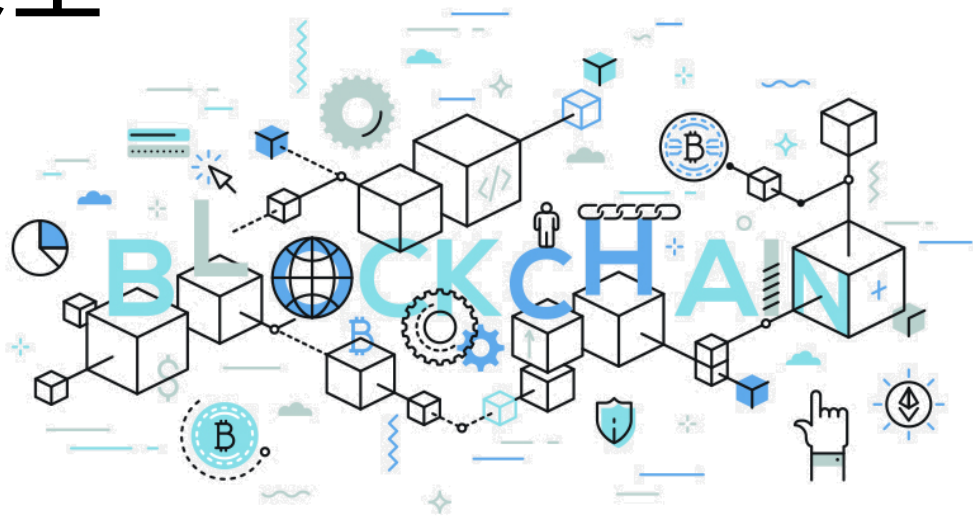


Blockchain系列(一)

私鏈、合約、ICO

主講人：陳東笙



免責聲明

以下分享內容
純為社團交流活動
無從事任何商業行為

注意事項：

簡報內容截錄自網路及參考書籍
並未取得作者授權，故僅供會中討論
請勿散佈，以免侵犯作者權利

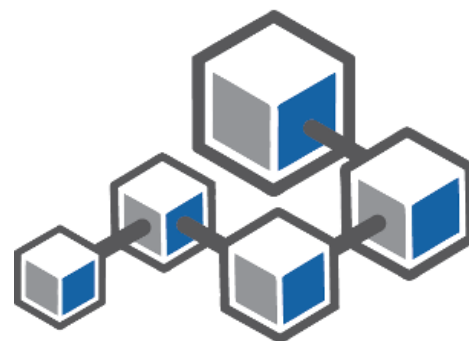
區塊鏈的特點



資料來源：[你不可不知區塊鏈的五大特色](#)

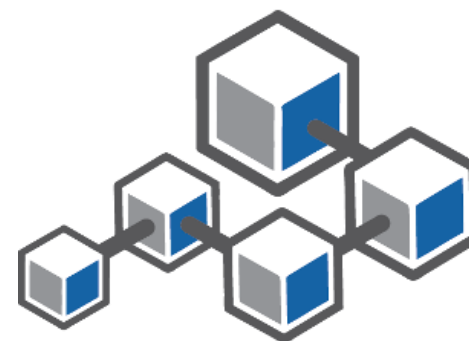
區塊鏈的分類(一)

- 區塊鏈 1.0
- 區塊鏈 2.0
- 區塊鏈 3.0



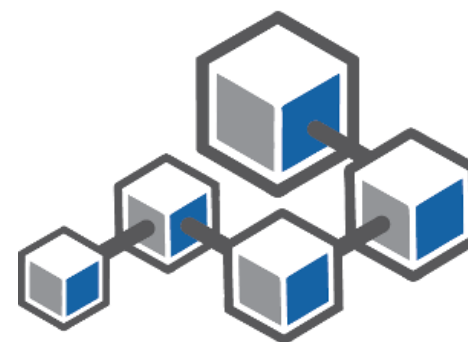
區塊鏈的分類(二)

- 公有鏈
- 聯盟鏈
- 私有鏈



區塊鏈的主流

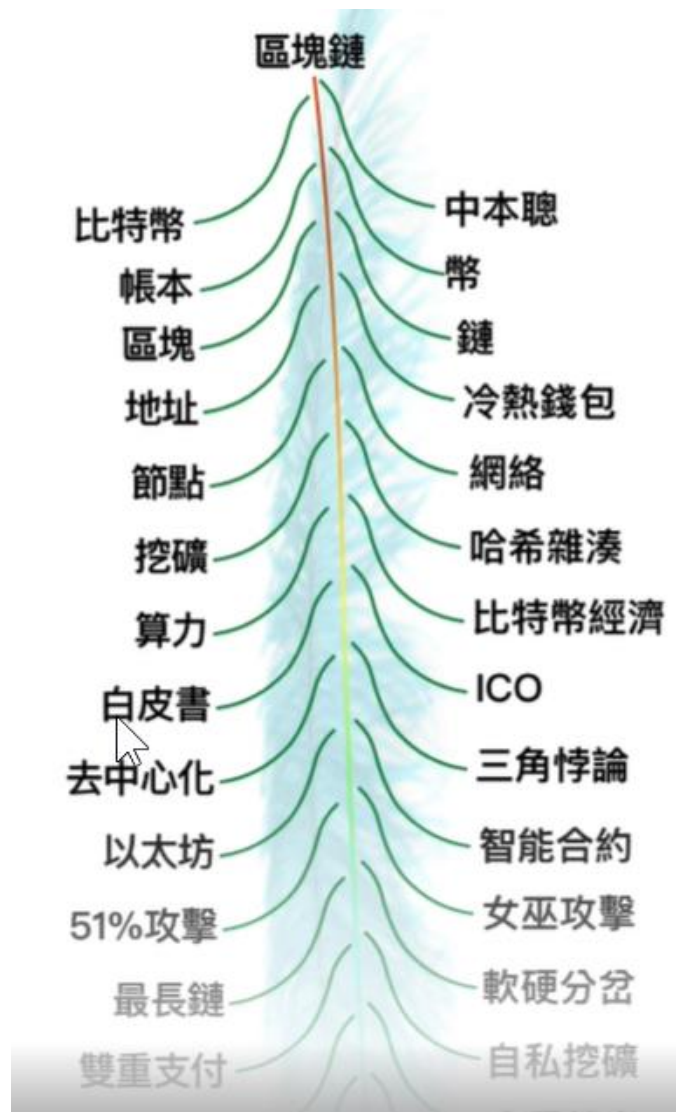
- Blockchain
- Hyperledger
- IOTA
- R3 Corda



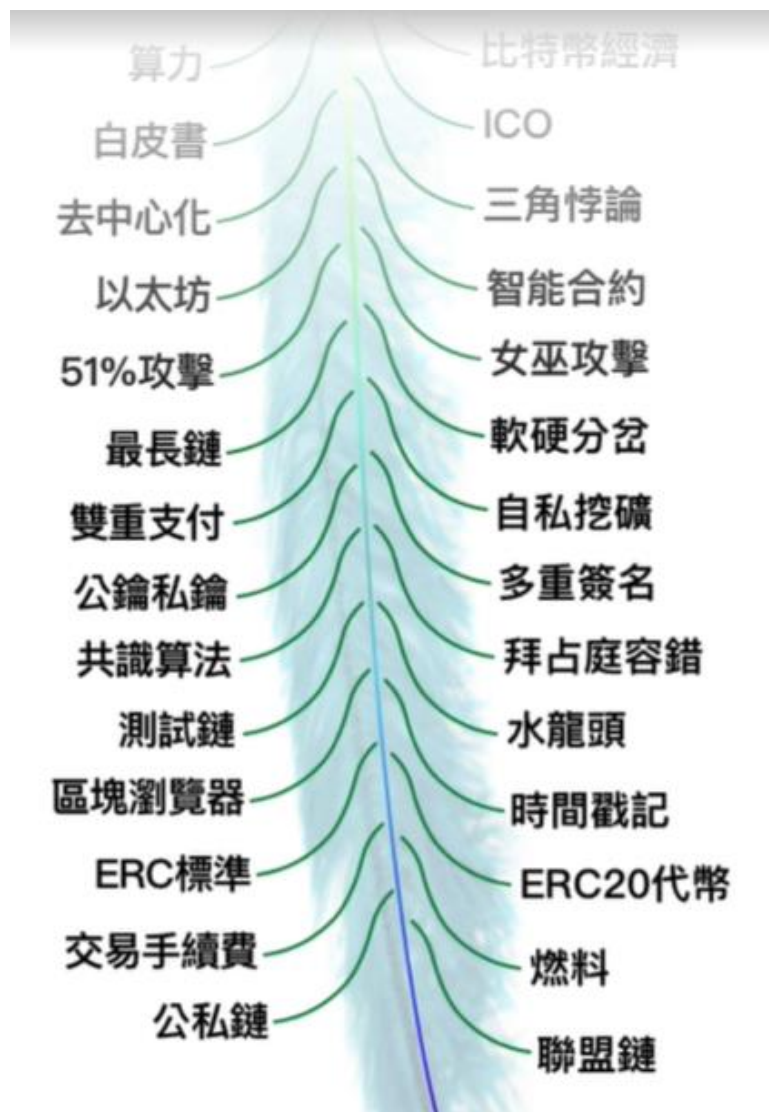
區塊鏈的四十個專有名詞



區塊鏈的四十個專有名詞(上)



區塊鏈的四十個專有名詞(下)



水龍頭

從Ropsten測試鏈水龍頭(faucet)取幣



取測試幣



MetaMask Ether Faucet

faucet

address: 0x81b7e08f65bdf564860c
balance: 95092908.03 ether

request 1 ether from faucet

user

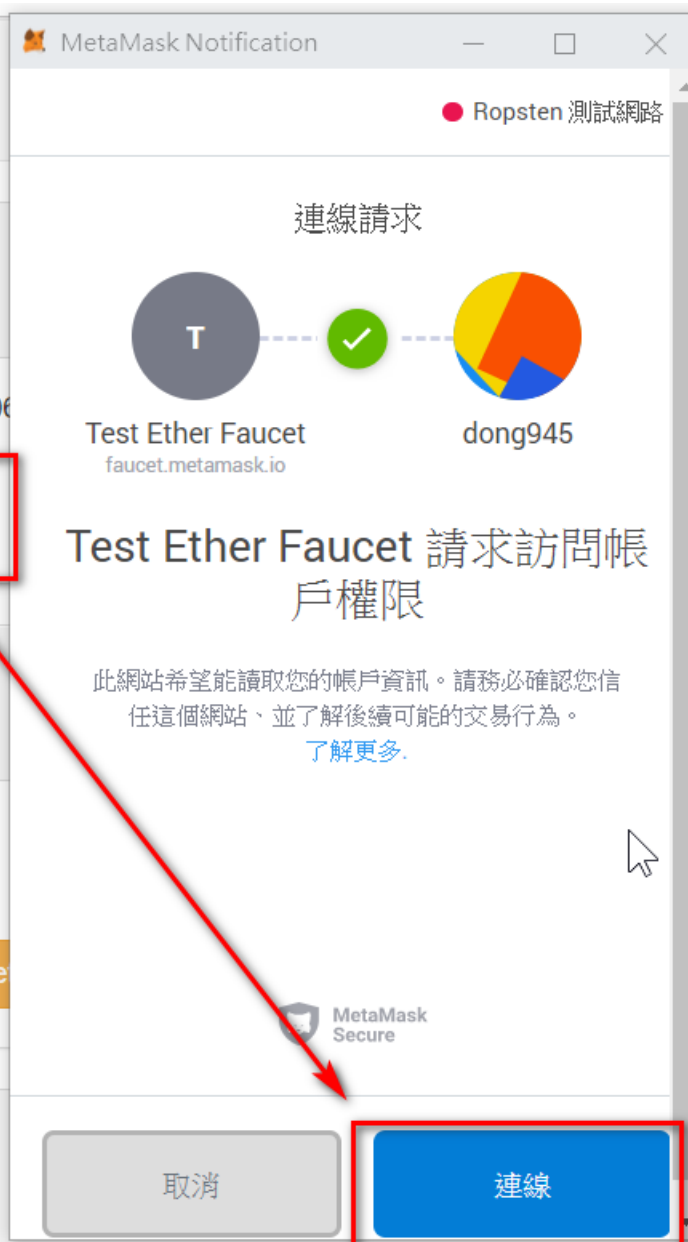
address: undefined
balance: ...
donate to faucet:

1 ether

10 ether

100 ether

transactions



MetaMask Ether Faucet

faucet

address: 0x81b7e08f65bdf5648606c89998a9cc8164397647
balance: 95092862.03 ether

request 1 ether from faucet

user

address: 0x912fa234014a923bc5f05e8989e3614b52bdfe48
balance: 1.00 ether
donate to faucet:

1 ether

10 ether

100 ether

transactions

0xe6d0654dbc9f64580244b51ff3f6b36d22419ae76115ee42976521f8d707ebfe

Test Ether Faucet Ropsten Transaction 0xe6d0654dbc9f64580244b51ff3f6b36d22419ae76115ee42976521f8d707ebfe

ropsten.etherscan.io/tx/0xe6d0654dbc9f64580244b51ff3f6b36d22419ae76115ee42976521f8d707ebfe

Follow Me 倉頡... 新增分頁 區塊鏈 eBook R語言 線上課程 線上書城 經緯度轉換 不動產相

Etherscan Ropsten Testnet Network All Filters Search by Ad Home Blc

Transaction Details

Sponsored: MythX Smart contract security analysis, Pro options for mission-critical dapps. [Start analyzing now](#)

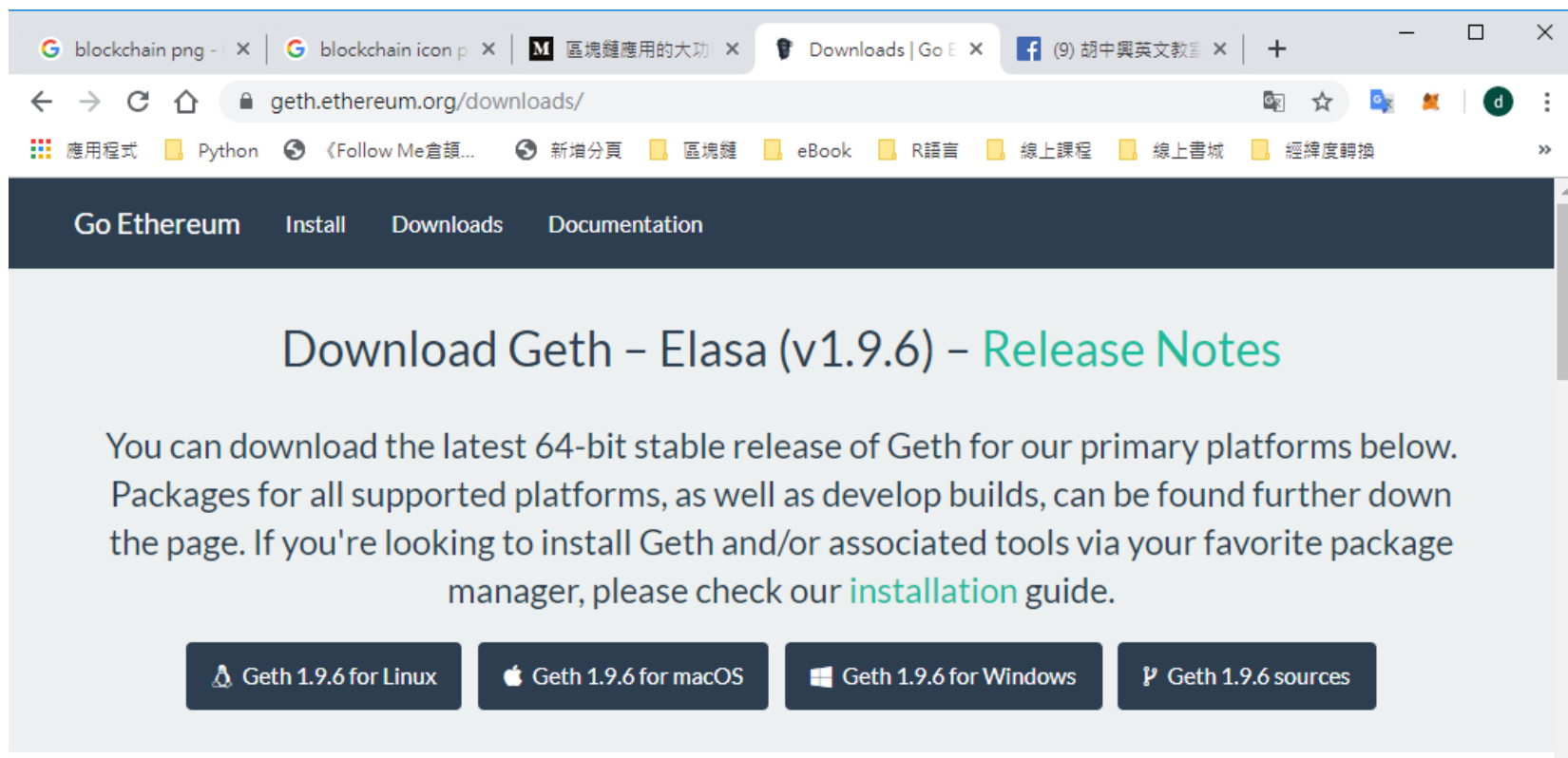
Overview State Changes New

[This is a Ropsten **Testnet** transaction only]

Transaction Hash:	0xe6d0654dbc9f64580244b51ff3f6b36d22419ae76115ee42976521f8d707ebfe
Status:	Success
Block:	6590725 6 Block Confirmations
Timestamp:	1 min ago (Oct-17-2019 02:51:19 PM +UTC)
From:	0x81b7e08f65bdf5648606c89998a9cc8164397647
To:	0x912fa234014a923bc5f05e8989e3614b52bdf48
Value:	1 Ether (\$0.00)
Transaction Fee:	0.000021 Ether (\$0.000000)

建一條私有鏈

下載網址：<https://geth.ethereum.org/downloads/>



安裝MetaMask

官方網址：<https://metamask.io/>



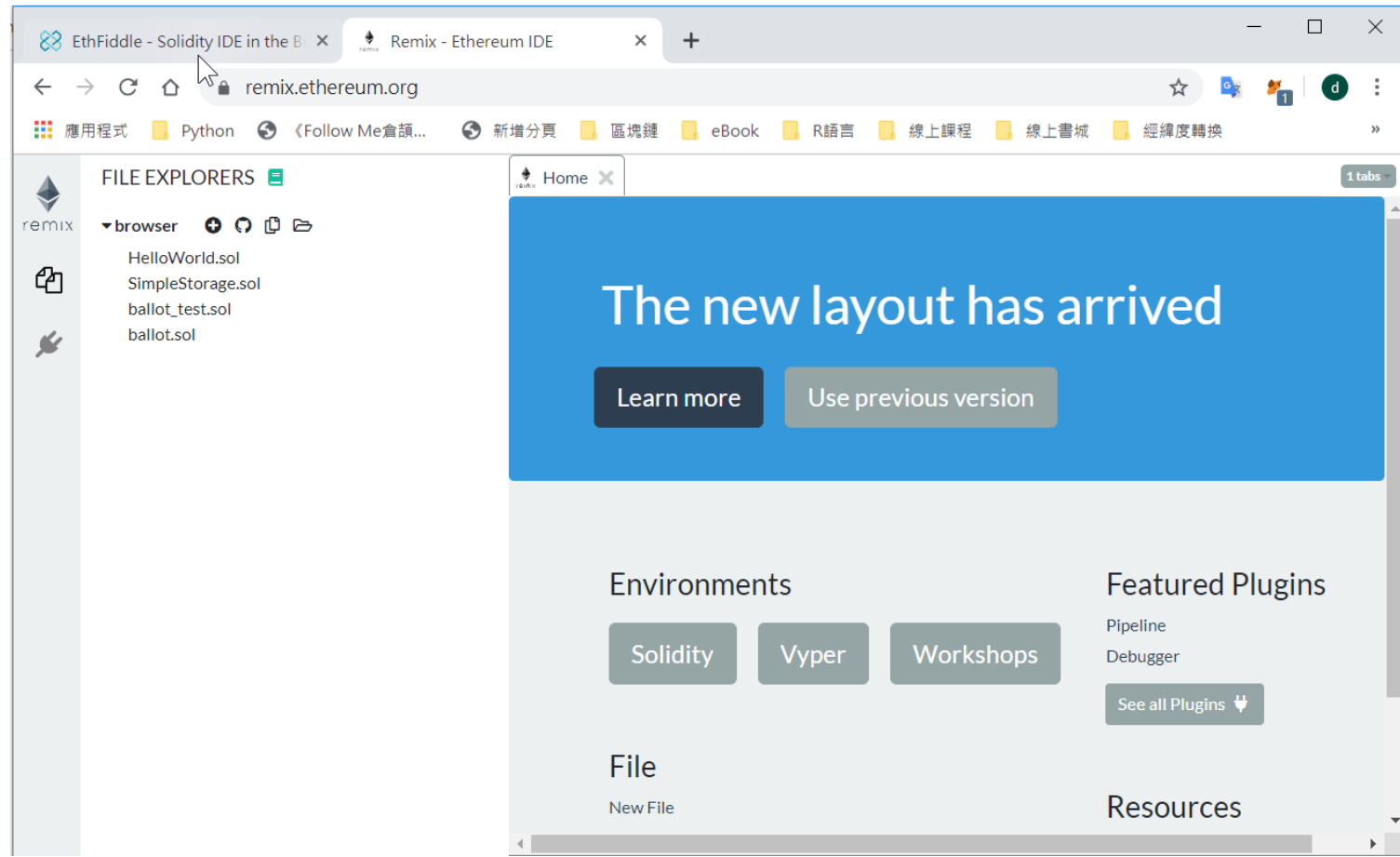
資料來源：[Chrome插件錢包 MetaMask](#)

Smart Contract 開發工具及語言

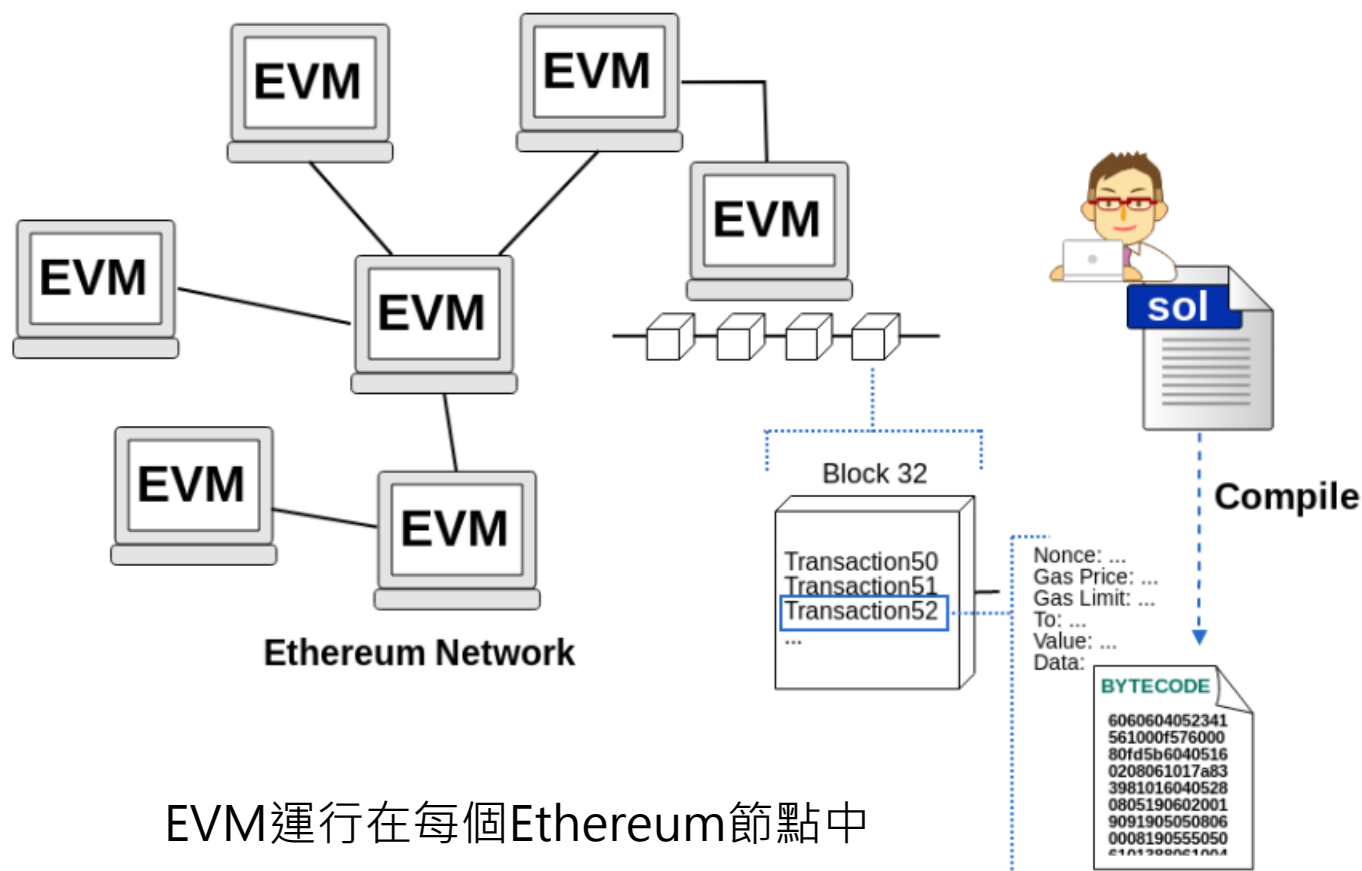
開發工具：Remix IDE、Visual Studio Code.....

開發語言：Solidity

Remix IDE



EVM (Ethereum Virtual Machine)



資料來源：[簡介Smart Contract](#)

ICO (Initial Coin Offering)

所謂ICO，全稱Initial Coin Offering，意思是“數字貨幣首次公開募資”，概念拷貝自股票市場的IPO,是指企業或非企業組織在區塊鏈技術的支持下發行代幣，向投資人募集虛擬貨幣（一般為比特幣、以太坊）的融資活動。

不同的是，IPO是企業為了發展而向公眾籌集資金，ICO是企業為了發展而向公眾籌集虛擬貨幣，將發行的標的物由IPO的證券變成了數字加密貨幣。ICO發行團隊在進行具體操作時，會先建立一個網站，發佈“ICO白皮書”，介紹所發行虛擬幣項目進行的虛擬幣融資情況。

資料來源：[MAB智庫百科](#)



ERC (Ethereum Request for Comment)

ERC並非一項技術或是程式，而是以太坊通用徵求意見協議（RFC）。

ERC為開發者提供了建設技術指導。而開發者可以通過提交EIP（Ethereum Improvement Proposal），向以太坊社區提交新的ERC標準提案。

提交內容包括協議規範和合約標準。
一旦該EIP獲得以太坊委員會的批准並最終定型，它就會成為一個新的ERC。



ERC20 Tokens

資料來源：[ERC20/ERC721](https://erc20.com/erc721)

ERC 20

ERC20包含：

- 6個函式
- 2個事件
- 3個Token資訊的函式

只要是智能合約中有撰寫以下的功能，都可視為是ERC20為基準的Token。

資料來源：[ERC20/ERC721](https://eips.ethereum.org/EIPS/eip-20)

6個函式

totalSupply() : Token的總供應量。

balanceOf(address _owner) : _owner地址中的餘額。

transfer(address _to, uint256 _value) : 發送數量為_value的Token到地址_to，觸發Transfer事件。

transferFrom(address _from, address _to, uint256 _value) : 從地址_from發送數量為_value的通證到地址_to，觸發Transfer事件。

approve(address _spender, uint256 _value) : 批准_spender提取一定數量的金額。

allowance(address _owner, address _spender) : 回報_spender從_owner提取的金額。

2個事件

`transfer(address indexed _from, address indexed _to, uint256 _value)`：當token被轉移時則會觸發。

`approval(address indexed _owner, address indexed _spender, uint256 _value)`：成功調用approve方法後則會觸發。

3個Token資訊的函式

Name：發行Token之名稱

Symbol：發行Token之代稱，例如StarBitEx發行Token代稱為SBT，而Symbol能在<https://etherscan.io/>上進行查詢。

Decimals：設定此Token最多能達到小位數點後多少位數，一般而言設定值為18，意即能到達小數點後18位數。

一鍵發幣

參考資料：

iThome『區塊鏈』專題：

<https://www.ithome.com.tw/article/105368>

CoinGecko(幣虎)：

<https://www.coingecko.com/zh-tw>

Blockchain.info：

<https://www.blockchain.com/>

iThome 鐵人幫幫忙：

<https://ithelp.ithome.com.tw/articles/10192847>

<https://medium.com/@ksin751119>

[以太坊智能合約基礎介紹](#)