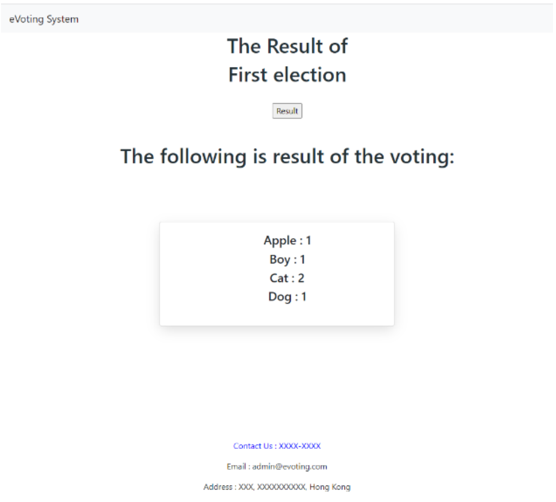
Please input your Ballot Tracker:

Contact Us : XXXX-XXXX

Email : admin@evoting.com

Address : XXX, XXXXXXXXXX, Hong Kong

Figure 17: Voting Page



eVoting System

The Result of
First election

The following is result of the voting:

Apple : 1
Boy : 1
Cat : 2
Dog : 1

Contact Us : XXXX-XXXX

Email : admin@evoting.com

Address : XXX, XXXXXXXXXX, Hong Kong

Figure 18: Voting Result Page

8. Testing

Function Test

1. Login Function Test		
Testing issue:	Result	
● Do not fill in username & password	Can’t login and remind to fill the information	√
● Input a wrong password	Can’t login and to the wrong password page	√
● Input correct data	Seccussful to Login	√

2. Sign Up Test		
Testing issue:	Result	
● Do not fill in anything	Can’t submit and have remind to fill the information	√
● Repeat fill in same username / email	Can’t submit and remind the username / email have been used	√
● Fill in incorrect password	Can’t submit and remind the correct form of password	√
● Password and confirmed password not same	Can’t submit and remind these two password do not same	√
● Input correct data	Seccussful to submit	√

3. Create New Voting activity Test		
Testing issue:	Result	
● Do not fill in anything	Can’t submit and have remind to fill the information	√
● Just randomly fill the option, and the option a or b is/are blank	Can’t submit and have remind to fill the information	√
● Just randomly fill the option, and the option a or b is/are not blank	Can submit but voting page only show the option before blanl option	--
● Fullfill the repuirement of input, but fill the same answer for the voting option	Can submit but when counting the vote, it will count to the first option	--
● Input correct data	Seccussful to submit	√

4. Generate the ballot tracker Test		
Testing issue:	Result	
● Click “Generate” button	Seccussful to show the ballot tracker	√

● Click “Print” button	No respond.	X

5. Generate the ballot tracker Test		
Testing issue:	Result	
● Click “Result” button with wrong privacy key	Fail to show the result	√
● Click “Result” button with correct privacy key	Seccussful to show the result	√

In Create New Voting activity test, there are two bugs here, although the system have the reminding statement here, but the user might have these mistake. Therefore, the system can fix the relevant bug in the future update.

In Generate the ballot tracker Test, the print button do not respond, because the programmer do not encode anything for the function. Therefore, the programmer can try to develop relenvant function.

Scenario Test

1. When the voting activity is in progress, the data in database has been amended.	
Result	
● The system would alert and pasue the voting activity when the data of latest block has been amended. ● If the data of the latest block has not been amended, there is no respond.	√

2. When the voter use a wrong ballot tracker to vote or vote two time with same ballot tracker.	
Result	
● Do not success to submit the ballot.	√

9. Verification and validation

This system mainly develops an electronic voting system through blockchain technology. It is hoped that the technology of blockchain can be used to add a layer of protection to all ballots to avoid hacking and affecting the results of the election. Therefore, in terms of design specifications, the system can achieve the ultimate goal of properly protecting the information of all valid ballot papers

On the other hand, the design of this system can meet the needs of most users, such as anonymous voting, security issues of ballots, one-person-one-voting, etc. However, in terms of verifying voters, the system has not been developed fully, which has slowed down the time to vote. In addition, the system has not developed remote voting, and cannot allow voters to vote anywhere.

10. Evaluation

Regarding project management, it would be better to make better arrangements such as time management. I am acting in different roles on the project with limited personal ability and experience. As an analyst, I could not consider the system operation at a macro level and therefore some problems appeared when I was testing the system. As a programmer, I could not make the coding professionally as I am weak in this aspect. I need to put more time into searching and therefore I mentioned the problem of time management at the beginning of this evaluation.

About the system design, as it is a local eVoting system, it cannot attain the optimal advantage of a system. For example, the voters would be restricted by place or time, they cannot cast the vote wherever and whenever they are available.

Besides, this system puts too much focus on protecting the data of the ballots and therefore it has ignored a lot of significant functions such as the verification of the voters.

11. Conclusions

In conclusion, blockchain technology brings many benefits to the storage and operation of data, especially to improve data security. Therefore, the widespread application of blockchain is the general trend. This report, using blockchain technology to develop an electronic voting system, found that it was of great help in protecting the data of the ballot. It can improve people's confidence in the electronic voting system and restore people's willingness to vote, bringing help to a democratic society. Therefore, all industries can start to use blockchain technology to develop more and more perfect systems. Also, it can help the existing system to protect the data in an advanced way.

12. References

Abuidris, Y., Hassan, A., Hadabi, A., & Elfadul, I. (2019, December). Risks and opportunities of blockchain based on e-voting systems. In 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing (pp. 365-368). IEEE.

Adeshina, S. A., & Ojo, A. (2014, September). Design imperatives for e-voting as a sociotechnical system. In 2014 11th International Conference on Electronics, Computer and Computation (ICECCO) (pp. 1-4). IEEE.

Alamleh, H., & AlQahtani, A. A. S. (2021, May). Analysis of the Design Requirements for Remote Internet-Based E-Voting Systems. In 2021 IEEE World AI IoT Congress (AIIoT) (pp. 0386-0390). IEEE.

Bartoletti, M., & Pompianu, L. (2017, April). An empirical analysis of smart contracts: platforms, applications, and design patterns. In International conference on financial cryptography and data security (pp. 494-509). Springer, Cham.

Benny, A. (2020). Blockchain based e-voting system. Available at SSRN 3648870.

Burkhardt, D., Werling, M., & Lasi, H. (2018, June). Distributed ledger. In 2018 IEEE international conference on engineering, technology and innovation (ICE/ITMC) (pp. 1-9). IEEE

Cheng, H., Dinu, D., & Großschädl, J. (2018, November). Efficient implementation of the SHA-512 hash function for 8-bit AVR microcontrollers. In International Conference on Security for Information Technology and Communications (pp. 273-287). Springer, Cham.

Courtois, N. T., Grajek, M., & Naik, R. (2014, September). Optimizing sha256 in bitcoin mining. In International Conference on Cryptography and Security Systems (pp. 131-144). Springer, Berlin, Heidelberg.

Dang, Q. H. (2015). Secure hash standard.

El Ioini, N., & Pahl, C. (2018, October). A review of distributed ledger technologies. In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems" (pp. 277-288). Springer, Cham.

Guegan, D. (2017). Public blockchain versus private blockchain.

Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain-based e-voting system. In 2018 IEEE 11th international conference on cloud computing (CLOUD) (pp. 983-986). IEEE.

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors, 21(17), 5874.

Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. Ieee Software, 35(4), 95-99.

National Academies of Sciences, Engineering, and Medicine. (2018). Securing the Vote: Protecting American Democracy. National Academies Press.

Perugini, M. L., & Dal Checco, P. (2015). Smart Contracts: a preliminary evaluation. Available at SSRN 2729548.

Prata, David & Araújo, Humberto & Santos, Cleorbete & Patel, Pratham. (2021). A Literature Review about Smart Contracts Technology. SSRN Electronic Journal. 8. 1-4.

Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry, 12(8), 1328.

Thuy, N. T. T., & Khai, L. D. (2020). A fast approach for bitcoin blockchain cryptocurrency mining system. Integration, 74, 107-114.

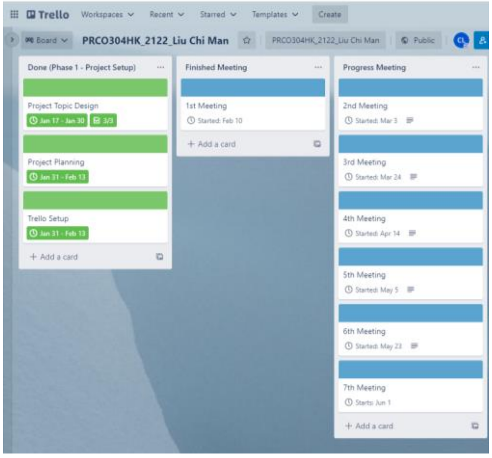
Yavuz, E., Koç, A. K., Çabuk, U. C., & Dalkılıç, G. (2018, March). Towards secure e-voting using ethereum blockchain. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-7). IEEE.

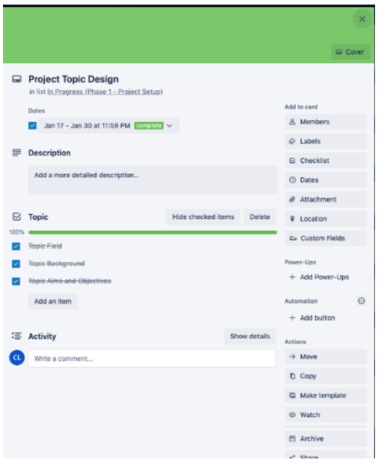
Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019, February). Research on the Application of Cryptography on the Blockchain. In Journal of Physics: Conference Series (Vol. 1168, No. 3, p. 032077). IOP Publishing.

13. Appendix

Project Management – Screen Captures of Trello

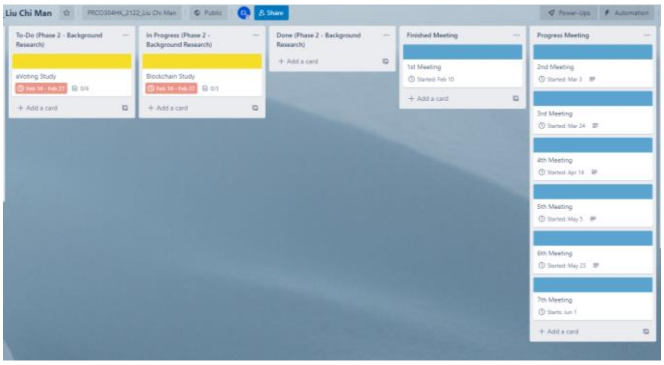
Date: 2022/02/10

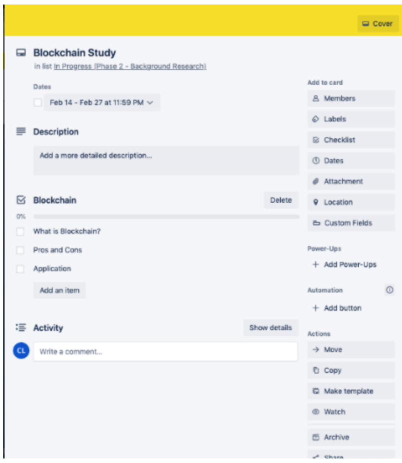




In 2022/02/10, the project finished topic design, project planning, and Trello set up.

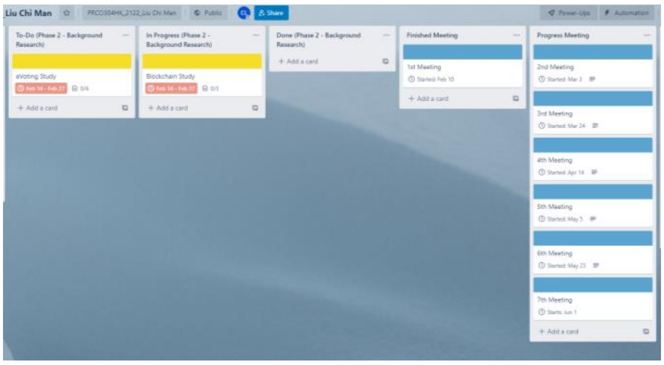
Date: 2022/02/17

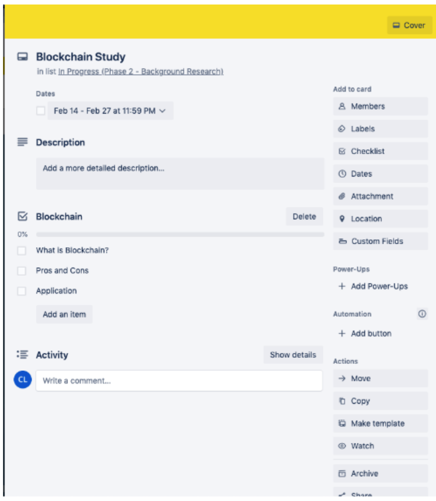




In 2022/02/17, the project started to have background research in Blockchain.

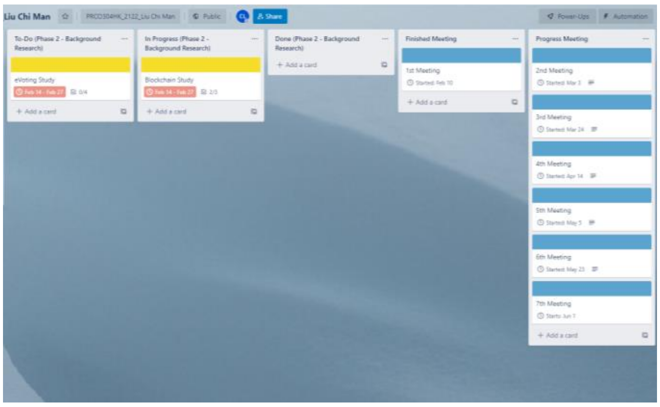
Date: 2022/02/24

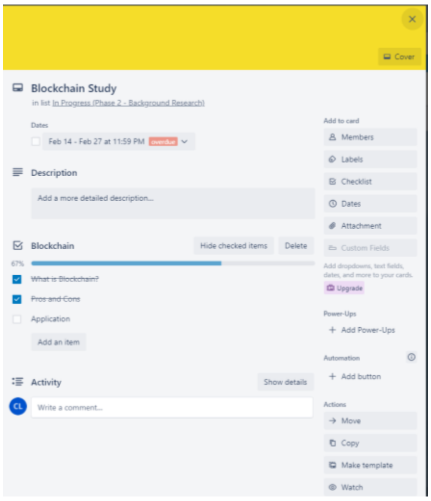




In 2022/02/24, the project started to have background research in Blockchain.

Date: 2022/02/24





Blockchain Study

in list In Progress (Phase 2 - Background Research)

Dates

□ Feb 14 - Feb 27 at 11:59 PM overdue

Description

Add a more detailed description...

Blockchain — Hide checked items — Delete

67%

☑ ~~What is Blockchain?~~

☑ ~~Pros and Cons~~

□ Application

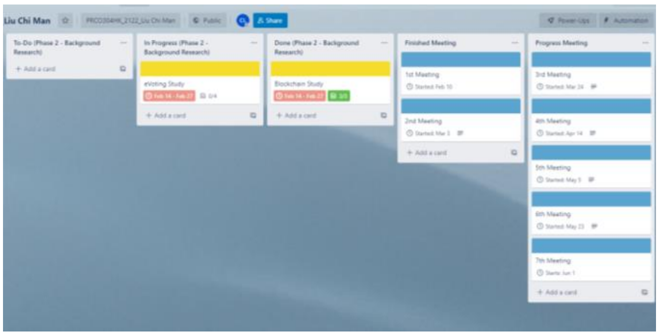
Add an item

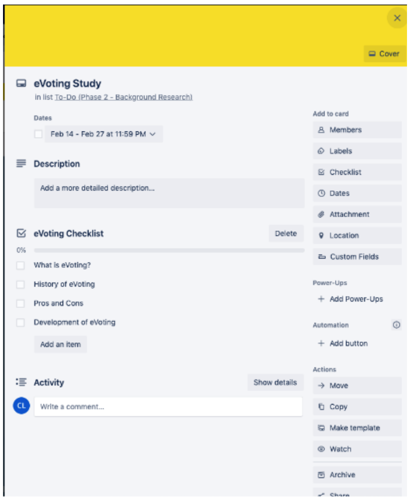
Activity — Show details

CL Write a comment...

In 2022/02/24, the project was delayed and the progress was still in background research of Blockchain.

Date: 2022/03/03





eVoting Study

in list To-Do (Phase 2 - Background Research)

Dates

□ Feb 14 - Feb 27 at 11:59 PM

Description

Add a more detailed description...

eVoting Checklist — Delete

0%

□ What is eVoting?

□ History of eVoting

□ Pros and Cons

□ Development of eVoting

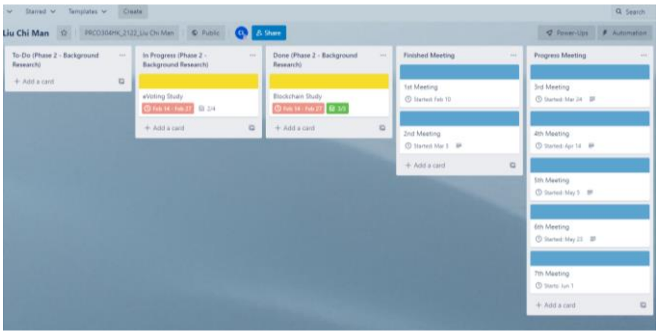
Add an item

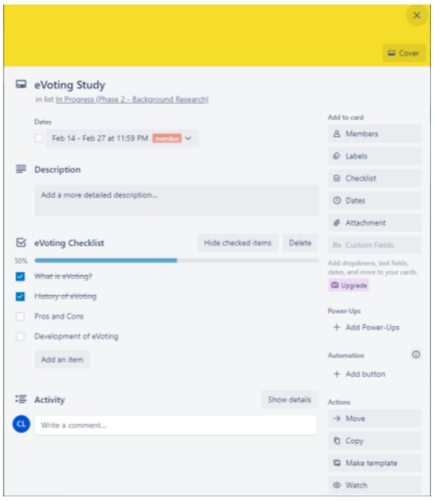
Activity — Show details

CL Write a comment...

In 2022/03/03, the project was delayed and the progress was still in background research of eVoting.

Date: 2022/03/10





eVoting Study

in list In Progress (Phase 2 - Background Research)

Dates

□ Feb 14 - Feb 27 at 11:59 PM overdue

Description

Add a more detailed description...

eVoting Checklist — Hide checked items — Delete

50%

☑ ~~What is eVoting?~~

☑ ~~History of eVoting~~

□ Pros and Cons

□ Development of eVoting

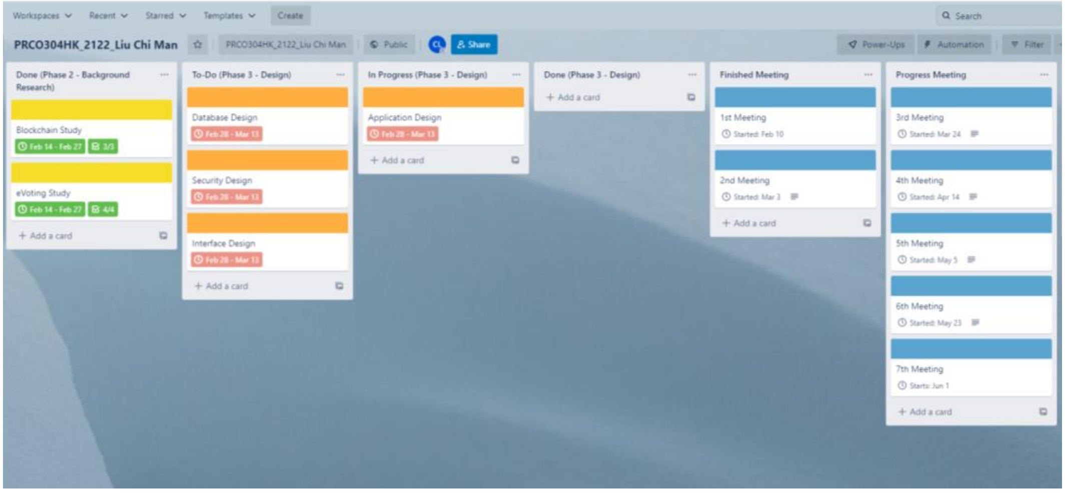
Add an item

Activity — Show details

CL Write a comment...

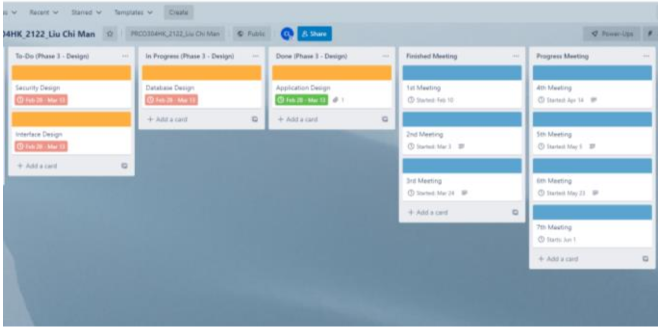
In 2022/03/10, the project was delayed and the progress was still in background research of eVoting.

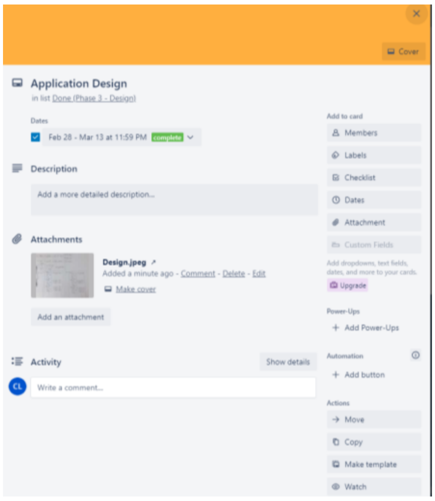
Date: 2022/03/17



In 2022/03/17, the project finished Stage 2 – Background Research and started the system design.

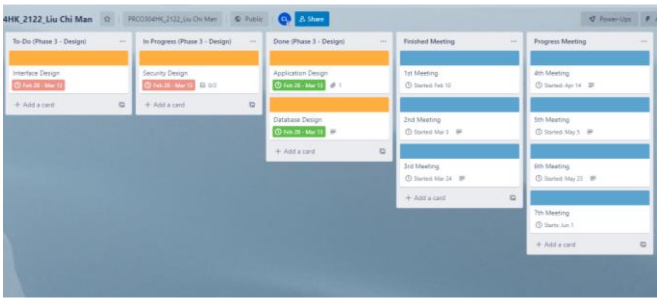
Date: 2022/03/24

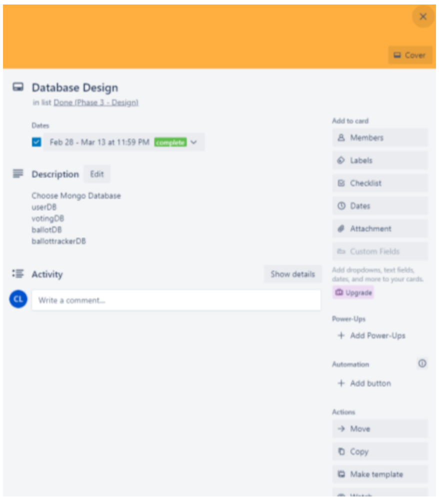




In 2022/03/24, the project finished project design and upload the draft design to Trello.

Date: 2022/03/31

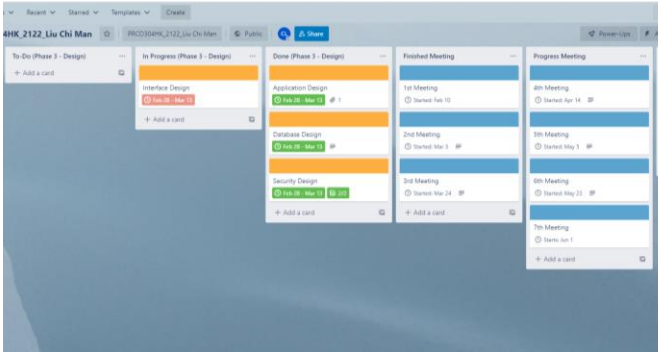




Choose Mongo Database
userDB
votingDB
ballotDB
ballottrackerDB

In 2022/03/31, the project finished database design.

Date: 2022/04/07



Recent Starred Templates Create

4HK_2122_Liu Chi Man PRCO304HK_2122_Liu Chi Man Public Share Power-Ups

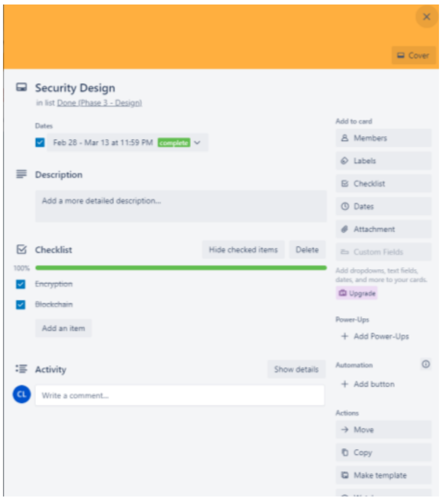
To-Do (Phase 3 - Design)
- + Add a card

In Progress (Phase 3 - Design)
- Interface Design — Feb 28 - Mar 13
- + Add a card

Done (Phase 3 - Design)
- Application Design — Feb 28 - Mar 13 1
- Database Design — Feb 28 - Mar 13
- Security Design — Feb 28 - Mar 13 2/2
- + Add a card

Finished Meeting
- 1st Meeting — Started: Feb 10
- 2nd Meeting — Started: Mar 3
- 3rd Meeting — Started: Mar 24
- + Add a card

Progress Meeting
- 4th Meeting — Started: Apr 14
- 5th Meeting — Started: May 5
- 6th Meeting — Started: May 23
- 7th Meeting — Starts: Jun 1
- + Add a card



Cover

Security Design
in list Done (Phase 3 - Design)

Dates
☑ Feb 28 - Mar 13 at 11:59 PM complete

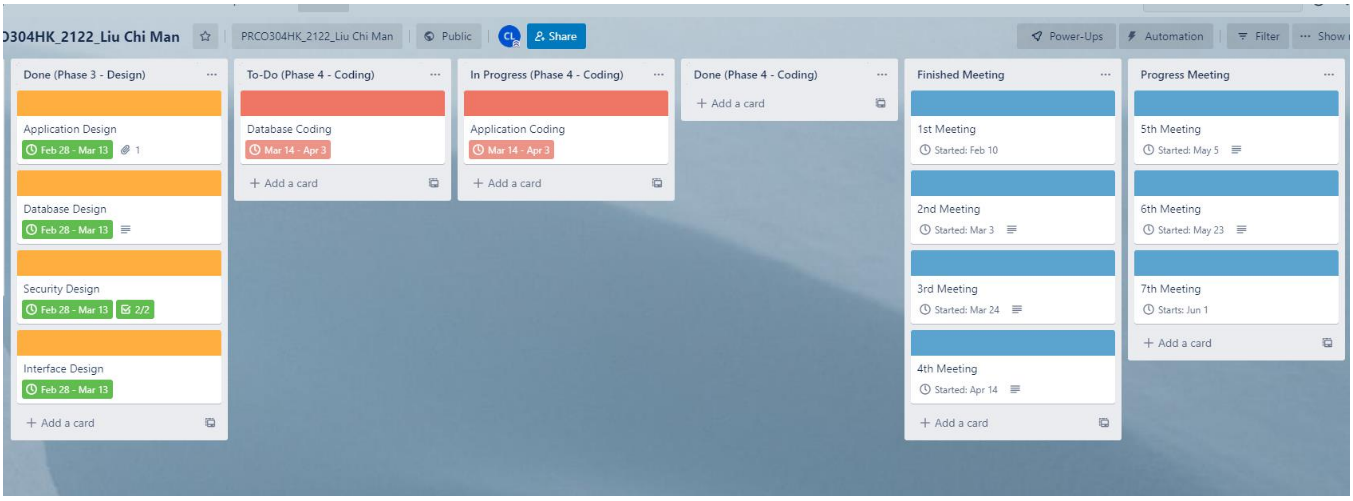
Description
Add a more detailed description...

Checklist — Hide checked items — Delete
100%
☑ ~~Encryption~~
☑ ~~Blockchain~~
Add an item

Activity — Show details
CL Write a comment...

In 2022/04/07, the project finished security design.

Date: 2022/04/14



D304HK_2122_Liu Chi Man PRCO304HK_2122_Liu Chi Man Public CL Share Power-Ups Automation Filter Show

Done (Phase 3 - Design)
- Application Design — Feb 28 - Mar 13 1
- Database Design — Feb 28 - Mar 13
- Security Design — Feb 28 - Mar 13 2/2
- Interface Design — Feb 28 - Mar 13
- + Add a card

To-Do (Phase 4 - Coding)
- Database Coding — Mar 14 - Apr 3
- + Add a card

In Progress (Phase 4 - Coding)
- Application Coding — Mar 14 - Apr 3
- + Add a card

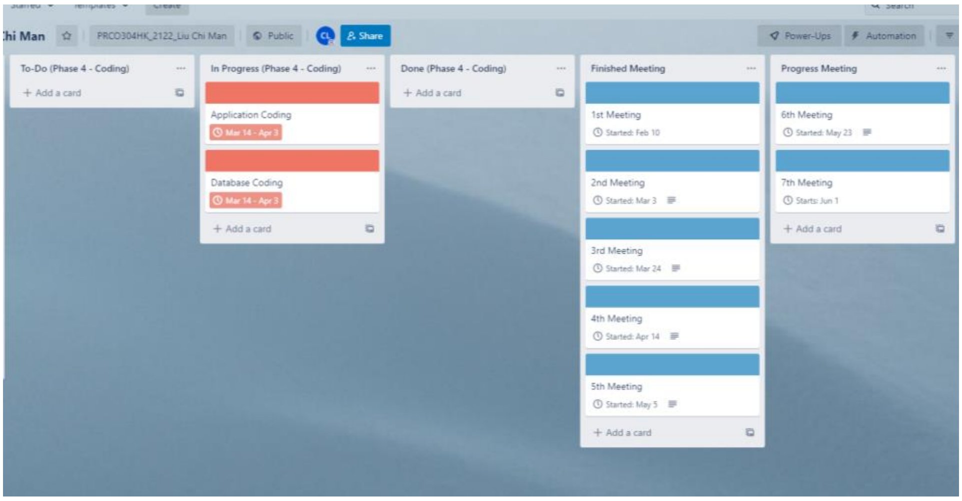
Done (Phase 4 - Coding)
- + Add a card

Finished Meeting
- 1st Meeting — Started: Feb 10
- 2nd Meeting — Started: Mar 3
- 3rd Meeting — Started: Mar 24
- 4th Meeting — Started: Apr 14
- + Add a card

Progress Meeting
- 5th Meeting — Started: May 5
- 6th Meeting — Started: May 23
- 7th Meeting — Starts: Jun 1
- + Add a card

In 2022/04/14, the project finished stage 3 – System Design.

Date: 2022/05/05



Starred Templates Create Search

hi Man PRCO304HK_2122_Liu Chi Man Public CL Share Power-Ups Automation

To-Do (Phase 4 - Coding)
- + Add a card

In Progress (Phase 4 - Coding)
- Application Coding — Mar 14 - Apr 3
- Database Coding — Mar 14 - Apr 3
- + Add a card

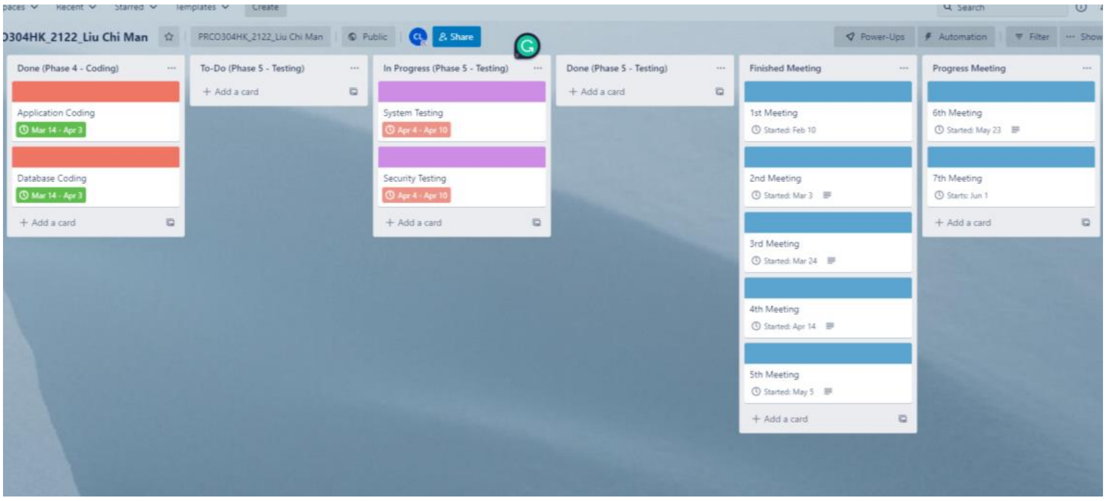
Done (Phase 4 - Coding)
- + Add a card

Finished Meeting
- 1st Meeting — Started: Feb 10
- 2nd Meeting — Started: Mar 3
- 3rd Meeting — Started: Mar 24
- 4th Meeting — Started: Apr 14
- 5th Meeting — Started: May 5
- + Add a card

Progress Meeting
- 6th Meeting — Started: May 23
- 7th Meeting — Starts: Jun 1
- + Add a card

In 2022/05/05, the project was still in the stage 4 – System coding.

Date: 2022/05/12



)304HK_2122_Liu Chi Man

PRCO304HK_2122_Liu Chi Man

Done (Phase 4 - Coding)
- Application Coding — Mar 14 - Apr 3
- Database Coding — Mar 14 - Apr 3
- + Add a card

To-Do (Phase 5 - Testing)
- + Add a card

In Progress (Phase 5 - Testing)
- System Testing — Apr 4 - Apr 10
- Security Testing — Apr 4 - Apr 10
- + Add a card

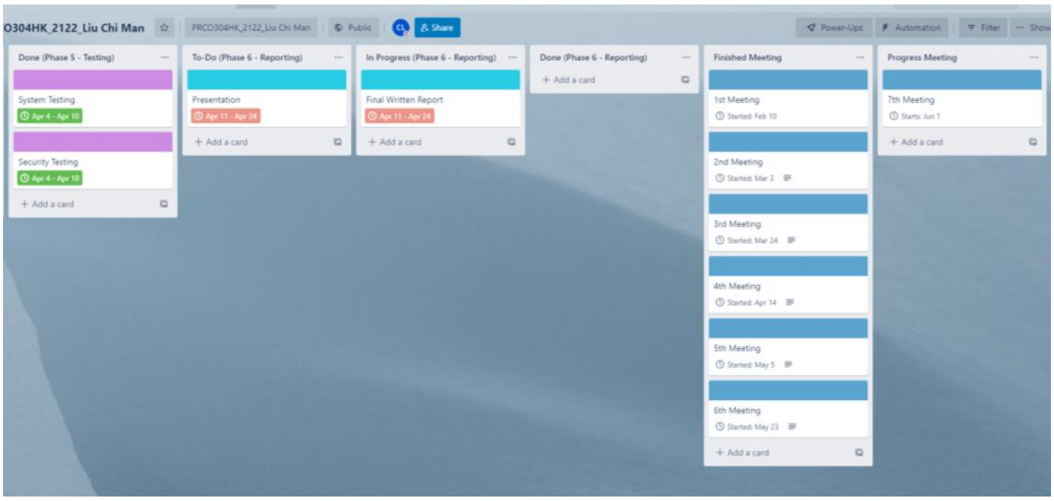
Done (Phase 5 - Testing)
- + Add a card

Finished Meeting
- 1st Meeting — Started: Feb 10
- 2nd Meeting — Started: Mar 3
- 3rd Meeting — Started: Mar 24
- 4th Meeting — Started: Apr 14
- 5th Meeting — Started: May 5
- + Add a card

Progress Meeting
- 6th Meeting — Started: May 23
- 7th Meeting — Starts: Jun 1
- + Add a card

In 2022/05/12, the project finished stage 5 – System Testing

Date: 2022/05/19-31



O304HK_2122_Liu Chi Man

PRCO304HK_2122_Liu Chi Man

Done (Phase 5 - Testing)
- System Testing — Apr 4 - Apr 10
- Security Testing — Apr 4 - Apr 10
- + Add a card

To-Do (Phase 6 - Reporting)
- Presentation — Apr 11 - Apr 24
- + Add a card

In Progress (Phase 6 - Reporting)
- Final Written Report — Apr 11 - Apr 24
- + Add a card

Done (Phase 6 - Reporting)
- + Add a card

Finished Meeting
- 1st Meeting — Started: Feb 10
- 2nd Meeting — Started: Mar 3
- 3rd Meeting — Started: Mar 24
- 4th Meeting — Started: Apr 14
- 5th Meeting — Started: May 5
- 6th Meeting — Started: May 23
- + Add a card

Progress Meeting
- 7th Meeting — Starts: Jun 1
- + Add a card

In 2022/05/19-31, the project was in progress at stage 6 – Reporting.