Abstract geometric lines in the top left corner, consisting of several overlapping, irregular polygons and lines in a light beige color.

# 系統安全

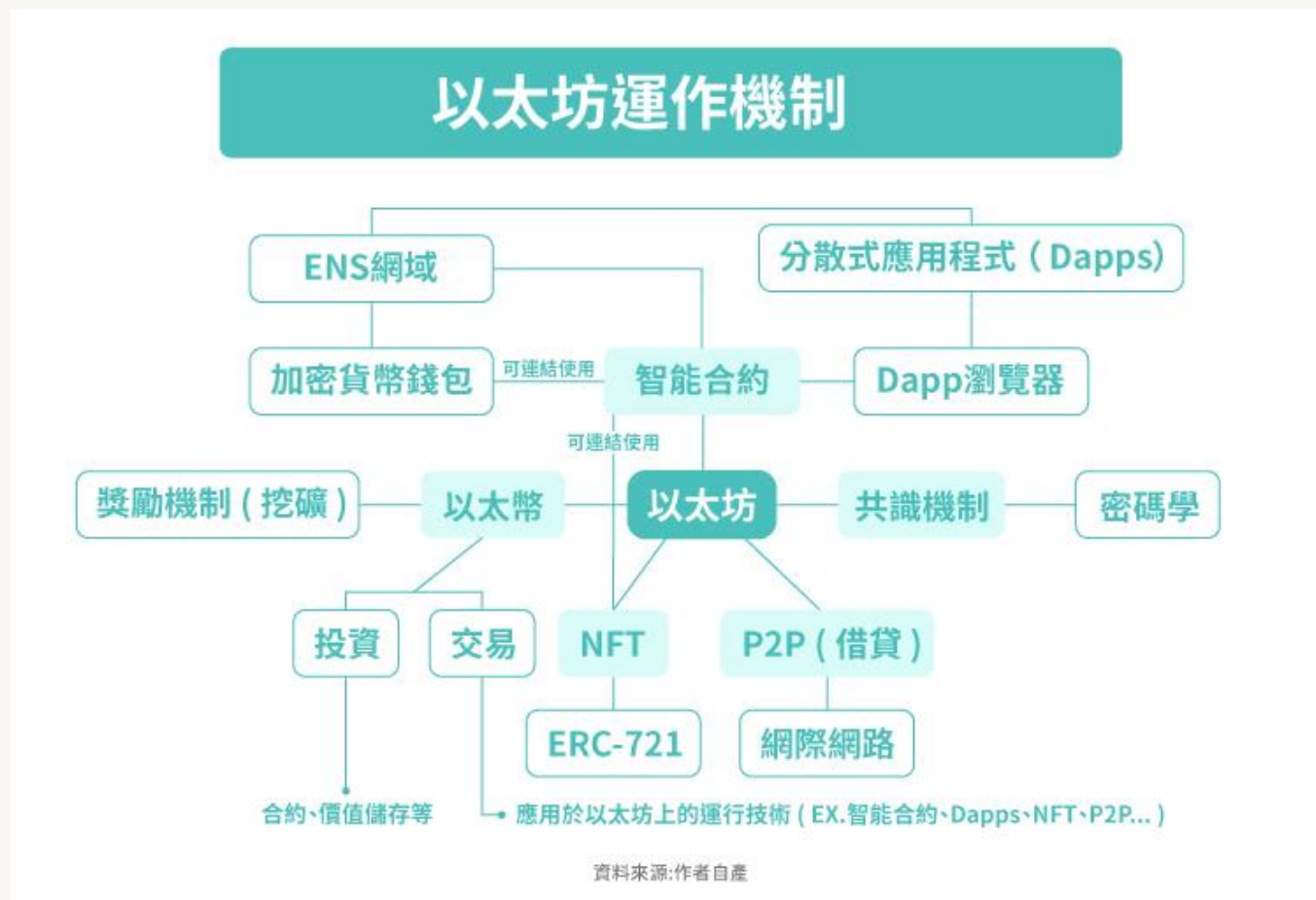
軟創三乙 511172176 李則霖

## 簡述

利用在系統安全課程所學，瞭解區塊鏈系統的安全性機制與防禦機制。並且使用智能合約在以太坊區塊鏈二層Abitrum鏈seoplia測試網部屬合約發行ERC20標準代幣，搭配前端、後端、資料庫及Matemask錢包增加使用體驗，並且提供智能合約安全性檢測。

1. \_\_\_\_\_ 以太坊區塊鏈系統
2. \_\_\_\_\_ 加密機制
3. \_\_\_\_\_ 攻擊與防禦
4. \_\_\_\_\_ 專案規劃

# 以太坊區塊鏈系統



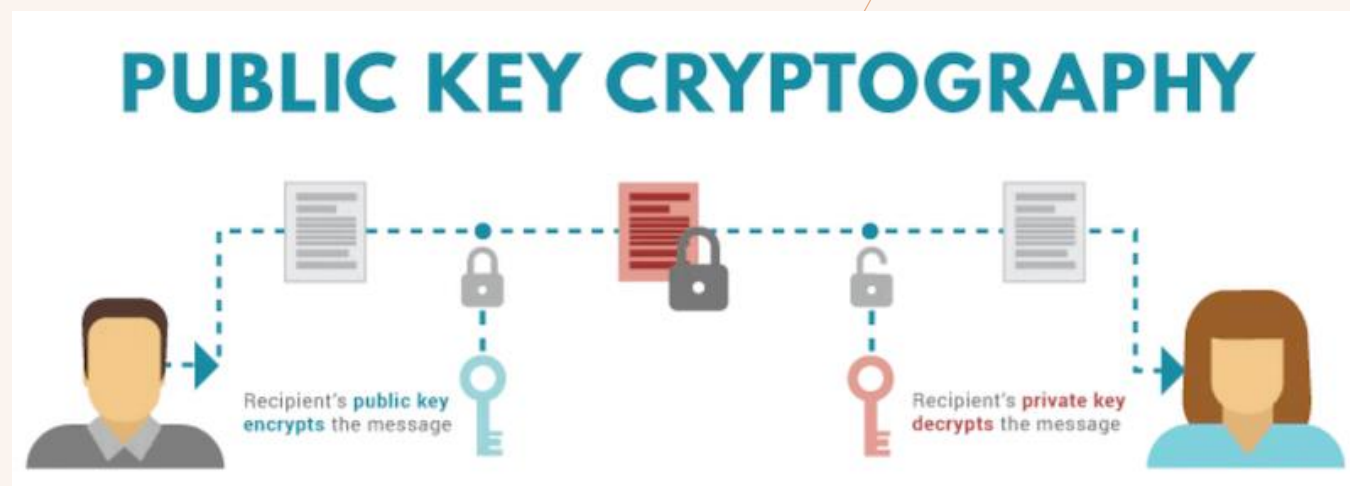
資料來源: 網路抓取

# 加密機制

**非對稱加密 (Asymmetric Cryptography)：**以太坊使用非對稱加密來生成公鑰和私鑰。每個用戶的交易都需要使用私鑰進行簽名，確保只有合法的所有者才能發送交易。公鑰則用來驗證簽名的正確性，從而確保交易的真實性和完整性。

**雜湊函數 (Hash Functions)：**以太坊使用Keccak-256雜湊函數來生成交易和區塊的唯一標識符（即雜湊值）。這些雜湊值保證了交易和區塊的不可篡改性。

**數位簽章 (Digital Signatures)：**使用Elliptic Curve Digital Signature Algorithm (ECDSA) 進行交易的，確保數位簽章交易發起者的身份驗證。



圖片來源:網路抓取

# 權益證明 (PROOF OF STAKE, POS)

## 質押 (Staking)

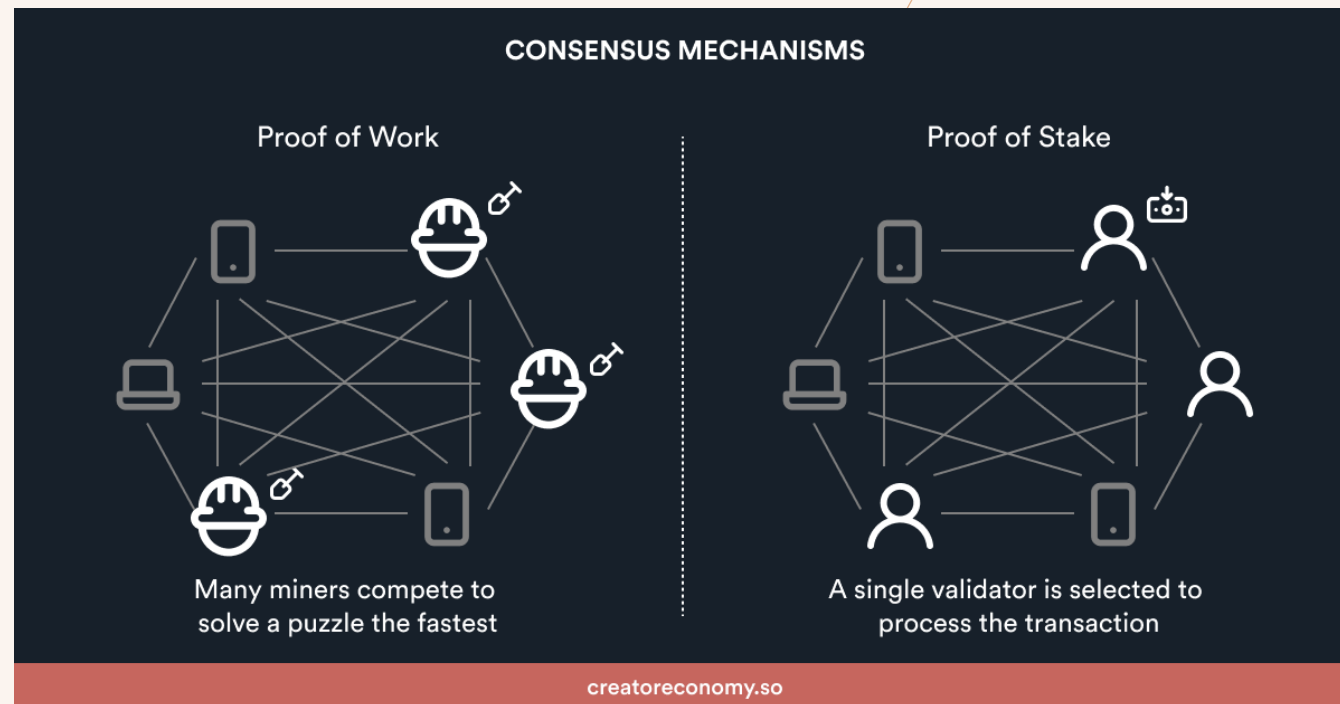
**保障系統的安全性：**質押資金相當於驗證者對其行為的保證，確保驗證者不會輕易作惡，因為作惡的代價是失去所質押的資金。

**維持網絡的去中心化和經濟激勵：**驗證者通過質押參與共識過程，並在誠實執行區塊驗證後獲得區塊獎勵，這為整個網絡的運行提供了經濟動力。

## 削減機制 (Slashing)

**雙重簽名 (Double Signing)：**驗證者在同一區塊高度生成並簽署兩個不同的區塊，這可能導致區塊鏈的分叉，是一種惡意行為。

**鏈外行為不一致：**如果驗證者的行為違背共識協議（如故意拖延區塊生成或重複提交無效提案），他們的質押資金也可能被削減。



圖片來源:網路抓取

# 專案規劃需求分析

發行代幣：

代幣名稱：Fjcu

代幣總量：21,000,000 枚

代幣標準：ERC-20

功能需求：

智能合約發行代幣

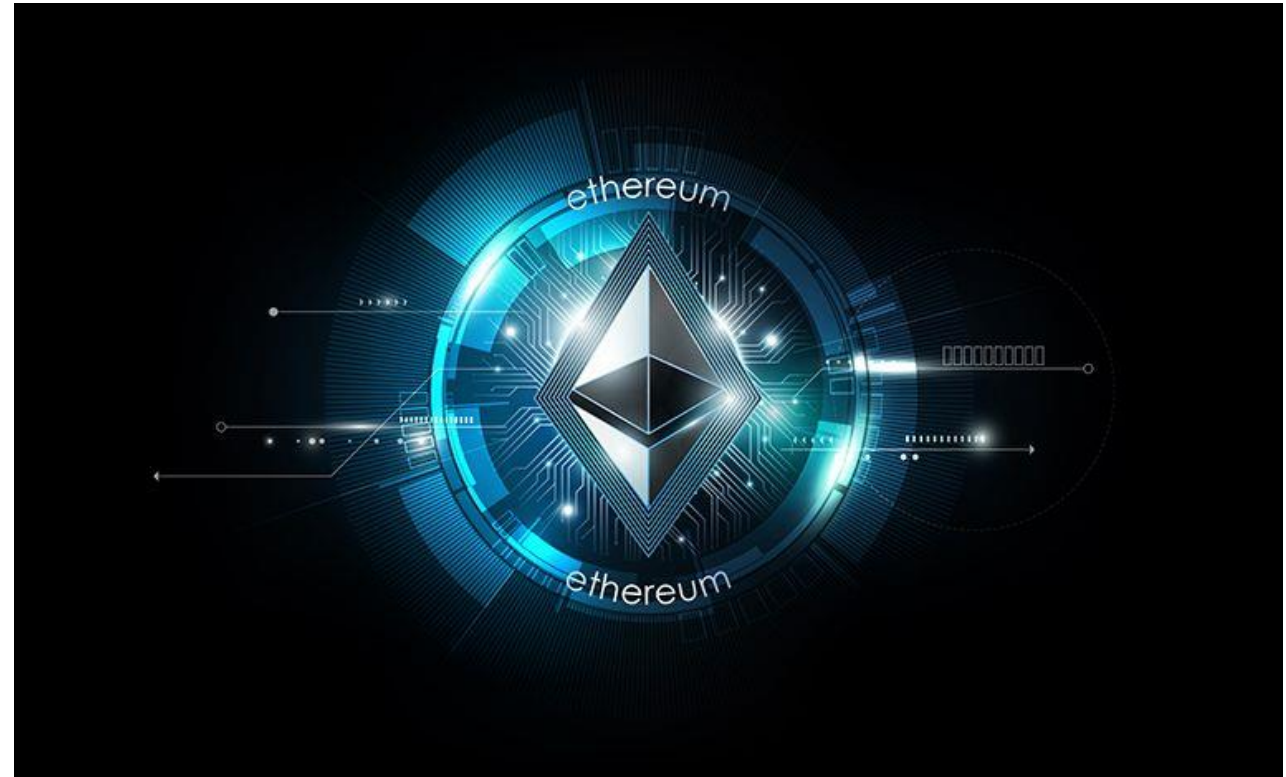
連接WEB3錢包

查詢錢包代幣餘額

轉帳代幣及簽署

查看交易記錄

檢查合約漏洞安全性



圖片來源:網路抓取

# 系統架構規劃

## 前端應用 (React.js) :

用戶界面，允許用戶與代幣進行互動，如查看餘額、轉帳等。

## 後端服務 (Node.js/Express) :

處理業務邏輯、與智能合約交互、與資料庫通信。

## 資料庫 (MongoDB) :

存儲用戶數據、交易記錄等。

## 使用者錢包 (MetaMask) :

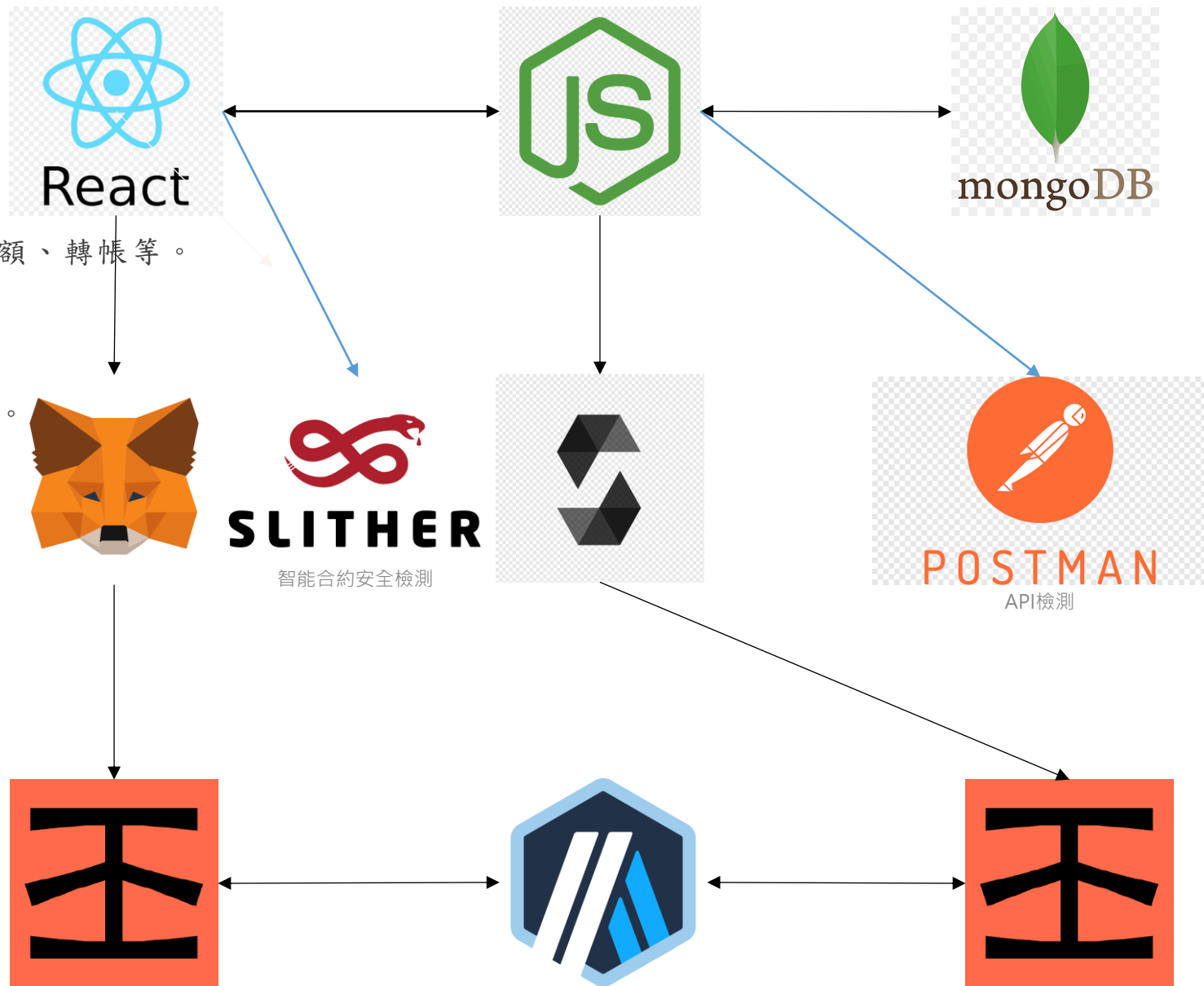
用戶的以太坊錢包，用於簽署交易和身份驗證。

## 以太坊區塊鏈 :

運行智能合約，管理代幣的發行和轉移。

## 區塊鏈節點服務 (Infura) :

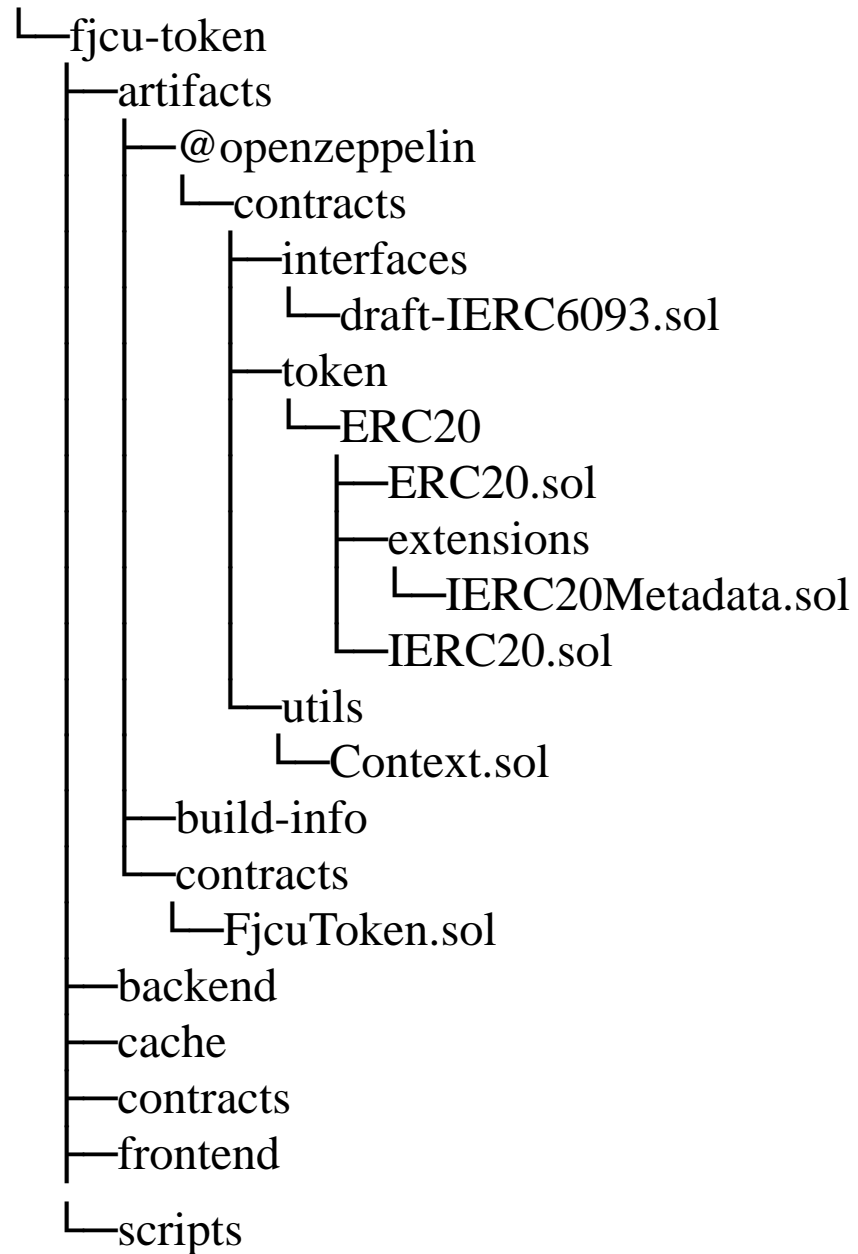
提供區塊鏈節點的訪問，避免自建節點的繁瑣。





# 目錄結構規劃

## BLOCKCHAIN



報告結束，感謝聆聽。

TSE,LIN LE

511172176@m365.fju.edu.com

[511172176 \(李則霖 LI, TSE-LIN\) · GitHub](#)

