

NCCU

以太坊原理與應用開發

Assignment2

Sample code:

<https://drive.google.com/drive/folders/1QvZBZXy6lcJgGmB4TSwYLP31Xmbas37R>

Due date: 12:00, Nov. 28, 2018

作業內容

- ▶ 完成Bank.sol智能合約
- ▶ 使用solc編譯智能合約
- ▶ 使用web3部署智能合約
- ▶ 透過web3使用合約function

Bank.sol

- ▶ 請將Bank.sol中未完成的function完成
 - ▶ mint
 - ▶ buy
 - ▶ transferCoin
 - ▶ transferOwner

```
// mint coin
function mint(uint256 coinValue) public isOwner {

    uint256 value = coinValue * 1 ether;

    // 增加 msg.sender 的 coinBalance
    // your code

    // emit MintEvent
    // your code

}
```

Bank.sol

```
// 使用 bank 中的 ether 向 owner 購買 coin
function buy(uint256 coinValue) public {
    uint256 value = coinValue * 1 ether;

    // require owner 的 coinBalance 不小於 value
    // your code

    // require msg.sender 的 etherBalance 不小於 value
    // your code

    // msg.sender 的 etherBalance 減少 value
    // your code

    // owner 的 etherBalance 增加 value
    // your code

    // msg.sender 的 coinBalance 增加 value
    // your code

    // owner 的 coinBalance 減少 value
    // your code

    // emit BuyCoinEvent
    // your code
}
```

```
// 轉移 coin
function transferCoin(address to, uint256 coinValue) public {
    uint256 value = coinValue * 1 ether;

    // require msg.sender 的 coinBalance 不小於 value
    // your code

    // msg.sender 的 coinBalance 減少 value
    // your code

    // to 的 coinBalance 增加 value
    // your code

    // emit TransferCoinEvent
    // your code
}
```

```
// 轉移 owner
function transferOwner(address newOwner) public isOwner {

    // transfer ownership
    // your code

    // emit TransferOwnerEvent
    // your code
}
```

solc

- ▶ 使用npm下載solc

```
npm install -g solc
```

- ▶ 編譯Bank.sol

```
solcjs -o ./contract --bin --abi Bank.sol
```

```
└─ contract
```

```
  └─ Bank_sol_Bank.abi
```

```
  └─ Bank_sol_Bank.bin
```

web3.js部署智能合約

- ▶ 使用npm下載web3

```
npm install web3
```

- ▶ 如果無法安裝，請使用系統管理員的身分執行

```
npm install --global --production windows-build-tools
```

- ▶ 安裝完成windows-build-tools後，再嘗試下載web3

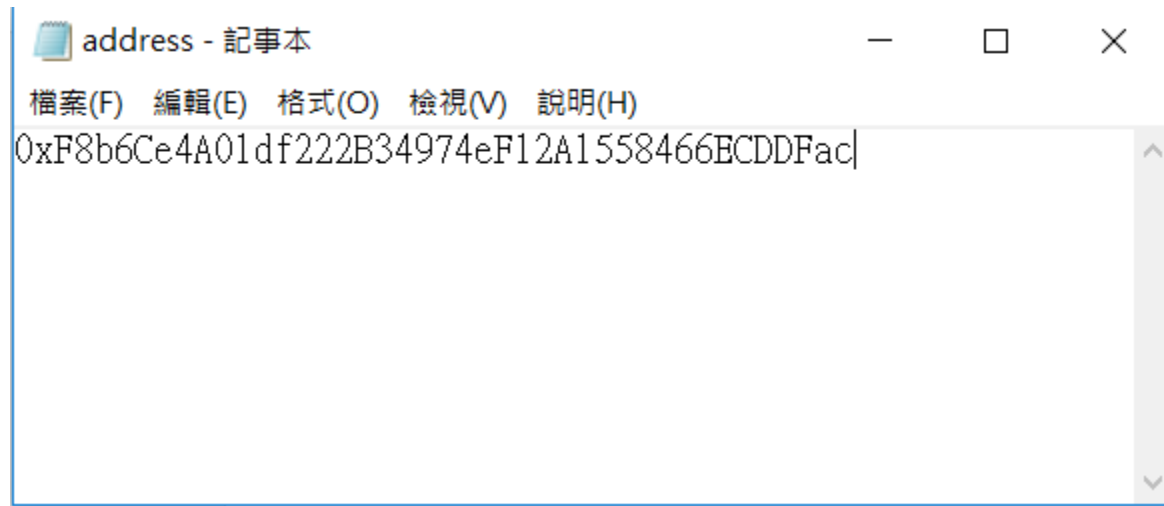
web3.js部署智能合約

- 完成deploy.js
node deploy.js

[illegible]

web3.js部署智能合約

- ▶ 部署成功後將合約address寫至address.txt
`fs.writeFileSync('./address.txt', contractAddress)`



web3.js使用合約function

- ▶ 完成exercise資料夾裡的：
 - ▶ mint.js
 - ▶ buy.js
 - ▶ transferCoin.js
 - ▶ transferOwner.js
 - ▶ coinBalance.js
 - ▶ owner.js
- ▶ 提供sample code：
 - ▶ deposit.js、withdraw.js、transfer.js、balance.js

web3.js使用合約function

- ▶ mint.js : accounts[0] mint $3 * 10^{18}$ coins

```
node mint.js
```

[illegible]

web3.js使用合約function

- ▶ buy.js : accounts[1] 向 accounts[0] 購買 $1 * 10^{18}$ coins

node buy.js

[illegible]

web3.js使用合約function

- `transferCoin.js` : transfer $1 * 10^{18}$ coins from `accounts[0]` to `accounts[1]`

```
node transferCoin.js
```

[illegible]

web3.js使用合約function

- ▶ transferOwner.js : accounts[0] transferOwner to accounts[1]

node transferOwner.js

[illegible]

web3.js使用合約function

- ▶ coinBalance.js : get accounts[0] coin balance in bank
node coinBalance.js

```
D:\Chiu\桌面\Assignment2>node coinBalance.js  
1000000000000000000000000
```

- ▶ owner.js : get contract owner
node owner.js

```
D:\Chiu\桌面\Assignment2>node owner.js  
0x15e40B72C280b6b7d64340BF2eFbeE20eb903a8D
```