**CS5363 Blockchain Technologies and Applications: Hw8 – Report**

**Decentralized App (DApp)**

Name: 王念祖

Student Id: 112164507

**Task: A Social Recovery Wallet DApp on Web3**

**Ｉ、Background Introduction**

在過往的紙幣時代，人們往往隨身攜帶一個小錢包，裡頭會存放自身的一小部份財產，用於出外交易使用，另外一大部份財產通常不會隨身帶著，而是存放於銀行之中，將錢財託管於一個信任的第三方機構，不過，在Web3數位世界中，沒有所謂的信任第三方，每個人可以生成一個EOA帳戶，用戶必須保管該帳戶所對應的私密金鑰，這把金鑰的權限可以花費其EOA帳戶中的所有金錢，因此私鑰的管理變得極度重要，一種安全的保管方式，常用帶有安全加密芯片的設備來儲存此私密金鑰，不過若設備損壞，隨之保存於其中的私鑰也會遺失，導致用戶失去所有資產。

為了解決以上問題，有一派的研究是討論如何安全備份與還原私鑰，而另一個派研究，則是此次選擇實作的方法，使用情境可以想像成上述的錢包與銀行保險庫的例子，每個人都有一個錢包(EOA帳戶)以及銀行保險庫(Smart Contract Wallet)，人們大多數的資產都存放在自己鏈上的保險庫之中，等自己手上的錢包金錢不足時，才去保險庫提領部份金錢來做使用，另外我們覺得錢包錢太多時，也可以對保險庫匯入金額進行儲蓄，這個保險庫的錢只能有事先設定好的EOA錢包才可以提領，不過，當我們此時的EOA錢包遺失時，恢復的方案就如同現實世界我們遺失錢包中的金錢一樣，但我們儲存在銀行中的錢還是我們的，此時我們只要發起保險庫事先設定好的監護人機制，這群監護人會為我們進行社交驗證，確認是我本人後，並且我可以提供我新錢包的地址，請監護人設定我的保險庫，改成使用我提供的新錢包來做提領，只要達到預期數量的監護人覆議，就可以重先設定我們保險庫能有哪一個EOA錢包做新的提款帳戶。

這種恢復方式，稱作Social recovery wallet，簡單來說它也是部署一個智能合約，作為可靠且可驗證的保險金庫管理，配合social authentication 中的監護人(guardian)角色來為金鑰遺失場景，做一個帳戶復原的機制。

**II、Features of Smart Contracts**

**一張含有 文字, 螢幕擷取畫面, 字型, 行 的圖片

自動產生的描述**

**2-1重要屬性 Important attributes**

**1. address public owner;** //此保險庫的帳戶擁有者(EOA address)

**2. uint public totalDepositAmount;** //此保險庫的總金額（wei 單位）

**3. uint public threshold;** //閾值，要多少 guardian 數量同意

**4. bool public isRecovering;** // 現在是否是在“帳戶恢復”階段

**5. uint public currRecoveryRound;** // 現在已經是第幾次的恢復

**6. address[] public guardians;** //儲存現在的所有監護人

**2-2 重要方法Important functions**

**1. constructor(uint \_threshold, address[] memory \_initialGuardians)**

部署階段，需設定閾值，以及所有監護人的地址，這裡就會固定好 n of m ，譬如n=5個監護人與m=2個同意會成功，n of m 之後就不能在更改，帳戶擁有者之後只能更換監護人地址，並不能更改監護人數量與閾值的比例

**2. function depositMoney() external payable onlyOwner**

存款功能（不能在恢復期間呼叫）

**3. function withdrawMoney(uint withdrawValue) external payable onlyOwner**

提款功能（不能在恢復期間呼叫）

**4. function removeGuardian(address removingGuardian) external onlyOwner**

帳戶擁有人可以移除（替換）監護人，不過因安全性需要等待一段時間（譬如3天），原因是避免惡意人士拿到帳戶擁有人的私鑰後，透過快速替換成對自己有利的監護人以轉移保險箱的帳戶擁有人

**5. function executeGuardianRemoval(address removingGuardian, address newGuardian) external onlyOwner**

等待移除監護人的時間到了，就可以立即刪除他，並需要在輸入一個新的監護人地址以替換移除者的位置，保持監護人數量的一致

**6. function cancelGuardianRemoval(address removingGuardian) onlyOwner external**

帳戶擁有者可以取消對監護人的移除操作

**7. function transferGuardian(address newGuardian) external onlyGuardian**

監護人可以將自己的監護人權利轉交給別人

**8. function initiateRecovery(address \_newOwnerAddr) onlyGuardian external**

任何一個監護人皆可以啟動此保險庫的恢復流程，發起此恢復流程的監護人，需指定希望將此保險庫權限交給哪一個的新帳戶擁有人地址

**9. function supportRecovery(address \_newOwnerAddr) onlyGuardian onlyInRecovery external**

任何一個監護人發現保險庫的恢復流程開始後，就可以覆議恢復流程，一樣需指定希望將此保險庫權限交給哪一個的新帳戶擁有人地址

**10. function cancelRecovery() onlyOwner onlyInRecovery external**

帳戶擁有人可以取消恢復流程，避免監護人共謀串通轉移帳戶到非帳戶擁有者想指定的新帳戶地址。

**11. function executeRecovery(address newOwner, address[] calldata guardianList) onlyGuardian onlyInRecovery external**

任何一個監護人可以提交所有覆議的監護人地址，並讓合約檢查是否符合閾值數量的監護人同意，之後就將保險庫權限改為指定的新帳戶地址。

2-2 Flow chart

一張含有 文字, 螢幕擷取畫面, 行, 圖表 的圖片

自動產生的描述

**III、How to use our Dapp?**

**3-1 Test and deploy our smart contract**

啟動 Ganache，選QUICKSTART

一張含有 文字, 螢幕擷取畫面 的圖片

自動產生的描述

測試合約的正確性

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

測試結果如下，確認沒有問題

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

部署合約

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

**3-2 configure and activate Dapp**

找到 social-recovery-dapp/social-recovery-dapp /contract/build/contracts/SocialRecoveryWallet.json，並獲取兩個值 “address” 跟 “abi” ，並且只需要複製其值

一張含有 文字, 軟體, 多媒體軟體, 螢幕擷取畫面 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 多媒體軟體 的圖片

自動產生的描述

把以上這兩個值，貼到social-recovery-dapp/social-recovery-dapp/src/pages/abi/SocialRecoveryConfig.js

一張含有 文字, 螢幕擷取畫面, 軟體, 多媒體軟體 的圖片

自動產生的描述

在此social-recovery-dapp/social-recovery-dapp/ 路徑下，啟動 Dapp

($ npm start)

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

連線到 <http://localhost:3000/>，應該類似長這樣，但右上的帳戶文字可能顯示不同文字或是沒有任何文字，其文字表示目前與Dapp連線的帳戶地址

一張含有 文字, 螢幕擷取畫面, 軟體, 作業系統 的圖片

自動產生的描述

先敘述一下，現在的情況，因爲預設在 Smart Contract 在部署階段時，預設threshold = 2, initialGuardians = Ganache 的前三個合約地址

一張含有 文字, 螢幕擷取畫面, 數字, 字型 的圖片

自動產生的描述

接下來，先用 MetaMask 創建以上的一些帳戶，作為等一下使用場景的測試，譬如account[0] (帳戶擁有人＋監護人), account[1] (監護人), account[3] (欲轉移的新帳戶擁有人)

MetaMask 匯入方式大同小異，這邊示範 account[0] 的方法  
1一張含有 文字, 螢幕擷取畫面, 多媒體, 字型 的圖片

自動產生的描述2一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片

自動產生的描述3一張含有 文字, 電子產品, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

4一張含有 文字, 數字, 字型, 螢幕擷取畫面 的圖片

自動產生的描述

5一張含有 文字, 字型, 網站, 網頁 的圖片

自動產生的描述6一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片

自動產生的描述

7一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片

自動產生的描述8一張含有 文字, 螢幕擷取畫面, 多媒體, 行動裝置 的圖片

自動產生的描述

9一張含有 文字, 螢幕擷取畫面, 軟體, 數字 的圖片

自動產生的描述10一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片

自動產生的描述

設定好後，將帳戶連線 Dapp ，可以重新整理Dapp網頁頁面

一張含有 文字, 螢幕擷取畫面, 字型, 軟體 的圖片

自動產生的描述一張含有 文字, 螢幕擷取畫面, 字型, 軟體 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面 的圖片

自動產生的描述

可以發現右上角的帳戶地址已經改為設定好的 ganache 的 account[0] 地址了，而其他的 account[1], account[3]也是同樣步驟新增至MetaMask，只是之前設置的 localhost 網路可以沿用不需重新設定。

一張含有 文字, 螢幕擷取畫面, 字型, 軟體 的圖片

自動產生的描述一張含有 文字, 螢幕擷取畫面, 多媒體, 小工具 的圖片

自動產生的描述

第一次連入Dapp 都需要確認連線，記得即使連線，Dapp 還是要重新整理讓右上角帳戶文字確保為對應要連線帳戶

接下來我們用Account2 (帳戶擁有人登入)

一張含有 文字, 軟體, 網頁, 作業系統 的圖片

自動產生的描述

回到Dapp頁面，首先介紹左上角的「logo」跟「首頁」點下去後，都是導向此Welcome to Social Recovery Wallet 字樣的主頁面

**3-3 Deposit and Withdraw**

接下來點擊右邊數過來第三個「帳戶金額」，若使用帳戶擁有人登入Dapp，則會顯示“存錢”和“領錢”按鈕可以操作

一張含有 文字, 軟體, 網頁, 作業系統 的圖片

自動產生的描述

但如果是用非帳戶擁有人登入Dapp，則無此兩個按鈕，但一樣看得到帳戶擁有人地址以及保險庫總金額，如下圖

一張含有 文字, 軟體, 網頁, 字型 的圖片

自動產生的描述

點擊「存錢」按鈕，輸入存款金額，按下確認

一張含有 文字, 軟體, 螢幕擷取畫面, 網頁 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述此時MetaMask會跳出交易確認

一張含有 文字, 螢幕擷取畫面, 軟體, 作業系統 的圖片

自動產生的描述

確定8000 wei 已經存入保險庫

點擊「領錢」按鈕，輸入提款金額

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述一張含有 文字, 螢幕擷取畫面, 軟體, 電腦圖示 的圖片

自動產生的描述一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

確定提出 2000 wei ，保險庫已經扣除剩 6000 wei

一張含有 文字, 軟體, 螢幕擷取畫面, 網頁 的圖片

自動產生的描述

如果要領出超過金庫總金額是無法的，會被擋下來。

**3-4 Guardian management**

接著來介紹右上Navbar的倒數第二個「監護人管理」功能點下去

同樣若用帳戶擁有者＋監護人權限登入，以下畫面介紹權限顯示：

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

假設我們試著刪除表格中第三個監護人，按下對應其位置的刪除鍵

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 電腦圖示 的圖片

自動產生的描述Metamask一樣需要您按下交易確認一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

可以看到現在第三個監護人變成等待刪除中，因為我們為了測試，在部署合約中，我們只需等到區塊鏈時間 10 秒即可變為刪除，但因為是測試鏈只有我們會挖新區塊更新時間，因此我們需做一個其他交易動作已更新最新區塊時間。我們可以在刪除第二個監護人，等一下可以測試我們「取消」功能

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

可以看到第三個監護人已經可以立即刪除了，我們就執行第三個監護人的「立即刪除」，不過刪除前，他需要我們新增新的監護人地址，我們就從 ganache 中挑選account[4]

一張含有 文字, 軟體, 螢幕擷取畫面, 網頁 的圖片

自動產生的描述

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 電腦圖示 的圖片

自動產生的描述 Metamask一樣需要您按下交易確認

可以看到第三個監護人已經換成新的帳戶地址擔任，我們剛剛加入刪除排程中的第二個監護人地址，也因等待時間到了，因此變成可以立即刪除，但這次我們要測試「取消」功能

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 字型 的圖片

自動產生的描述 Metamask一樣需要您按下交易確認

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

可以看到第二個監護人又恢復到任期狀態

3.5 Account Recovery

接著來介紹右上Navbar的最後一個「帳戶復原」功能點下去

同樣若用帳戶擁有者＋監護人權限登入，以下畫面介紹權限顯示

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

先使用 account[1] (僅監護人身份) 與Dapp連線

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

接下來發起交易，並且我們先隨意指定一個account[7] 來表示自己想將金庫權限隨意轉移給他人。

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 字型 的圖片

自動產生的描述 Metamask一樣需要您按下交易確認

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

此時我們可以發現帳戶已經進入第一次的恢復流程，並且帳戶狀態是恢復中，上方的按鈕也變成可以覆議跟總結，並且下方的表格也紀錄著account[1]是希望將新 owner跟account[7]，接著我們先回到 account[0](就是擁有帳戶擁有者＋監護人權限)的帳戶，將其重新連線Dapp。

一張含有 文字, 軟體, 網頁, 作業系統 的圖片

自動產生的描述

此時可以發現帳戶在恢復狀態下，存錢與領錢的按鈕都不再顯示，此時account[0] 的帳戶復原頁面比一般監護人多一個按鈕，也就是取消恢復流程，因為account[0] 發現自己沒有委託恢復，但account[1]卻偷啟動恢復流程想轉移，幸好 account[0] 即使發現並按下「取消恢復流程」

一張含有 文字, 軟體, 螢幕擷取畫面, 網頁 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 字型 的圖片

自動產生的描述 Metamask一樣需要您按下交易確認

一張含有 文字, 軟體, 網頁, 螢幕擷取畫面 的圖片

自動產生的描述

帳戶狀態又復原回正常狀態

接下來我們來走一次復原成功流程，假設今天account[0]遺失私鑰，無法在發起交易，他快速聯絡 account[1]監護人，希望他發起恢復流程，並交給他希望轉移的新帳戶(account[3])，因此我們用account[1] 登入連線Dapp，並發起第二次的恢復流程，並輸入account[0]交代的account[3]作為新帳戶擁有人

一張含有 文字, 軟體, 螢幕擷取畫面, 網頁 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 作業系統 的圖片

自動產生的描述 Metamask一樣需要您按下交易確認

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

可以看到第二次的恢復流程啟動，並且account[1]此次選account[3]作為newOwner，不過要真正成功復原當初設定需要兩個數量監護人贊同，因此account[0]需聯絡第三個監護人account[4]，account[4]對account[0]的本人進行社交認證成功後，同意為其執行帳戶復原操作，因此我們登入account[4] 連線Dapp，複製account[1]提出的地址，點選“覆議恢復請求”，貼上後送出。

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 字型 的圖片

自動產生的描述 Metamask一樣需要您按下交易確認

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

並且看到已有兩個監護人支持同一個新帳戶擁有人地址後，就可以按下“總結提交“按鈕，並再次輸入新帳戶擁有人地址以及覆議的兩位監護人地址

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 軟體, 字型 的圖片

自動產生的描述 Metamask一樣需要您按下交易確認

一張含有 文字, 軟體, 網頁, 網站 的圖片

自動產生的描述

一張含有 文字, 軟體, 網頁, 作業系統 的圖片

自動產生的描述

到帳戶管理頁面，可以發現帳戶擁有人已經被成功轉移給新帳戶account[3]！

**IV、Other Discussion**

其他安全性問題：

**V、References**