NCCU
以太坊原理與應用開發

Assignment2

Sample code:
https://drive.google.com/drive/folders/1QvZBZXy6IcJgGmB4TSwYLp31Xmbas37R

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

}
```

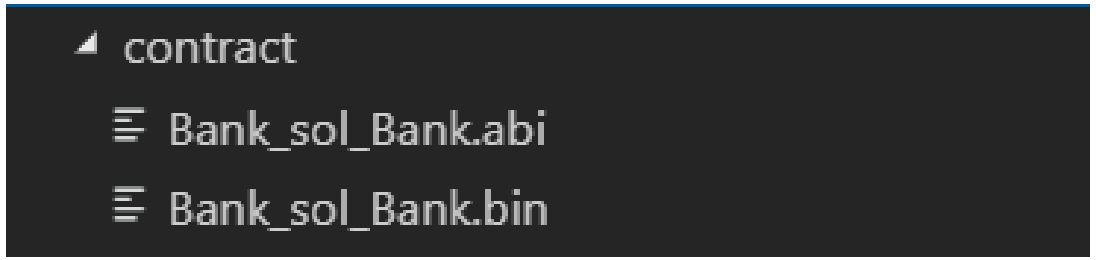
solc

- 使用npm下載solc

  npm install -g solc

- 編譯Bank.sol

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



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

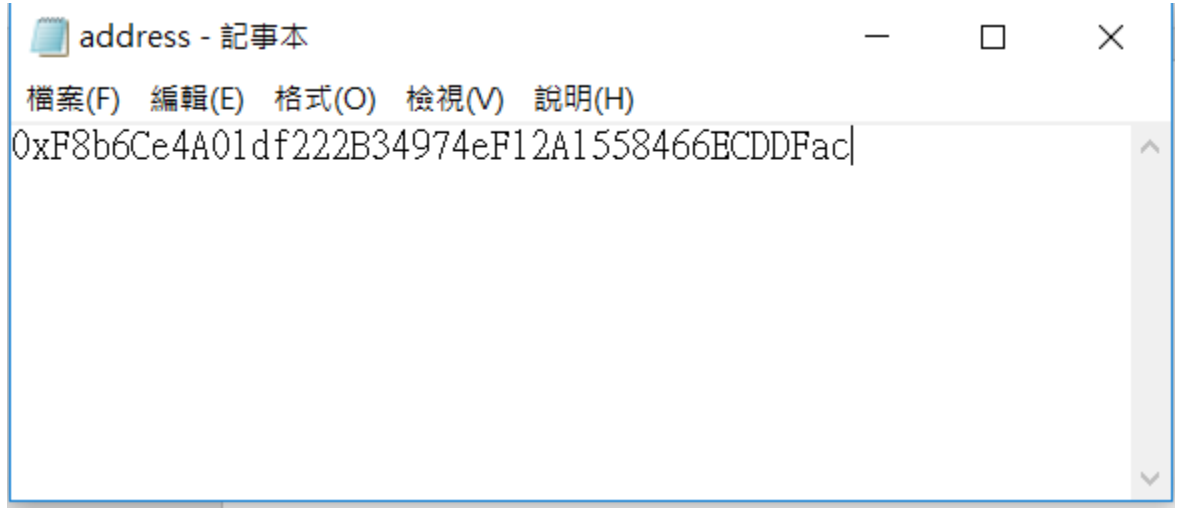
  node deploy.js

```
D:\Chiu\桌面\Assignment2>node deploy.js
{ transactionHash: '0xdd086bde6ab5310da498ce6069fd7f5853e9f17c12b26d2c1f0c6a032a997552',
  transactionIndex: 0,
  blockHash: '0xa643186eb99ef3c39f0051bb64371dc2dde193b96c63256ce2a812bd70102cc6',
  blockNumber: 4,
  gasUsed: 1900365,
  cumulativeGasUsed: 1900365,
  contractAddress: '0xF8b6Ce4A01df222B34974eF12A1558466ECDDFac',
  status: true,
  logsBloom: '0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000',
  events: {} }
```

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

```
D:\Chiu\桌面\Assignment2>node mint.js
{ transactionHash: '0x51354c9ff97a3cc2f6f16e5b38211547f75ce8418f088a20834efcf0c350bae4',
  transactionIndex: 0,
  blockHash: '0x1a796f7b6efc883dfd50b0df7babfb3c4d6754bf2d09c43de0a4d22860c3ec6e',
  blockNumber: 10,
  gasUsed: 44200,
  cumulativeGasUsed: 44200,
  contractAddress: null,
  status: true,
  logsBloom: '0x00000000000000000000000040000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0001000000000000000000000000000000000000000000000000000000000100000000000000000000000000000000000000000000000000002000000040000000000000000000
0000000000000000000040000000000000000000000000000000000000000000000000000000000000000000000000000000800000000000000000002000000000000000000
0000000000000000000000000000000000000000000000000040000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000',
  events:
   { MintEvent:
      { logIndex: 0,
        transactionIndex: 0,
        transactionHash: '0x51354c9ff97a3cc2f6f16e5b38211547f75ce8418f088a20834efcf0c350bae4',
        blockHash: '0x1a796f7b6efc883dfd50b0df7babfb3c4d6754bf2d09c43de0a4d22860c3ec6e',
        blockNumber: 10,
        address: '0xF8b6Ce4A01df222B34974eF12A1558466ECDDFac',
        type: 'mined',
        id: 'log_3c9308ba',
        returnValues: [Object],
        event: 'MintEvent',
        signature: '0x8069ef4945469d029cc32e222031bccdc99b2eaaf4ee374cd268012f7ddee907',
        raw: [Object] } } }
```

web3.js使用合約function

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

  node buy.js

```
D:\Chiu\桌面\Assignment2>node buy.js
{ transactionHash: '0xd286e8f4965e7fbf2b091efa6db706fb4d0a3307960adc3f4657a464700d00e0',
  transactionIndex: 0,
  blockHash: '0x27404a42baf872a92b411d8619ab74f29569e48a3f0b34f2677aab2e86e6d214',
  blockNumber: 11,
  gasUsed: 46331,
  cumulativeGasUsed: 46331,
  contractAddress: null,
  status: true,
  logsBloom: '0x00000000000000000000000800000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
04000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
10000000000000000000400000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000004000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000',
  events:
   { BuyCoinEvent:
      { logIndex: 0,
        transactionIndex: 0,
        transactionHash: '0xd286e8f4965e7fbf2b091efa6db706fb4d0a3307960adc3f4657a464700d00e0',
        blockHash: '0x27404a42baf872a92b411d8619ab74f29569e48a3f0b34f2677aab2e86e6d214',
        blockNumber: 11,
        address: '0xF8b6Ce4A01df222B34974eF12A1558466ECDDFac',
        type: 'mined',
        id: 'log_6b41fd04',
        returnValues: [Object],
        event: 'BuyCoinEvent',
        signature: '0x4c5ad1aea676c1e1613de5416105424342b84655de046903409dea58418bedff',
        raw: [Object] } } }
```

web3.js使用合約function

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

  node transferCoin.js

```
D:\Chiu\桌面\Assignment2>node transferCoin.js
{ transactionHash: '0xf0e1da669fb463207913368aa7145813f56705eefe4d537d111d9e48c133b8e8',
  transactionIndex: 0,
  blockHash: '0xe8a49b24a85f994a680b38fef8fc878935acd7e1c17ff23b4520b6b3d638eb20',
  blockNumber: 12,
  gasUsed: 51373,
  cumulativeGasUsed: 51373,
  contractAddress: null,
  status: true,
  logsBloom: '0x00000000000000000000000040000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000040000000000000000000000000000000000000000000000000000000000000000000000040000000000000000000
00000000000000000000400000000000000000000000000000000000000000000000000020000000000000000800000000000000000000020000000020000000000
00000000000000000000000000000000000000000000000040000000000000000000000000000000000000000000000000000000000000000800000000000000000000
00020002000000000000000000000000000000000000000',
  events:
   { TransferCoinEvent:
      { logIndex: 0,
        transactionIndex: 0,
        transactionHash: '0xf0e1da669fb463207913368aa7145813f56705eefe4d537d111d9e48c133b8e8',
        blockHash: '0xe8a49b24a85f994a680b38fef8fc878935acd7e1c17ff23b4520b6b3d638eb20',
        blockNumber: 12,
        address: '0xF8b6Ce4A01df222B34974eF12A1558466ECDDFac',
        type: 'mined',
        id: 'log_c48b1520',
        returnValues: [Object],
        event: 'TransferCoinEvent',
        signature: '0x941d755df54ad0234b406209d0c923107cabf6d4f1ce335b8ae5d89d6a28c2d2',
        raw: [Object] } } }
```

web3.js使用合約function

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

  node transferOwner.js

```
D:\Chiu\桌面\Assignment2>node transferOwner.js
{ transactionHash: '0x7f1d2b968871a524ebddbc5aa24881fa2d2aa17031ee21d3a2608f5a3b24f2ca',
  transactionIndex: 0,
  blockHash: '0xb082b76c4abad20482ba76527eafb47f1c9b75b5fc80bd7a18281374508dca07',
  blockNumber: 13,
  gasUsed: 30569,
  cumulativeGasUsed: 30569,
  contractAddress: null,
  status: true,
  logsBloom: '0x00000000000000000000000400000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
040000000000000000000000000000000000040000000000000000000000000000000000000000000000000000000000000000000000000000040000000000000000
100000000000000000040000000000000000000008000000000000000000000000000008000000000000000000020000000000000000
000000200000000000000000000000000000040000000000040000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000',
  events:
   { TransferOwnerEvent:
      { logIndex: 0,
        transactionIndex: 0,
        transactionHash: '0x7f1d2b968871a524ebddbc5aa24881fa2d2aa17031ee21d3a2608f5a3b24f2ca',
        blockHash: '0xb082b76c4abad20482ba76527eafb47f1c9b75b5fc80bd7a18281374508dca07',
        blockNumber: 13,
        address: '0xF8b6Ce4A01df222B34974eF12A1558466ECDDFac',
        type: 'mined',
        id: 'log_294f6b41',
        returnValues: [Object],
        event: 'TransferOwnerEvent',
        signature: '0x587a4fcff87b7be11c779eb502f8b2584f996387d8b8cda0e5113fef424f7316',
        raw: [Object] } } }
```

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
100000000000000000
```

- owner.js ： get contract owner

  node owner.js

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