

Blockchain 區塊鏈

資訊與通訊研究所

Information and Communication Research Lab (ICL)

區塊鏈旗艦計畫

區塊鏈
應用共
創機制

食安
履歷

病歷
轉遞

公益
眾籌

...

數位
資產

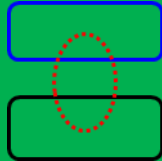
典範
應用

法定貨幣

非典型貨幣

其他價值幣

連結



強化資料正確性、應用層之詐欺交易偵測、
強化實名認證、節點資源監控、服務資料監管、
智能合約開發與漏洞偵測工具

區塊鏈基礎設施環境

簡報大綱

- ◆ Ethereum 現況及趨勢
- ◆ Ethereum 問題
- ◆ 計畫目標
- ◆ 實作成果

Blockchain – Bitcoin / Ethereum

□ Blockchain:

block chain, a distributed **database**. Hold both **data** and **programs** in some implementations.

□ Bitcoin:

Designed as **peer-to-peer**, serves as the public ledger of all bitcoin transactions.

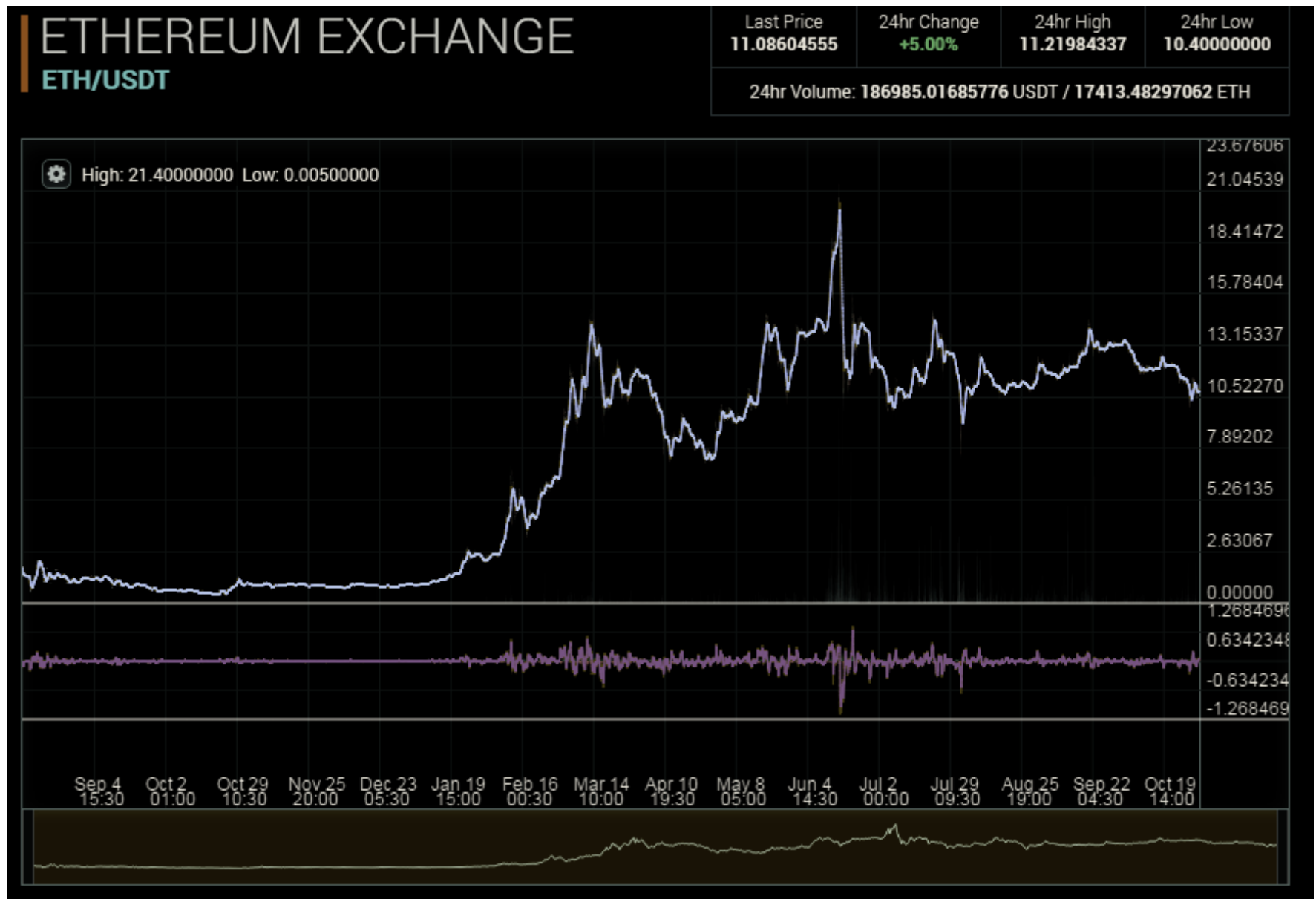
□ Ethereum:

A Next-Generation Cryptocurrency and **decentralized** Application Platform. The generalized blockchain for **smart contract** development

市場現況及趨勢 - Ethereum

- 基於區塊鏈技術，具備完整的底層協議，可供開發者和投資者使用，並能為企業提供更透明的公開交易紀錄，Ethereum被認為能夠在企業和普通人間構建自己的自治組織、智能合約、與應用
- 2015年11月，微軟宣布使用Ethereum作為其區塊鏈服務（EBaaS，Ethereum Blockchain-as-a-Service），部署在微軟的雲端平台 Azure 上
- 2016年1月，由全球42家銀行組成的 R3 CEV 聯盟，支持區塊鏈基礎設施項目，宣布將會使用Ethereum和微軟 Azure的EBaaS服務
- 自從微軟 Azure 和 R3 CEV 的公告出來之後，Ether的價格出現大幅增長，交易量亦同步放大

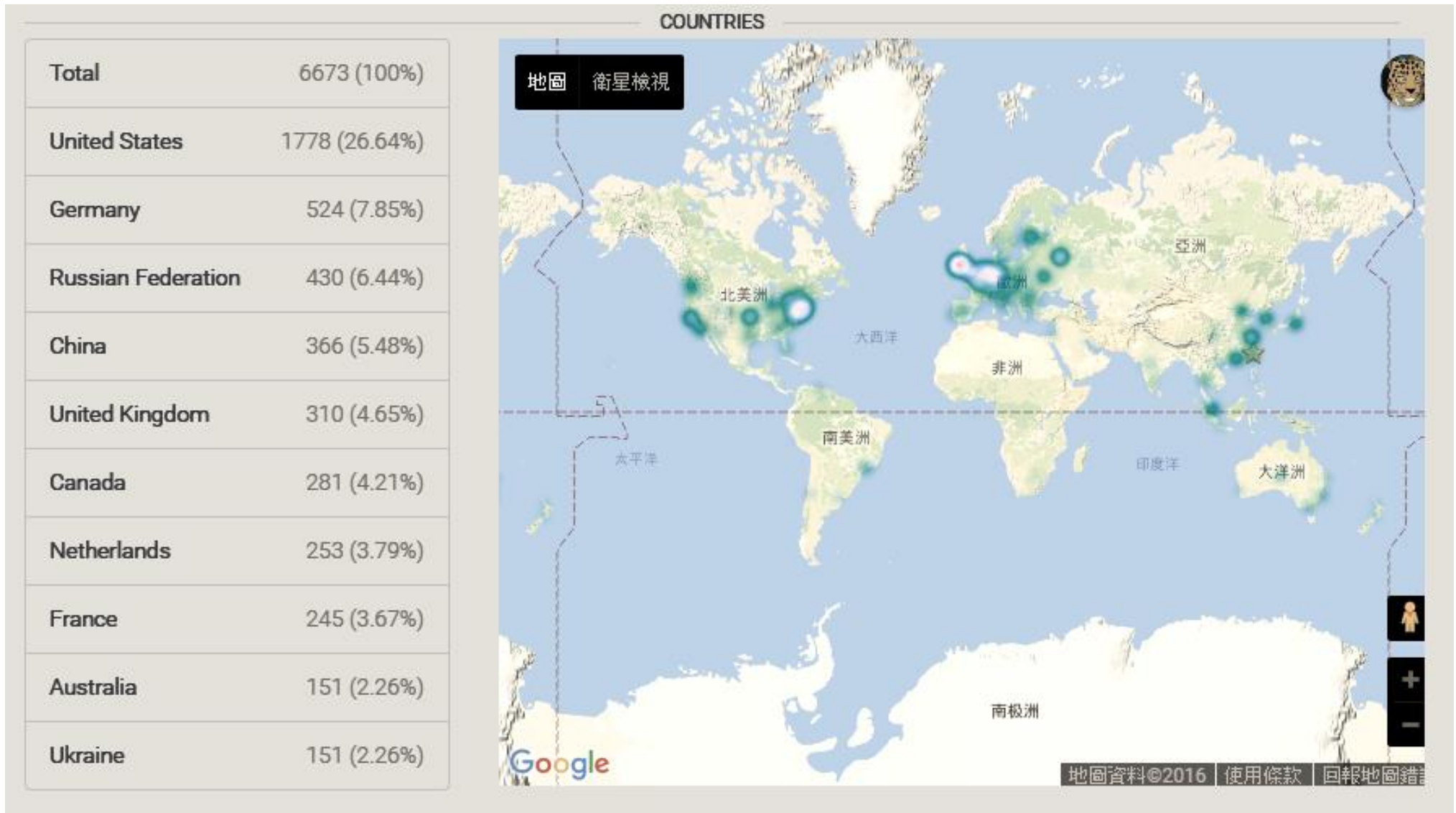
市場現況及趨勢 - Ethereum



市場現況及趨勢–Ethereum

- ❑ Ethereum目前的貨幣交易量為全球加密貨幣第二名
- ❑ Ethereum目前的節點數(node)為6673，已超越Bitcoin的5318
- ❑ Ethereum的交易速度和交易容量遠大於Bitcoin
- ❑ Ethereum目前已成為世界第二大的blockchain

市場現況及趨勢–Ethereum nodes



Ethereum簡介

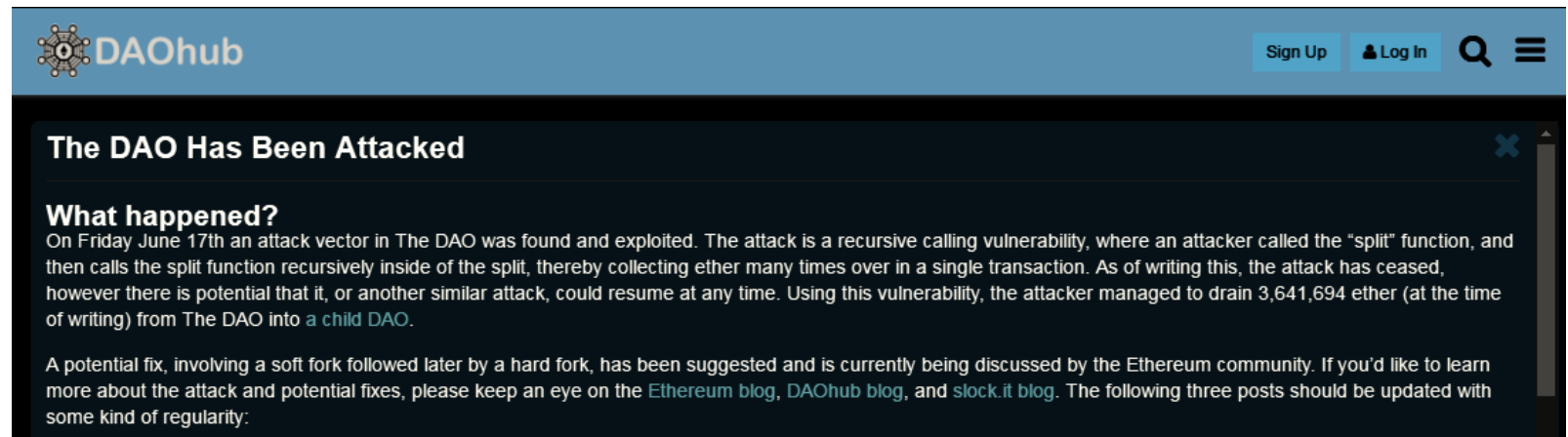
- Ethereum是一個public blockchain，任何人都可以參加，所以沒有權限控管
- Ethereum目前使用PoW共識機制，區塊時間約14秒，預計明年改成PoS以及加強privacy
- 每秒交易量約25筆
- 發送交易需要手續費，因此Ethereum有貨幣系統ether
- Ethereum支援smart contract，其程式語言是Turing complete
- Ethereum使用Ethereum virtual machine(EVM)，smart contract在其中執行
- EVM中無法對網路、檔案系統存取

Ethereum簡介

- Ethereum程式由Ethereum foundation所維護，也有網友上傳程式碼
- Ethereum與微軟合作，推出Ethereum Blockchain as a Service
- Ethereum未來會對交易量/交易速度進行改善，可能的方式包括state channel和sharding

Ethereum 問題

- ❑ 在Ethereum的public chain上，每個block產生時間約為14秒左右，同樣等待6確認的話，所需時間約為84秒
- ❑ 在Ethereum的public chain上，目前的架構所能處理的速度極限是25筆交易/每秒；這樣的處理速度，推廣blockchain 技術較為不易。
- ❑ 智能合約開發需非常注重安全性，否則即會發生如DAO的智能合約遞迴漏洞被攻擊的重大事件。



Ethereum 問題 – The DAO被攻擊

- ❑ The DAO是基於Ethereum所成立的去中心化眾籌新創公司，於2016/05共籌得12M ether，相當於150M美金
- ❑ The DAO的營運依賴智能合約，它並不像傳統的公司般有管理階層架構，決策則依據token權重投票來表決
- ❑ 在加密經濟以及FINTECH的領域中，全世界都在關注The DAO的發展與動態，但在獲得如此高的期待同時，卻於6/17發生The DAO被駭客攻擊的事件
- ❑ 駭客使用SplitDAO的遞迴攻擊漏洞，一共盜取了3.7M ether，幸好在分出子DAO後，其款項限定必須在28天後才能挪用，使得開發團隊有時間來因應此一嚴重事態
- ❑ 但此一事件已造成The DAO以及Ethereum的嚴重傷害

Ethereum 問題 – The DAO被攻擊

□ 攻擊手法分析:

1. Propose a split and wait until the voting period expires. (*DAO.sol, createProposal*)
2. Execute the split. (*DAO.sol, splitDAO*)
3. Let the DAO send your new DAO its share of tokens. (*splitDAO -> TokenCreation.sol, createTokenProxy*)
4. Make sure the DAO tries to send you a reward before it updates your balance but after doing (3). (*splitDAO -> withdrawRewardFor -> ManagedAccount.sol, payOut*)
5. While the DAO is doing (4), have it run *splitDAO* again with the same parameters as in (2) (*payOut -> _recipient.call.value -> _recipient()*)
6. The DAO will now send you more child tokens, and go to withdraw your reward before updating your balance. (*DAO.sol, splitDAO*)
7. Back to (5)!
8. Let the DAO update your balance. Because (7) goes back to (5), it never actually will.

Ethereum 問題 – The DAO被攻擊

□ SplitDAO

```
function splitDAO(
    uint _proposalID,
    address _newCurator
) noEther onlyTokenholders returns(bool _success) {

    ...
    // Move ether and assign new Tokens
    uint fundsToBeMoved =
        (balances[msg.sender] * p.splitData[0].splitBalance) /
        p.splitData[0].totalSupply;
    if (p.splitData[0].newDAO.createTokenProxy.value(fundsToBeMoved)(msg.sender) == false)
        throw;

    ...
    // Burn DAO Tokens
    Transfer(msg.sender, 0, balances[msg.sender]);
    withdrawRewardFor(msg.sender); // be nice, and get his rewards
    totalSupply -= balances[msg.sender];
    balances[msg.sender] = 0;
    paidOut[msg.sender] = 0;
    return true;
}
```

Ethereum 問題 – The DAO被攻擊

□ 遞迴攻擊成立:


```
from DAO.sol:
function withdrawRewardFor(address _account) noEther internal returns (bool _success) {
    if ((balanceOf(_account) * rewardAccount.accumulatedInput()) / totalSupply < paidOut[_account])
        throw;

    uint reward =
        (balanceOf(_account) * rewardAccount.accumulatedInput()) / totalSupply - paidOut[_account];
    if (!rewardAccount.payOut(_account, reward))
        throw;
    paidOut[_account] += reward;
    return true;
}

exploit:
function payOut(address _recipient, uint _amount) returns (bool) {
    if (msg.sender != owner || msg.value > 0 || (payOwnerOnly && _recipient != owner))
        throw;
    if (_recipient.call.value(_amount)()) { ➡ Call SplitDAO() again
        PayOut(_recipient, _amount);
        return true;
    } else
        return false;
}
```

Ethereum 問題 – The DAO被攻擊

□ 遞迴攻擊搬運記錄:

 etherchain.org


Blockchain ▾

Accounts ▾

Statistics ▾

Tools ▾

Pools ▾

Tx Hash, Address or Block 

Address `0x304a554a310C7e546dfe434669C62820b7D83490` Balance: 3641694.2418985067 Ether | [Buy more](#)

經驗分享

- 目前我們採用Ethereum consortium chain，以Ethereum為基礎架構，不連上public chain的情況下，可build聯盟間互連版本的consortium chain，保留blockchain大多數的優點，並透過建置適當的網路節點、修改設定、開發智能合約來解決上述的pain point
- 在應用情境方面，可做到兩倍於public chain的交易量，完成交易通知時間5秒內。

經驗分享

◆ 在聯盟鏈上我們做了以下事情來增加交易量與縮短交易時間：

- 縮短區塊認證時間
- 智能合約複雜度分析、優化、與拆解
- 分析CPU與交易簽章驗證速度之關連
- 分析GPU與系統負載之關連

APPLICATION

JSON-RPC API

DATA &
COMMUNICATION

P2P
protocol

RLP

Token
system

Smart
contracts

Transactions

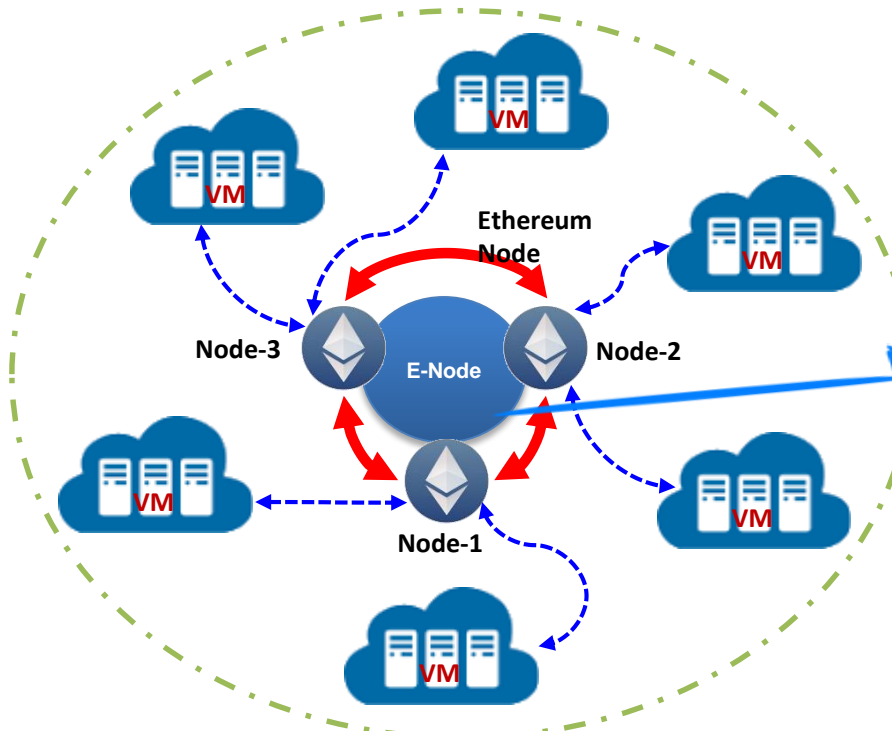
Blocks

CORE

EVM

Consensus
protocol

Ethereum 經驗分享-實作案例

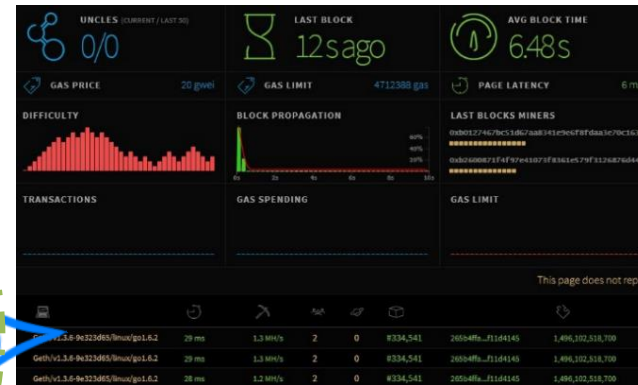


使用大量交易測試 Ethereum 最快處理 Blocks 效能與最大容許交易量

信用狀(L/C) 開立紀錄

信用卡交易紀錄

序號	出票日	入票到期日	出票金額	入票金額	手續費	匯率	幣別
1	2016/05/09	2016/05/10	1,470	1,470	17.005	TWD	
2	2016/05/09	2016/05/10	1,470	1,470	24.912	TWD	
3	2016/05/09	2016/05/11	1,470	1,470	31.884	TWD	
4	2016/05/09	2016/05/11	1,470	1,470	7.120	TWD	
5	2016/05/09	2016/05/11	1,470	1,470	11.220	TWD	
6	2016/05/09	2016/05/11	1,470	1,470	947	TWD	
7	2016/05/09	2016/05/11	1,470	1,470	494	TWD	
8	2016/05/09	2016/05/11	1,470	1,470	1,308	TWD	
9	2016/05/09	2016/05/11	1,470	1,470	544	TWD	
10	2016/05/09	2016/05/11	1,470	1,470	384	TWD	
11	2016/05/09	2016/05/11	1,470	1,470	410	TWD	
12	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
13	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
14	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
15	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
16	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
17	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
18	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
19	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
20	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
21	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
22	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
23	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
24	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
25	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
26	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
27	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
28	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
29	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
30	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
31	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
32	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
33	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
34	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
35	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
36	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
37	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
38	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
39	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
40	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
41	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
42	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
43	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
44	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
45	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
46	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
47	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
48	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
49	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
50	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
51	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
52	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
53	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
54	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
55	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
56	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
57	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
58	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
59	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
60	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
61	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
62	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
63	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
64	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
65	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
66	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
67	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
68	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
69	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
70	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
71	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
72	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
73	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
74	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
75	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
76	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
77	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
78	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
79	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
80	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
81	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
82	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
83	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
84	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
85	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
86	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
87	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
88	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
89	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
90	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
91	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
92	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
93	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
94	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
95	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
96	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
97	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
98	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
99	2016/05/09	2016/05/11	1,470	1,470	340	TWD	
100	2016/05/09	2016/05/11	1,470	1,470	340	TWD	



相關 Ethereum 即時處理資訊過程將在此 Dashboard 可以同時監看處理過程



Sender

Account Address
0x00E1ABCEDF018

Identify
Daniel

Password

Receiver

Account Address
0x00E1ABCEDF388

Amount
20,000

Send Clear



透過手機完成一筆交易應用

2 行動裝置透過API將此交易資料傳至主機處理



3 主機再將資料交由Ethereum處理此筆紀錄，確保安全寫入資料庫



1. 迅速安全資料庫
2. 利用Smart Contract 執行不同應用

Ethereum 經驗分享-實作案例

SEND

QUE

Sender Account Address :
A321654987
0x48d2173c4ced56921702cd606

Sender Identity :
A321654987

Sender Password

Receiver
A987654321
0xec61df740330d4af415141b14a

\$ Amount
432

Note
Dollars

傳送交易

SEND

CLEAR

交易傳送功能

SEND

QUERY

\$ Amount
432

Note
Dollars

SEND

CLEAR

Status
Succeeded

Transaction Hash
0xd25ee7fb6f1150925bfdc7150fea88ec679431bc895353a511b3ac36d1a356ea

Sent Time
2016/06/06 14:04:04

Confirmed Time
2016/06/06 14:04:15

START

狀態由 Pending 到 Succeeded 表示交易成功

SEND

QUERY

Transaction Hash
0xd25ee7fb6f1150925bfdc7150fea88ec679431bc895353a511b3ac36d1a356ea

查詢交易

QUERY

CLEAR

Query For
Transaction hash0xd25ee7fb6f1150925bfdc71...

Time
2016/06/06 14:04:11

Deposit Account and Bank Code
0x48d2173c4ced56921702cd60699f4d8b926d...

Flow
↓

Deposit Account and Bank Code
0xec61df740330d4af415141b14a7943406172...

Amount
327

Note
Dollars

交易查詢功能

Ethereum 經驗分享-實作案例

1. 此使用者管理介面包含註冊使用者、啟動/凍結使用者、更新使用者、使用者列表、及單一使用者查詢等功能。
2. 此使用者為 Ethereum Blockchain 的交易使用者。
3. Module: userMngr.html

The screenshot shows the userMngr.html interface. It includes a 'User List' section with a table of users, a 'Query User Info' section with a search bar, and an 'Account Address' section with a table of account addresses. Green arrows point to the 'User List', '單一使用者查詢' (Single User Query), and 'Account Address' sections.

User Name	User Identity	User UUID	User Status	User Address
王小明	A123456789	b68fe5c9-874a-4ef2-aaeb-a6f18454368d	Active	0x2a539cd40a3dbbe2e1ea6e5cd1c794428c2d5c
王老明	A987654321	7f53fe1f-3d29-42ed-a243-0c3b7d811e0e	Active	0x4080d6ba0407f4dbd2abf1ce18f32e9192491d70
陳二豐	A321654987	ca41d545-bd88-4e0e-a523-fb40dc8f49	Active	0xc3cf68362e5f5d22384e8d4d7097f61dc9c9da8a1
許建興	N123456789	c15a76cc-1c5d-47b4-a141-dbb49921fa9a	Active	0x98615a832d79bb258c8514b0e4758ca2277708d5
馬克2號	M123456789	961c18dc-53ef-41f3-b3dd-474d84a84a3	Active	0x2076f440215c0ad9e481cf74d2878b21e9d700f

User Identity	User Name	User UUID	User Status	User Address
A123456789	王小明	b68fe5c9-874a-4ef2-aaeb-a6f18454368d	Active	0x2a539cd40a3dbbe2e1ea6e5cd1c794428c2d5c

User Address (trunc.)	Bank Address (trunc.)	Account Address	Bank Account	Account Type	Account Status
0x2a539cd4	0x4d7b57e1	0x17ae98edd4cb0c47989e2bb260780d415ea74	ID_000001	digital	Active

The screenshot shows the userMngr.html interface. It includes a 'Register Users' section with a form for registering a new user, an 'Activate / Inactivate Users' section with a form for activating or deactivating a user, and an 'Update Users' section with a form for updating a user. Green arrows point to the '註冊使用者' (Register User), '啟動/凍結使用者' (Activate/Deactivate User), and '更新使用者' (Update User) sections.

Register Users

User Name: 王大同
Identity: H000000400
Password:
Confirm Password:

Note, the operation will generate a new account in Ethereum

Register Clear

Status: Succeeded

Registered Time: 2016/11/22 12:49:12
Confirmed Time: 2016/11/22 12:49:21

Activate / Inactivate Users

User Identity: H000000400
User Password:

Activate Inactivate Clear

Status: Succeeded

(In)Activated Time: 2016/11/22 12:49:36
Confirmed Time: 2016/11/22 12:49:39

Update Users

User Identity: H000000400
User Password:
User Name: 王小明

Update Clear

Status: Succeeded

Updated Time: 2016/11/22 12:50:09
Confirmed Time: 2016/11/22 12:50:19

Ethereum 經驗分享-實作案例

Register Deposit Accounts

User Identity: H000000400
User Password: *****
Account Type: current
Bank Account: C_000002
Bank Code: 012

Note, the operation will generate a new account in Ethereum

Register Clear

Status: Succeeded

Registered Time: 2016/11/22 12:56:47
Confirmed Time: 2016/11/22 12:56:56

Activate / Inactivate Accounts

Account Address: 0x6b6f0534b27ed1f271c44114fbd1c01616d39e5
User Identity: H000000400
User Password: *****

Activate Inactivate Clear

Status: Succeeded

(In)Activated Time: 2016/11/22 12:57:29
Confirmed Time: 2016/11/22 12:57:46

註冊帳號
(欄位列表)

帳號列表

單一帳號查詢

1. 此帳號管理介面包含註冊帳號、啟動/凍結帳號、帳號列表、及單一帳號查詢等功能。
2. 此帳號代表交易帳號。
3. 相關欄位元素參考左圖。
4. Module: accountMngr.html

Account List

Show Clear

Number of Accounts: 4

Account Address	Bank Account	Account Type	Account Status	Bank Address (trunc.)	User Address (trunc.)
0x17ae98edd4cb0c47989e2bb260780df4154ea74	D_000001	digital	Active	0x4d7b57e1	0x2a539cd4
0x856128973e023ab4b669efcbcfdd7f459a97eb2c	D_000002	digital	Active	0x42cb1514	0x4080d6ba
0x851a68ef850583995c0ba1bef16ecf7c71852000	C_000001	current	Active	0xeebb704	0x5cf8362
0x6b6f0534b27ed1f271c44114fbd1c01616d39e5	C_000002	current	Active	0x42cb1514	0x4c9f859d

Query Account Info

Account Address: 0x6b6f0534b27ed1f271c44114fbd1c01616d39e5
Query Clear

Query for: Account 0x6b6f0534b27ed1f271c44114fbd1c01616d39e5

Account Address	Bank Account	Account Type	Account Status	Bank Address (trunc.)	User Address (trunc.)
0x6b6f0534b27ed1f271c44114fbd1c01616d39e5	C_000002	current	Active	0x42cb1514	0x4c9f859d

Ethereum 經驗分享-實作案例

1. 傳送交易管理介面包含傳送交易、交易列表、結算、及單一交易查詢。
2. 相關欄位元素參考右圖。
3. Module: txMngr.html

Perform Clearing

Since Date

To Date

Bank Code

Show Clear

Status: Ready

Bank Code	Flow	Bank Code	Amount
-----------	------	-----------	--------

Query Transaction Info

Transaction Hash

Query Clear

Send Transactions

Sender Account Address

Sender Identity

Sender Password

Receiver Account Address

Amount

Note

Send Clear

Status: Succeeded

Transaction Hash 0xdccdfab948f1e40c806784416d3d8e0f258a685ff63e4595019b258c2bc975d

Sent Time 2016/11/24 09:51:05

Confirmed Time 2016/11/24 09:51:19

Transaction List

Since Date 11/03/2016

To Date 11/24/2016

User Identity A123456789

Show Clear

Timer: 2 sec

Status: User Identity A123456789

Number of Transactions: 3

Time	Deposit Account and Bank Code	Flow	Deposit Account and Bank Code	Amount	Note
2016/11/17 08:59:56	0x17ae98eddd4cb0c47989e2bb260780df4154ea74, 005	-->	0x856128973e023ab4b669e1c6f7459a97eb2c, 012	100	Webman
2016/11/24 09:51:10	0x17ae98eddd4cb0c47989e2bb260780df4154ea74, 005	-->	0x851a68ef850583995c0ba1bef16ecf7c71852000, 017	100	Transaction Testing
2016/11/24 10:12:06	0x17ae98eddd4cb0c47989e2bb260780df4154ea74, 005	-->	0x856128973e023ab4b669e1c6f7459a97eb2c, 012	85	Testing Transaction

共識機制

- Consensus mechanism:

- **POW**: weight of vote determined by computational resource spent
- **Proof of Stake (POS)**: variant of POW in which difficulty of a miner is inversely proportional to the miner's stake
- **Delegate-based POS**: variant of POW in which a generated block needs to be further confirmed by multiple “delegate” participant nodes, where nodes with higher stakes are more likely to be chosen as delegates.
- **Deposit-based POS**: A miner needs to make a deposit for being a miner, and the deposit will be confiscated if it partakes in an attack against the system.
- **Quorum / PBFT**: Practical Byzantine Fault Tolerance algorithm, which provides high-performance Byzantine state machine replication, processing thousands of requests per second with sub-millisecond increases in latency.

閃電網路

- 在public chain中閃電網路的概念亦為近來被探討可解決效能問題的技術：
- ✓ 閃電網絡是基於**鏈下交易**達成的，不需將所有交易皆記錄於blockchain中，可將多筆交易紀錄整合成單一筆交易再上傳至blockchain
- ✓ 微支付通道：達成鏈下交易的一種方式，也是解決巨量交易最重要的部份，主要應用在小額交易上。
- ✓ 交易方將貨幣皆存放於通道內，每有一筆交易皆會更新通道內交易方資產額，隨著多筆交易進行資產額也隨之更新；通道關閉時，交易方領回貨幣並將最後的資產狀態上傳至blockchain。

計畫目標

- 強化實名認證：透過特定認證之Token傳遞以及加密機制採用，使用者即可確認雙方身分，實體身分資訊可連結政府戶政資訊抑或是與自然人憑證服務整合均可。
- 權限控管：完成鏈上參與節點的權限控管機制，可針對不同目的的節點給予相對應的權限，可設定任意節點皆可連線進入區塊鏈並發出交易請求，未經授權的任意節點皆無法做認證，從基本上阻斷了51%攻擊，讓聯盟鏈中的區塊資料也能安全的守護。
- 及時通知：讓服務供應者能及時且主動的通知使用者，避免由後台伺服器不間斷的去查詢區塊鏈，提供一種基於區塊鏈本身的過濾機制，整合後台通知服務，讓使用者能獲得及時的通知。

計畫目標

- ❑ 區塊鏈底層舞弊與攻擊偵測：針對區塊鏈底層多種類型的舞弊與攻擊偵測與分析，有效識別並預防舞弊或攻擊擴大與損失。
- ❑ 改善共識機制：將透過修改共識機制，獲得一個高效且具備容錯能力的區塊鏈系統。
- ❑ 確保交易和使用者的隱私：支援交易內容隱藏，非交易雙方無法得知交易內容，保障使用者隱私權。
- ❑ 強化應用層資料正確性：區塊鏈保障了鏈上資料不被竄改，但無法防止不正確的資料被寫入區塊鏈，將設計應用層寫入資料的雙向確認與簽章機制，以降低寫入錯誤資料的機率，並可做為資料正確性發生爭議時的證據。

計畫目標

- ❑ 應用層之詐欺交易偵測：對應用服務的交易紀錄與交易紀錄產生的樣式進行分析以察覺詐欺交易。
- ❑ 服務資料監管：透過服務監控系統所蒐集到的各類原始資料，設計作為法規監管上之分析基礎，透過採用事件指紋碼比對或是群集事件特徵等手段，規劃可回報自訂特定事件，如設定洗錢模板事件，藉此增強應用面服務運行之各類特殊事件需求支援。
- ❑ 節點資源監控：監控各類區塊鏈應用所需的節點營運管理、資源使用狀況、問題回報服務以及計費服務等，都可透過統一介面來管理。
- ❑ 智能合約開發與漏洞偵測工具：提供便利的智能合約發展環境，降低區塊鏈應用開發門檻。

結論

- ❑ 比特幣蓬勃發展並廣為人知，但作為第一代blockchain，其交易量與擴充性已無法應付目前各種需求
- ❑ Ethereum作為次世代blockchain有著各種優點，但其public chain在某些應用上限制仍多，因此可採用其consortium chain
- ❑ ICL在blockchain上有足夠的經驗，具備效能、反應速度、安全、並能根據各種不同需求來發展智能合約，以及中介層

謝謝大家!