

EPISTAR

區塊鏈與虛擬貨幣的關係

Ruby Tseng (曾敏涵)

2018.08.10

EPISTAR

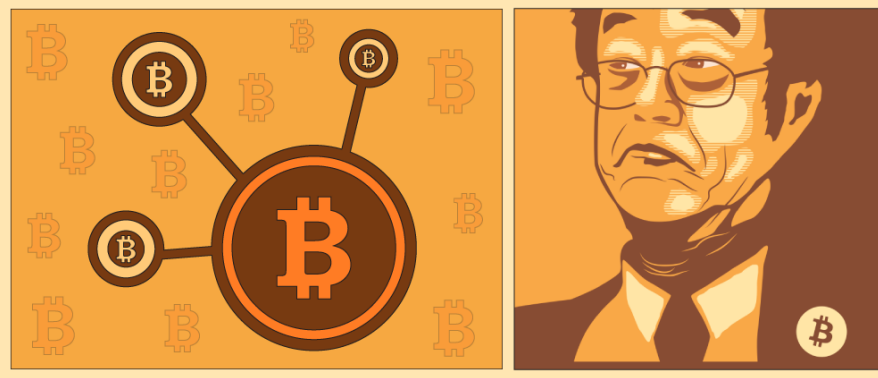
大綱

1. 一切的起源 – 比特幣
2. 區塊鏈：讓數位資產無法造假
3. 區塊鏈運作流程
4. 以太坊介紹
5. 以太坊如何運作
6. 四大虛擬貨幣比較

EPISTAR

一切的起源 – 比特幣

比特幣 Bitcoin



由中本聰(Satoshi Nakamoto)於2008年提出的概念, 包含比特幣區塊鏈(Bitcoin)這套轉帳系統, 以及比特幣(BTC)這個數位貨幣。

比特幣為何會漲價?

比特幣總量固定 (2,100 萬枚) 供給有限 , 若越多人想買 (需求越多) , 價格就會越高。

兩種人會想買BTC

想使用比特幣區塊鏈 (Bitcoin) 這套轉帳系統的使用者、預期比特幣 (BTC) 未來會漲價的投資者。

比特幣 Bitcoin

如何獲得比特幣？

組電腦挖礦



到交易所買幣

挖礦

一套吸引大家**貢獻自己電腦運算資源的獎勵機制**，電腦運算資源會幫助比特幣區塊鏈運作。挖礦獎勵是每 10 分鐘提供 12.5 枚比特幣（時價約 10 萬美金）。透過「挖礦」賺取比特幣的人，就稱為**礦工**。

買幣

透過數位貨幣交易所，道理就像是買賣美金、日幣也得透過匯兌所一樣。雖然一枚比特幣價值數千美金，但是你也可以用 100 元台幣到全家、萊爾富，買等值的零點幾枚比特幣。

比特幣 Bitcoin



比特幣安全性

常被駭嗎？

比特幣區塊鏈這套轉帳系統，將近 10 年來還沒有成功被駭過。**被駭客入侵並損失資金的是交易所**。這**就像是匯兌所發生搶案**，與銀行轉帳系統是否安全是兩回事。



比特幣和區塊鏈的關係

比特幣區塊鏈是一套仰賴「**存簿記帳**」的轉帳系統

區塊鏈是比特幣的防偽 (tamper proof) 機制

存簿上記錄的是誰在什麼時候轉了多少錢。
傳統貨幣 ATM 是由「銀行」來確保轉帳紀錄的正確性，而比特幣是由「區塊鏈技術」**擔保轉帳紀錄正確性**。

比特幣 Bitcoin



比特幣三大特性

實用性

持有比特幣的人，才能使用比特幣區塊鏈的轉帳服務，將交易紀錄寫在比特幣區塊鏈上。用比特幣做跨國轉帳，理論上會比使用銀行轉帳**更便宜**，且收款方能**更快收到錢**。

投資性

比特幣供給總量有限，所以市場需求越大，比特幣的價格就會上漲。各國政府、企業是否接受以比特幣付款，就直接影響市場對比特幣的需求大小，是造成價格波動的因素之一。

投機性

比特幣的價格並不理性。

e.g. 今年 5 月時以比特幣轉帳的速度，已經比今年 1 月時更快，但比特幣的價格卻只有當時的一半。也就是說，**比特幣的價格高低與產品好壞並沒有絕對關係**。

EPISTAR

區塊鏈：讓數位資產無法造假

區塊鏈：讓數位資產無法造假

區塊鏈的顛覆性

區塊鏈的重要功用是**數位資產的防偽**



防偽需求有多大，
區塊鏈潛力就有多大。

如何防偽？



= 存簿內頁



= 在存簿內頁標註內碼



負責保管存簿、驗證交易和記帳

彼此獨立且互不相識，但**各自都有一份相同版本的存簿**。

區塊鏈：讓數位資產無法造假



區塊鏈弱點

交易速度太慢

比特幣**每秒只能交易 3 到 5 筆交易**，相對於 Paypal 每秒數百筆交易、VISA 每秒數千筆交易都慢得多。

沒有隱私性

比特幣的交易內容都是**匿名公開**在網路上，就像是全球的 Email 內容被完全公開一樣，只是大家不知道付款者、收款者實際上是誰。

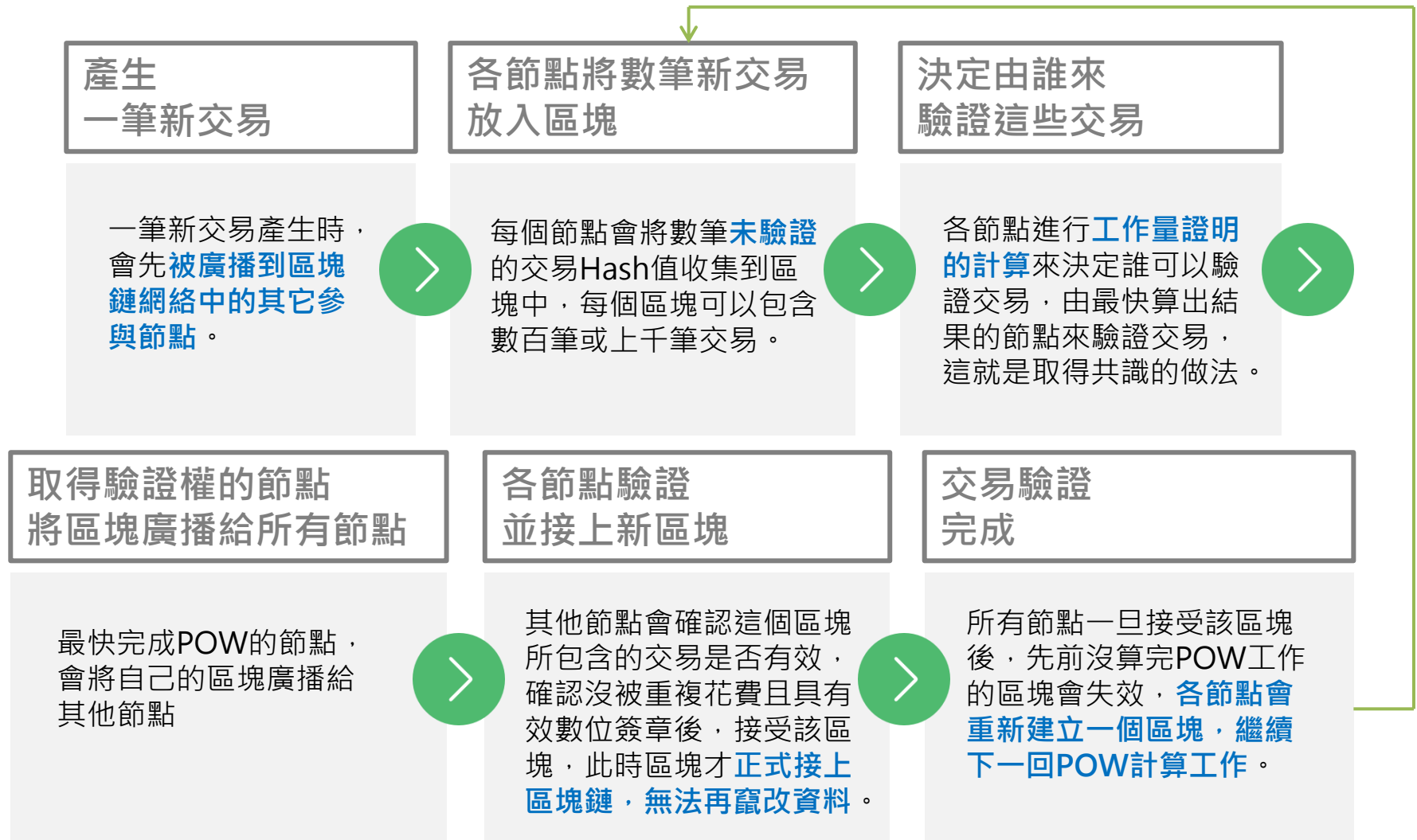
安全性可能不足

比特幣的安全性仰賴多少礦工願意加入，並貢獻電腦運算能力。因此「挖礦」這套誘因機制必須吸引到足夠的礦工。**如果礦工不足，其實區塊鏈並不一定多安全。**

EPISTAR

區塊鏈運作流程

區塊鏈運作流程



© EPISTAR Corporation. All Rights Reserved.

EPISTAR



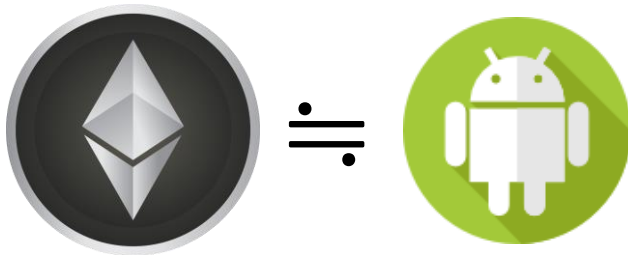
以太坊介紹

ethereum

以太坊介紹

以太坊 vs 比特幣區塊鏈

比特幣是**區塊鏈**、**應用相互綁死的轉帳系統**。
以太坊是用**區塊鏈**打造的**應用平台**，可以讓**很多不同的應用程式**，**建立在以太坊平台上**。



軟體工程師可以直接使用**以太坊的既有資源**，
建立基於**區塊鏈**的應用（Decentralized App），
但不需要自己從頭建構新的**區塊鏈**。



以太坊：用**區塊鏈**打造的**應用平台**

以太幣的用途

使用以太坊（Ethereum）上的應用，使用者必須付以太幣給以太坊。

數位貨幣

挖礦



與比特幣最大的差別

能作為運行以太坊所需之**燃料(gas)**

EPISTAR

以太坊如何運作

以太坊如何運作



以太坊的應用
由多個智慧合約組成

透過區塊鏈上的電腦執行程式，達成資產交換自動化，也因此無法人為干預。



執行一個SM
需要多少Eth?

取決於智慧合約所需要執行的運算數量多寡、單價決定。

以太坊如何運作

以太幣優點

用以太坊執行智慧合約，有別於用企業的雲端運算平台 (e.g. AWS) 執行程式碼。
能夠確保程式被貫徹執行，而不受到政府要求下架或企業審查的限制、干預。
例如中國有不少被官方禁止的翻牆軟體，之前就想從 Amazon 搬家到以太坊上。

以太幣缺點

交易速度慢

以太坊每秒只能處理 **10 到 15 筆交易**

成本昂貴

以太坊與 Amazon 的雲端服務比較，Amazon 的 CP 值比以太坊高了 100 萬倍

EPISTAR

四大虛擬貨幣比較

四大虛擬貨幣比較

比特幣



- 僅作**貨幣**使用
- 2009年開始發行
- 1650萬枚比特幣在流通 (或被挖掘)
- 市值約2751億美元
- 總量上限為2100萬枚 (它是通貨緊縮)

以太幣

具有開源**智慧合約(SM)**功能的公共區段鏈平台，SM是儲存在區塊鏈上的程式，雙方達成合約條款就能執行



- 屬於一個**更廣泛的應用網絡**
- 2015年開始發行
- 9300萬枚以太幣在流通
- 總市值約711億美元
- 無限量供應 (它是通貨膨脹)

瑞波幣

瑞波幣只需**3.6秒**就能完成交易
透過企業區塊鏈網路RippleNet，協助商業客戶提升**跨國支付交易效率**，提供**跨境支付解決方案**

- 有一個可以在全球範圍內的支付網絡-RippleNet
- 2012年開始發行
- 390億枚瑞波幣在流通
- 市值約218億美元
- 總量上限為1000億枚 (它是通貨緊縮)



快速在全球移轉數十種不同的貨幣

萊特幣

萊特幣的交易大約只需要**兩分鐘**
(比特幣平均的300分鐘)
萊特幣被認為更適合用於支付

- 僅作**貨幣**使用
- 2011年開始發行
- 530億枚萊特幣在流通
- 市值約165億美元
- 總量上限為8400萬枚 (它是通貨緊縮)



© EPISTAR Corporation. All Rights Reserved.

EPISTAR

Thank You!