



區塊鏈的未來？

Blueprint or Bubble for a New Economy?

蔡國裕

- 現職：逢甲大學資訊工程學系副教授(2019年8月1~迄今)
- 學歷：臺灣科技大學資訊管理博士
- 經歷：
 - 中國文化大學應用數學系助理教授(2019年4月1日~2019年7月31日)
 - 中國文化大學應用數學系助理教授(2016年8月1日~2019年3月31日)
 - 華夏科技大學資訊管理系助理教授，2012年8月1日~2016年7月31日
 - 臺灣科技大學資通安全研究與教學中心博士後研究，2009年9月28日~2012年6月31日
 - 中華民國資訊安全學會教育與推廣委員會委員，2011年5月1日~2012年6月4日
 - 英國ISG短期研究 (Information Security Group, Royal Holloway, University of London)，2007年7月~2007年9月

從瘋狂到泡沫

- 1986-1990年，日本房地產僅東京都地價就相當於美國全國的土地價格



從瘋狂到泡沫(續)



天價的核桃

Bitcoin



比特幣/Bitcoin (BTC)

US\$3,966.78 -0.5%↓

1.00000000 BTC 0.0%↑

USD ▾



買/賣 ▾

加密貸款 ▾

總市值

Rank #1

網站

bitcoin.org

瀏覽器

blockchair.com

blockchain.info

live.blockcypher.com

bitcoinblockexplorers.com

btc.tokenview.com

社群

[Reddit](https://www.reddit.com/r/bitcoin)

[Twitter](https://twitter.com/bitcoin)

[Facebook](https://www.facebook.com/bitcoin)

bitcointalk.org

原始碼

[Github](https://github.com/bitcoin/bitcoin)

標籤

[Cryptocurrency](#)

總市值

US\$69,796,685,352

24 小時交易量

US\$7,804,251,559

24 小時低價 / 24 小時高價

US\$3,951.00 / US\$4,031.35

現有供應量 ?

17,595,287 / 21,000,000

Bitcoin(續)



Ethereum



以太幣/Ethereum (ETH)

US\$137.31 -1.2%↓

0.03456975 BTC -0.88%↓

USD ▾



買/賣 ▾

加密貸款 ▾

總市值

Rank #2

網站

ethereum.org

瀏覽器

etherscan.io

ethplorer.io

blockchair.com

blockscout.com

enjinx.io

社群

[Reddit](https://reddit.com/ethereum)

[Twitter](https://twitter.com/ethereum)

[Facebook](https://facebook.com/ethereum)

forum.ethereum.org

bitcointalk.org

原始碼

[Github](https://github.com/ethereum)

標籤

Smart Contract Platform

總市值

US\$14,457,660,344

24 小時交易量

US\$4,116,020,367

24 小時低價 / 24 小時高價

US\$136.59 / US\$141.51

現有供應量 ?

105,285,715 / ?

Ethereum(續)



藉區塊鏈傳銷 半月騙3.8億



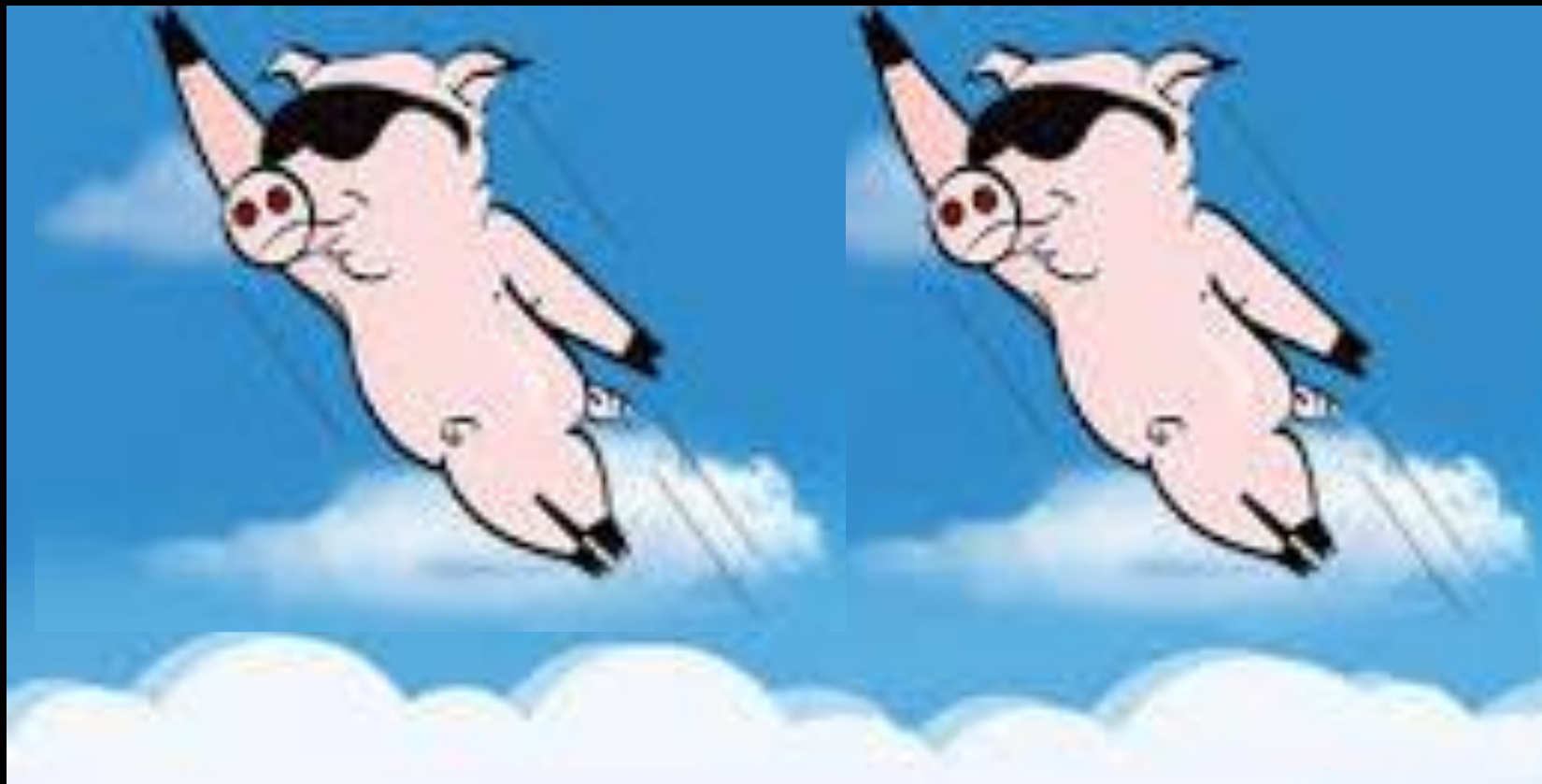
6月8日，香港警方偵破虛擬貨幣投資詐騙案，拘捕8名涉案人。（中新社）

虛擬貨幣炒作火熱下，大陸「區塊鏈傳銷」騙局正猖狂。據西安市警方日前破獲的一起案件，就有一個詐騙集團利用一種叫「大唐幣」的虛擬貨幣，宣稱每天最高有3%的報酬率，在短短半個月之內騙取8600萬元人民幣（約3億8700萬台幣）。

投資比特幣大騙局 三周吸金逾5千萬



可以飛天的豬在哪裡？

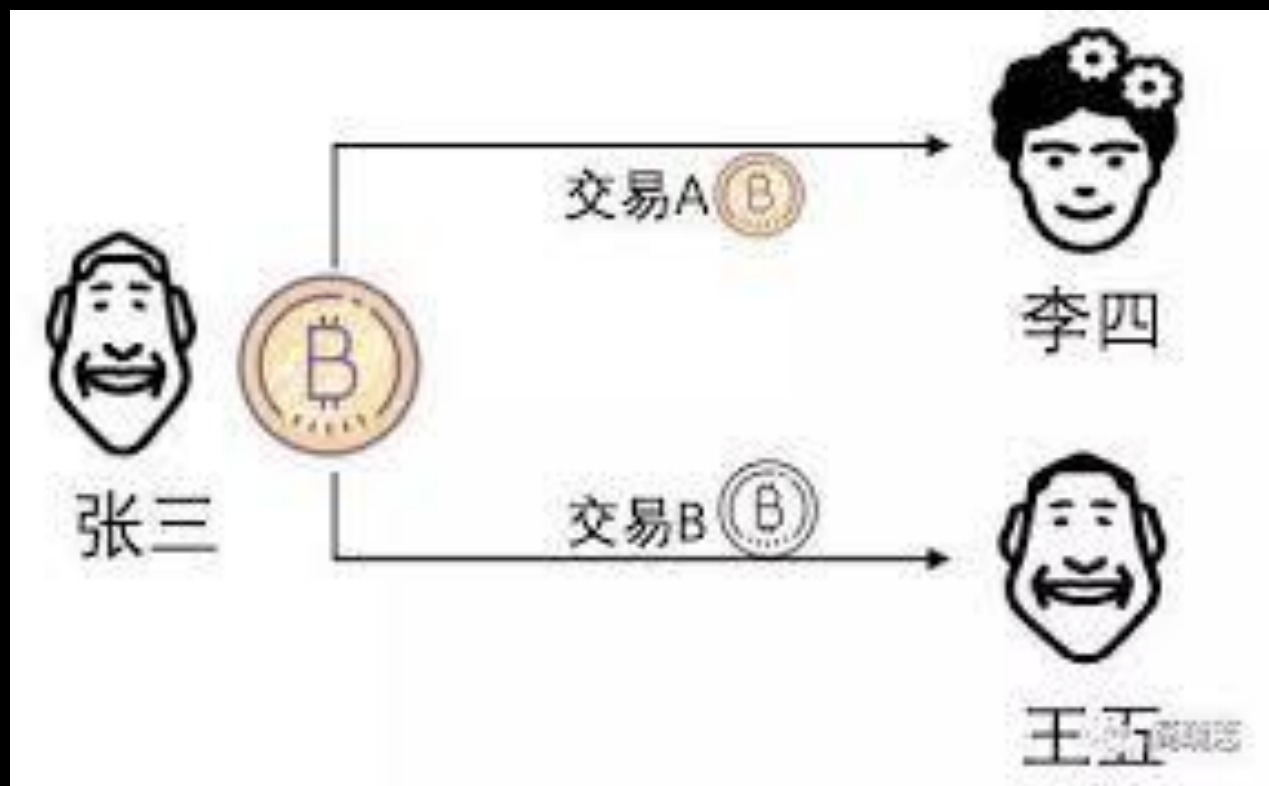


何謂區塊鏈

- 區塊鏈技術由密碼學、數學及演算法組成
- 每一個區段包含前一個區段的加密雜湊、相對應的時間戳記以及資料
- 串接並保護內容的串連交易記錄

區塊鏈1.0：貨幣

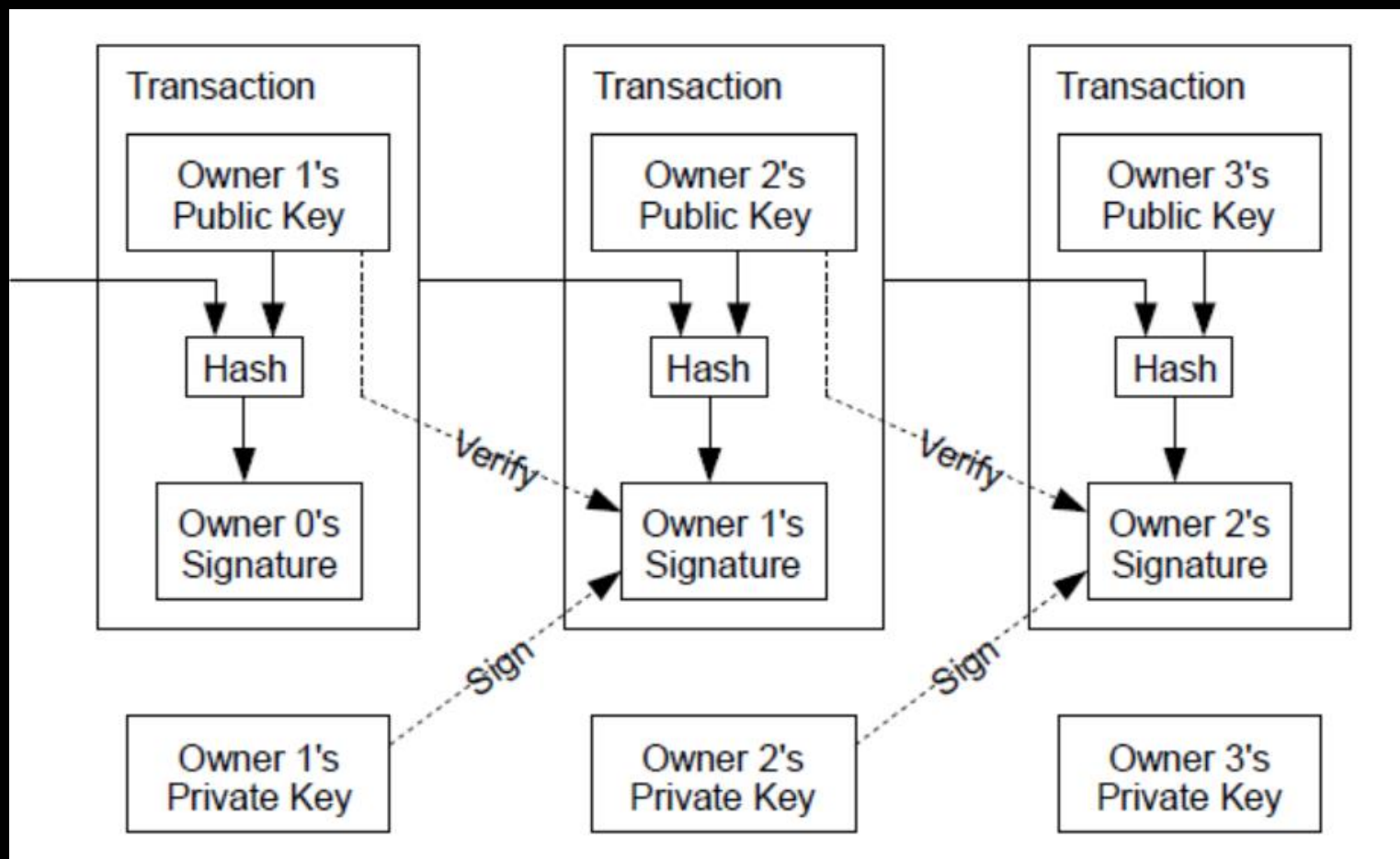
- 數位貨幣的安全議題：雙重支付
 - 解決方法：需要有可信賴的中心



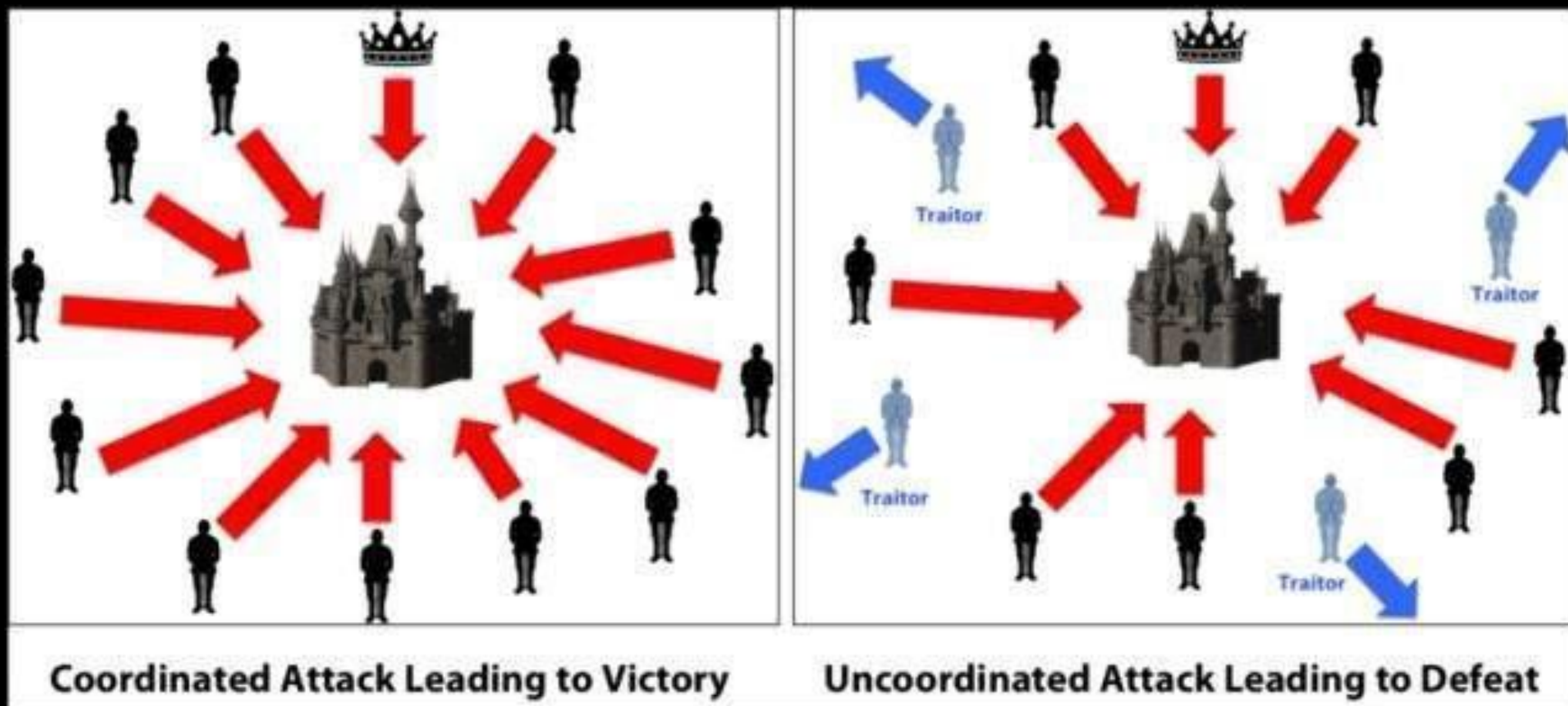
區塊鏈1.0：貨幣(續)

- 比特幣特性
 - 去中心化
 - 採用點對點網路與共識主動性
 - 公開透明的交易紀錄帳本
 - 隱私
 - 不可逆性
 - 開放原始碼

區塊鏈技術

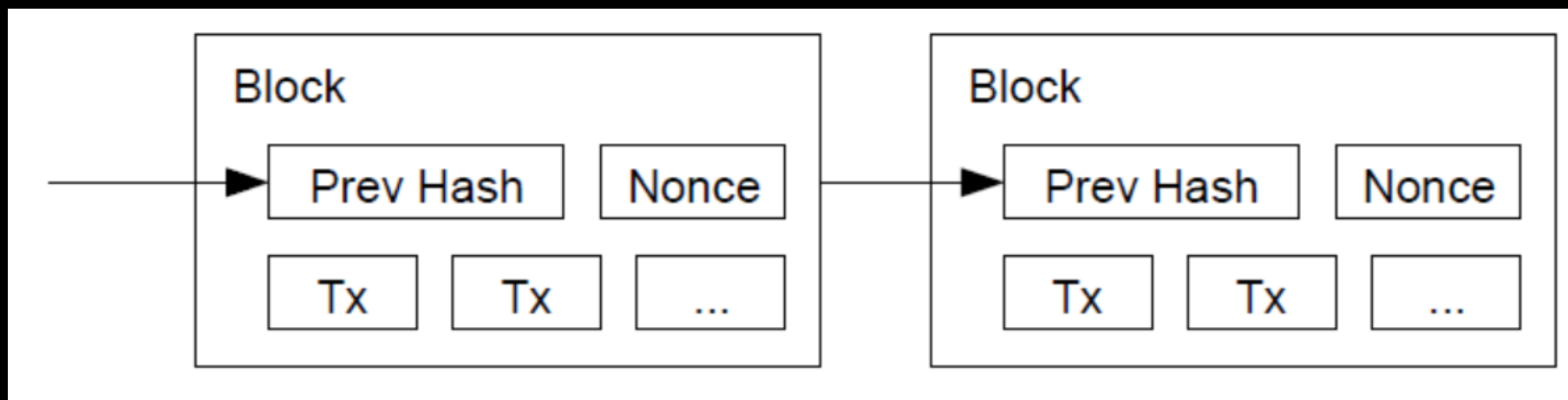


拜占庭將軍問題

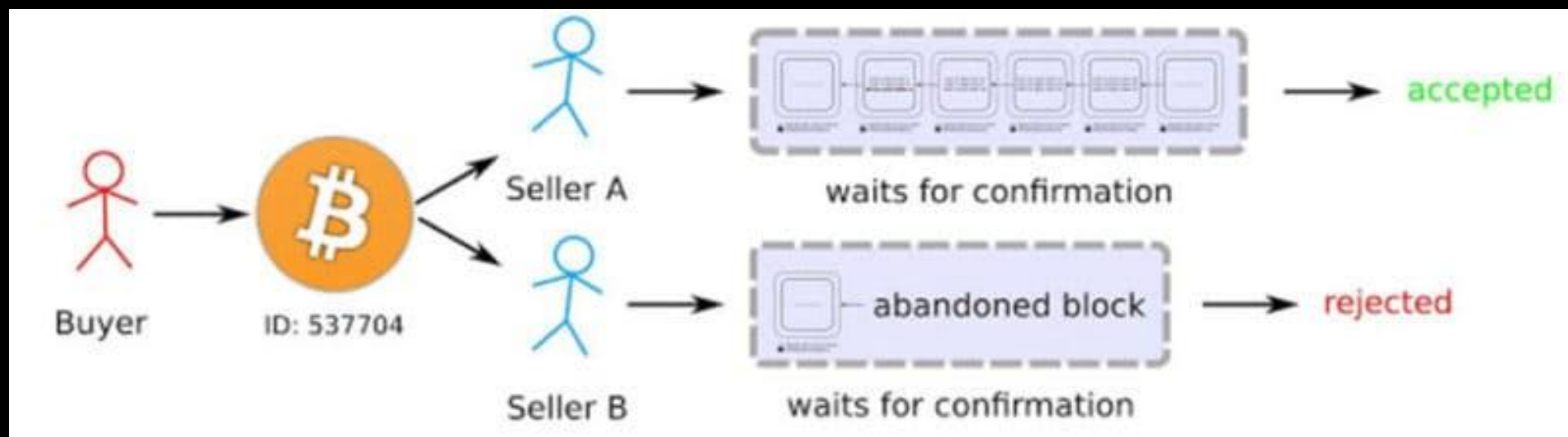


比特幣解決雙重支付

- 工作量證明(Proof-of-Work)
 - 節點必須完成一個計算工作才能其他節點廣播消息



比特幣解決雙重支付(續)



比特幣運作原理

- 一筆新交易產生時，會先廣播到區塊鏈網路中其它參與的節點
- 各節點進行POW的計算決定交易的有效性，由最快算出結果的節點驗證交易
- 最快完成POW的節點，會將自己的區塊廣播給其他節點
- 其他節點會確認這個區塊所包含的交易是否有效，確認沒被重複花費且具有有效數位簽章後，接受該區塊，此時區塊才正式接上區塊鏈，無法再竄改資料
- 所有節點一旦接受該區塊後，先前沒算完POW的區塊會失效

區塊鏈 2.0：合約

- 金融服務：可以讓銀行業者在沒有第三方中介的情況下進行資金移轉與外匯交易
- 群眾募資：區塊鏈導向募集平台發行專屬數位貨幣募集資金，也可以分配數位股權給早期支持者
- 智慧資產：以區塊鏈為導向的可交易資產，包括實體資產與無形資產，任何資產都可以在區塊鏈上註冊，所有權屬於擁有私鑰的人，擁有者可以藉由轉移私鑰給另一方出售資產
- 智慧合約：合約雙方同意或不同意某事，無須信任彼此。智慧合約由代碼定義，也是由代碼執行的，完全自動且無法被干預
 - 自治：合約一旦啟動就會自動運作，不需要合約的發起者進行任何干預
 - 自足：透過提供服務或發行資產來獲取資金，當需要時就可以使用這些資金
 - 去中心化：不依賴單個中心化的伺服器，而是分散在各個網路節點自動運作

智慧合約



區塊鏈3.0：超越貨幣、經濟、市場的公正應用

- 去中心化的域名系統：可以避開網路審查機制的Namecoin，用以檢驗網路或名系統(Domain Name System，簡稱DNS)的註冊資訊
 - Namecoin取代DNS，運任不受任何政府或企業控制
- 言論自由/反審查之應用：Alexandria將Twitter發言編碼至區塊鏈上，建立不可篡改的歷史紀錄系統。
 - 即時記錄Twitter消息，避免內容遭審查而被移除
- 數位藝術-區塊鏈驗證服務：使用雜湊函數與時間戳記，以永久且公開方式記錄與保存服務
- 去中心化政府服務：提供無國界、去中心化、基於區塊鏈的政府服務選項，如比特幣婚禮

第一個區塊鏈婚禮



世界公民計畫的區塊鏈護照



<https://keybase.io/Satoshi>



8181 3268 159E 51D1

Given Name

SATOSHI

Last Name

NAKAMOTO

Time Stamp

20141017-13:40UTC

Block #325,789

e251dcf4d45370606c3c45092432f7068e6951ef6fa44835

Expires

Block #378,349

<0x159E51D1<<RSA<<2048/4096<<AES256<

[illegible]

ahead	Wichita
mural	potato
spindle	letterhead
minnow	inventive
backfield	onlooker
standard	torpedo
endorse	visitor
crowfoot	Brazilian
checkup	gravity
drunken	scavenger

實務案例-食品安全管理

- WalMart公司宣布導入區塊鏈系統，運用於旗下產品的追溯與追蹤食品商的管理
 - 開始使用區塊鏈的技術的產品分別是美國製造的包裝食品與中國進口的豬肉食品
 - 將食品產銷履歷儲存在區塊鏈的平台上，任何人都可以去追蹤查詢，但沒有人可以去篡改
 - 食物貨品每經過一個供應鏈環節就需要記錄一次
 - 讓Walmart追蹤產品的時程從7天濃縮成2.2秒



食安區塊鏈



交易區塊鏈



影視區塊鏈



影視產業新改變 區塊鏈應用更加多元

螞蟻金服：我們可以用區塊鏈識別真假茅苔



比特幣相關新聞



蘋果先發制人！ 禁止挖礦加密貨幣

新開發者指南中的新規則：

應用程式和顯示在應用程式內的第三方廣告，不得執行不相關的背景工作，例：加密貨幣挖礦

理由：

挖礦不僅損耗電池、讓裝置過熱，也對裝置資源造成不必要的壓力。

防止未來有人利用蘋果裝置挖礦較不耗電的加密貨幣，或是集合多台裝置共同挖礦的行為。



趨勢
解讀

The Time Is Now!



Q&A!