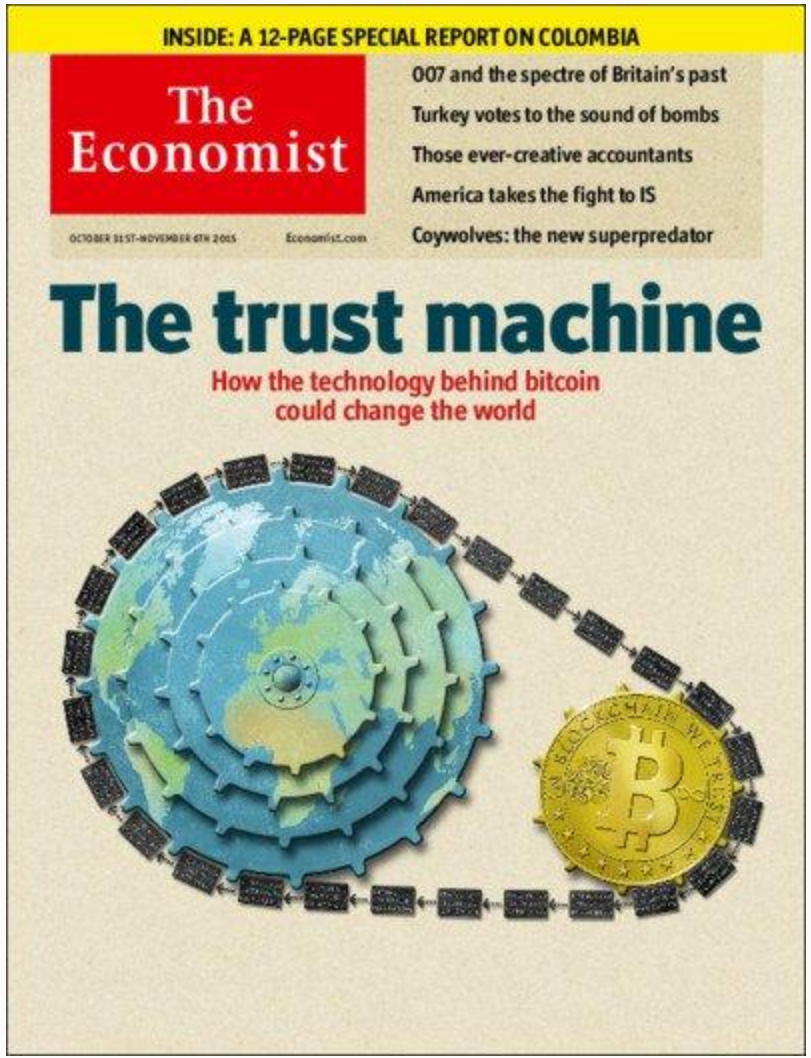
金融科技與區塊鏈

鑑往知來,打造數位金融基礎建設

Dr. Liao (廖世偉), National Taiwan University, Google Founders' Award recipient

November 2015

(March 2016: adapted for Central Bank)



經濟學人:

狂熱是永恆的源泉 -- 未來將屬於分散式帳本技術, 但普及為時尚早, 在技術最終得到應用前, 過高的期望往往會帶來失望

最近金融人對眾多FinTech activities的反應:

- **第一種反應:“台灣第一部電腦是銀行買的”**
  - **My answer: FinTech vs. TechFin: Before, 金融互聯網 vs. 互聯網金融**
    - **Now, FinTech + TechFin. 以下, 用 FinTech一字來代表兩者。**
- **第二種反應:“跟我講5個keywords”**
  - **My answer: Forget about Buzzwords. 回歸本質:**
    - **Trust machine**
    - **Open, Shared**
    - **Secure**
    - **Market-proven**
    - **0-margin cost**


my 5-page Blockchain gospel: Page 1:

區塊鏈是資訊科學和社會科學的結晶

- 比特幣的基礎建設是區塊鏈 (Trust Machine)，取信於人，已運行超過7年，身為眾矢之的，被千錘百鍊，更取信於人。
- 更重要的是，區塊鏈導入的信任機制 (Trust Machine) 使傳統產業 (如金融業) 可以加速變革與創新。
- 區塊鏈對信任機制的衝擊
  - Today: 對金融體制的信任 → 將財產交給銀行來保管
  - Today: 對政府機構的信任: 身分認證 (護照、駕照、健保卡, ...) → 將個人隱私資訊交給政府保管
  - Today's problems：銀行服務可再提升便利性嗎？政府機構能更提升效率嗎？
  - Blockchain will usher in a *better world* tomorrow

世界運行需要信任機制存在

- 過去我們必須完全仰賴信任第三方 (銀行, 政府...) 來傳遞價值與證明資產所有權。
- 受到法規與其它因素限制, 這類領域少有競爭 → 但如此架構下難有變革與創新。
- 導入區塊鏈解決方案:點對點的價值傳遞鏈, 在一個由密碼學保護的共享帳本上, 沒有任何單一實體可以竄改帳本上的資料。
    - 不須完全仰賴第三方如銀行、政府, 區塊鏈本身就是具信任機制的基礎建設
    - 區塊鏈將變革與創新導入過去缺乏競爭的產業環境。

Blockchain: Internet 2.0

- 區塊鏈像是互聯網，沒有獨裁者能完全擁有或掌控它，這是一個多中心化的協議。

- Inspectability: 區塊鏈是完全公開且任何人都可以在上面創新，就如同互聯網當初發展崛起的過程一樣。

- 任何人都可以在區塊鏈上創建能夠改變世界的新服務或應用，並且鼓勵市場競爭來改善現有系統！

小結

＊比特幣是去中心化的數位價值聯網，但實質影響力遠超過虛擬貨幣本身。

＊區塊鏈導入了新的信任機制，為眾多傳統領域注入變革，如同過去互聯網改變世界的模式。

＊信任 與 value 息息相關

＊區塊鏈是開源形式，開放心態 → 任何人都容易建立新的服務和應用。

＊這是一個快速成長的新領域，充滿各式各樣的可能與機會。

FinTech & Blockchain

趨勢,應用與基礎建設

廖世偉

「區塊鏈技術將改變金融業」

李顯龍, United Overseas Bank 80th anniversary (Nov 2015)

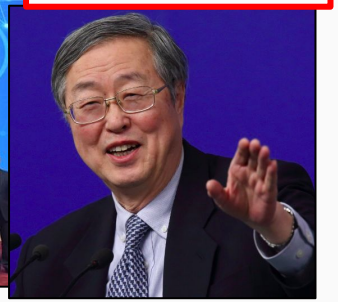
“Blockchains, which is used for bitcoin, but can also be used for many other applications like real-time gross settlement, or trade finance verification. So our banks and our regulators must keep up to date and up to scratch with these developments“

2016國際情勢

全球超過43家銀行組成R3聯盟
共同研發區塊鏈技術標準

中國政府牽頭成立:
中國區塊鏈研究聯盟
中關村區塊鏈產業聯盟

多國央行已展開
區塊鏈技術研究



Nasdaq

London Stock Exchange

TOKYO STOCK EXCHANGE

多國證交所已展
開區塊鏈交易之
測試與研究

2016國際情勢：
Equity, Currency, … Digital assets: $$$$$

- 美國 SEC（The US Securities and Exchange Commission）在2015年12月批准了Overstock用區塊鏈發行股票的計畫。CEO Patrick Byrne 引領時代，選擇創新，公平，公正，公開的區塊鏈技術，並大幅降低了發行成本。
- 英國首相的首席科學顧問 Sir Mark Walport 也建議英國政府，在主要公共服務上，例如稅收、福利或簽發護照等採用區塊鏈技術。
- 在中國大陸，區塊鏈相關研究也正積極開展，中國人民銀行行長周小川在2016年2月接受媒體採訪時，再次提到央行正研究發行“數字貨幣”。
- 區塊鏈 相關新創企業全球融資已超過10億美元(規模為1995年網際網路時代的4～5倍 $$$$$)

國際區塊鏈的商業應用

- 數位化貨幣
- 數位證券化應用
- 供應鏈產銷履歷
- 公民電子投票
- 健康醫療紀錄
- 智慧合約
- 商業登記

Two Things I heard at 世界互聯網大會 2015

1. ISOC (Internet Society) vs. IUN (Internet United Nations)

    誰來組網?

    Policy vs. Mechanism

2. “Blockchain is infrastructure booster
    Blockchain makes possible: Investment, Development & Operations”: Announced on the 1st day of 世界互聯網大會 (2015-12-16)

See the next slide

Source of IUN: Sherman Tuan


E BOOSTER
BLOCKCHAIN MAKES POSSIBLE: INVESTMENT, DEVELOPMENT & OPERATIONS.
BUILDING A DIGITAL SILK ROAD FOR WIN-WIN COOPERATION
Information Infrastructure Partnership
数字丝路·合作共赢论坛
信息基础设施共建
WORLD INTERNET CONFERENCE
5 INFRASTRUCTURE BOOST

2016國際情勢 (5/5)
Taiwan: 急起直追

- 2016年3月, 行政院長張善政指出, 中央銀行總裁至立法院報告, 提到「數位貨幣」是很重要的進展。行政院長請央行強化白皮書裡數位貨幣的章節, 並請金管會, 財政部共同配合。
- 金管會金融科技辦公室執行秘書蔡福隆在臺灣大學記者會上強調他對金融科技暨區塊鏈領域的期許：他希望我們區塊鏈的研發能做好產政學的無縫接軌, 扮演臺灣FinTech領頭羊的角色。
- 2016年5月 金融科技白皮書提到區塊鏈是未來5大方向之一。
- GCoin: 鑑往知來, 打造數位金融基礎建設

Gcoin 區塊鏈 Pilots

支付結算系統

顧客忠誠計劃

供應鏈

私募平台

票據平台

多中心化交易所

Outline

- Blockchain 本質（Blockchain gospel）
- 國際情勢
- What should be our strategy?
- 金融：玩真的應用
- 回歸本質：Monetary history (History is important!)
  - 錢的本質＝？
  - 發行法幣會遇到的困難
  - Bitcoin Blockchain不是橫空出世, 是百年的醞釀
  - 3 lessons from 百年醞釀
- 大議題: 數位金融基礎建設
  - 基礎建設: 4D 問題
  - Blockchain: Trust Machine that solves 4D
- Gcoin Blockchain
- Look into the Future

What should be our strategy? (1/2)

先問一個問題：為何 FAGA 公司 such as Google and Apple 要投入這麼貴的員工們來做 open source？難道只是單純 for better world? Or for better business also?

- Intel Compiler vs. Google Android or OpenStack
- Software vs. Service (SaaS): IP vs. Know-how
- 去除舊思維：“此路是我開，此樹是我栽，要從此山過，留下買路的名利”
- 互聯網：未來的尊嚴是從今日的貢獻累積出來的。

What should be our strategy? (2/2)

With Open source:

- You can 培育金融科技人才.
- Beware: Service Lock-in vs. Service Option: 北韓 vs. Freedom
- 掌握業務邏輯：Find the open-source that supports Governance best
- 不炒短線：Global: Scalability
- Gcoin stands for Governance and Global.

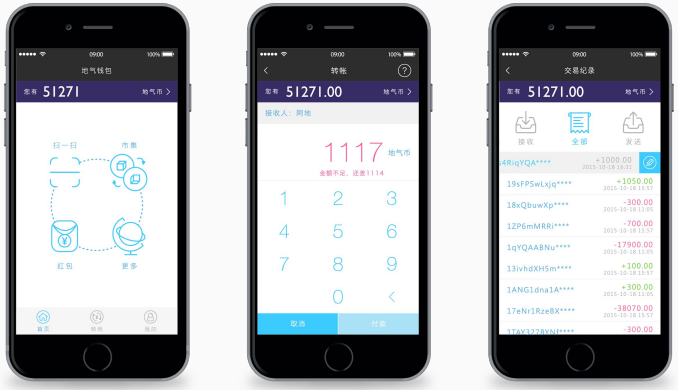
G-coin.org: Open for you.

區塊鏈技術應用

- 區塊鏈行動支付系統
- 區塊鏈交易平台

區塊鏈行動支付系統

- **問題**：線上支付等需要藉由區塊鏈達到數字化，使權益擁有人直接存取，進行交易、獲取交易資訊等，而不需透過中介商。
- **方案**：藉由區塊鏈技術提供一套 ID 管理系統，僅有私鑰的擁有者可以存取資產，擴充原有行動錢包的支付場景。



價值：區塊鏈免除交易中介者 (intermediaries) 的金流成本。**預估使用區塊鏈的支付結算成本可降至 0.00025 % (0.025 bp)** [1]

區塊鏈對支付系統的效益

區塊鏈強調交易即清算

✓不會有帳不平的問題

- ✓ GCOIN 區塊鏈平均 15 秒完成結算

✓不需要額外的對帳成本 (人力+系統)

區塊鏈的不可竄改特性

✓讓系統安全性有多一層的保護；由區塊鏈技術降低的信任成本為全球金融機構每年省下200億美元。See [2]

區塊鏈對支付系統的效益

區塊鏈為一套 P2P 分散式架構系統

✓透過密碼學的保護，交易可直接在手持裝置端做完並且發送

- ✓ 降低server負擔
  - 經測試，交易的產生過程佔整體時間超過 70%
- ✓ 可支援小額線下付款，增加支付市場份額
  - 預估使用區塊鏈技術可增加10%支付市場份額[3]

支付區塊鏈的案例

- BIS(國際清算銀行)指出區塊鏈技術可能應用到中央銀行的運作
- 顧問公司艾特集團(Aite Group)預估銀行一年投資 7500 萬美元在區塊鏈技術改善支付系統
- 高盛集團(Goldman Sachs)替旗下的區塊鏈技術結算系統「SETLCoin」申請專利
- Circle 提供基於區塊鏈技術的美元轉帳，於2015年獲得 5000 萬美元融資
- Coinbase 提供數字貨幣的行動錢包服務，於2015年獲得7500萬美元融資

全球知名金融機構已積極加速佈局投資[4]

區塊鏈交易平台

- **問題**: 交易平台需要可追蹤性，讓金流可被追蹤並視覺化以避免被濫用。
- **方案**: 區塊鏈技術提供一份可共同驗證的分散式帳本系統，可應用於個種交易平台。

區塊鏈技術降低 99% 交易結算風險 [5]

區塊鏈對交易系統的效益

加速交割效率 (→15秒)

✓數字化股權藉縮短交割時間可降低 99% [6] 結算風險

可追蹤性、流動性

✓區塊鏈原生支援次級市場，交易門檻大幅降低

- ✓ 區塊鏈使 Pre-IPO trading 更具吸引力
- ✓ 2015年股權眾籌平均投資人數僅6人，平均融資成功率約為20%，金額更是只有總目標金額的7%。

區塊鏈的交易平台案例 (證券)

- **NASDAQ 使用區塊鏈發行 pre-IPO 股票**
  - 該技術可以降低系統性成本的80%至90%，因為交易的主要成本在於清算過程
- **Overstock 創建了tØ區塊鏈股權交易平台**
  - 2015 年 12 月，美國證券交易委員會(SEC)批准在 Overstock 通過區塊鏈來發行公司股票
  - 至少 5 家企業已通過該區塊鏈平台發行股票
- **UBS 於 2015 年 9 月完成測試並推出了 Smart Bonds 系統，用於各類債券的發行和交易**
  - UBS 認為，區塊鏈系統未來 2 年內一定會商業化

區塊鏈股權交易平台 2 年內會商業化

Outline

- Blockchain gospel and 國際情勢
- What should be our strategy?
- 金融：玩真的應用
- 回歸本質：Monetary history (History is important!)
  - 錢的本質＝？
  - 發行法幣會遇到的困難
  - Bitcoin Blockchain不是橫空出世, 是百年的醞釀
  - 3 lessons from 百年醞釀
- 大議題: 數位金融基礎建設
  - 基礎建設: 4D 問題
  - Blockchain: Trust Machine that solves 4D
- Gcoin Blockchain
- Look into the Future

錢的本質是什麼？

貨幣的發展 → Need a “Trust Company” → ？

以物易物

商品貨幣

金屬貨幣

央行發行法幣

History of Trust Co. > History of Banks

- 銀票 and 胡雪巖
  - Receipt of your possession.
  - Is it a sufficient and satisfactory Trust Company?
- 央行的出現，發行法幣，但是否就是 a sufficient Trust Company?

發行法幣遇到的困難

法幣發行的困難:

a. 低效率
   - 反應在國際支付的高手續費

b. 信用風險
   - 過度增加自身信用或信用管理不善 → 銀行倒閉
   - E.g. 當銀行 (“Trust Company”)只有5根金條,
   - 卻發給您50000個receipt(錢) 時？
   - E.g. QE
   - → Should Trust Company be replaced by Trust Machine (Blockchain)?

發展數位人民幣的四大理由

- by 人民銀行行長周小川
  1. 低成本
  2. 紙版人民幣換版需10年，而且還是會有人民幣偽幣問題！
  3. Financial inclusion: 普惠金融
     e.g. 偏鄉沒有ATM
  4. 安全: 沒有運鈔危險、假鈔危險、逃稅危險

Blockchain不是橫空出世, 是百年的醞釀

10頁投影片，近百年的醞釀:
1. 世紀經濟論戰:凱因斯 vs. 海耶克

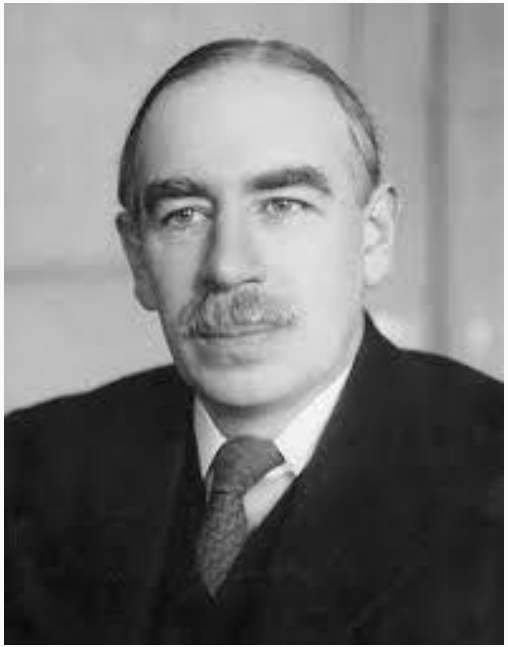
- 凱因斯恐懼:
  - Supply and Demand curves don't intersect!
  - 預測100年內會發生，80年就發生了？Next 80 years?
  - 倫理學的發展尚未ready for 凱因斯恐懼
    - Proof-of-work.
    - Love/belonging, in Maslow's hierarchy of needs.

- John Maynard Keynes' Planned economy
  "Capitalism is the astounding belief that the most wickedest of men will do the most wickedest of things for the greatest good of everyone."

- Hayek's Market economy: 貨幣銀行學中的貨幣政策中立
  - Say NO to 政府的管制與干預

- 1980's vs. post-2008: 金融海嘯後政府介入量化寬鬆 : "In the long run"

- Reflection today: 國家不能無限制印鈔票，過度印鈔票會讓貨幣貶值
  - 經濟危機的暫時緩解，卻帶來長期噩夢



1883~1946年，英國經濟學家
John Maynard Keynes

10頁投影片,100年的醞釀 (2/10)

Nobel Prize Winner, 1974. Great economist of the 20th century

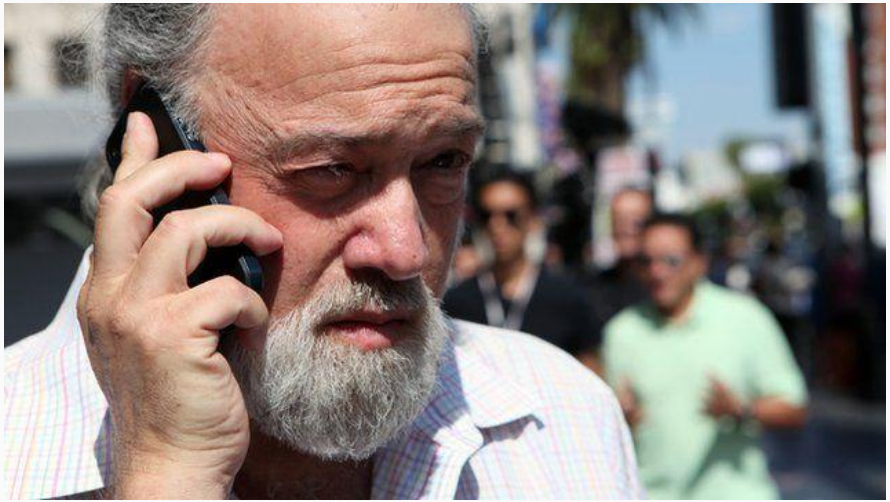
- 古典經濟學派大師 F. A. Hayek 強調自由市場力量
  由市場競爭產生最好交易方式 (貨幣)。
  政府不再具有創造貨幣的壟斷權力,
  讓貨幣非國家化。
  - Hayek's 革命性建議:
    "廢除中央銀行制度,允許私人發行貨幣,並自由競爭,這個競爭過程將會發現最好的貨幣"
  - "一般商品,服務市場上自由競爭最有效率, 貨幣也是如此."
- "Denationalization of Money" (貨幣的非國家化), published in 1976, is widely discussed and debated, till this day!

不可追蹤的數位法幣: eCash

1982年Dr. David Chaum提出注重隱私 (privacy) 的密碼學網路支付系統

- 可算是比特幣區塊鏈支付技術在 privacy方面的雛形，當然eCash就犧牲了traceability，**與區塊鏈不同**。
- eCash 並非去中心化，這點也與區塊鏈不同: See next slide for 去中心化。
- 1982: "Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups"
- 1988: “Untraceable Electronic Cash” Crypto’88.
- Panama papers

David Chaum 提出不可追蹤的基於密碼學之數位法幣: eCash。不可追蹤才能像法幣一樣具有流通的優勢 - 1982.

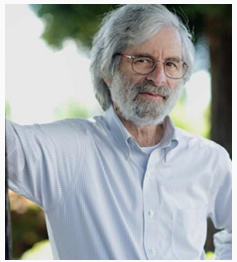


多中心化：Byzantine Generals' Problem, 1982

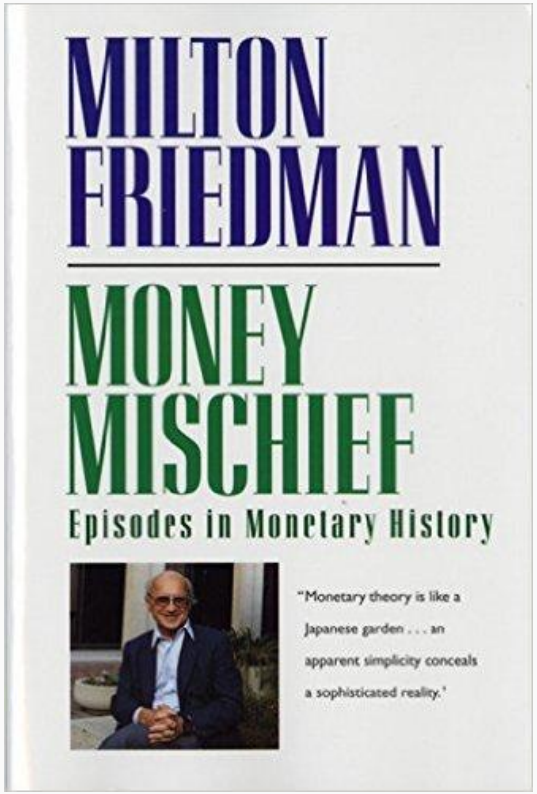
1982年 Leslie Lamport formulated Byzantine Generals' Problem

- Leslie Lamport received Turing Award
- 1999年 Barbara Liskov published an algorithm that addresses Byzantine Generals' problem
  - PBFT algorithm: Practical Byzantine Fault Tolerance
  - Assumes at most ⅓ failure nodes
    - vs. 51% attack
  - Barbara Liskov also received Turing award
  - PBFT is targeting about a dozen nodes.
- In comparison, bitcoin blockchain: Targeting 10k nodes! But TPS is tiny.

Barbara Liskov & Leslie Lamport
2008 & 2013's Turing Award
Programming &
Consensus Protocol



貨幣的禍害 (Money Mischief) published in 1992



貨幣學派(Monetarism)始祖 Milton Friedman 主張經濟自由並強調貨幣作用, 極力反對Keynes的政府干預的論點, 主張各國央行不應無限制的開動他們的印刷機.

- 千百年來,如何用最科學的方式來對財富進行計價,並以最經濟的方式來交易: Challenge!
- 主張單一規則貨幣政策, 制定貨幣供應增長的數量法則。即使政府過度干預貨幣擴張與緊縮, 一段時間產出仍會回到equilibrium.
- 一個自動化裝置,可以按程序來發行貨幣

Nobel Prize Winner, 1976. Great economist of the century.

Adam Back: Hashcash (6/10)

Adam Back proposed Hashcash「雜湊現金」系統 in 1997.

- 為一種工作量證明(proof of work)的演算法。這種算法必須仰賴一類稱為「成本函數」的不可逆函數這種函數「很容易驗證」;但不容易被破解。
  - 最早應用在阻止垃圾郵件

Wei Dai: B-money (7/10)

Wei Dai proposed an Anonymous, Distributed electronic cash system: B-money.

- B-money appeared in an email exchange at a Cryptography Symposium 1998
- 引入工作量證明演算法，通過解決計算難題
- 加上去中心化共識 創造貨幣的構想。

以上5頁投影片看到 Fin vs. Tech 跨領域對話的重要性。

- Hayek vs. Chaum
- Friedman vs. Back and Dai

跨領域後，照理說1998年就應可以有人去implement B-money出來叫Bitcoin？

- 但Wei Dai 仍停留在發想構思階段。
- 而且Wei Dai 並沒有結合 Adam Back的雜湊cash system。
- 而且共識演算法直到2008年中本聰 invented Bitcoin's Proof-of-Work algorithm 才做出了大規模的Trust Machine: Addressed Byzantine Generals Problem and 4D. (See later slides)

Hal Finney to 中本聰's Bitcoin

- Hal Finney proposed in 2005: 可重複使用的工作量證明機制 (reusable proof of work),
  此機制同時將1997年Adam Back的 hashcash (「雜湊現金」演算法), 與1998年 Wei Dai 的 B-money做結合優化而成。
  - 可惜Finney身體不好 (died in 2014), 與Mr. Dai一樣停留在發想構思。
  - 此機制直到2008年被中本聰應用在比特幣上, 才大功告成。
- 我的9字箴言:跨領域, 玩真的, 做中學。停留在發想構思是不行的。
  - Google及IETF即信奉這9字箴言。中本聰信奉這9字箴言。
  - 頂著幹出來 Bitcoin, 改變世界。

類似黃金的有價資產:比特幣

以上比特幣的優點:

- **工作量證明（Proof of work）**
- **信用風險最小化**
- **多中心、Trust Machine instead of Trust Company**
- **交易都透明記錄在區塊鏈上**

問題:

- 比特幣的發行沒有實物或發行人支持
- 匯率波動性高（Volatility）
- 交易頻率受限（Scalability）

Next: Unlike Bitcoin, Our Belief:
數字貨幣應連結既有價值 → 數位資產觀念

3 Lessons from 百年醞釀的金融歷史進程

Lesson 1 from 百年醞釀的金融歷史進程

1. 40多年前還是金本位
2. Then, Collapse of Bretton Woods system. Excessive QE today
3. Bitcoin：類似黃金挖礦: non-Excessive, but 僅由交易所決定 Market Value, 沒連結已經存在的資產，並產生價值。
   a. 比特幣經過百年醞釀, 不是橫空出世, 但比特幣的價值卻是橫空出世!
      比特幣價值太 volatile, 沒有 backing.
4. 數字貨幣應連結既有價值。並配合法規，政策，KYC，AML才可能成功到超過1-2% among all currency values.

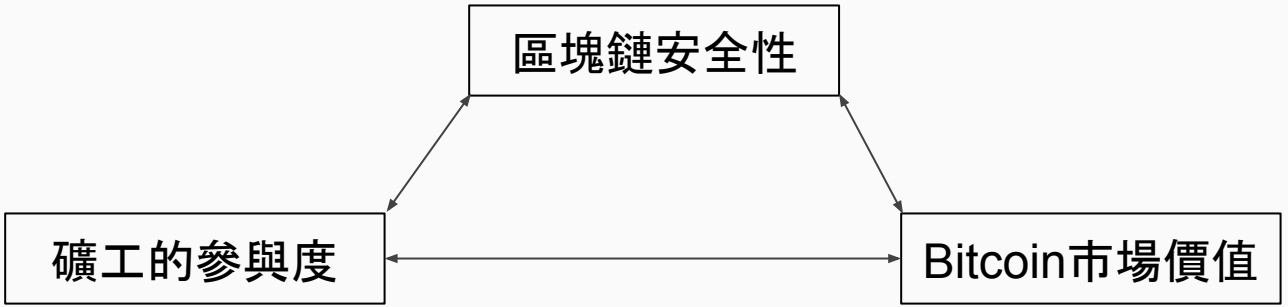
法規不應掐死：a. 若我們不做，到時Google, Wall Street or 美國政府控制未來的數位貨幣基礎建設?

b. 1-2% is small anyway. Note it's smaller than 地下金融.

Lesson 2 from 百年醞釀的金融歷史進程

不只需要跨領域(Fin+Tech)，只有寫code (open-source, internet-style) 又去落實 的中本聰, 才是最後落地了FinTech的里程碑：Bitcoin.

- 中本聰真正了解經濟 and 科技 (密碼學，隱私安全，算法算力): 設計出一個 Virtuous Cycle!



Ecosystem Picture: Princeton course

Lesson 3: 金融現代化的三部曲 (Trilogy of FinTech) 可以靠Blockchain帶來 EFG 的好處

e.g., Bank on internet

e.g., AliPay, 餘額寶, 第三方支付

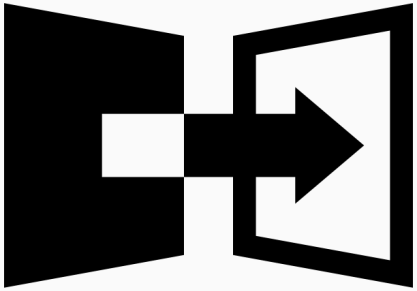
e.g., Nasdaq adopts blockchain backbone for stocks

- Digital Finance時代的核心技術: Big data and Blockchain (Digi-ledger).
- Digital Finance digitizes everything: Gives you E, F, G:
  - Efficiency
  - Finality (Security)
  - Gongping, Gongzheng, Gongkai (Inspectability)

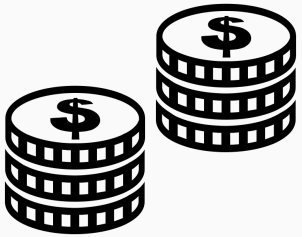
Today’s 議題: 數位金融: 數位資產, 數位貨幣

務本:先看基礎建設 (4D and Blockchain)

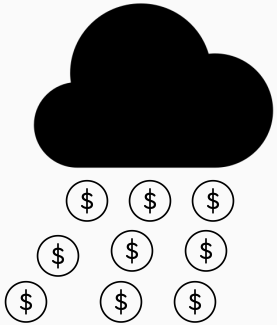
Technology-wise 表述 Digital Finance問題



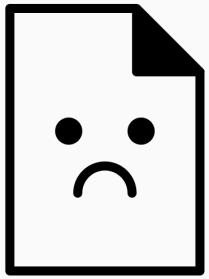
Duplication



Double Spending



Dilution



Data Lost

Digital Finance之前發展不起來的原因:

4D → Blockchain 如何一次解決:

Blockchain 如何解決 4D 問題

- Duplication:
  - Protected by the Proof-of-work mechanism
  - Every client has a copy of the list of transactions
- Double Spending:
  - The transaction needs to be confirmed by the nodes in the Blockchain network.
  - For example, Bitcoin protects against double spending by verifying each transaction added to the Blockchain to ensure that the inputs for the transaction had not previously been spent
- Dilution:
  - The amount of coin can be limited by proper design via protocol and algorithm.
  - Decentralized system: no central authority controls the right to issuing currency
- Data lost:
  - All transactions are trackable and are recorded in the Blockchain