

台大資管系

從比特幣，區塊鏈 到首次代幣發行(ICO)

Initial Coin Offerings

陳 恭

政大金融科技研究中心副主任

政大資科系教授

2018/06/01

緣起：比特幣的創新與影響

2009
上線

Bitcoin: A Peer-to-Peer Electronic Cash System

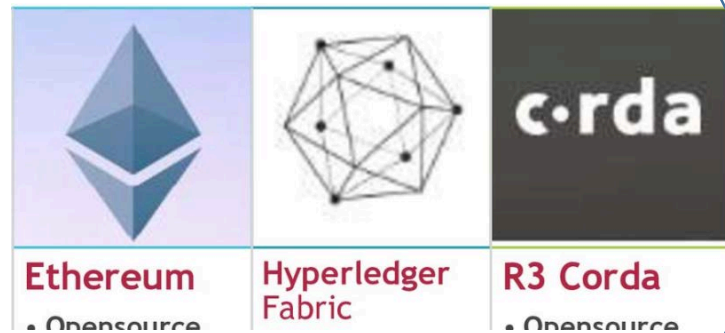
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Crypto-currencies 幣圈



Blockchains 鏈圈

ICO



Outline

- 一、比特幣回顧：密碼貨幣知多少
- 二、區塊鏈的發展與應用
- 三、首次代幣發行(ICO)

比特幣的創新



1. 從密碼貨幣談起 (Crypto-currencies)

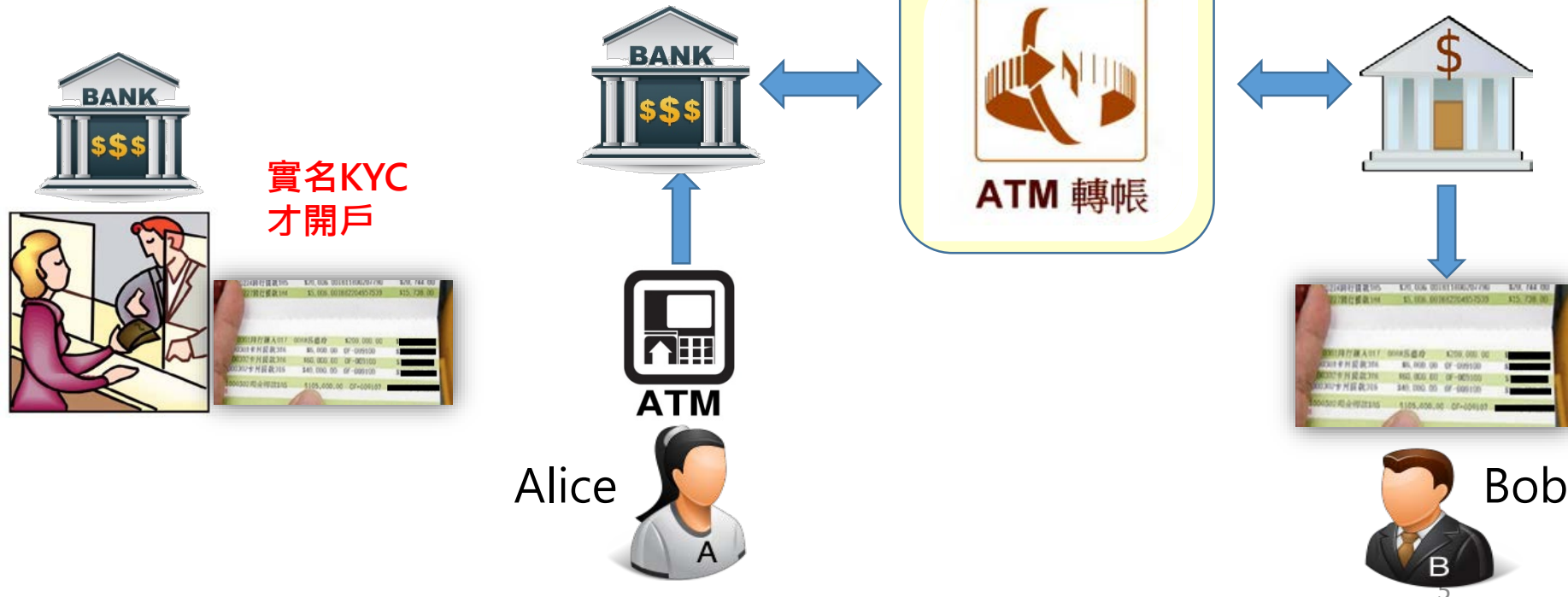
第一個密碼貨幣: 比特幣Bitcoin

從現況看比特幣的創新 (1/4)

● 銀行提供

- 帳戶與身份識別管理
- 金流服務
- 帳簿記錄(record/ledger)
- 信任 (專業與政府監管)

- 搭配許多金融市場基礎設施 (FMI中介)
 - 財金，證交，...



從現況看比特幣的創新 (2/4)

- Bitcoin is a **Crypto-currency** : cryptography + currency
- 密碼貨幣：採用公私鑰技術，安全哈希函數
- 不依託任何實物(黃金、白銀或是法償貨幣等)
- 也不是由一個獨立的發行機構發行，
- 是使用密碼學技術來創建，在網路上發行和交易的數位虛擬貨幣(通貨)。

圖 3 數位通貨分類

Source: 央行



比特幣的創新 (3/4)



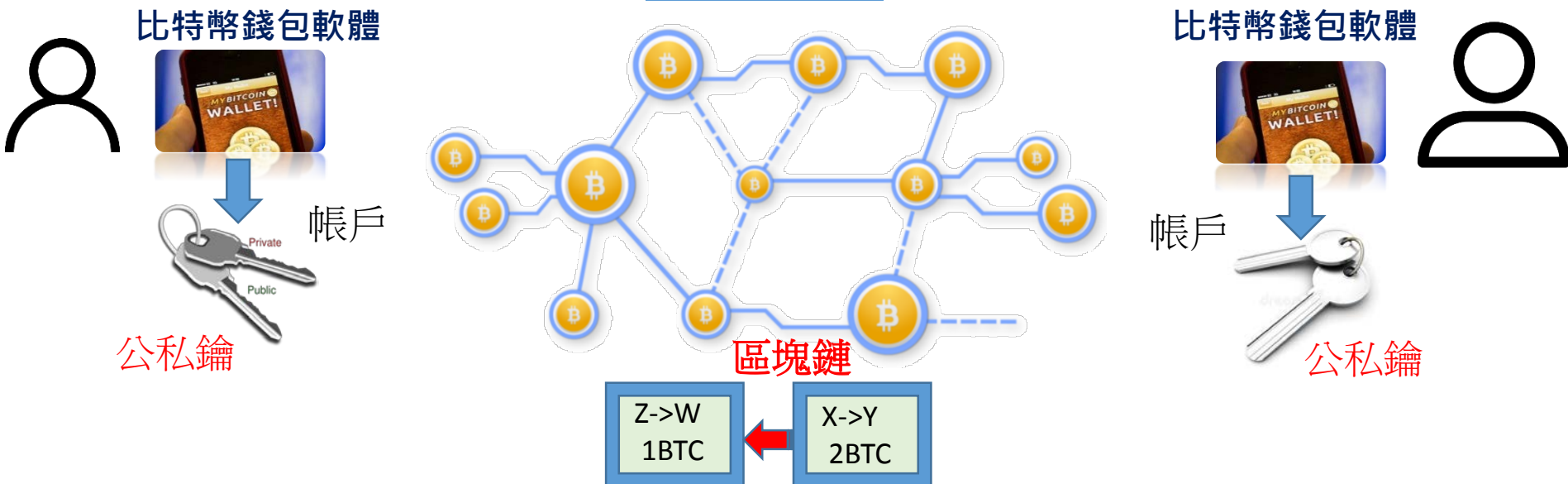
bitcoin

Be Your Own Bank

基於密碼學原理
的數位貨幣

- 身份識別 → 公鑰
- 帳戶 → Hashed value
[3AWzFFySuZux2Az8MZxZaTck8mJdZ1bRmD](#)
- 金流服務 → 私鑰
- 帳簿記錄 → 區塊鏈

比特幣網路

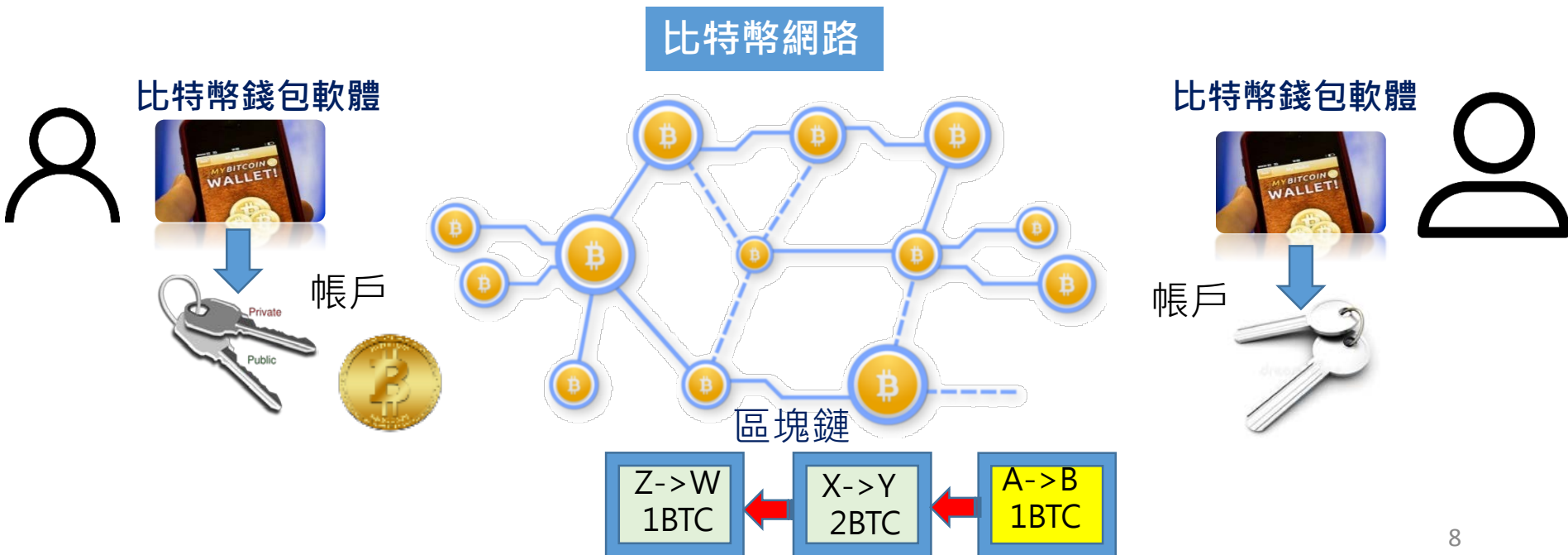


比特幣的創新 (4/4)

- 身份識別 → 公鑰
- 帳戶 → Hashed value
[3AWzFFySuZux2Az8MZxZaTCk8mJdZ1bRmD](#)
- 金流服務 → 私鑰
- 帳簿記錄 → 區塊鏈
- 信任 → 毋需中間人, 也無監管

兩造之間
直接轉帳

- In Bitcoin, We Trust

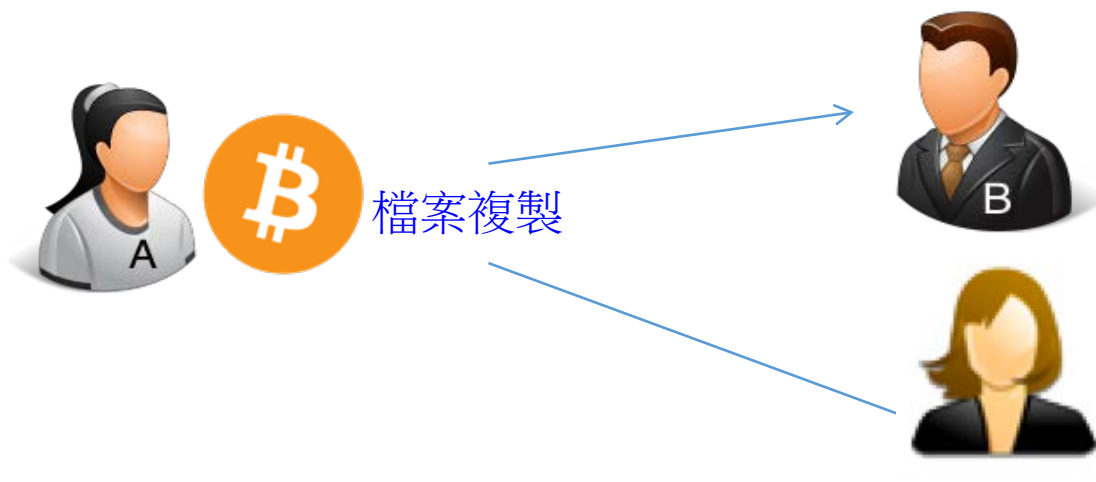


比特幣的主要貢獻：解決數位貨幣難題

- Ownership--誰的錢



- 無中心機構又可確保不會雙重支付 (double spending)



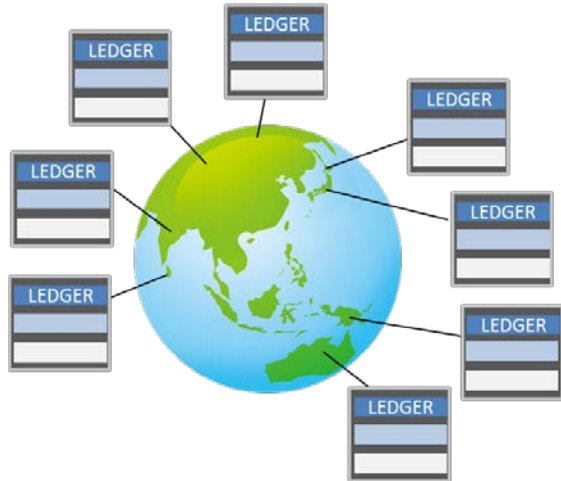
比特幣的創新利器：區塊鏈

In Blockchain, We Trust

區塊鏈：分散式共享帳簿



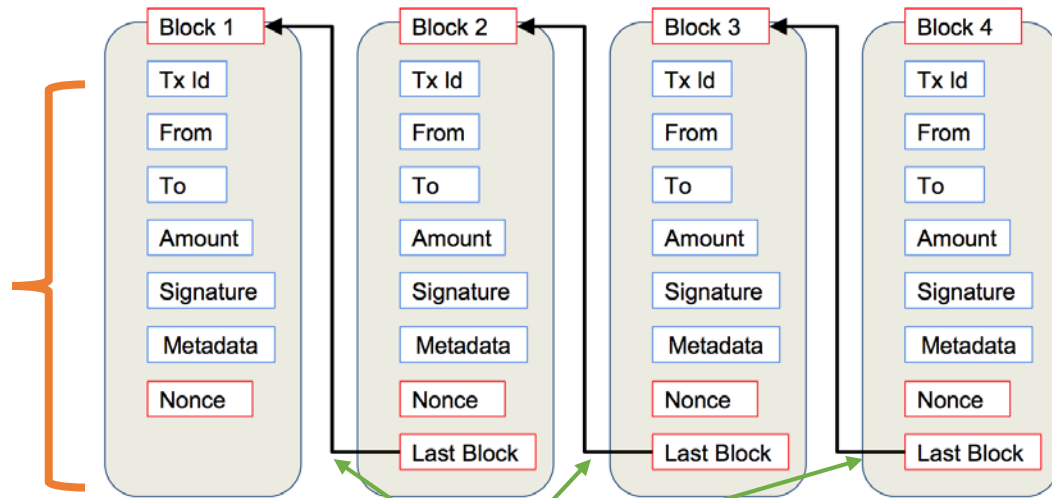
分布全球的比特幣網路



- 區塊鏈是比特幣的**共享帳簿**：所有交易記錄以區塊鏈形式存放在其網路中的每個節點。

區塊鏈 = 區塊 + 鏈

from	to	amount
1b874A...	16BZZe8...	1.0
167sdu...	13kjhfg...	15.0
1lkj382S	1238fhdj...	6.0
1398fda...	1lkj382S...	500.0
1348dd...	1SD48sd...	34.0
1354sd...	13kjhfg...	1.0
148958...	1asdytrr...	0.0001
1598fjk...	154gkeR...	3.0
13kjhfg...	16BZZe8...	2.0
167sdu...	1487djhk...	5.0
13kjhfg...	1238fhdj...	2445.0



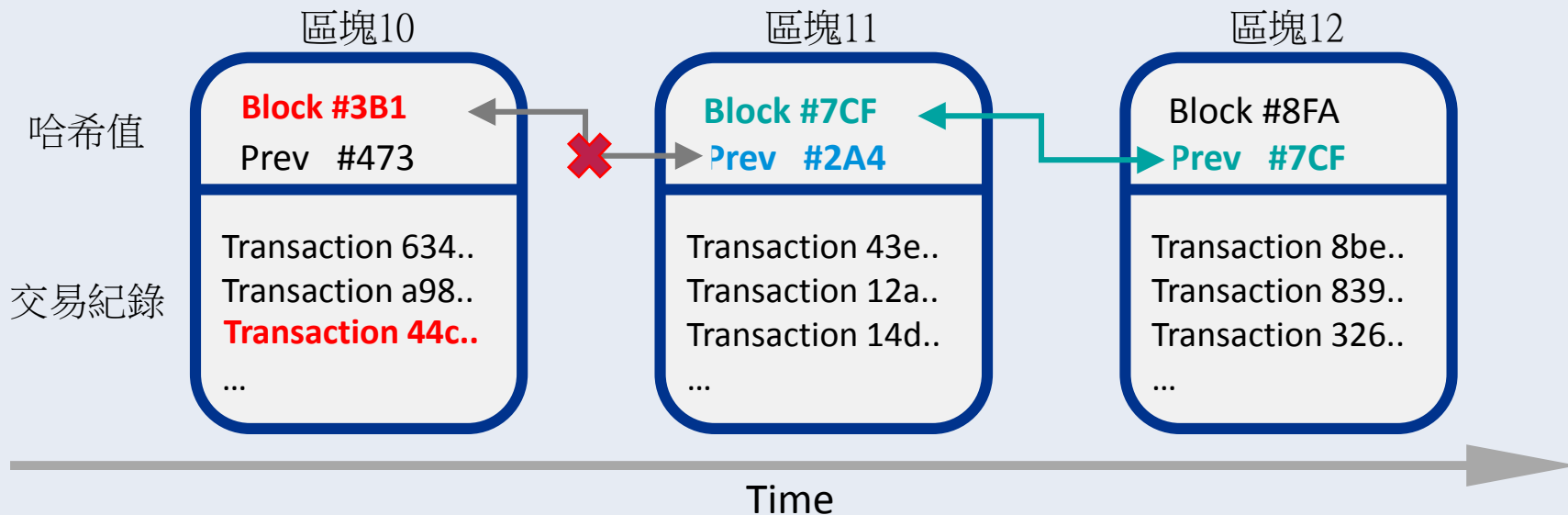
- 特殊的(基於密碼學)鏈 1

區塊：
由支付交易紀錄構成

區塊鏈內資料 (帳簿) 不能塗改

安全哈希函數：SHA() = 一串獨一無二，不可逆的英文數字串 (哈希值)

- 每個區塊皆有獨一無二的流水號及哈希值(hash)
- 區塊Header會紀錄前一個區塊的哈希值，並包含最新的交易紀錄
- 由於存在鍵連關係，修改區塊內的交易內容，就會改變區塊的哈希值，而被發現



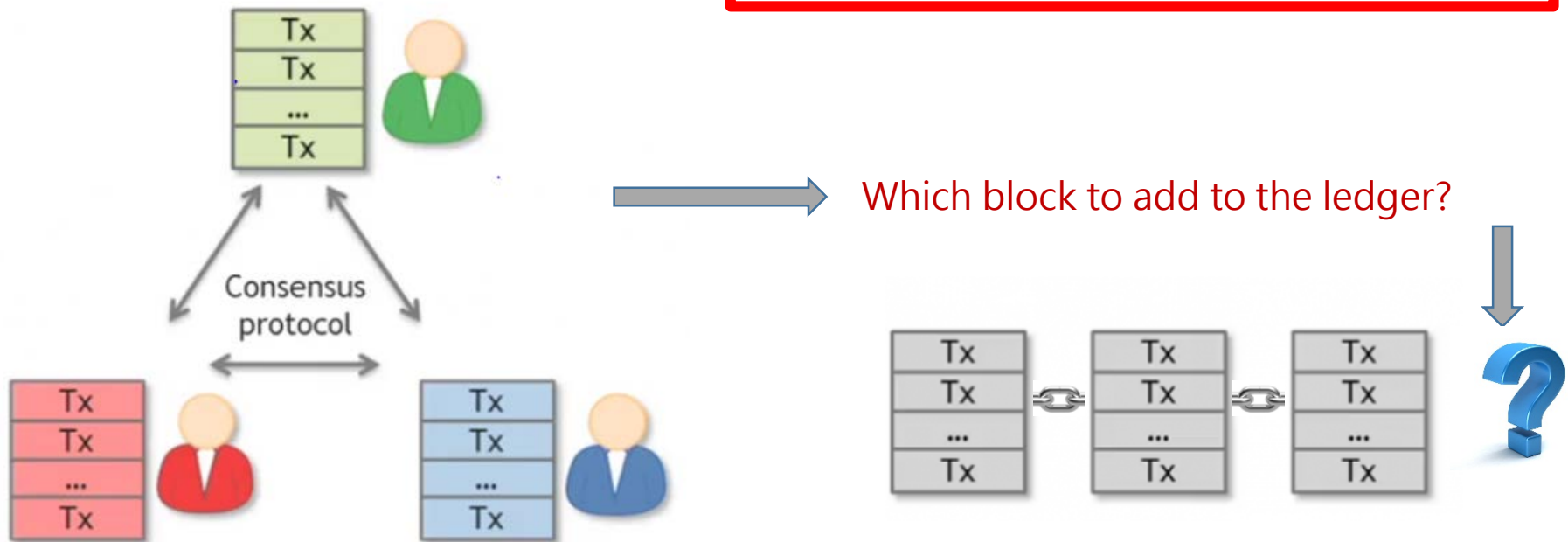
- 帳簿紀錄交易內容: 只能新增，不能修改歷史紀錄

共識記帳 (Consensus)

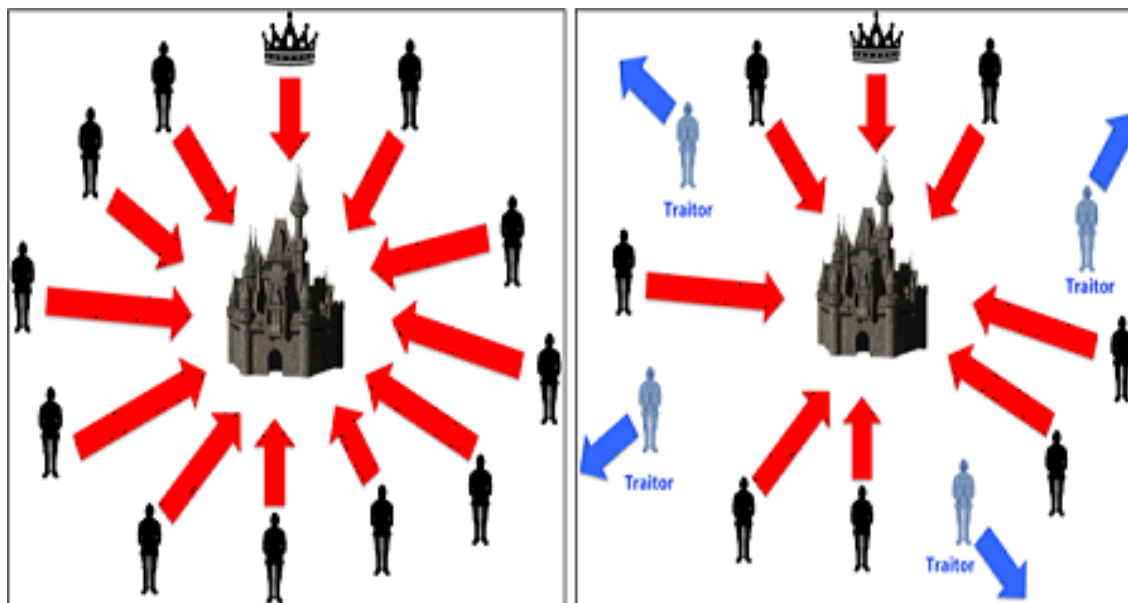
- 區塊鏈網路中的各個節點，透過一個分散式的共識過程來記帳。

Not all nodes are trust-worthy.

"A blockchain based system is as secure and robust as its consensus model."

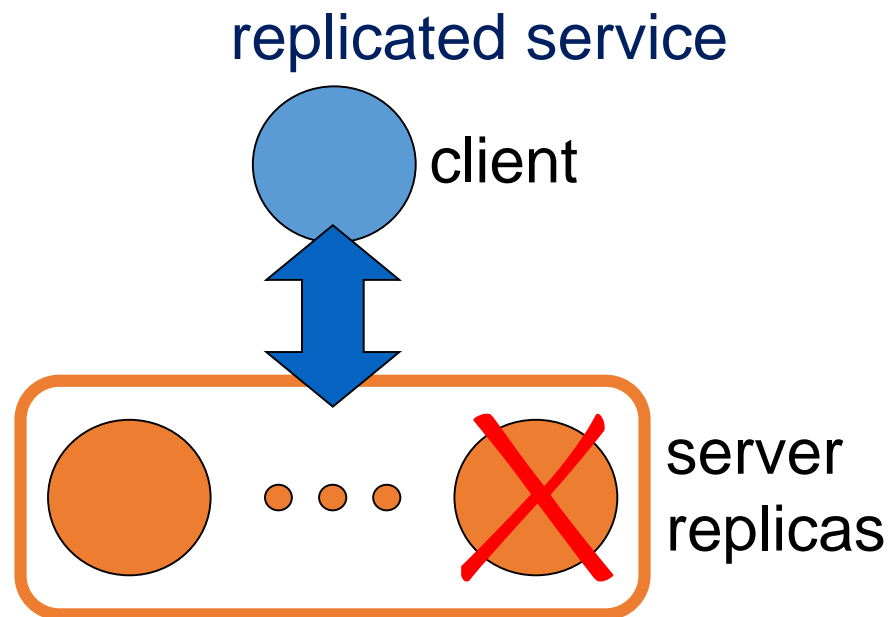


- 分散式系統的古典問題：拜占庭大將軍(Byzantine generals)
- 拜占庭聯軍：彼此不信任，如何取得進攻或撤退的共識？



BFT分散式共識演算法

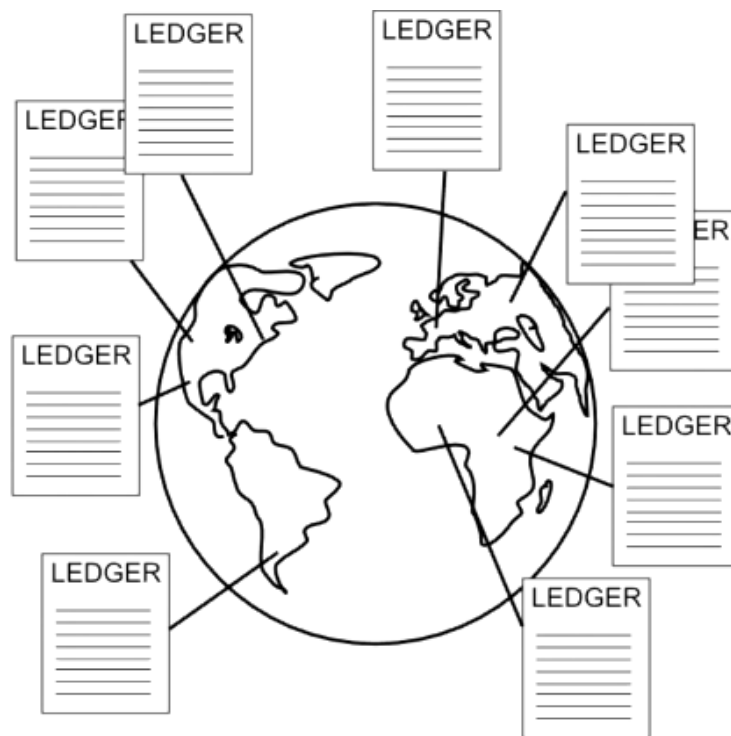
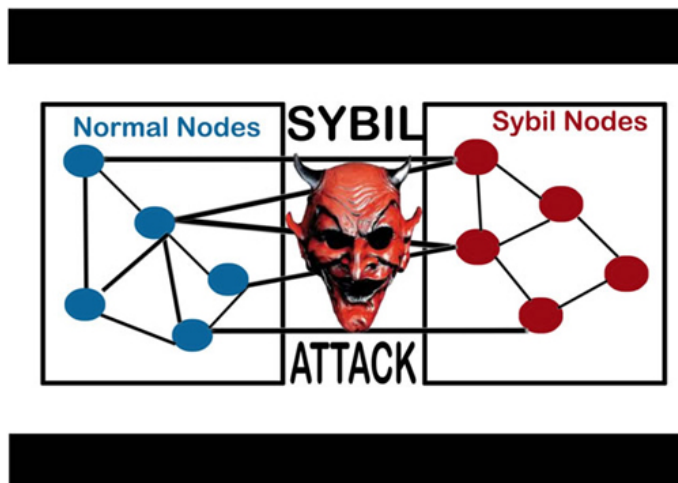
- In general, no solutions with fewer than $3f+1$ generals can cope with f traitors.
- Practical Byzantine Fault Tolerance (PBFT)
 - 1999 Castro and Liskov
 - 效能好，但延展性差
 - 節點數(replicas) <100



比特幣帳本共識的挑戰

- 要在成千上萬個網際網路的節點間，達成對帳本的共識
- 要面對**女巫攻擊(Sybil attack)**的可能性

• **設定成本門檻：參與共識投票 要付出電腦計算資源**



<https://www.searchenginegenie.com/101-articles/Sybil-attack.html>

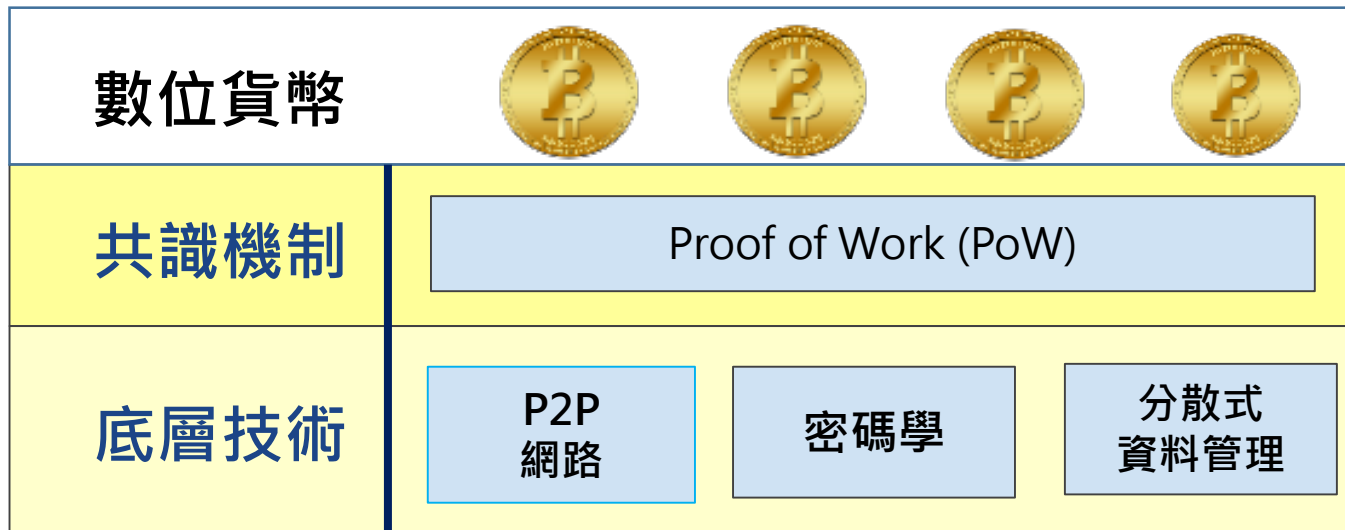
小結：比特幣區塊鏈

每筆交易交由集體共識後，記入各自的區塊鏈帳本中，帳本內容不能竄改

共識機制
Consensus

P2P分散式網路與資料庫

密碼學技術
Cryptography



一、比特幣

二、區塊鏈發展與應用

三、ICO

1. 提供智能合約設施，發展區塊鏈多元應用
2. 從公有鏈邁向企業應用之私有與聯盟鏈

1. Scalability

- Transactions peed
- Data storage growth
- Security and privacy
- ...

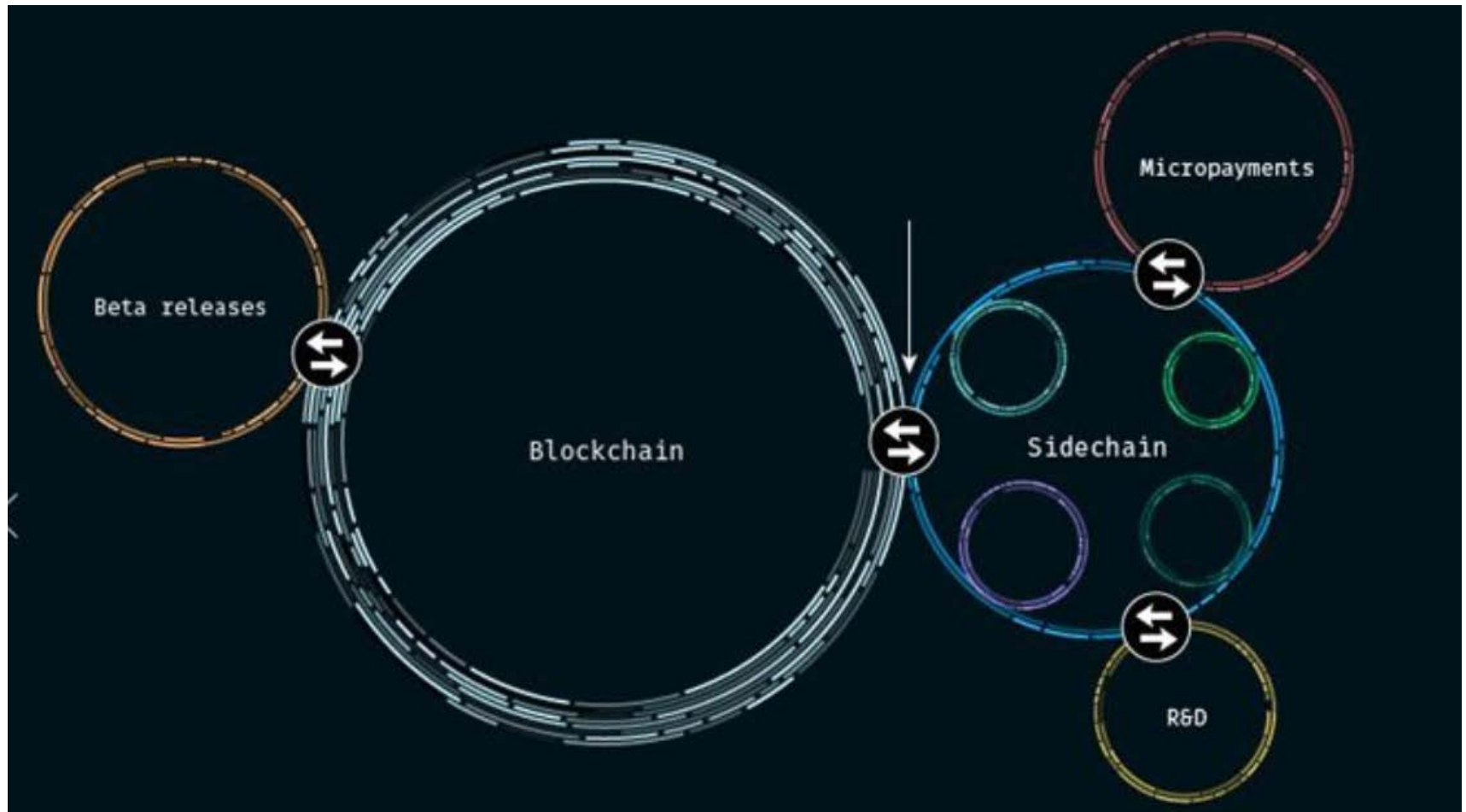
2. Blockchain as a Platform: Smart contracts

3. Enterprise Blockchains...

4. ...

Scalability: many proposals

- Public blockchain: State channels, Side-chains, ...



2.1 智能合約 (Smart Contracts)

從比特幣到以太坊(Ethereum)

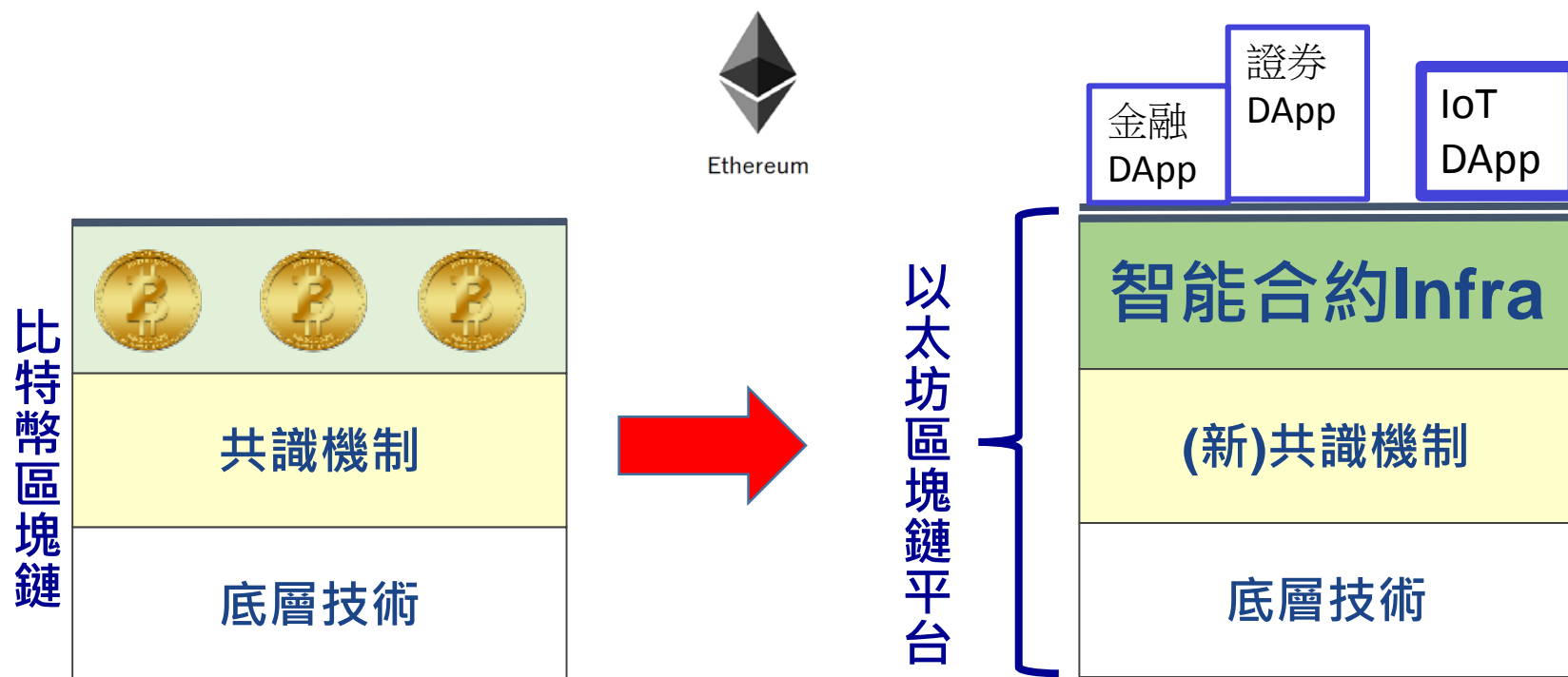


Ethereum



智能合約：以太坊區塊鏈平台

- 以太坊區塊鏈提供支援通用的運算邏輯(智能合約)，可以發展多元應用 (Decentralized App)
- 也提供密碼貨幣Ether(以太幣ETH)



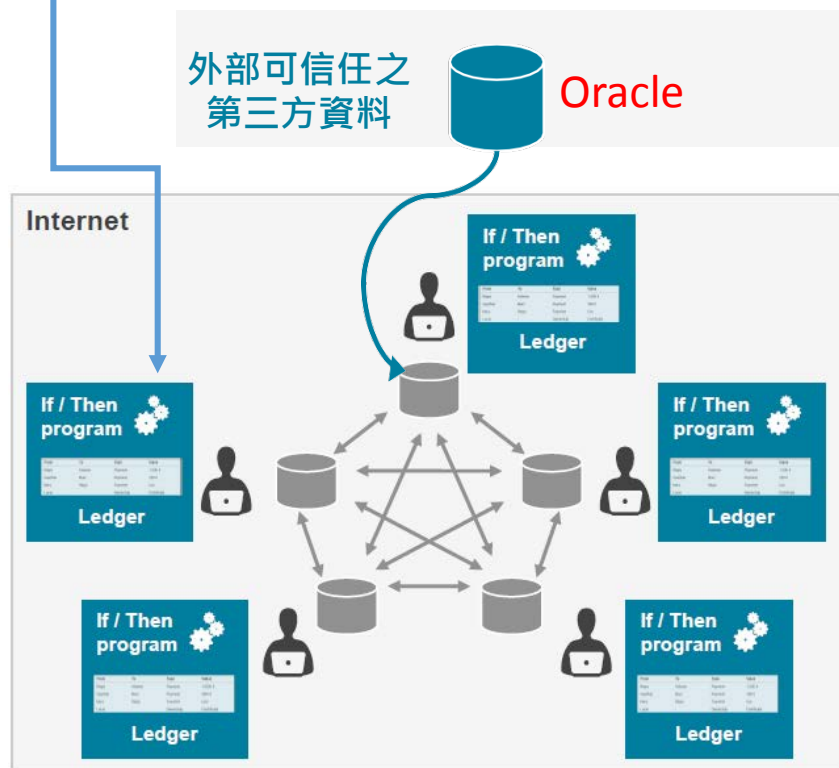
智能合約的運作

開發與部署



● 智能合約

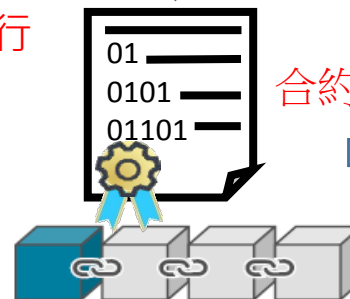
- 部署並執行於區塊鏈式的應用程式
- 事件觸發，自動執行
- 常需要外部可信賴資料源



事件驅動



觸發
智能合約
執行



合約條款判斷

資產移轉



2.2 企業區塊鏈平台

- 限定區塊鏈網路之參與成員
 - 實名制
 - 權限管控
- 高效能共識機制
- 交易隱私保護

2018 GSS Solution Day

Digital Workplace 再進化

AI
Blockchain

Cloud

Security

深入談

公有鏈 (原生虛擬貨幣)

- 結點數多，無信任假設
- 共識費時費力 (e.g. 挖礦)
- 共識結果有分叉可能
- 可匿名使用
- 交易內容公開
無監理

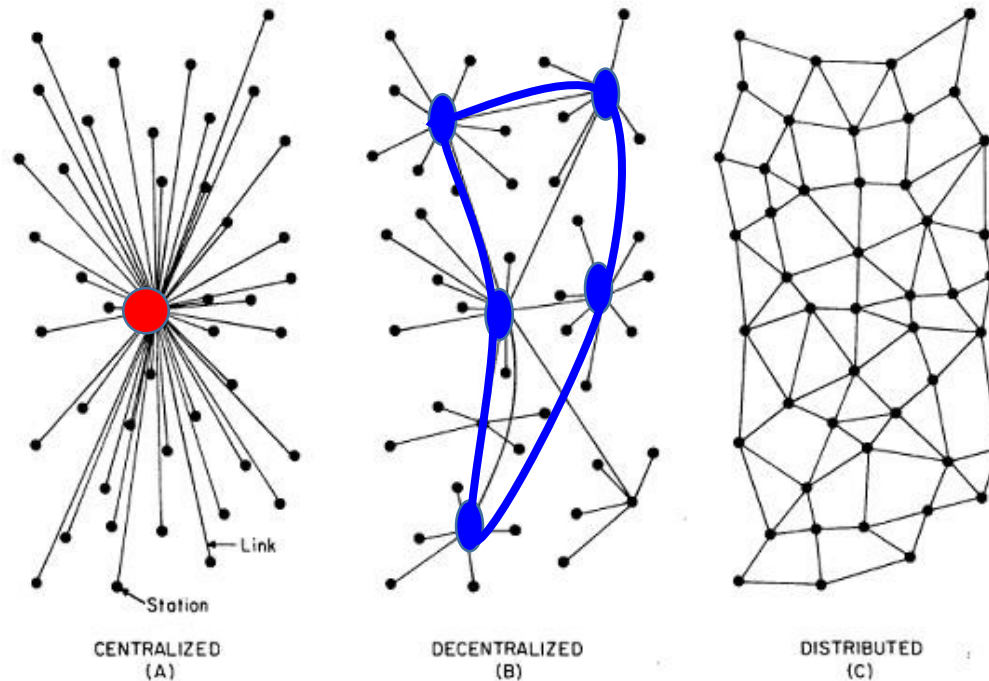
私有鏈/聯盟鏈 (無虛擬貨幣)

- 結點數少，有信任假設
- 高效能共識
- 共識結果確定性
- 實名制
- 交易內容需隱私保護
有監理要求

聯盟鏈 (Consortium Blockchain)

Private Shared Ledger

- 聯盟鏈：沒有一個強大的中心，而是多個組織(公司)共同制定規則，聯合運作



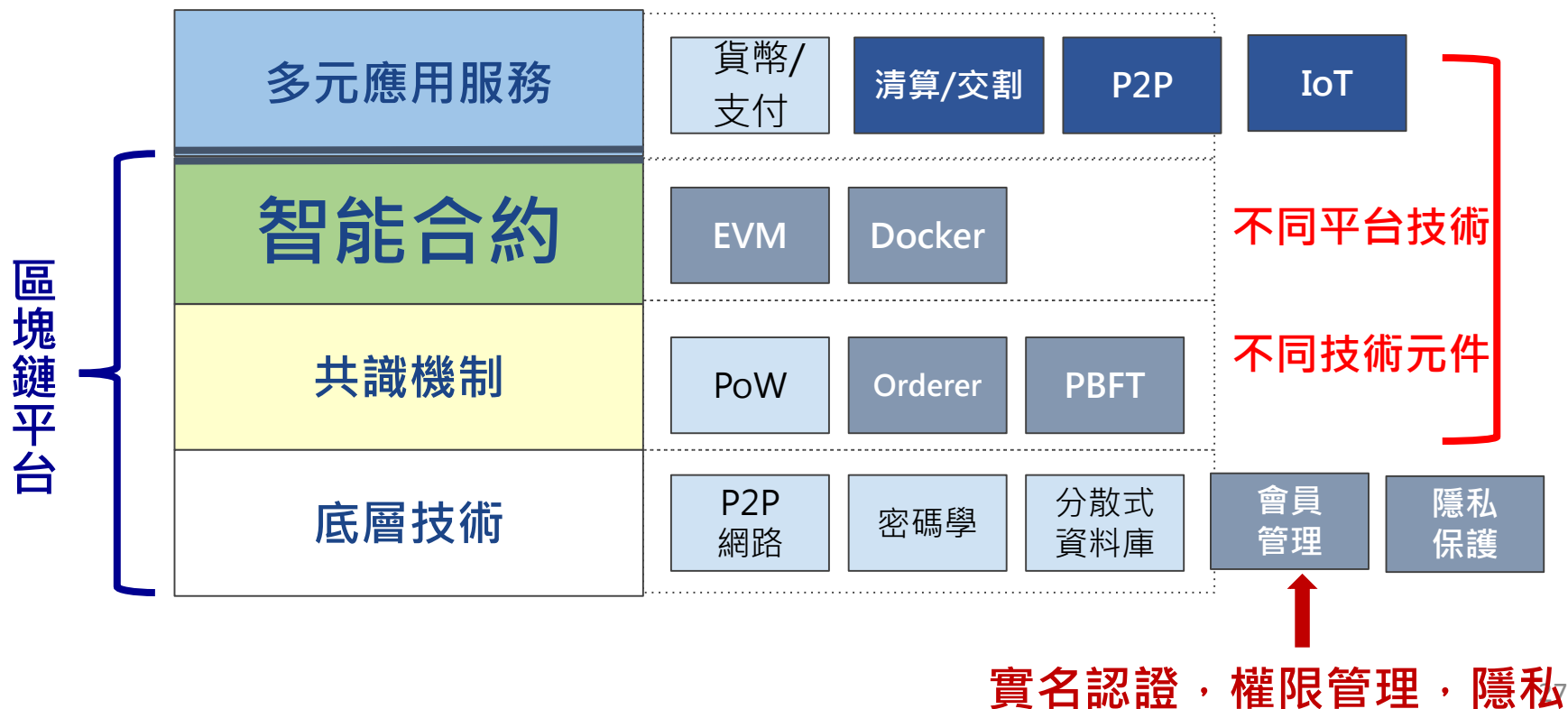
傳統中心制

聯盟鏈
(B2B2C)

公有鏈，P2P

企業區塊鏈平台技術趨勢與挑戰

- 高效能共識，會員權限管理，資料隱私保護
- 延展性挑戰，效能提升
- 跨鏈整合標準與機制
- 監理實務



三個知名企業區塊鏈平台



- Quorum：基於以太坊
- JP Morgan 投資開發
- 支援交易加密，保護隱私
- 分散式高效能共識(RAFT, BFT)
- 企業以太坊聯盟(EEA)



- Fabric：Hyperledger基金會
- IBM創始開發，主要推手
- V0.6 到1.0改版大
 - 以交易通道保護隱私，複雜又彈性低
 - PBFT共識改為 Execute-Order-Validate 共識，效能高



- R3：金融機構為主之聯盟
- 高會費，較封閉
- Corda平台：
 - 獨特分散式帳簿技術(DLT)
 - 交易對手導向之資料分享
 - 趨中心化之共識機制
 - 交易效能中等

2.3 區塊鏈智能合約 應用範例

- Record Keeping & Provenance (溯源)
- Digital Assets Management

2018 GSS Solution Day

Digital Workplace 再進化

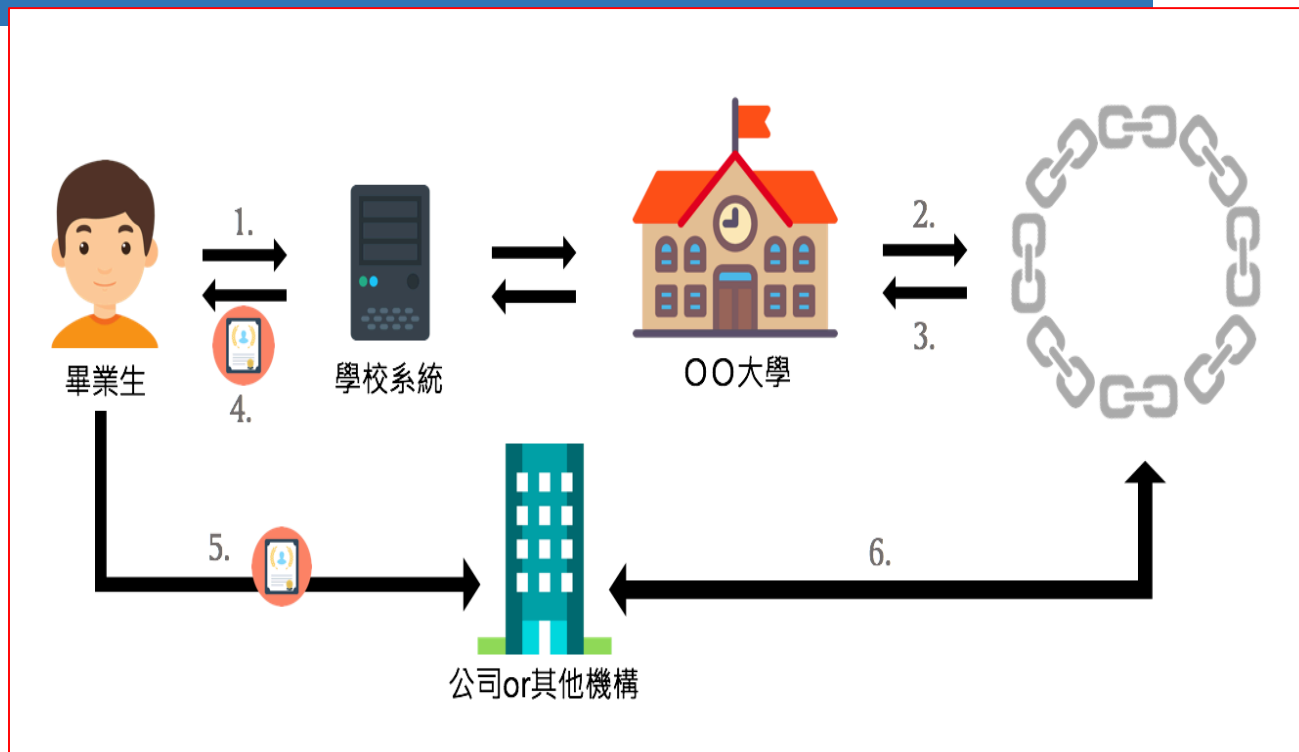
AI
Blockchain

Cloud

Security

深入談

範例：學歷或各種成就證明



1. 畢業生畢業時向學校的資訊系統申請畢業證書，學校相關單位進行審查
2. 在確認該學生符合畢業資格後，系統將學生畢業相關資料紀錄，以安全哈希值方式紀錄於區塊鏈上
3. 同時取得此筆紀錄在區塊鏈上的交易序號，然後透過資訊系統製作一份電子畢業證書給該畢業生
4. 電子畢業證書上紀錄著該生的學歷資料，以及那個獨一無二的交易序號
5. 當該畢業生報考國家考試或應徵工作時，可將此電子證書上傳給考試院或求職公司
6. 考試院或公司機構就可據其證書的交易序號，到區塊鏈上查詢此證書的真偽

範例：數位資產的管理

- 在區塊鏈上發行數位資產，例如紅利點數

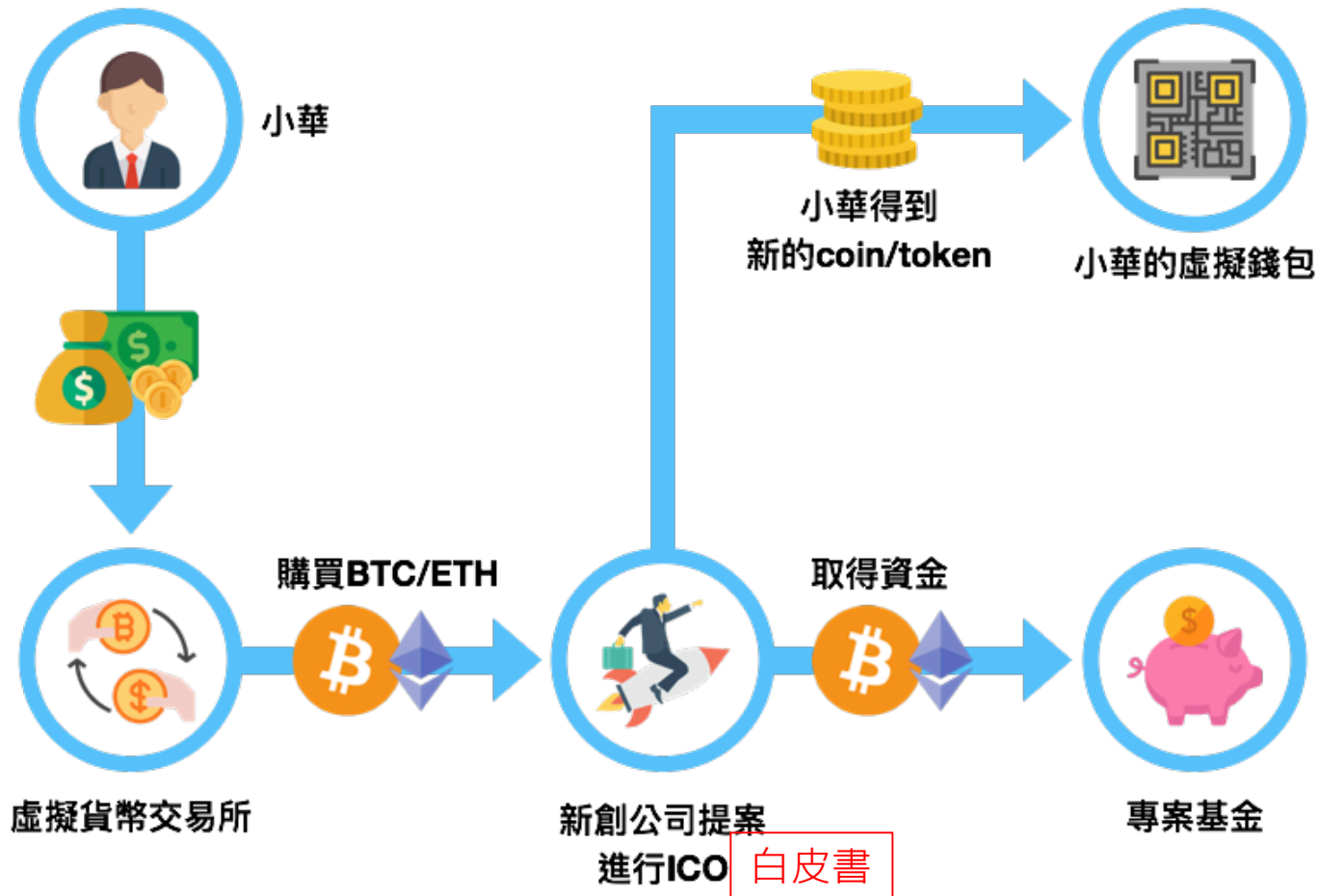


2. Initial Coin Offerings (ICO)

區塊鏈殺手級應用？

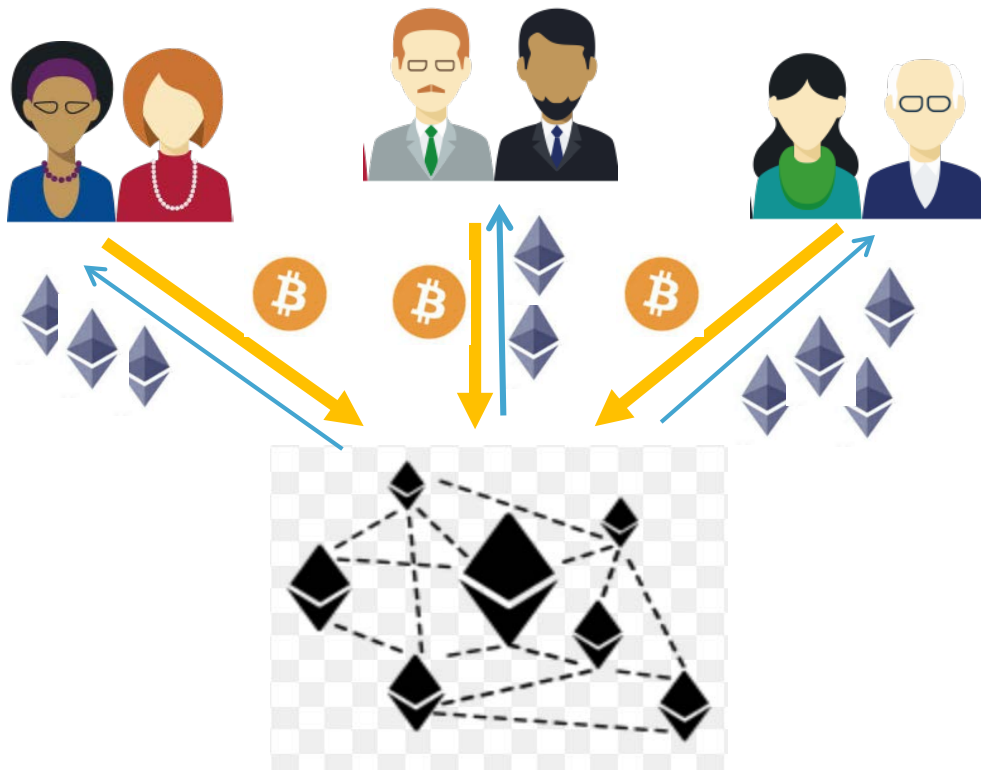
Initial Coin Offering (ICO)

- 一種新型態的網路群眾募資 (crowdfunding)
- IPO發行股票，ICO發行新的coin/token



Initial Coin Offering (ICO)

- 史上經典案例：以太坊(Ethereum)
 - 籌措資金開發以太坊區塊鏈
 - 用預鑄的 ETH(以太幣) 換 比特幣 (2000:1開始，結束時1337:1)
 - 在42天內便募集了3萬多個比特幣，當時價值約當1,700多萬美元



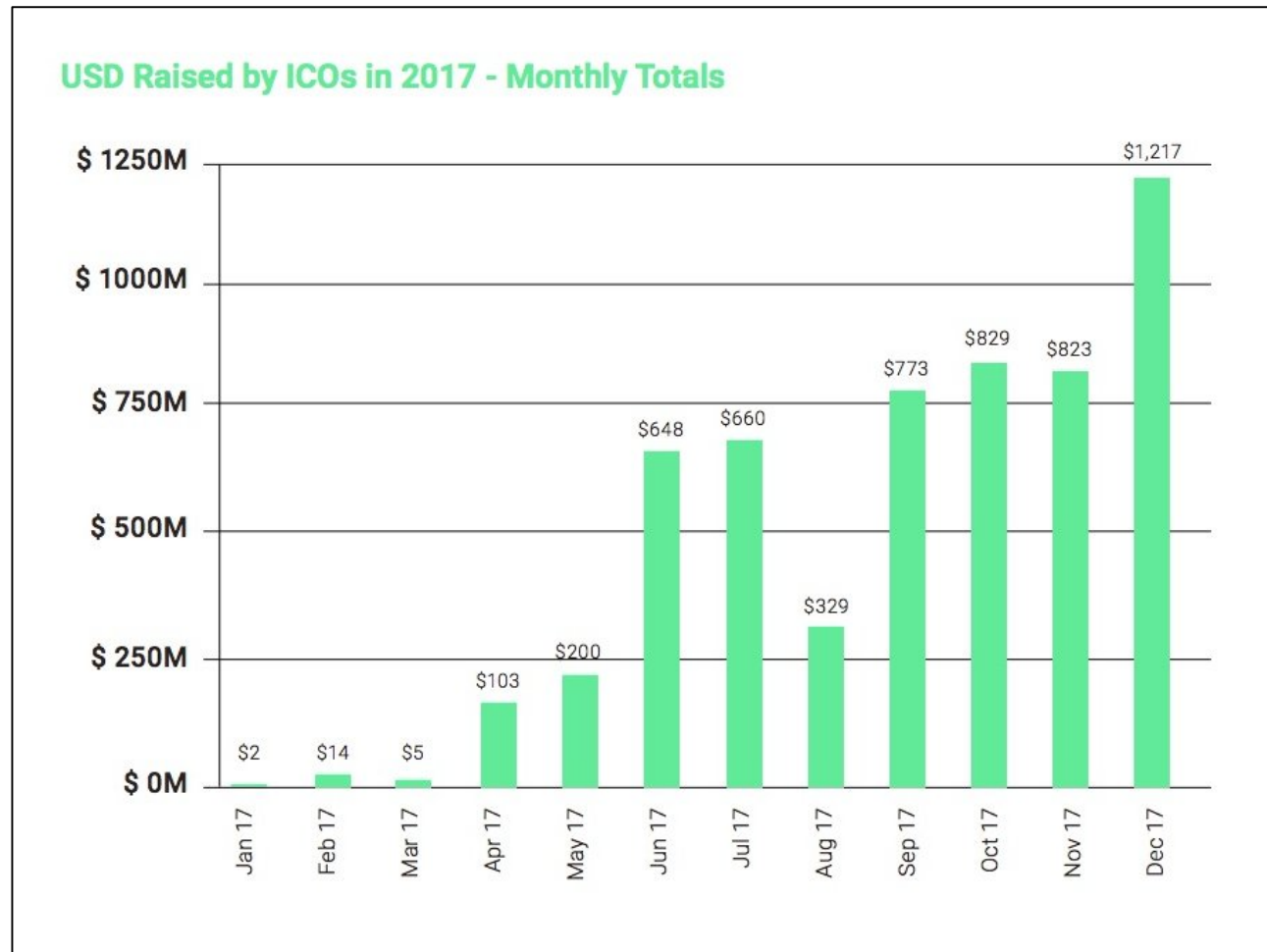
- 發行以太幣建構以太坊生態系
- 使用以太坊必須有以太幣

- 目前
比特幣：以太幣 = 12:1
- 漲幅超過100倍

- 區塊鏈產品或服務發想→白皮書與團隊介紹
- 規劃**token sale**
 - 數量上限 或是 限定期間
 - 私募 與 公募
 - 發行量目標：
 - 上限(hard cap)：發行上限
 - 下限(soft cap)：未達此目標會退回所募得coins
 - 一次性或多輪
 - 定價：發行之兌率？
 - 募得資金之分配比例
- 設計網站與行銷活動進行募資

2017 : Year of ICO

- 2017 is the year of ICO: 435 projects, total capital **\$5.6 billion**, 12.7 million in average



Why? ICO大幅成長的原因

- 從創業者、投資者與技術平台三方來分析
 - **創業者**：ICO可直接訴諸投資人，免除中間機構的審核；在創業初期，**透過產品白皮書的資訊，便就快速取得投資者資金**，此讓ICO比起其它籌資管道有明顯的優勢。
 - **投資者**：ICO 均以虛擬貨幣發行代幣，由於比特幣與以太幣對美元的兌率近期持續上漲，帶動了投資者對虛擬貨幣的無限想像，**短期市場 (Cryptocurrencies exchange) 上流通性高**，暫無漲跌幅的限制，也自然獲得眾多投資蜂擁地投入ICO的市場。
 - **技術平台**：以太坊提供 ERC-20, ERC-223, ERC-721的token 標準智能合約介面與範例，**大幅降低token發行的技術門檻**。
(絕大多數的ICO都是採用ERC-20)

- 初級市場的爆量成長
 - 上千種的Tokens在網路上發行
- 帶動次級市場：虛擬貨幣交易所 (Exchange) 的成長

Crypto-currencies 幣圈



















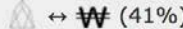
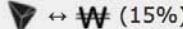
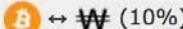















世界前6大虛擬貨幣交易所 (2018/5/24)



BnB



#	Name	Region	Total Vol. 24h	Fee	Fiat money	Pairs	Top pairs by volume	Features
1	 BitMEX		565,445.59 BTC	-0.05%/-0.025% (Maker) 0.075%/0.25% (Taker)		10	 (98%)  (0%)  (0%)	Futures contract (100x leverage), Stop Limit
2	 BINANCE		232,200.49 BTC	0.1%		321	 (18%)  (8%)  (6%)	
3	 BITFINEX		140,215.35 BTC	0%-0.1% (Maker) 0.1%-0.2% (Taker)	\$ € 	192	 (29%)  (22%)  (17%)	Margin trading, BitGo Instant
4	 bithumb		83,541.93 BTC	0%-0.15%	₩	29	 (41%)  (15%)  (10%)	
5	 GDAX		49,069.15 BTC	0% (Maker) 0.1%-0.25% (Taker)	\$ £ C\$ € 	12	 (32%)  (31%)  (11%)	Margin trading, Stop orders, API sandbox
6	 HitBTC		42,416.12 BTC	0.01% (passive) 0.1% (active)	€  	743	 (23%)  (14%)  (11%)	Add token

知名虛擬貨幣交易所Binance 幣安



\$2,361,353,943 USD
292,415 BTC

2018/04



交易中心

Labs

LaunchPad

Info

加入我們

幫助中心

公告中心

登錄 或 註冊

繁體中文

QLC Competition Has Now Concluded (04-08)

Binance Has Distributed March GAS (NEO) (04-06)

Binance Delists Centra (CTR) Token (04-05)

BNB / BTC

Binance Coin

最新價
0.0016047 \$12.99

24h漲跌
-0.0000360 -2.19%

24h最高價
0.0016823

24h最低價
0.0015771

24h成交量
4,618.21 BTC

價格(BTC)	數量(BNB)	成交金額(BTC)
0.0016073	45.00	0.07232850
0.0016070	160.00	0.25712000
0.0016069	10.10	0.01622969
0.0016068	27.40	0.04402632
0.0016066	37.51	0.06026357
0.0016065	184.09	0.29574059
0.0016062	12.30	0.01975626
0.0016061	105.89	0.17006993
0.0016060	95.56	0.15346936
0.0016058	4.14	0.00664801
0.0016057	84.42	0.13555319
0.0016056	14.35	0.02304036
0.0016055	40.49	0.06500670
0.0016050	34.00	0.05457000
0.0016048	81.46	0.13072701
0.0016047	67.14	0.10773956
0.0016047 ↑		
0.0016018	98.00	0.15697640
0.0016017	54.29	0.08695629
0.0016015	130.06	0.20829109
0.0016014	130.00	0.20818200
0.0016011	174.05	0.27867146
0.0016010	305.70	0.48942570



限价 市價 止盈止損

買入 BNB BTC 餘額: -

賣出 BNB BNB 餘額: -

價格: 0.0016002 BTC

市場 ↑	最新價	漲跌
★ ADA/BTC	0.00002657	4.65%
★ ADX/BTC	0.00008977	2.06%
★ AE/BTC	0.0002228	4.75%
★ AION/BTC	0.0003578	4.93%
★ AMB/BTC	0.00004214	2.56%
★ APPC/BTC	0.00006000	14.11%
★ ARK/BTC	0.0003369	1.26%
★ ARN/BTC	0.00014446	3.91%
★ AST/BTC	0.00004382	7.77%
★ BAT/BTC	0.00003102	8.23%
★ BCC/BTC	0.093823	1.60%
★ BCD/BTC	0.002932	1.81%
★ BCPT/BTC	0.00005637	4.04%
★ BLZ/BTC	0.00006049	6.85%

最新成交

0.0016047	2.72	22:49:03
0.0016017	0.02	22:49:03
0.0016014	2.00	22:49:01
0.0016017	1.02	22:49:00
0.0016017	1.00	22:48:59
0.0016048	1.27	22:48:58
0.0016010	2.73	22:48:55

台灣知名虛擬貨幣交易所 OTCBTC



\$12,620,591 USD ←

OTCBTC

场外交易

币币交易

上市申请 帮助中心 简体中文 登录 注册

BTC/ETH

最新价 **15.65981182** = ¥50538.09
24H涨跌 **-4.59%**
24H最高价 **16.41723417**
24H最低价 **15.18276592**
24H成交量 **235.03905212 BTC**

分时 1分钟 5分钟 15分钟 1小时 2小时 4小时 1日 一周

开= 15.7711478 高= 15.8928078 低= 15.6925981 收= 15.7217970



自选	ETH	BTC	USDT	Q BTC
币种	最新价 / CNY估值	涨跌		
BTC / ETH	15.65981182 / ¥50538.09	-4.59%		
EOS / ETH	0.01785603 / ¥ 57.63	-8.09%		
OTB / ETH	0.00104493 / ¥ 3.37	40.61%		
TRX / ETH	0.00007861 / ¥ 0.25	-4.32%		
ZEC / ETH	0.44446250 / ¥ 1434.39	1.00%		
BCH / ETH	1.48193795 / ¥ 4782.58	-2.47%		
NEO / ETH	0.13103418 / ¥ 422.88	-0.45%		
QTUM / ETH	0.03192105 / ¥ 103.02	-1.79%		
GXS / ETH	0.00660000 / ¥ 21.30	4.76%		
LTC / ETH	0.25375872 / ¥ 818.94	-2.81%		
XRP / ETH	0.00128788 / ¥ 4.16	8.22%		
XLM / ETH	0.00013183 / ¥ 0.43	-81.17%		
ADA / ETH	0.00042982 / ¥ 1.39	5.93%		
GAS / ETH	0.00000000 / ¥ 0.00	0.00%		
RNTB / ETH	0.00014000 / ¥ 0.45	-7.35%		
ICTA / ETH	0.00062300 / ¥ 2.01	-66.43%		
KIN / ETH	0.00000025 / ¥ 0.000807	-16.67%		

买单			卖单		
总价(ETH)	数量(BTC)	价格(ETH)	价格(ETH)	数量(BTC)	总价(ETH)
0.38570365	0.02	15.55671918	15.87099633	0.06	0.96187856
0.15500000	0.01	15.50000000	16.02813491	0.09	1.45710316
0.95451944	0.06	15.39958060	16.18527349	0.06	0.98092566
1.13373528	0.07	15.24244202	16.34241206	0.01	0.12380603
0.93503945	0.06	15.08530344	16.49955064	0.02	0.24999311
0.66156285	0.04	15.00000000	16.50000000	0.11	1.76029557
0.02091570	0.00	14.97176332	16.65668922	0.02	0.37856107

手续费: 0.1% 去设置

买入 BTC		ETH 可用: 0	卖出 BTC		BTC 可用: 0		
买价	15.89280777	ETH	卖价	15.57809871	ETH		
	≈ ¥51290.02			≈ ¥50274.38			
数量		BTC	数量		BTC		
25%	50%	75%	100%	25%	50%	75%	100%

Token Value?

投資 or 投機？

- Cryptographic Token的分類維度

- 技術平台

- 區塊鏈原生：coins like BTC, ETH, Litecoin
- ERC Tokens (沒有專屬區塊鏈)

- 目的或實用性

- Payment token (crypto-currency)



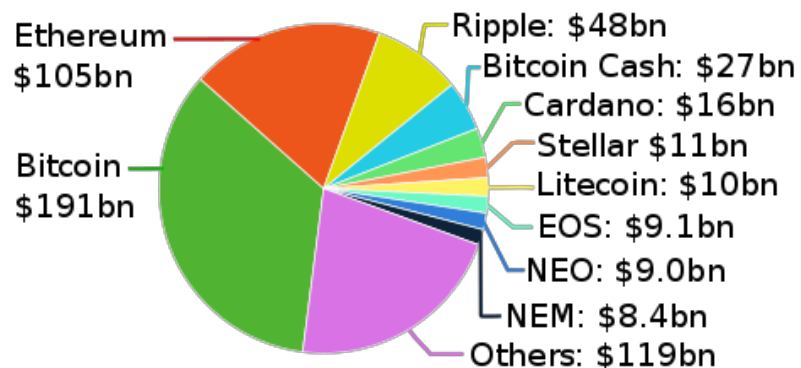
- Utility token



- Asset token (like securities)

- 價值來源?

- Network tokens
- Asset-backed



範例： The good, bad and ugly of ICO

“ICO籌資 5件有1件是詐騙”

2018/05/22中時

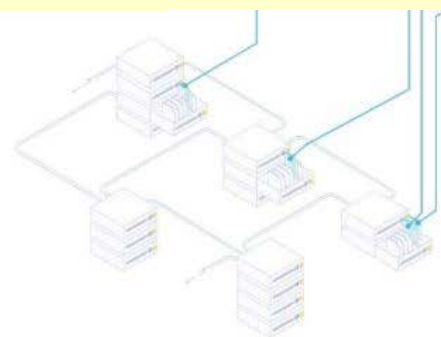


A. Filecoin: 史上最高募款紀錄

- Filecoin的ICO在60分鐘內募集到約2.5億美元，為目前金額最高案例。

願景：實現硬碟共享

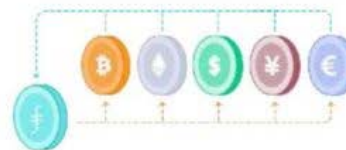
Utility token



A decentralized storage network, powered by a blockchain and a token. Built by Protocol Labs.



Earn Filecoin for hosting files and mining



Exchange Filecoin for tokens or fiat

Filecoin的運作模式

- 願景：實現硬碟共享
- 解決問題：重要資料「意外」消失、儲存成本高
- 解決手法：
- 藉由發行代幣（Filecoin）把供需兩方連接在一起
 - 供給：讓願意共享自己硬碟空間的人（礦工）可以賺得代幣，
 - 需求：儲存檔案在他人硬碟內則要支付代幣作為酬勞。
 - 代幣可以儲存在電子錢包以後使用 Filecoin 的服務，
或者也可以拿到交易所兌換成其他加密貨幣或法幣。
- 代幣分配：吸引礦工、合作夥伴、建立基金會
 - 70% sold, 10% partners, 15% self, 5% community
- 核心價值：發行代幣建構生態系

B. 龐氏騙局：BitConnectX (BCC) ICO

2018/01/18: 區塊鏈平台 Bitconnect 昨日宣布關閉，其發行的加密代幣 BCC (BitConnect) 24 小時內下跌超 97%，投資者損失慘重。

與各個互聯網理財平台相似，投資者在 Bitconnect 把錢借給需要的公司，以獲得回報。不同的是，必須使用加密貨幣投資，以及奇高的收益率。

他們的套路並不新鮮，只是披上了區塊鏈的外衣。100 美金起投，週期 299 天，月收益率可達 40%。Bitconnect 還有一個多層分銷機制，可推薦新用戶獲得酬金，這使其看上去更像一個直銷平台。

Bitconnect 2016 年底通過 ICO 發行了 2800 萬個加密貨幣 BitConnect，簡稱 BCC。平台上的貸款產品都以美元標價，但只能接受 BCC 投資。用戶在平台上存入比特幣來交換 BCC，同時投資回報也是用 BCC 支付。這導致了 BCC 的需要量和價格飆升。在不到一年的時間裡，BCC 一度漲到 430 美元一個，成為全球市值排名 12 的虛擬幣。截至發稿時，BCC 24 小時跌幅超 97%，現在的價格僅為 6 美元。--source: 36Kr



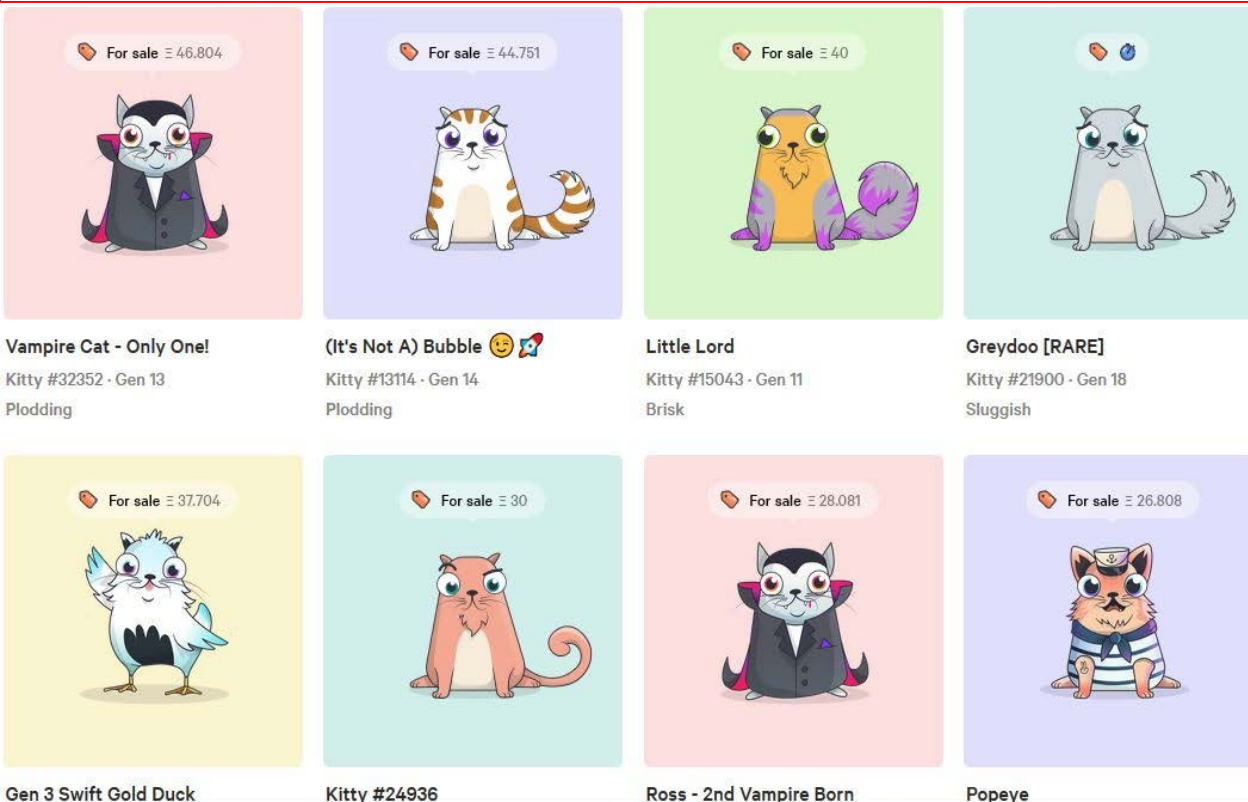
How to Determine if an ICO is a Scam



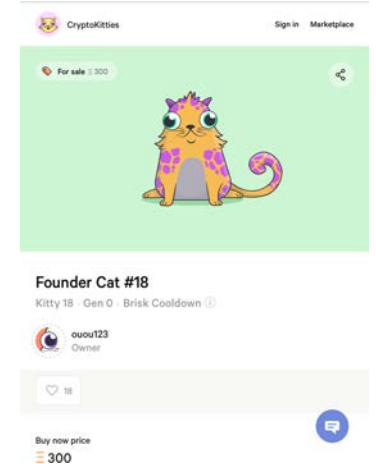
C. 以太貓

CryptoKitties

- 這是一款將「飼養」、「蒐集」、「哇~超可愛」集大成的遊戲。
- 每隻貓都完全屬於你，他不能被複製、帶走、摧毀。
- 世界上第一款建構區塊鏈上的DApp遊戲。
- 買、賣或生小貓。



2018/01/18最高價格的貓：
區塊編號18，最新成交價格
達到264,736美元，約 780
萬台幣。



Tokenization and Token Economy

(Crypto) Token: 密碼權證

(基於密碼通貨的可交易之數位權益憑證)

Enabled by **Crypto-currency/Blockchain**

- from *crypto-currencies* to *crypto-assets*
 - *Tokenize everything?*

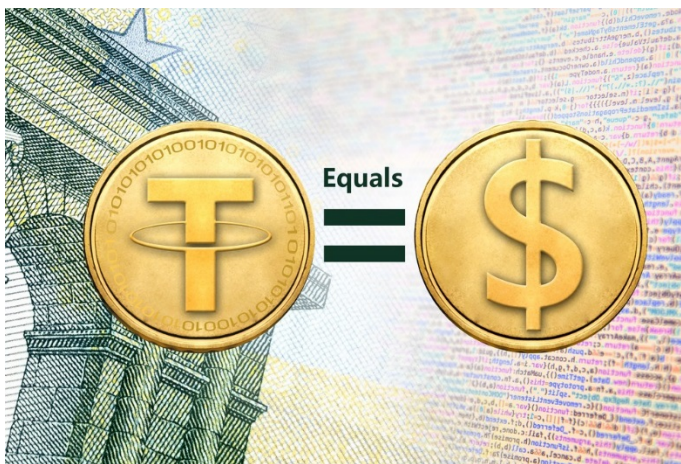
Asset-Backed Tokenization

- **價值少波動性**：以實體或數位資產，作為所發行之token的價值依據
- **安全可靠**：區塊鏈支援可溯源，無法變造的token
- **高流動性**：次級市場交易便利

範例：USDT-USD backed Token

- “ Tether 發行 USDT 的方式很簡單。只要發行 1 枚 USDT，就會有 1 元美金存入信託帳戶內。這樣才能確保使用者隨時拿著 USDT，到某個交易所肯定能換回美金存到使用者的銀行帳戶。如果哪一天，使用者拿 USDT 卻換不到美金，那 USDT 的價格就會崩盤。”

-- 區塊鏈勢



結語：ICO所帶動風潮方興未艾

- 從比特幣，區塊鏈到ICO：快速的演變，帶來監理的挑戰
- 極短的時間內，ICO 變成一個炙手可熱的議題，這顯現市場上渴望創新商業模式的契機，但如何讓這樣的商業模式變成一個健全的生態圈，迄需主管機關給予適當的引領與鼓勵。
- 若在合理的框架管理下運用，ICO不失為數位商業模式的典範，風險或許不在ICO本身，而在於“專案”
- ICO持續性監測需求？發展軌跡存證平台？

The End



Thanks

謝謝聆聽

政大資科系教授兼金融科技中心副主任
陳 恭 博士 chenk@cs.nccu.edu.tw