

# CS5363 Blockchain Technologies and Applications: Hw7 - Report

## Smart Contract

Name: 陳紹雲

Student Id: 0853426

---

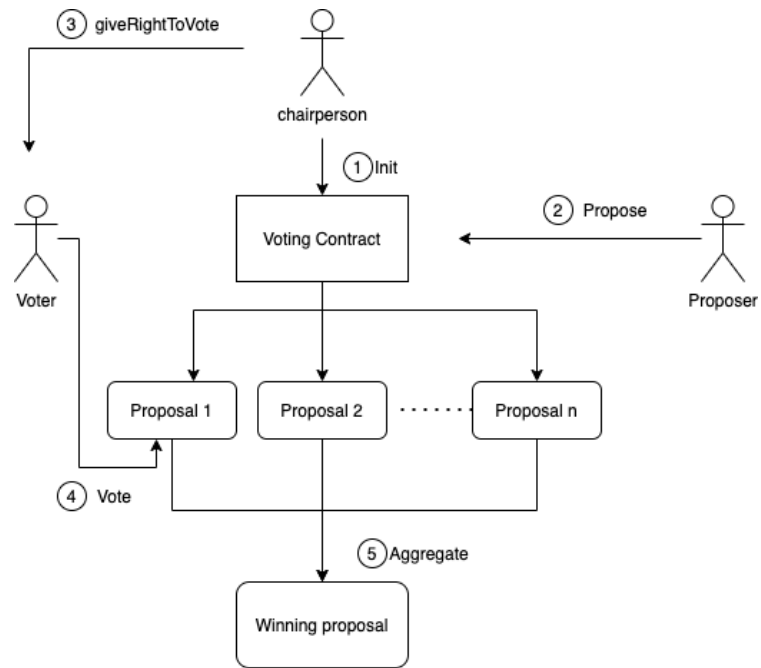
### Task 1: Voting in an Organization

#### Introduction

- 合約初始化一個投票合約，在開始時間之前允許使用者提案，期間內允許使用者投票，最終統計得到最高票的提案。

#### Design

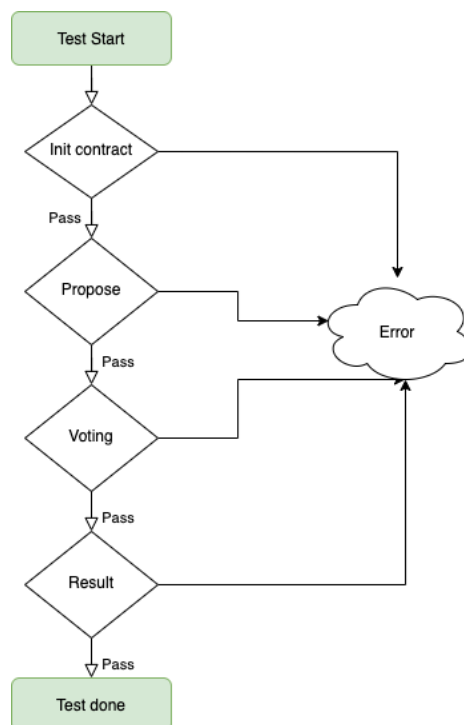
- Functional Description (Voting.sol)
  - 創立合約的人這邊定義成 chairperson
  - giveRightToVote: chairperson 可以給予使用者投票權重跟投票權。
  - extendVoting: , chairperson 可以延長投票時間。
  - createProposal: 允許使用者在投票期間前提案，定義提案名稱、提案內容、初始化投票以及紀錄提案者。
  - vote: 擁有投票權的使用者可以透過這個函數來投票，除了驗證時間在期限內之外，每個使用者只有一票，該函數會把投票者的投票狀態記錄在 struct 裡面。
  - winningProposal: 這個函數可以在投票結束後，從這個函數得到最終的結果。
- Design Diagram & Flow Chart (Explain the operation process in your contract)



1. Chairperson 初始化投票合約
2. 在投票期限前由使用者自行提案
3. 給予相關投票人投票權限
4. 投票人開始投票
5. 統計投票結果，並返回最高票提案

## Testing

- Testing Flow Chart (Explain how can you ensure your contract is correct)



- Test cases (Ensure your test cases provide enough testing coverage)

- 測試合約是否有成功初始化起始時間與結束時間
- 測試合約是否能夠提案
- 利用 timemachine 快轉時間到投票期間，投票者是否可以執行投票
- 利用 timemachine 將時間快轉到投票結束，確認可以返回投票結果

### Other Discussion

- 可能會有兩個最高票產生
- 上鏈時間差問題

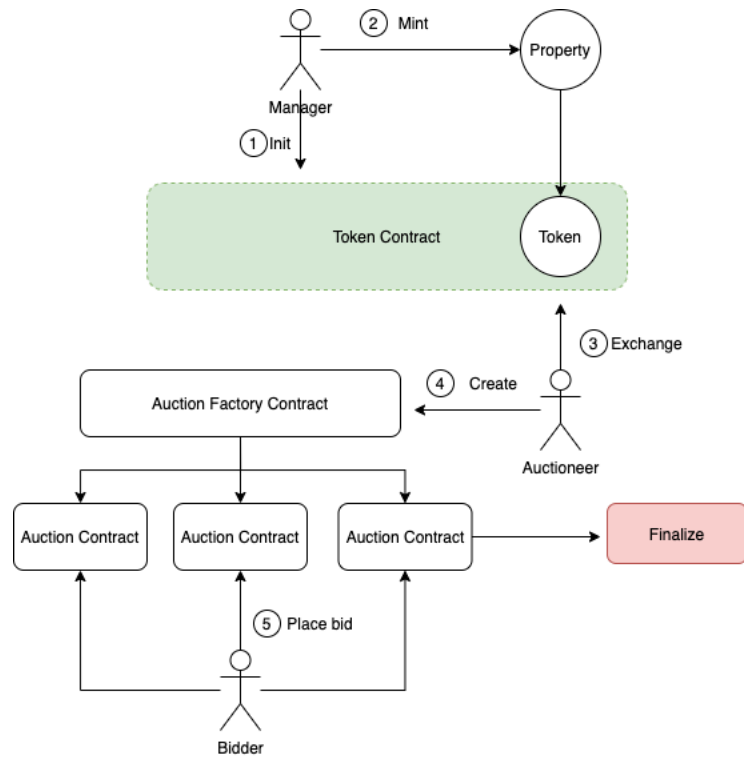
## Task 2: Token & Smart Property

### Introduction

- 代幣合約，manager 可以初始代幣合約、以及 mint token，mint 後的代幣被放在代幣合約中，其他使用者可以透過 exchange 函數來獲得代幣，並且允許使用者間可以轉移代幣。
- 拍賣合約，使用者可以透過 factory 合約來開啟拍賣，使用者先定義拍賣期限以及代幣，並且將代幣轉移到子合約中，子合約允許使用者來競標，最終價高者獲得代幣。

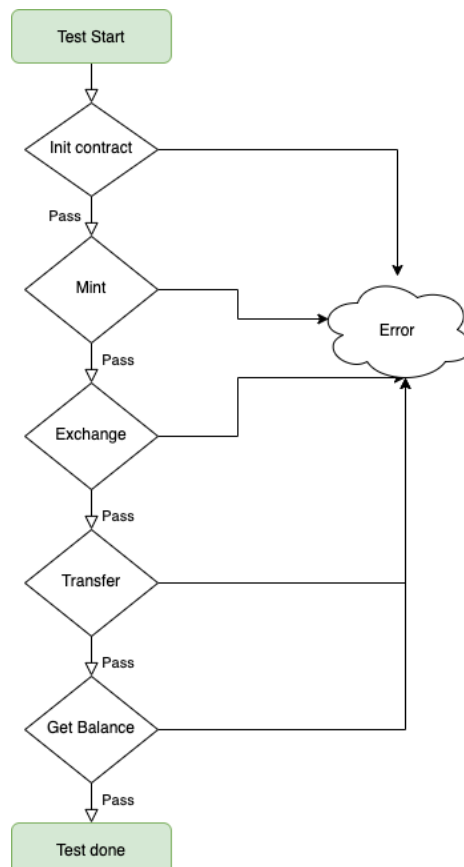
### Design

- Functional Description (Token.sol)
  - mint: 允許 manager 鑄造代幣在代幣合約中
  - transferFrom: 使用者可以透過函數轉移代幣
  - approve: 事先允許他方能夠移轉代幣
  - exchange: 使用者可以跟代幣合約用以太幣交換代幣
- Functional Description (AuctionFactory.sol)
  - createAuction: 使用者可以透過這個函數建立代幣競標
  - allAuctions: 得到所有競標的子合約位址
- Functional Description (Auction.sol)
  - getHighestBid: 得到當前最高的競標金額
  - placeBid: 使用者透過該函數來參與競標
  - finalize: 使用者透過該函數，若得標則獲得代幣，沒得標則取回以太幣
- Design Diagram & Flow Chart (Explain the operation process in your contract)



## Testing

- Testing Flow Chart (Explain how can you ensure your contract is correct)



- Test cases (Ensure your test cases provide enough testing coverage)
  - 測試 Manager 能夠透過代幣合約來 mint 代幣
  - 測試使用者可以透過 Exchange 函數使用以太幣跟代幣合約交換代幣
  - 測試使用者之間可以交換代幣
  - 測試使用者可以透過 balanceOf 來獲得使用者代幣數量

### Other Discussion

- Any notable design concern you find...