區塊鏈

王擎天 著
Reyer Chu
20170918

Overview

1. 概述: 關於區塊鏈，這些應用場景都為你準備好了
2. 技術: 走進區塊鏈的世界，破解新世紀的財富密碼
3. 影響力: 變革全球市場，區塊鏈有何洪荒之力
4. 應用實例:區塊鏈走進生活，各領域將百花齊放
5. 未來可能: 殺手級應用全面來襲，從老闆到學生都想玩

區塊鏈將開啟未來世界的大門

- 網路的三大效應
  - 去中心化
  - 去邊界化
  - 去中間化
- 區塊鏈是什麼?
  - 去中心化的資料庫
  - 公共記錄核帳的分散式帳本
  - 協議（共識機制）是公開開放的

How to Use Blockchain

共識機制 (共識演算法)

- PoW (Proof of Work) 工作量證明
  - 挖礦 -> 取得記帳權 -> 其它結點驗證儲存
- PoS (Proof of Stake) 權益證明
- DPoS (Delegated PoS) 股份權益證明

- Pool 驗證池

POS (Proof of Stake) 權益證明

- http://www.jollen.org/blog/2017/02/blockchain-developer-proof-of-stake.html
- PoS 是為了取代 PoW，以減少大量運算所造成的資源消耗
- PoS
  - 大多採用 mint 機制，而不是 mining 機制 (貨幣是一開始就決定好數量並發行)
  - 大家一起討論，誰是下一個「鑄幣廠」，被選上的人就負責鑄造新硬幣。所有的節點都是鑄幣廠，也都有機會獲選鑄造新硬幣
    - ➔ 不是「中央鑄幣廠」的機制，而是去中心化的機制
    - ➔ 以每個節點的權益（stake）來決定負責創造新區塊的節點
  - 有別於 bitcoin 的挖礦 (mining)
    - Bitcoin mining 機制，是所有人在比賽創造新區塊，靠的是運算能力；誰創造了新的區塊？是無法預期的，所以是誰創造了下一個區塊，是非常隨機的（random）

DPoS (Delegated PoS) 股份權益證明

- http://me.tryblockchain.org/blockchain-dpos-bm-eos.html

Blockchain Characteristics

- 傳統帳本vs. 區塊鏈帳本
  - 去中心化
  - 開放性
  - 自治性
  - 訊息不可篡改
  - 匿名性

震驚全世界的第一個區塊鏈 – 比特幣

- 90年代初期: 匿名電子現金 Ecash by David Chaum
- Bit gold, RPOW, b-money, …

- 銀行帳戶 (虛擬錢包) <-> Bitcoin wallet
- 帳戶密碼 <-> Private key (存於 wallet)

Bitcoin History

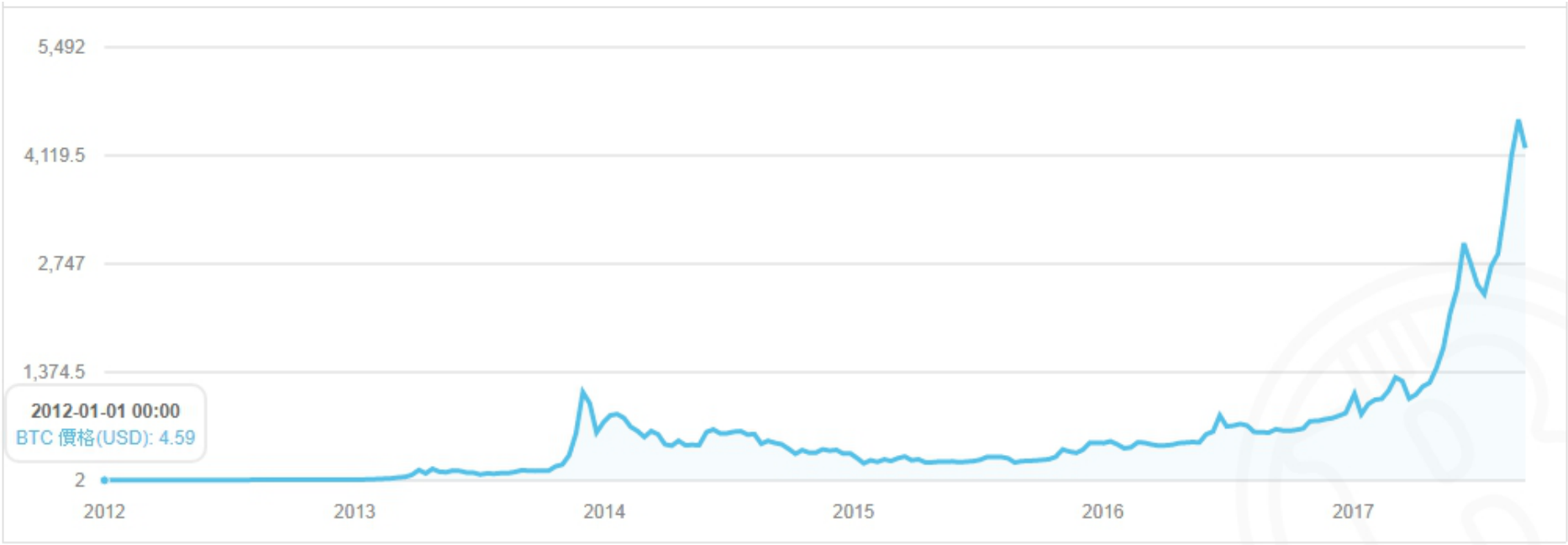
- 2008: [論文發表] by “中本聰 Satoshi Nakamoto”
  - Bitcoin: A Peer-to-Peer Electronic Cash System

  => Blockchain
- 2009/1/3: [系統啟動] ” 中本聰” 以挖出的 50 個 bitcoin 正式啟動 bitcoin 金融系統
- 2010/5: [首次實體交易] 有使用者以 10000 個 bitcoin 買一個 $25 的比薩
- 2011/4: “中本聰” 宣布隱退

- 2010/4: Bitcoin 市值 $14 cent
- 2010/夏: 開始大漲
- 2011/6: $27

Bitcoin Price History

- 2012/1/1 ($4.59) ~ 2017/9/10 ($4213.18)



以上圖表反映的是MaiCoin的每日買價和賣價的平均價位

How to get Bitcoin?

1. 挖礦 (→ 礦池)
   - 挖礦獎勵
     - 2009年: 50 元 bitcoin
     - 每 4 年減半 (=> 2013~2016年: 25元)
   - 挖礦難度 (約兩週調整一次)
     - 每挖出 2016 次礦
       - → 調整難度 st. 平均每 10 min 挖到一次
       - → 難度的變化取決於解題的速度
   - 最小單位: 10 ^ (-8) 元
     - ➔ 2140年之後獎勵 < 最小單位
     - ➔ 全部挖到的總額是有限的: ~2100萬 bitcoin
2. 交易

Bitcoin Characteristics

- 虛擬數位化
- 帳本公開
- 限量發行
- 無法偽造
- 去中心化
- 匿名
- 不需政府背書支持
- 付款不可逆
- 快速遠距
- 低成本 (手續費)

Bitcoin 運作 (1/2)

- [銀行帳戶] Bitcoin wallet
  - [帳戶號] Bitcoin address
    - [密碼] Private key <-> public key (via Base58 coding)
- Bitcoin address:
  - 27~30 英數字元構成
    - 第一個字元是 1 (1 個private key) or 3 (多個private keys, 需要其他人背書)
  - 每個 Bitcoin address 只會被用來交易一次
- Private key
  - 遺失無法補法 , 即使知道 bitcoin address, 看得到卻無法用

Bitcoin 運作 (2/2)

- 礦工生成 block (上次挖到的礦的部分資訊, 新礦資訊, 收到的交易資訊) 透過 IRC (Internet Relay Chat) 廣播
  - 拒絕太舊 (前 11 個 blocks 生成時間的中位數) 或太新 (2 小時內) 的 block
  - 被 100 次挖到 → 成熟的 block
  - 主分支上成熟 block 才有獎勵
- Open source → 任何人都可以免費使用電子錢包, 開戶, 挖礦, 轉帳交易等服務, 但也要付費的
  - 無手續費的交易優先權較低

Bitcoin 面臨的問題

- 流通性
  - 限量發行
  - 匯率波動大
- 通縮 → 無法透過調節來穩定匯率
  - 遺失不能補發
- 傳播 loading
  - 傳播所有 blocks in blockchain
- 確認費時
  - 暫時性的重複花費
- POW 衍生問題 (資本主義弊端)
  - [運算能力] 要與 [挖到礦的機率] 成某種正向關係
    - E.g. Log(運算能力) 正比於 (挖到礦的機率)

全世界為什麼都在研究區塊鏈

- 各國都在爭相研究
  - 美國德拉瓦州
    - 改變民營公營企業後端辦公方式 (股份登記, 資本結構表管理, 股東溝通, ...)
  - 美國 DARPA (國防高等研究計畫署)
    - 創造駭客無法入侵的傳訊系統
  - 美國Microsoft & R3
    - 加速使用分散是帳本科技 (投資, 借貸, ...)
    - R3: 2015/9 成立的 NY FinTech 公司 R3CEV, 召集全球各大銀行組成的區塊鏈聯盟, 共同開發 Distributed Ledger Technologies
  - 俄羅斯國家結算存營所
    - 股東會投票系統
  - 英國政府科學辦公室
    - 減少詐欺, 貪腐, 錯誤和紙本集中作業程序的成本
  - Blockchain Education Network
    - Blockchain 會讓金金融界達到人類史上前所未有, 難以置信的 “透明性” 和 “可審計性”

Blockchain Pros

- 資料訊息不可篡改, 更加安全
  - Vs. 傳統方式: 藏起來
  - 密碼學 + 共識演算法 → 共享 DB 記錄不可篡改
- 異構多活, 高可用性
  - 共識演算法 → 某個節點出問題, 不影響作業
  - 可使用不同程式語言, 不同架構, 來實現不同版本的全節點交易
- 新型分工機制, 更高效率
  - 傳統方式: 找共同上級 vs. 共識機制 (權責明確, 不需讓渡權力, 不需第三方機構成本)
- 智能合約, 更加先進
  - 智能合約 = 一段運行於 blockchain 的 source code
    - 透明, 可信任, 自動執行, 強制履約

Blockchain Cons

- 性能問題有待突破
- 隱私問題有待加強
- 升級修復機制有待探索

Blockchain 發展趨勢

- 中心化及去中心化兩個極點間, 存在新的領域
  - 不同的非中心化程度, 滿足不同場景特定需求
- 解決效能瓶頸
  - 閃電網路: 將大量的微小支付移到主鏈之外
  - Corda (分布式帳本平台): 僅將 blockchain 作為爭議仲裁及強制執行的最後手段
- 安全性
  - 對 blockchain 盲目信任可能導致嚴重後果
    - E.g. 智能合約漏洞導致數位資產損失
  - Hybrid database: 傳統 DB + Blockchain
- 法規 & 技術標準
  - 跨鏈操作, 互聯互通