

區塊鏈應用開發 Day 2

BLOCKCHAIN DAPP EXPERTS

<https://www.bde.tw/r/pgJ>

Office Hour

10/23 12:30~13:00

BLOCKCHAIN DAPP EXPERTS

<https://www.bde.tw/r/lam>

DApp 入門

(Decentralized Applications)

BLOCKCHAIN DAPP EXPERTS

DeFi

<https://www.bde.tw/r/ytp>

BLOCKCHAIN DAPP EXPERTS

Game

<https://www.bde.tw/r/VHI>

BLOCKCHAIN DAPP EXPERTS

以太坊手機錢包

- 手機錢包：Coinbase Wallet

<https://www.bde.tw/r/hfq>

創建新錢包

BLOCKCHAIN DAPP EXPERTS

coinbase | Wallet

The easiest and most secure crypto wallet



Create a new wallet

I already have a wallet



Legal

Please review the Coinbase Wallet Privacy Policy and Terms of Service.

Terms of Service



Privacy Policy



Accept





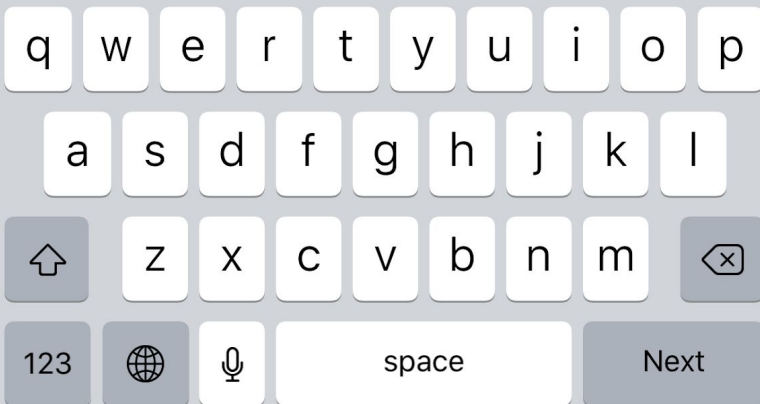
Pick your username

This is how other Wallet users can find you and send you payments.

@hschen2k



✓ Available



Set your privacy preferences

You can always change this later in settings

Public Recommended

Other Wallet users can search for my username and send me crypto



Private

Other Wallet users cannot search for my username



Crypto transactions take place on public blockchains. When your username is set to Public, advanced users can look up your addresses on the blockchain and view your transaction history.

Next

儲存助記碼

BLOCKCHAIN DAPP EXPERTS



Protect Your Wallet

Add an extra layer of security to keep your crypto safe.



Use Touch ID

Recommended



Set up Passcode



Back up your Wallet

You will be shown a secret recovery phrase on the next screen. The recovery phrase is the only key to your wallet. It will allow you to recover access to your wallet if your phone is lost or stolen.



I understand that if I lose my recovery phrase, I will not be able to access my account.

Back up now

Later



Recovery phrase

! Not backed up

1	2	3
4	5	6
7	8	9
10	11	12

These 12 words are the keys to your wallet. Back them up on the cloud or back them up manually. Do not share this with anyone.

Back up to iCloud

Back up manually



Manual backup

Write down recovery phrase

1	2	3
4	5	6
7	8	9
10	11	12

Copy to clipboard


Write these 12 words down, or copy them to a password manager.

Next


切換測試網路



PROFILE

 @bdetw

SECURITY

Recovery Phrase 

App Lock

CONNECTIONS

Default Network

Ropsten

WalletLink

0

[Connect to Coinbase](#)



Transfer coins from your Coinbase account to Coinbase Wallet

ADVANCED

Advanced Settings

Fantom Opera

Optimism

Polygon

xDai

ETH TESTNETS

Arbitrum Testnet

Avalanche Fuji

Fantom Testnet


Görli

Kovan

Optimism Kovan

Polygon Mumbai

Rinkeby

Ropsten 



BDE
BLOCKCHAIN DEVELOPERS



Active Network

ETH

Ethereum



Kovan

Rinkeby

Ropsten

Görli

Optimistic Ethereum

XRP

Mainnet



Testnet

XLM

Mainnet



Testnet



Active Network

ETH

Ethereum

Kovan

Rinkeby

Ropsten



Görli

Optimistic Ethereum

XRP

Mainnet



Testnet

XLM

Mainnet



Testnet



請求測試用以太幣



BOOKMARKS



Your bookmarks will show up here



MetaMask Ether Faucet

faucet

address: 0x81b7e08f65bdf5648606c89998a9cc8164397647

balance: 86921558.17 ether

request 1 ether from faucet

user

address: 0x511e19526d05f3998dc43b5b2ca2de3de4dd3023

balance: 0.00 ether

donate to faucet:

1 ether

10 ether

100 ether

transactions



- ETH 水龍頭: Ropsten Faucet

<https://faucet.ropsten.be/>

<https://faucet.metamask.io/>

<https://faucet.dimensions.network/>

Demo

BLOCKCHAIN DAPP EXPERTS

Day2 練習 1:

<https://app.compound.finance/>

1-1.到上方 DeFi 網站存入 ETH 產生利息後並截圖存檔

1-2.到下方 CrappyBird 遊戲中輸入自己的學號並取得一分以上的分數後完成上傳分數交易

<https://bdetw.github.io/CrappyBird/>

休息一下~~~
10:05繼續

DApp 開發

(Decentralized Applications)

BLOCKCHAIN DAPP EXPERTS

Ethereum

應用層

DApp

以太坊
衍生應用

合約層

智能合約

EVM

協議層

HTTP

RPC

Whisper

共識層

PoW
(Proof Of Work)

網路層

P2P
網路

數據層

區塊

區塊
"鏈"

交易
交易池

Merkle
樹

非對稱
加密

Event
事件

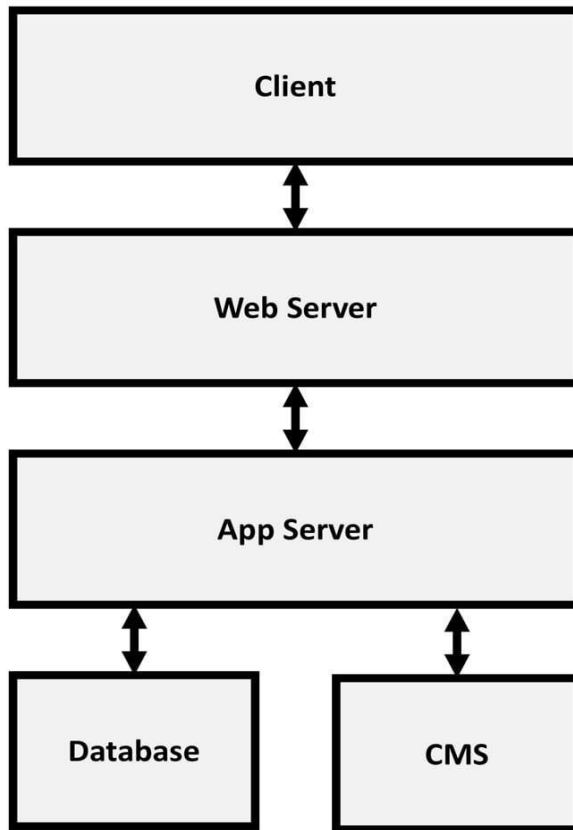
儲存層

日誌

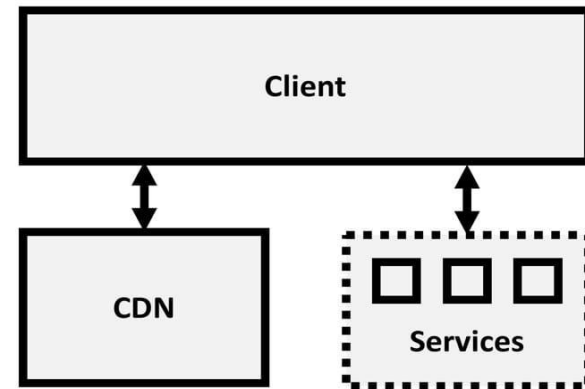
LevelDB

Web3 & JAMStack

Traditional Web



JAMstack



智能合約

- 以太坊上的應用程式
- 程式碼與資料的集合
- 經典應用: ICO / ERC-20
- DAPP: 加密貓 / ERC-721
- DeFi、NFT

智能合約

- **執行環境**: EVM (Ethereum Virtual Machine)
- Solidity -> EVM
- Java -> JVM

智能合約

- 程式語言 : Solidity
- Solidity 語法類似 JavaScript

// [SPDX-License-Identifier](#): MIT

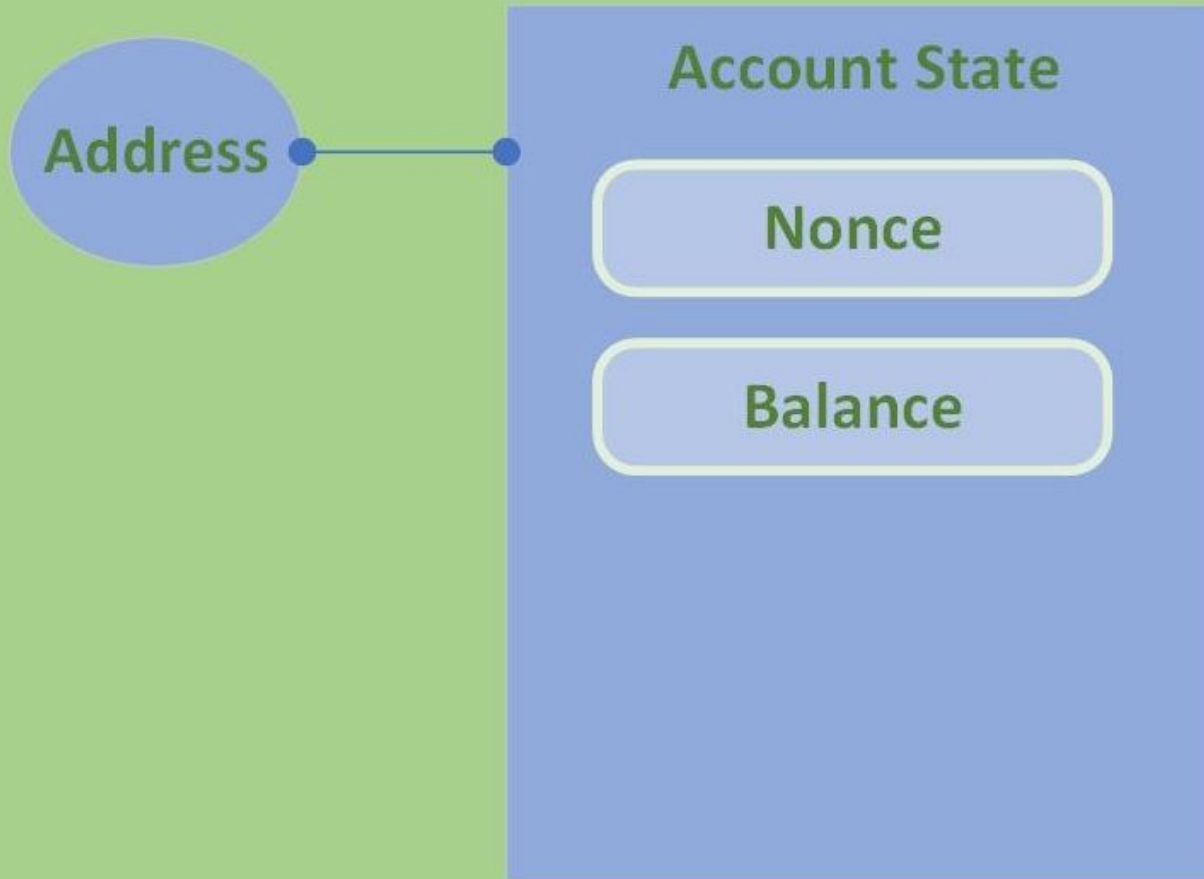
```
pragma solidity ^0.8.0;
```

```
contract HelloWorld {  
    function hello() public pure returns(string memory) {  
        return "Hello World!";  
    }  
}
```

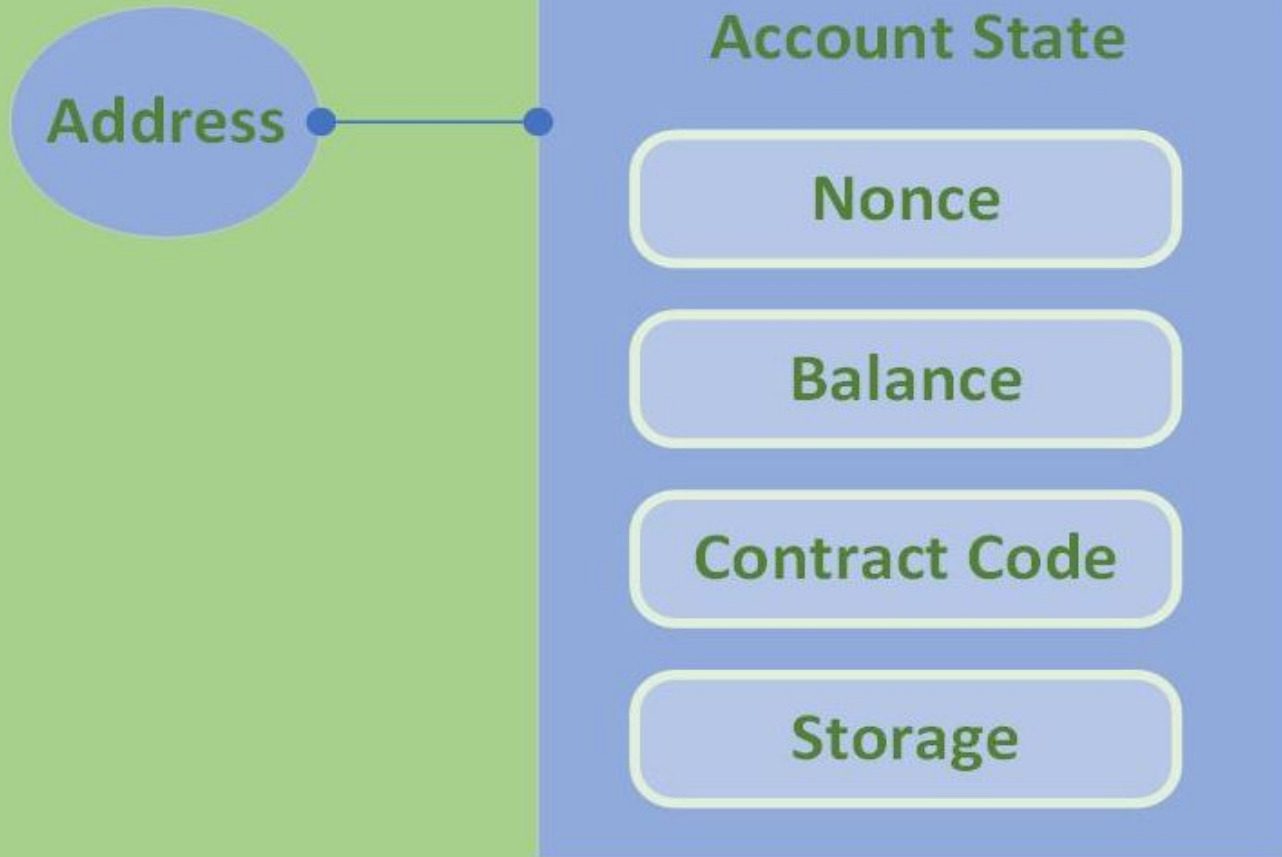
帳戶類型

- 外部帳戶: EOA (Externally Owned Account)
- 合約帳戶: Contract Account

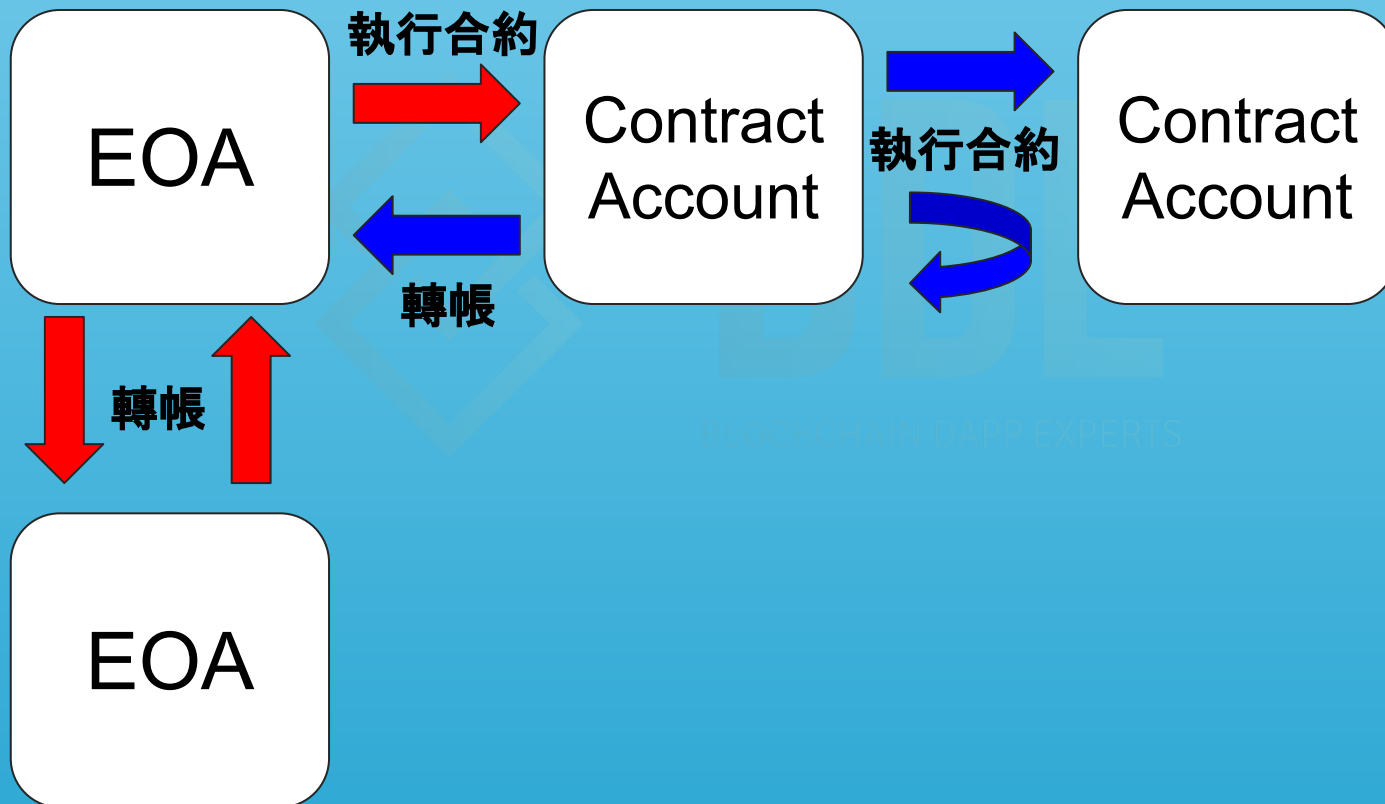
Externally Owned Account(EOA)



Contract Account (CA)



帳戶功能



智能合約開發

- 開發工具 : GitHub, Remix
- GitHub - <https://www.bde.tw/r/vnI>
- Remix - <https://www.bde.tw/r/1wN>

BLOCKCHAIN DAPP EXPERTS

註冊 GitHub

BLOCKCHAIN DAPP EXPERTS



[Why GitHub?](#) ▾ [Team](#) [Enterprise](#) [Explore](#) ▾ [Marketplace](#) [Pricing](#) ▾

Where the world builds software

Millions of developers and companies build, ship, and maintain their software on GitHub—the largest and most advanced development platform in the world.

[Sign up for GitHub](#)



Welcome to GitHub!
Let's begin the adventure

Enter your email

✓ jasonchen.sti@gmail.com

Create a password

→|



Continue



Password is strong

Make sure it's at least 15 characters OR at least 8 characters including a number and a lowercase letter.

You're almost done!

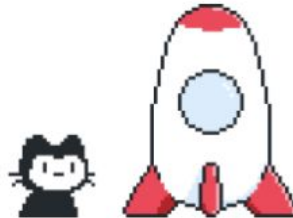
We sent a launch code to `jasonchen.sti@gmail.com`

→ Enter code

Didn't get your email? [Resend the code](#) or [update your email address](#).



Here's your GitHub launch code, @jasonchen-sti!



Continue signing up for GitHub by entering the code below:

148360

Open GitHub

[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)

Create your first project

Ready to start building? Create a repository for a new idea or bring over an existing repository to keep contributing to it.

[Create repository](#)[Import repository](#)

Recent activity

When you take actions across GitHub, we'll provide links to that activity here.

Learn Git and GitHub without any code!



Using the Hello World guide, you'll create a repository, start a branch, write comments, and open a pull request.

[Read the guide](#)[Start a project](#)

🚩 Universe schedule is now live



Join us virtually on Oct. 27 and 28 (PDT). Check out sessions across Security, DevOps, Developer Productivity, and Communities. Register to start building your customized Universe schedule.

[Save your seat for free](#)

All activity

Introduce yourself

The easiest way to introduce yourself on GitHub is by creating a README in a repository about you! You can start here:

jasonchen-sti/README.md

```
1 - 🙋 Hi, I'm @jasonchen-sti
2 - 👀 I'm interested in ...
3 - 🌱 I'm currently learning ...
4 - 💖 I'm looking to collaborate on ...
5 - 📫 How to reach me ...
6
```

申請 API Key

BLOCKCHAIN DAPP EXPERTS

<https://www.bde.tw/r/viA>

[Settings](#) / Developer settings

GitHub Apps

OAuth Apps

Personal access tokens

Personal access tokens

[Generate new token](#)

Need an API token for scripts or testing? [Generate a personal access token](#) for quick access to the [GitHub API](#).

Personal access tokens function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to [authenticate to the API over Basic Authentication](#).

GitHub Apps

OAuth Apps

Personal access tokens

New personal access token

Personal access tokens function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to [authenticate to the API over Basic Authentication](#).

Note

Remix

What's this token for?

Expiration *

30 days



The token will expire on Sun, Nov 21 2021

Select scopes

Scopes define the access for personal tokens. [Read more about OAuth scopes](#).




- | | |
|--|--------------------------------------|
| <input type="checkbox"/> repo | Full control of private repositories |
| <input type="checkbox"/> repo:status | Access commit status |
| <input type="checkbox"/> repo_deployment | Access deployment status |
| <input type="checkbox"/> public_repo | Access public repositories |
| <input type="checkbox"/> repo:invite | Access repository invitations |
| <input type="checkbox"/> security_events | Read and write security events |

<input type="checkbox"/> admin:repo_hook	Full control of repository hooks
<input type="checkbox"/> write:repo_hook	Write repository hooks
<input type="checkbox"/> read:repo_hook	Read repository hooks
<input type="checkbox"/> admin:org_hook	Full control of organization hooks
<input checked="" type="checkbox"/> gist	Create gists
<input type="checkbox"/> notifications	Access notifications
<input type="checkbox"/> user	Update ALL user data
<input type="checkbox"/> read:user	Read ALL user profile data
<input type="checkbox"/> user:email	Access user email addresses (read-only)
<input type="checkbox"/> user:follow	Follow and unfollow users
<input type="checkbox"/> delete_repo	Delete repositories
<input type="checkbox"/> write:discussion	Read and write team discussions
<input type="checkbox"/> read:discussion	Read team discussions
<input type="checkbox"/> admin:enterprise	Full control of enterprises
<input type="checkbox"/> manage_runners:enterprise	Manage enterprise runners and runner-groups
<input type="checkbox"/> manage_billing:enterprise	Read and write enterprise billing data
<input type="checkbox"/> read:enterprise	Read enterprise profile data





Remix 入門

BLOCKCHAIN DAPP EXPERTS

FILE EXPLORERS

Workspaces   

default_workspace

contracts


scripts

tests

README.txt

Home

1 tabs



Quicklinks

[Guide for migrating the old File System](#)

Migration tools:

- [Basic migration](#)
- [Download all Files](#) as a backup zip
- [Restore files](#) from backup zip


Help:

[Gitter channel](#)

[Report on Github](#)

0

☐ listen on network



Search with transaction hash ...

```
\`remix.exeCurrent()\` in the command line interface
- Right click on a JavaScript file in the file explorer and then click \`Run\`
```

The following libraries are accessible:

- [web3 version 1.5.2](#)
- [ethers.js](#)
- remix (run remix.help() for more info)

SOLIDITY COMPILER

COMPILER 

0.8.7+commit.e28d00a7

☐ Include nightly builds

LANGUAGE

Solidity

EVM VERSION

compiler default

COMPILER CONFIGURATION

☒ Auto compile

☐ Enable optimization

200

☐ Hide warnings

 Compile <no file selected>

DEPLOY & RUN TRANSA...

ENVIRONMENT

JavaScript VM (London)

ACCOUNT 

0x5B3...eddC4 (100)

GAS LIMIT

3000000

VALUE

0

wei

CONTRACT

NO COMPILED CONTRACTS

OR

At Address

Load contract from Address



SETTINGS



Github Access Token

Manage the access token used to publish to Gist and retrieve Github contents.

Go to github token page (link below) to create a new token and save it in Remix. Make sure this token has only 'create gist' permission.

<https://github.com/settings/tokens>

TOKEN:



Save

Remove



Themes



Dark (dark)



Light (light)

BDE

BLOCKCHAIN DAPP EXPERTS

Demo

BLOCKCHAIN DAPP EXPERTS

Day2 練習 2:

<https://github.com/>

- 2-1.註冊 GitHub 網站帳號並申請 API Key
- 2-2.到 Remix 網站中編譯部署 HelloWorld.sol, 並測試執行後截圖存檔
- 2-3. 將智能合約上傳到 IPFS 並記下 IPFS 的 Hash 值
- 2-4. 將智能合約上傳到 Gist 並記下 Gist 的網址

<https://remix.ethereum.org>

HelloWorld.sol

```
// SPDX-License-Identifier: MIT
```

```
pragma solidity ^0.8.0;
```

```
contract HelloWorld {
```

```
    function hello() public pure returns(string memory) {
```

```
        return "Hello World!";
```

```
    }
```

```
}
```

休息一下~
11:10繼續

Solidity 入門

BLOCKCHAIN DAPP EXPERTS

單位

- 1 ether = 1,000 finney
- 1 finney = 1,000 szabo
- 1 szaboo = 1,000 gwei
- 1 gwei = 1,000,000,000 wei
- 1 ether = 10^{18} wei

布林型態

- 關鍵字: bool
- 內容: true / false
- 運算子:

! && || == !=

整數型態

- int

int8 int16 ... int256

- uint

uint8 ... uint256

整數型態

- 比較運算子：

<= < == != >= >

- 算數運算子：

+ - * / %(取餘數) ** (冪) << >>

常數型態

- 數值
 - 字串
- “Hello”



列舉型態

- **關鍵字** : enum
- enum State { Created, Locked, Inactive }

地址型態

- **關鍵字** : address
- **屬性** : .balance 餘額 (單位 wei)
- **函式** : .transfer() 轉帳

BLOCKCHAIN DAPP EXPERTS

陣列型態

- 宣告: $V[i]$

V : 資料型態 i : 陣列長度

```
uint[8] eight;
```

```
uint[] temp;
```

```
uint[] public a = [1, 2, 3];
```

陣列型態

- **屬性：.length 取得陣列長度**

`uint[8] eight;`

`eight.length` 值為8

- **函式：`.push()` 新增元素至動態陣列**

(鍵值)對應型態

- **關鍵字** : mapping

mapping(address => uint) public balances;

key : address

value : uint

- **key存取** : balances[userAddress];

自訂結構型態

- **關鍵字** : struct

```
struct Custom {  
    address owner;  
    uint totalBalance;  
}
```

Solidity API

- 區塊與交易
- 錯誤處理

區塊與交易

- `block.number (uint)`: 目前區塊號碼
- `msg.sender (address)`: 發起交易者地址
- `msg.value (uint)`: 交易發送的以太幣
- `tx.gasprice (uint)`: 交易的 gas 價格

錯誤處理

- `require(bool condition)` 常用
判斷外部錯誤，不滿足條件拋出異常
- `assert(bool condition)` 少用
判斷內部錯誤，不滿足條件拋出異常

函式修飾器

- **關鍵字** : modifier
- 通常用於植入其他函式檢查前置條件
- 被植入的函式主體將置於“_;

BLOCKCHAIN DAPP EXPERTS

函式修飾符

- payable: 該函式能傳入以太幣
- view: 該函式不能修改狀態
- pure: 該函式不能修改且不能讀取狀態

BLOCKCHAIN DAPP EXPERTS

合約繼承

- **關鍵字** : is

```
contract A {}
```

```
contract B is A {}
```

- **子合約可以訪問父合約非 private 的內容**

程式庫

- **關鍵字**: library
- **特殊合約**: 可以部署, 但無狀態變數
- **部署一次**, 可重複使用, 節省 gas
- **使用方式**: using ... for ...

常用程式庫

- OpenZeppelin

<https://github.com/OpenZeppelin/openzeppelin-contracts>

- SafeMath, ERC20, ERC721, ...

事件

- **宣告：**

```
event LogEventName(uint param);
```

- **呼叫：**

```
emit LogEventName(10);
```

Demo

BLOCKCHAIN DAPP EXPERTS

Day2 練習 3:

<https://ropsten.etherscan.io/>

3-1.部署 HelloWorld.sol 到 Ropsten 測試網路, 並上傳原始碼至 Ropsten 的 Etherscan 網站

3-2.部署 1_Storage.sol 到 Ropsten 測試網路, 並上傳原始碼至 Ropsten 的 Etherscan 網站

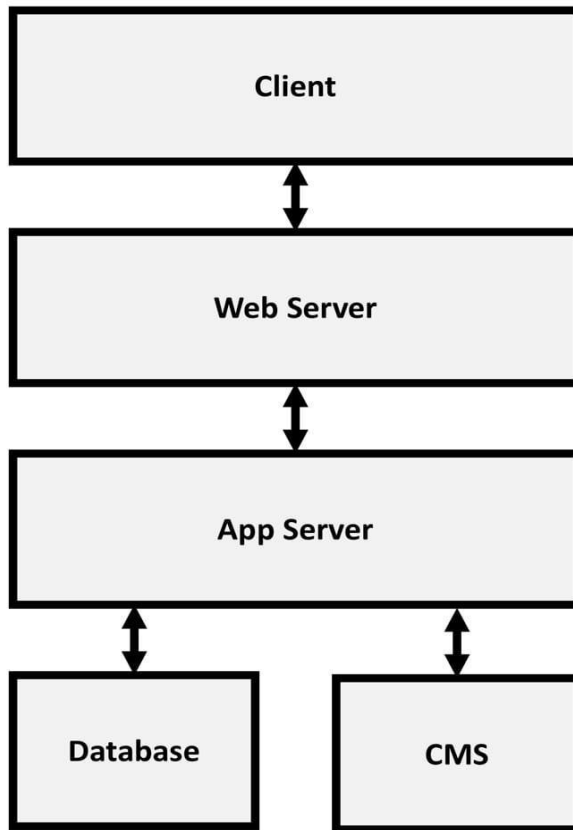
3-3.部署 2_Owner.sol 到 Ropsten 測試網路並上傳原始碼至 Ropsten 的 Etherscan 網站

Web3.js 入門

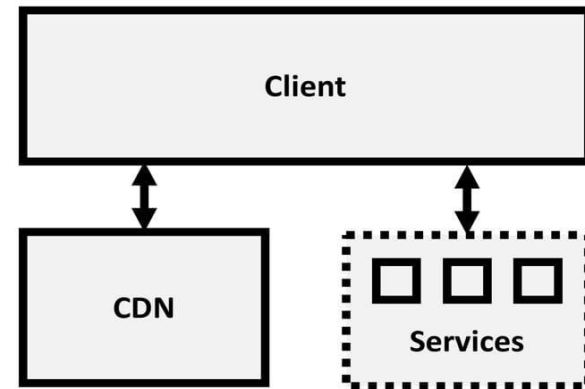
BLOCKCHAIN DAPP EXPERTS

Web3 & JAMStack

Traditional Web



JAMstack



CrappyBird 專案

- 網站:

<https://taipeiblockchain.github.io/CrappyBird/>

- 專案原始碼:

<https://github.com/TaipeiBlockchain/CrappyBird>

CrappyBird

- 原始版本：

https://github.com/TaipeiBlockchain/CrappyBird/blob/master/index_old.html

- 上鏈版本：

<https://github.com/TaipeiBlockchain/CrappyBird/blob/master/index.html>

CrappyBirdPlus 專案

- 專案原始碼：

<https://github.com/bdetw/CrappyBird>

Demo

BLOCKCHAIN DAPP EXPERTS

Day2 作業：

CrappyBird 智能合約網址

- 1.將 CrappyBird 智能合約部署至 Ropsten上，並上傳原始碼至 Ropsten 的 Etherscan 網站
- 2.將 CrappyBird 專案 fork 至個人的 GitHub 帳號中，修改網頁中的智能合約地址為新部署的地址。
- 3.將 fork 後的專案部署至 GitHub Pages 上並記下網址。

Day2 作業：

<https://www.bde.tw/r/aFp>

4.將今日練習中1-1、2-2的截圖存檔上傳至 IPFS, 並記錄上傳成功的檔案 hash 值

Day2 作業：

5.將練習與作業所記錄的資訊填入下方格式：

ID:學號,

1-1:IPFS的Hash值,

2-2:IPFS的Hash值,

2-3:IPFS的Hash值,

2-4:Gist的網址,

3-1:智能合約帳號地址,

3-2:智能合約帳號地址,

3-3:智能合約帳號地址,

Project:部署至 GitHub Pages 的 CrappyBird 專案網址

Day2 作業：

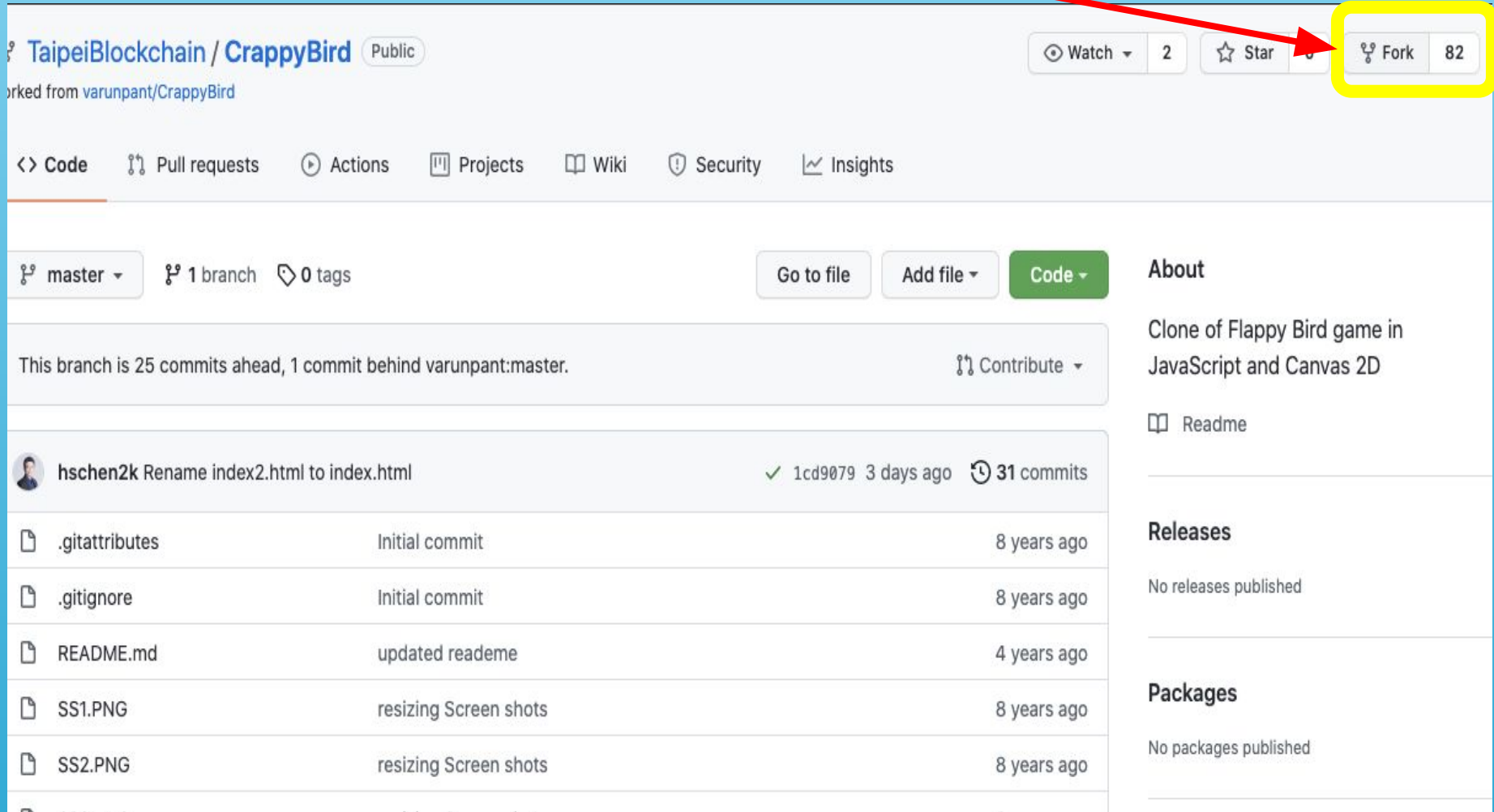
6.發送一筆交易含16進位資料填寫上方資訊的 Hex
值至下方錢包地址

0x173c38B04624b708822CD1551cDfF8071E175c62

作業補充說明

BLOCKCHAIN DAPP EXPERTS

將 CrappyBird 專案 fork 至個人的 GitHub 帳號中



TaipeiBlockchain / CrappyBird Public

Worked from varunpant/CrappyBird

Watch 2 Star 0 Fork 82

Code Pull requests Actions Projects Wiki Security Insights

master 1 branch 0 tags

Go to file Add file Code

This branch is 25 commits ahead, 1 commit behind varunpant:master. Contribute

hschen2k Rename index2.html to index.html ✓ 1cd9079 3 days ago ⌚ 31 commits

.gitattributes	Initial commit	8 years ago
.gitignore	Initial commit	8 years ago
README.md	updated reademe	4 years ago
SS1.PNG	resizing Screen shots	8 years ago
SS2.PNG	resizing Screen shots	8 years ago

About

Clone of Flappy Bird game in JavaScript and Canvas 2D

Readme

Releases

No releases published

Packages

No packages published

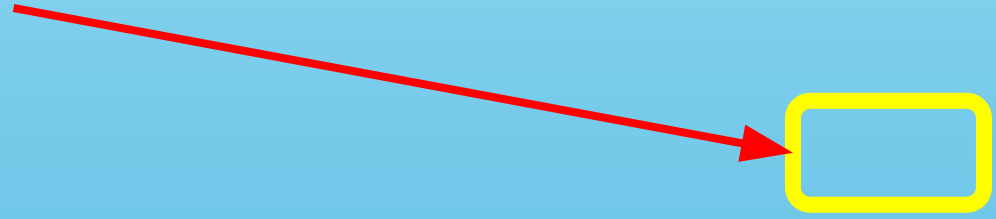
修改 index.html 網頁中的智能合約地址為新部署的地址

font_small_5.png	Initial commit	8 years ago
font_small_6.png	Initial commit	8 years ago
font_small_7.png	Initial commit	8 years ago
font_small_8.png	Initial commit	8 years ago
font_small_9.png	Initial commit	8 years ago
hit.ogg	Initial commit	8 years ago
index.html	Rename index2.html to index.html	3 days ago
index_old.html	Rename index.html to index_old.html	3 days ago

medal_bron	881
medal_gold	882
medal_plati	883
medal_silve	884
point.ogg	885
replay.png	886

```
} else {  
    alert("請先安裝MetaMask");  
    // 处理用户没安装的情况， 比如显示一个消息  
    // 告诉他们要安装 MetaMask 来使用我们的应用  
}  
// 现在你可以启动你的应用并自由访问 Web3.js:  
});  
  
function startApp() {  
    //var crappyBirdAddress = "0x77b0AB154BC318...Ef9F6f40Af365Ef3C4d630Fa";  
    var crappyBirdAddress = "0x1d63Be7B6FE519055Ffe6555659759754D7E607c";  
    crappyBird = new web3js.eth.Contract(CrappyBirdABI, crappyBirdAddress);  
    userAccount = web3.currentProvider.selectedAddress;  
    console.log("userAccount = " + userAccount);  
    /*
```

將 fork 後的專案部署至 GitHub Pages 上並記下網址



休息一下~~~

BLOCKCHAIN DAPP EXPERTS



BDE Youtube 頻道:

<https://bitlly.co/ogvpb>

台北行銷科技社群:

<https://www.meetup.com/Taipei-MarTech/>

台北區塊鏈社群:

<https://www.meetup.com/Taipei-Blockchain/>

台北敏捷 AI 社群:

<https://www.meetup.com/Taipei-Agile-AI/>

區塊鏈系列文章:

<https://ithelp.ithome.com.tw/users/20111706/ironman/>

👉 喜歡我們的課程請按讚分享 👍

BDE 區塊鏈商學院粉絲專頁:

<https://www.facebook.com/bdetwcom>