

基於區塊鏈2.0智慧素養教育合約的初探研究

林億雄¹

中興大學應用數學系暨統計所

2018 年 09 月 27 日

¹任職單位：台灣首府大學教育研究所助理教授 Email : yhslin@tsu.edu.tw

Table of contents

Section.1 本文動機與相關文獻回顧

Subsection 1.1 互動式機器人的大腦詞彙解決方案

Subsection 1.2 區塊鏈的基本概念

Section.2 區塊鏈在教育領域上的實際應用

Subsection 2.1 區塊鏈在教育領域上的實際應用

Subsection 2.2 智慧素養教育合約流程圖

Section.3 以太坊 Ethereum 區塊鏈 2.0

Section.4 素養、智能合約、區塊鏈技術

Section.5 待解問題

互動式機器人的大腦詞彙解決方案

- (1) 使用大量工讀生收集輸入詞彙，簡稱**工人智慧**。
- (2) **機器學習**：**開放式網路爬蟲**，進行文字探勘(Text Mining)，結合主題模式 (Topic Model / Latent Dirichlet Allocation / LDA)，來完成主題與關鍵詞彙。
- (3) **機器學習**：**限制式網路爬蟲**，範圍僅止於Moodle + MOOCs 上進行探勘結合主題模式，來完成主題與關鍵詞彙。
- **問題**：網路社群資料來源合乎**GDPR**隱私權保護？

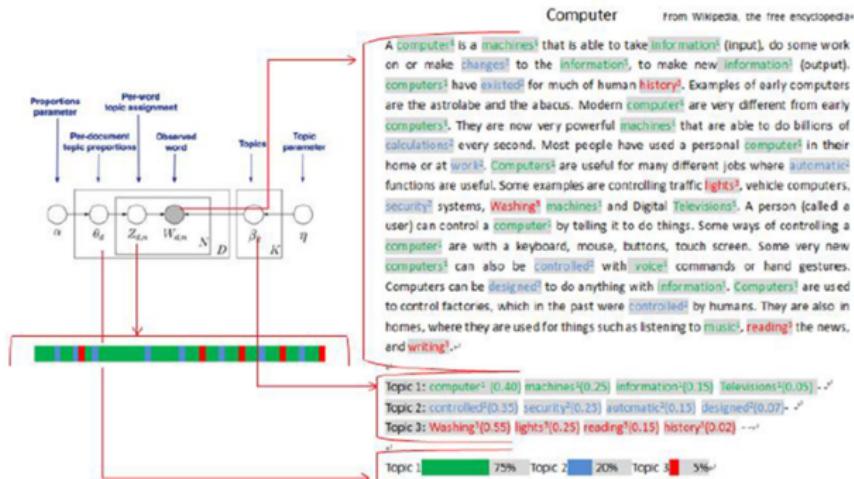
IBM Watson ([影片1](#))

互動式機器人的大腦詞彙解決方案

隱私權 - 健康區塊鏈觀念的啟發

- Tori Adams (2015/12), Vice President, ConsenSys Civic, (US Government Practice) <https://www.linkedin.com/pulse/blockchain-smart-contracts-health-booz-allen-hamilton-tori-adams>
- 區塊鏈可以協助建立以人為本的通用電子健康紀錄或將它稱為健康區塊鏈，**經過個人同意分享的醫療數據可被存儲在稱為數據湖（data lake）的數據存儲庫中。**
- 數據湖上的醫療數據將可成為多種健康、遺傳、預防醫學等研究分析的寶貴工具。此外，健康區塊鏈上收集的數據，**可依據個人的獨特條件與狀態提供個人化的建議與回饋。**
- 個人與醫療保健提供者間的智慧合約可用於確保個人遵守個人化建議的治療方案，**並根據個人的真實行為數據（如穿戴裝置記錄個人運動數據的智慧資產）來回饋績效鼓勵（如 healthcoin 智慧資產），以實現個人醫療保健目標。**

林億雄, 2013, The Choice of Prior to **Latent Dirichlet Allocation** for fitting topic models,
第二十二屆南區統計研討會, 國立高雄大學

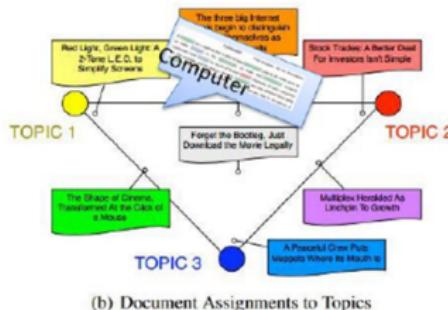


林億雄, 2013, The Choice of Prior to **Latent Dirichlet Allocation** for fitting topic models,
第二十二屆南區統計研討會, 國立高雄大學

Outline
Topic Model : Latent Dirichlet Allocation
Conclusion and Future Works

Topic Models
Topic Models
Latent Dirichlet Allocation (LDA)
Topic Modeling Tool : Mallet

Topic Models : Documents exhibit multiple topics



· (展示1)、文字探勘軟體示範

相關已發表文獻

- 林億雄，2013, **The Choice of Prior to Latent Dirichlet Allocation for fitting topic models**, 第二十二屆南區統計研討會, 國立高雄大學
- 林億雄，2015, **巨量資料分析研究運用在Moodle平台系統資料**, 2015年醫療雲端-數位學習-第五屆醫療數位學習研討會暨台灣醫療數位學習學會, 高雄醫學大學附設中和紀念醫院, 2015/10/03
- 郭添財，林億雄, 2017, **教育大數據時代的創新發展**, 台灣教育期刊, No.708, P.17-24.
- 林億雄，郭添財，蔡奎如，2018，**關於IBM Watson結合主題模式應用在智慧問答系統建置的初探研究**, 教育科技與學習, Vol.6, No. 1。 (已接受)
- 林億雄，郭添財，2018，**人工智慧對高等教育教學之挑戰與問題**, 台灣教育期刊, No.712, P.21-31

TextMining + Topic Models 應用在 Moodle



IBM Watson + Topic Model 應用在智慧問答



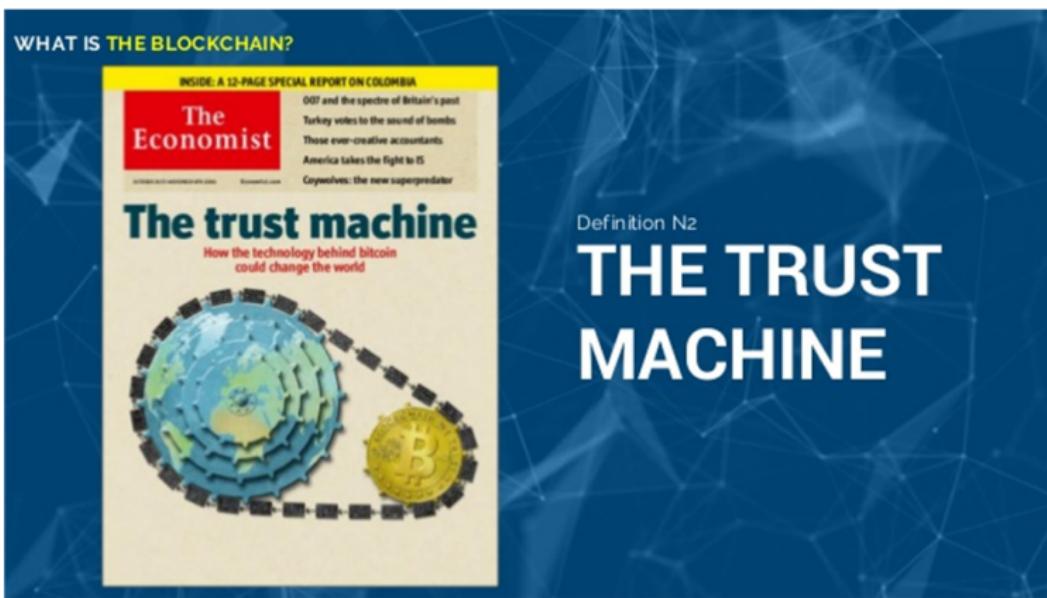
教育大數據時代的創新發展



人工智能對高等教育教學之挑戰與問題



區塊鏈 = The Trust Machine



臺灣網路認證公司策略長 杜宏毅 (2016) 指出
如果 Blockchain 真的是一個 **Trust Machine**

為什麼在金融服務的**實務上**, 我們還會需要

1. 准許制 Permissioned Model
2. 實名制 Rea-name / Non-anonymous System
3. 法規尊崇 Regulatory Compliance
4. 究責與賠償 Accountability & Liability

只有兩種可能



可能一：Blockchain
根本不是一個 Trust Machine

可能二：所謂 Trust Machine 的 Trust,
並不包括這些我們所需要的 Trust

區塊鏈

- 區塊鏈源自於比特幣交易的技術，本質上是一個去中心化的資料庫，通過分散式的節點進行網路數據儲存、驗證傳遞和交流，其最大的特徵是不依賴中央管理的方式處理數據，並將自由化市場落實在區塊鏈裡。區塊鏈不但能夠做比特幣交易，更能夠進行智能交易、電子商務等活動。
- 歐盟**GDPR**的個資法施行，區塊鏈可以作為個人隱私與資訊安全的解決方案。

報告內容

- 有趣的雅浦島巨石石幣故事
- 區塊鏈在教育領域上的實際應用
- 智慧素養教育合約流程圖
- 以太坊 Ethereum 區塊鏈 2.0
- 素養、智能合約、區塊鏈技術
- 待解問題與未來推廣

區塊鏈的基本概念

有趣的雅浦島巨石石幣故事

雅浦島的巨大石幣類似現代網路交易



雅浦島(Yap)是太平洋西部加羅林群島中的一個島，也是密克羅尼西亞聯邦最西的一個州。雅浦島約有1.2萬人，土地面積約100平方公里，當地人以圓如盤狀、中間有個洞的石頭作為交易媒介，並稱這種石幣為「拉伊」（Rai）。



Large *rai* stone in the village of Gachpar (2002).

拉伊石幣的交易類似現代網路交易

- 擁有拉伊石幣有如同擁有不動產，每個家庭維護自己的帳本資料。
- 以拉伊石幣所做的交易將由付款人到部落的會議中心向所有人宣布完成這項轉讓，部落中每個家庭自動更新自己的帳本。
- 拉伊石幣放在哪裡並不重要，重要的是誰擁有它。

建立全球大規模去中心化系統

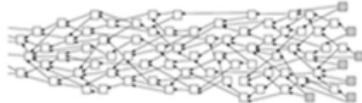
- 擁有全球及時通訊網路
- 建立機制，公開展示帳本
- 提供適當獎勵，可以有人協助維護帳本

區塊鏈 1.0、2.0、3.0

- 目前區塊鏈的演進大約可以分為三個主要階段，第一階段也就是以**比特幣**作為代表，這個體系將區塊鏈建立起來
- 而第二階段是以以太坊為主，以太坊（**Ethereum**）也是一個開源的公共區段鏈平台，其中以太幣（Ether）也是透過專用加密技術的去中心化的虛擬貨幣，到目前為止以太幣已經是市值第二高的加密貨幣，僅次於比特幣。
- 區塊鏈的第三階段目標就是超級帳本，以IBM及Linux基金會所創辦的「超級帳本計畫（**Hyperledger Project**）」、或針對物聯網而設計的區塊鏈**IOTA**為例，這是第一款專門為大型企業所設計的區塊鏈模組，主要是希望讓企業可以更輕鬆的導入區塊鏈技術，也代表著區塊鏈的發展日趨成熟。



Tangle



IOTA

Blockchain



Bitcoin
Ethereum

Blockchain Demo

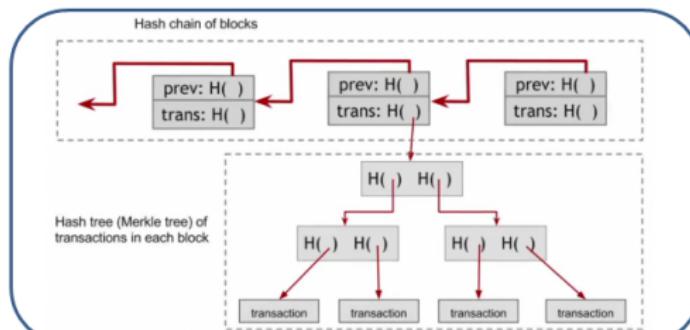
區塊鏈運用到的概念環環相扣

- 以下三點是區塊鏈能夠成為價值交換網絡的要素
- 資產的所有權可以被確認
 - 密碼學中的非對稱公開金鑰加密讓資產所有權可被確認
- 交易資訊無法被竄改
 - Hash函數讓區塊鏈中的所有交易資訊無法被竄改
- 共識去中心化成為信任機器
 - 工作量證明(PoW)演算法讓所有節點達成共識
- 請見區塊鏈實作Demo：<https://anders.com/blockchain/>

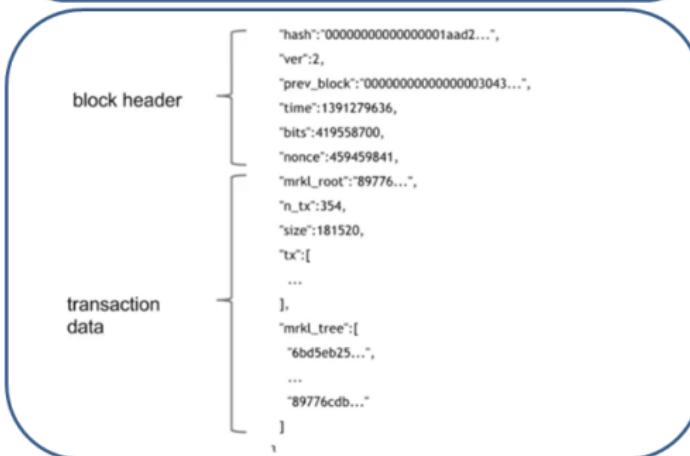
└ Section.1 本文動機與相關文獻回顧

└ Subsection 1.2 區塊鏈的基本概念

Blockchain data structure



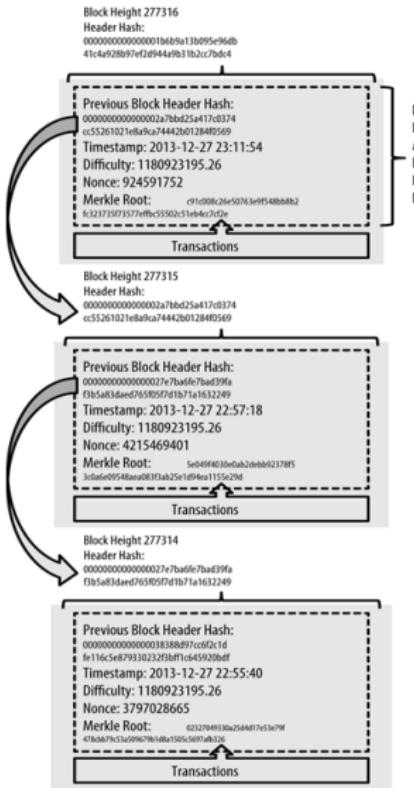
Block structure



└ Section.1 本文動機與相關文獻回顧

└ Subsection 1.2 區塊鏈的基本概念

Bitcoin block header structure



比特幣區塊鏈的特色

- 交易識別確認
 - 使用公開金鑰驗證機制，確認交易的真實性，使用者不可否認。
 - 屬於「可驗證的匿名制」，保留貨幣交易的特性。
- 資料無法篡改
 - 使用「區塊」與「鏈結」確保交易資料無法篡改。
 - 使用「條件雜湊(Hash<Difficulty)」與「前區塊雜湊」。
- 節點資料同步
 - 使用「工作量證明(POW : Proof of Work)」達到節點資料收斂同步。
 - 使用「分散式拓撲」，保留總困難指數高的分支，刪除總困難指數低的分支

區塊鏈運用到的概念

- 公/私鑰密碼學
- 點對點檔案共享
- 分散式運算
- 網路通訊協定
- 非實名機制
- 區塊鏈帳本
- 加密協議
- 加密貨幣

金融海嘯促使區塊鏈發展

- 號稱史上最嚴格個資保護法的歐盟GDPR於2018年上路。
- 2008年9月，以雷曼兄弟（Lehman Brothers Holdings Inc.）倒閉為開端，金融海嘯在美國爆發並向全世界蔓延。為應付危機，各國政府採取量化寬鬆等措施，救助由於自身過失而陷入危機的大型金融機構。這些措施帶來了廣泛的質疑，並一度引發了「佔領華爾街」運動，各界對政府的信心開始動搖。
- 中本聰(2008)發表了一篇名為《比特幣：一種對等式的電子現金系統》
- Bill Gates (1994) Said That '**Banking Is Necessary, Banks Are Not**' .
- 馬雲(2018)主張不應奢望以投資區塊鏈來一夕致富，比特幣是泡沫。他強調，投資區塊鏈技術是為了解決**數據隱私、安全和可持續性問題**，並不是一種投機的標的。比特幣是區塊鏈技術的第一個應用，但現在區塊鏈不只是比特幣。



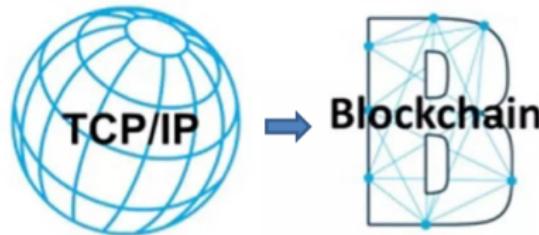
《大賣空》是一部2015年美國劇情片，是亞當·麥凱執導並和查爾斯·蘭道夫共同編劇。改編自麥可·路易斯的2010年同名書籍，主要描述2007年–2008年環球金融危機和泡沫經濟時期所發生的故事。[\(影片2\)](#)

網路傳遞「資訊」區塊鏈傳遞「價值」

- 第一代的網路主要傳遞**資訊**



- 新一代的網路將可傳遞**價值**，如:**資產轉移**



中本聰-Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

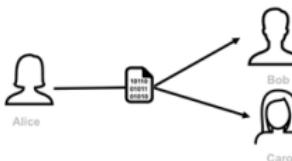
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

In 2008, Satoshi Nakamoto published a paper titled
Bitcoin: A Peer-to-Peer Electronic Cash System

數位貨幣系統二大難題

- 雙重支付問題

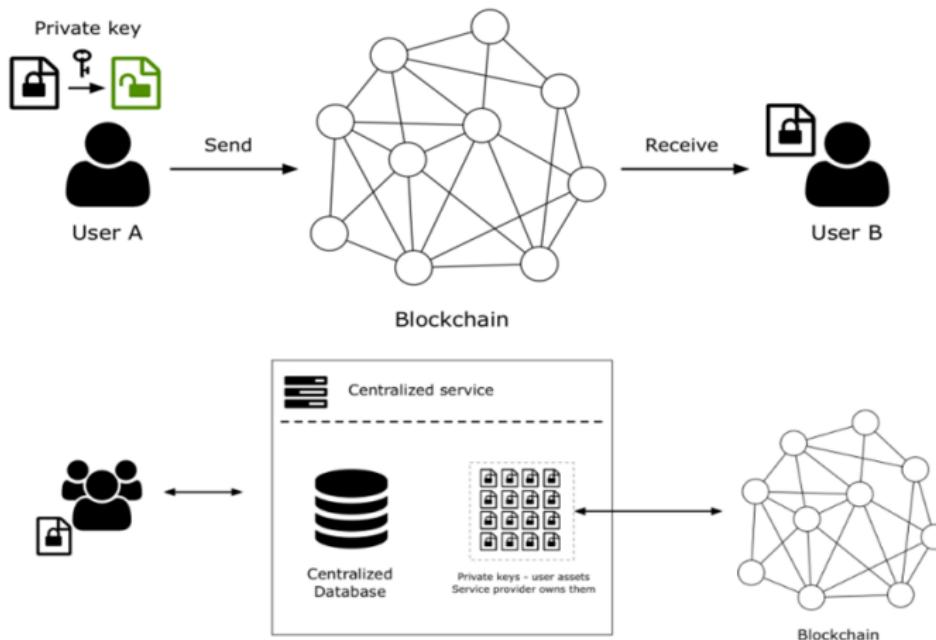


Double-Spending Problem: If Alice sends money in digital format to Bob, Bob cannot know for sure if Alice has deleted her copy of the file and she can choose to send the same file to Carol.

- 拜占庭將軍信任問題



去中心化網路交易



分散式運算

- SQL 集中式檔案管理系統
- Hadoop 分散式檔案系統 (影片 3)
- 區塊鏈：礦工節點下載總帳本資料

比特幣全網算力、耗電碳排放

- 摩爾定律：微處理器每18個月速度成長1倍。
- 比特幣全網投入的算力，2008 到 2013年6月，算力成長7倍。到了2014年6月成長 845 倍，2014年全網的算力是全世界 500 強的超級電腦算力總和的 6000 倍。
- 耗電上的碳排放量，如果 **1 bitcoin=1000** 美金，每年約產生 820 萬噸碳(等同賽普勒斯一年的排放量)，如果 **1 bitcoin = 100,000** 美金，每年約產生 8億2500 萬噸碳(等同德國一年的排放量)，如果 **1 bitcoin = 1,000,000** 美金，每年約產生 82 億噸碳(等同全世界一年的排放量20%)。

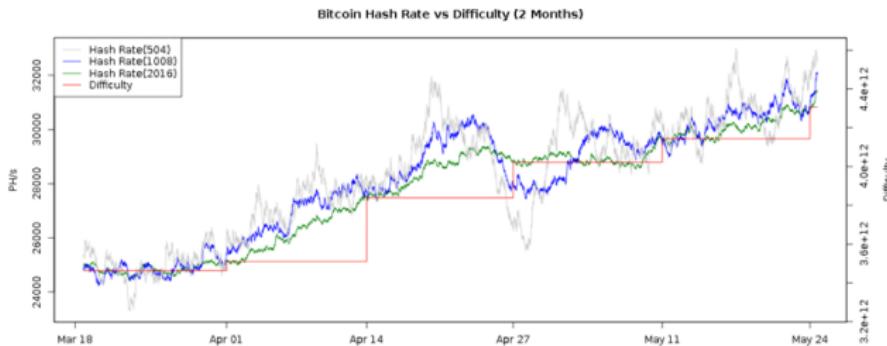
比特幣值多少錢挖礦才划算？

- 螞蟻礦機 S9 擁有 13.5 THash NT\$30,000 – SHA 256 算力 $\sim 13.5\text{TH/s}$ – 功耗 1100瓦特
- 目前挖礦效率最高的電腦是專為比特幣挖礦特製的螞蟻 S9 矿機，**一天可以產出 0.0013 個比特幣(2018/03)**，每天會消耗 32.8 度電。假設以一天要產一個比特幣計算，礦場需要運轉 770 台螞蟻 S9 矿機才能達成。這麼多礦機同時運作，每天要耗費 25,256 度的電。
- 一天挖一個比特幣需要 25,256 度電量，以非營業用電非夏天月份的費率計算，超出 1,001 度以上費率為 1 度電 4.83 元，因此電費約為 12 萬元。夏天的電費費率較高，超出 1,001 度以上費率為 1 度電 6.13 元，一天挖一個比特幣就要花費約 15 萬元。因此即使不計場地、人力和折舊等諸多額外成本，要在台灣靠比特幣挖礦賺錢，**比特幣的價格夏天至少要在 5,000 美元以上，非夏天至少要在 4,000 美元以上，才能支應龐大的電費成本(2018/03)**。
- 一般筆記型電腦的 19V 4.74A 就是電壓 19V 最大電流 4.74 安培， $19 \times 4.74 = 90.06 \times 24\text{hr} / 1000 = 2.16$ 度，一千瓦耗電一小時等於一度電，以一度 4 元，**筆記型電腦一天電費 8.64 元**。
- **2018/07 成本已經翻一倍，螞蟻 s9 矿機，一天約僅可產出 0.00065 個比特幣**

挖礦算力計算-以螞蟻礦機S9為例

Common Info		
Your hash-rate:	1350000000000 hashes/second	
Difficulty:	5178671069072 times difficult than difficulty 1	
Exchange Rate:	\$7.887,5000000/BTC (krakenUSD)	
Block time:	52 years, 2 months, 2 weeks, 1 day, 22 hours, 39 minutes, 27 seconds/block	
Network total:	39.902,136 Thash/second	
Profit		
Time Interval	BTC	US dollar
per Second	0,0000001 BTC	\$0,00005984
per Hour	0,00002731 BTC	\$0,21542735
per Day	0,00065550 BTC	\$5,17025640
per Week	0,0046 BTC	\$36,1918
per Month	0,020 BTC	\$157,18
per Year	0,239 BTC	\$1,888,44

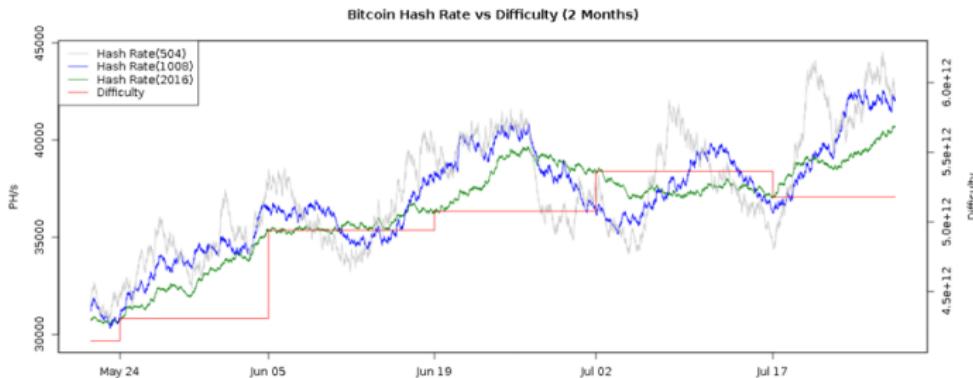
Bitcoin Difficulty 2018/05



Bitcoin Difficulty 2018/07

Bitcoin Difficulty: 5,178,671,069.072
 Estimated Next Difficulty: 5,809,357,037,628 (+12.18%)
 Adjust time: After 364 Blocks, About 2.2 days
 Hashrate(?): 42,253,399,210 GH/s
 1 block: 8.8 minutes
 Block Generation Time(?): 3 blocks: 25.4 minutes
 6 blocks: 52.9 minutes
 Updated: 12:55 (2.2 minutes ago)

Difficulty: 5178671069872	BTC/USD: 7941
1000000 KHash	2.023e-9 BTC/hour
1000 MHash	4.056e-8 BTC/day
1 GHash	3.399e-7 BTC/week
0.001 THash	0.000001457 BTC/month
	0.0001607 USD/hour
	0.0003056 USD/day
	0.002699 USD/week
	0.01157 USD/month





Article

A Statistical Analysis of Cryptocurrencies

Stephen Chan¹, Jeffrey Chu¹, Saralees Nadarajah^{1,*} and Joerg Osterrieder²

¹ School of Mathematics, University of Manchester, Manchester M13 9PL, UK;
stephen.chan@manchester.ac.uk (S.C.); jeffrey.chu@manchester.ac.uk (J.C.)

² School of Engineering, Zurich University of Applied Sciences, 8401 Winterthur, Switzerland;
joerg.osterrieder@zhaw.ch

* Correspondence: saralees.nadarajah@manchester.ac.uk; Tel.: +44-161-275-5912

Academic Editor: Charles S. Tapiero

Received: 7 April 2017; Accepted: 27 May 2017; Published: 31 May 2017

Abstract: We analyze statistical properties of the largest cryptocurrencies (determined by market capitalization), of which Bitcoin is the most prominent example. We characterize their exchange rates versus the U.S. Dollar by fitting parametric distributions to them. It is shown that returns are clearly non-normal, however, no single distribution fits well jointly to all the cryptocurrencies analysed. We find that for the most popular currencies, such as Bitcoin and Litecoin, the generalized hyperbolic distribution gives the best fit, while for the smaller cryptocurrencies the normal inverse Gaussian distribution, generalized *t* distribution, and Laplace distribution give good fits. The results are important for investment and risk management purposes.

Keywords: exchange rate; distributions; blockchain; Bitcoin

區塊鏈在教育領域上的實際應用

區塊鏈在教育領域上的實際應用

區塊鏈上的分散式教育平台



利用區塊鏈技術及其智能合約支付平台的優勢，ODEM將使學生和教授直接互動並參與教育和學習的交流，而無需中介機構的參與。

區塊鏈認證服務 – Proof of Existence

Proof-of-Existence

Publish PoE

Verify PoE

About

Contact

Publish Proof-of-Existence Upload the file & get the PoE link

Name:

Your Name

Email:

Your Email ID

Message:

(Optional) I am the original creator of this file & this Blockchain-based PoE is the proof.

File to Generate PoE

Click here or drag and drop your document in the box.
The file will NOT be uploaded. The cryptographic proof is calculated client-side.

What is it?

This is a tool to generate a Proof-of-Existence of a file or record on Blockchain. By submitting this form you will be uploading the file's signature with its associated information into the Private Decentralized Public Ledger. Records stored here can later be fetched to prove that this file existed on particular date & time with the associated information.

Computationally & Technologically it is impossible to fake the Document's signature and/or modify the past records. Hence this PoE can be used to prove the file's existence in legal matters.

How it works?

- **Step 1:** Fill the form & Upload the file
- **Step 2:** Copy the link & Share it with people you want to prove its existence
- **Step 3:** Anyone with link or file can verify the existence of the file at particular date & time.

使用者可以在網頁端針對藝術作品、或軟體進行雜湊運算，證明該事物的著作權。

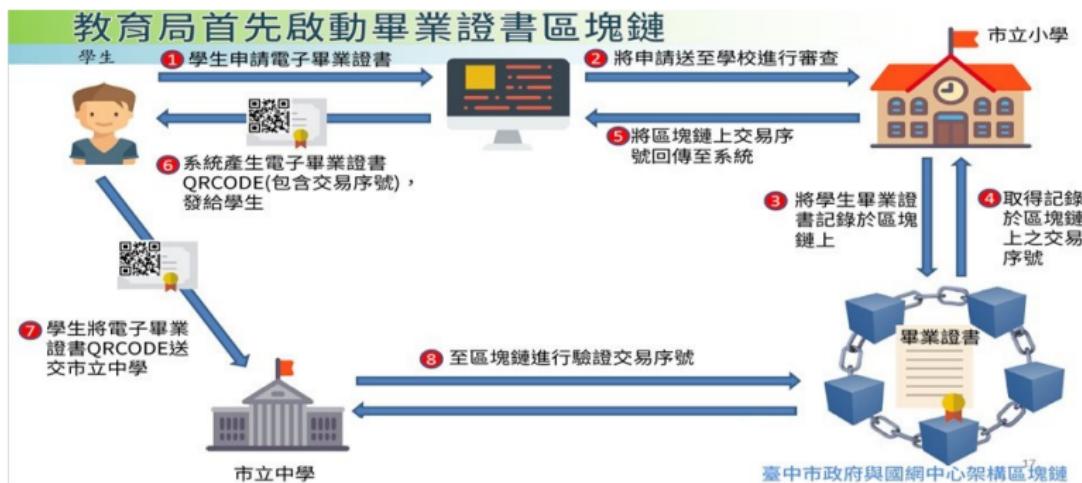
區塊鏈透明助學

- 區塊鏈的智慧合約有無數用途，智慧素養教育合約就是其中一種。如果有人給孩子提供上學資助，可以透過智慧合約**自動確認學習進度，滿足學習合約後，自動觸發後續資金撥付給下個學習模組**。
- 區塊鏈學習合約能夠使學習者和資助者之間完全以點對點方式進行協調，公開透明，對雙方都是正向激勵。

數位文憑+區塊鏈技術

- 麻省理工學院（MIT）數位文憑採用比特幣區塊鏈技術，當學生下載專屬Wallet後即產生一組公鑰與私鑰，將公鑰傳給MIT寫入數位紀錄中，並在該區塊鏈中加上認證碼，區塊鏈上並沒有文憑資訊，只有MIT建立該紀錄的時戳，MIT再寄出含公鑰的數位文憑，由學生手機上的私鑰驗證本人，已於2017年夏天執行一項前導計畫，採用了區塊鏈技術讓111名畢業生透過智慧型手機的行動程式領取他們的數位文憑，成為全球首批頒發虛擬證書的大學之一。
- 國立成功大學(NCKU)為了確保大學和研究所入學甄試的資料真實性，看中區塊鏈去中心化、不可篡改的特性，使用區塊鏈保存學生的學習歷程記錄，也在2017年8月展示與台灣金融研訓院、永豐金控共同推出證書區塊鏈i-Certificate後，近期成大在證書區塊鏈上又有新進展，透過分散式帳本技術IOTA的底層帳本架構Tangle，開發了自主身分認證系統TangleID，用來記錄學生的學習歷程。

區塊鏈 + 證書



臺中市政府與國網中心一同建置小學畢業證書區塊鏈的應用，畢業生申請電子證書後，經過教網中心**指定的驗證單位驗證**，系統會將該畢業證書資訊，記錄到區塊鏈上，產生**JSON檔和QR Code**供學生保存，日後畢業生即可以使用QR Code取得電子證書
(2017/12；圖片來源／蕭景燈)。

區塊鏈在畢業證書上的應用

- 臺中市政府與國網中心一同建置小學畢業證書區塊鏈的應用，畢業生申請電子證書後，**經過教網中心指定的驗證單位驗證**，系統會將該畢業證書資訊，記錄到區塊鏈上，**產生JSON檔和QR Code供學生保存**，日後取得電子證書。
- (區塊鏈 Proof of Authority 認證證明共識機制)**

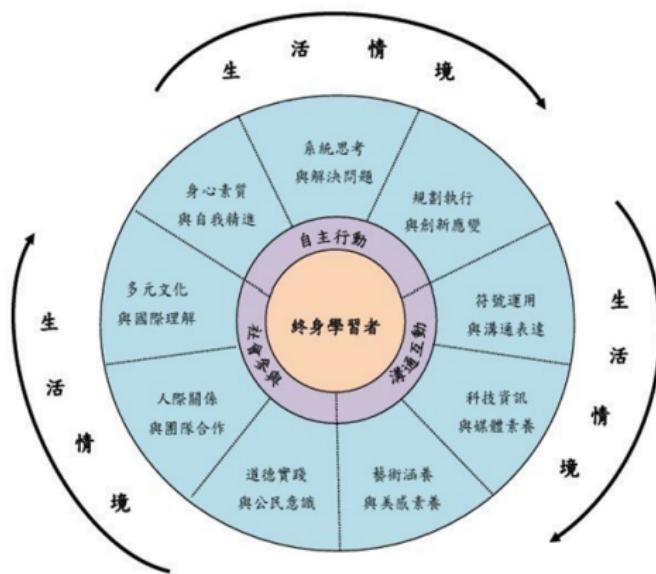


智慧素養教育合約流程圖

智慧素養教育合約流程圖

教育合約+區塊鏈技術 (1)

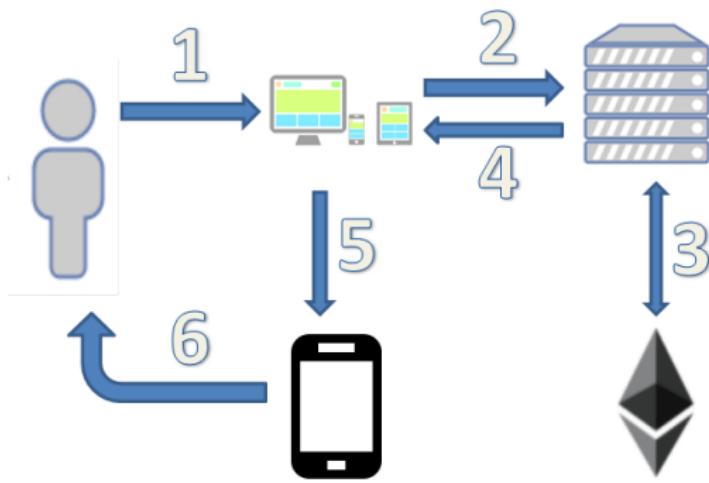
- 區塊鏈 + 素養 + 智能合約 → 應用教育領域
 - 區塊鏈是解決方案：**個人隱私與資訊安全的解決方案**。
 - 素養 (**literacy**) 是指「識別、理解、解釋、創造、運算及使用不同環境下印刷與書面資料的能力。為涉及個人能夠實現目標、發展知識和潛能，並充分參與社區及廣大社會的**連續學習**」。
 - 智能合約(Smart Contract)一詞由尼克薩博 (Nick Szabo) 於1990 年代初期提出倡議可**將交易的條款透過電腦化來落實**。



「素養」是一個簡約的理論架構。這個理論架構有很大的彈性，12年課綱中的「三大面向、九大項目」，都是在這個架構下長出來的東西。

圖／取自教育部

基於區塊鏈2.0智慧素養教育合約流程圖



1: 進入網頁輸入 Ethereum Address。

2: 後端伺服器認證，進行使用者學習歷程紀錄，如：Moodle、Moocs。

3: Ethereum 雲端認證，智能合約於區塊鏈執行，結合 Moodle 或 Moocs。

4: 將智能合約所產生的 JSON 檔和 QR Code，傳至網頁供使用者保存。

5: 將所產生 JSON 檔和 QR Code，傳送至使用者手機下載保存。

6: 使用者可由手機查看教育合約執行內容。

區塊鏈市場3大主流



以太坊 **ETHEREUM** 區塊鏈 2.0

以太坊 - 區塊鏈2.0

- 2013年Vitalik Buterin 公開介紹以太坊，並發布以太坊的白皮書。以太坊是一個開源的區塊鏈平台，其交易的貨幣稱為以太幣(ETH)，與比特幣一樣具有挖礦機制，其智能合約系統為一大特色，讓開發者可以撰寫智能合約然後提交給以太坊虛擬機(EVM)進行編譯，並且部署到區塊鏈上，每個被部署在以太坊區塊鏈的智能合約都具有一個位址。

以太坊升級

- 2016年以太坊創始人Vitalik Buterin 發布以太坊關鍵改進的紫皮書（Mauve Paper），並且試圖解決二大問題：
- (1)比特幣以工作量證明（proof-of-work）為基礎的共識機制低效、耗能、不綠色環保
- (2)改善以太坊功鏈系統吞吐量（throughput）和容量不足支撐全球大範圍高頻次使用。

以太坊升級

- **針對第一個問題**，紫皮書提出一個新的基於權益證明（*proof-of-stake*；PoS）的共識機制，命名為 Capser，能讓參與「挖礦」的方式，從原來使用專門定製「礦機」並消耗電力能源進行大量計算爭奪以區塊的構造和收益權，轉變成直接將資金兌換為以太幣注入以太坊區塊鏈，「挖礦」相關的智能合約（Smart Contract）自動根據資金的注入量成比例隨機分配區塊的構造和收益權，這一新的共識機制有望使以太坊公鏈變得更安全、更高效和更綠色。
- 除此，在Ethereum Rinkeby 測試網域則採用認證證明（*proof-of-authority*；PoA）的共識機制，僅提供認證的位址才能進行確認交易。

以太坊升級

- 針對第二個問題，關於吞吐量和容量的局限，紫皮書提出了縮短區塊產生間隔時間（blocktime）和分區（sharding）這兩個解決方案。在保證安全的前提下，新的算法把區塊產生間隔時間從12秒降低為4秒，使吞吐量提升為現在的三倍。以太坊每個節點無需處理全網所有事務（transaction）和儲存全網所有的數據，只要關注其中一個或幾個分區的事務和數據即可，所有節點通過分工配合來完成覆蓋所有分區的目標。這麼做能使以太坊的容量增大為現有的80倍。同時，由於各分區的事務可以並發處理，吞吐量再獲提升，變為現有水平的240倍（ 3×80 ）。

智能合約 Smart Contract

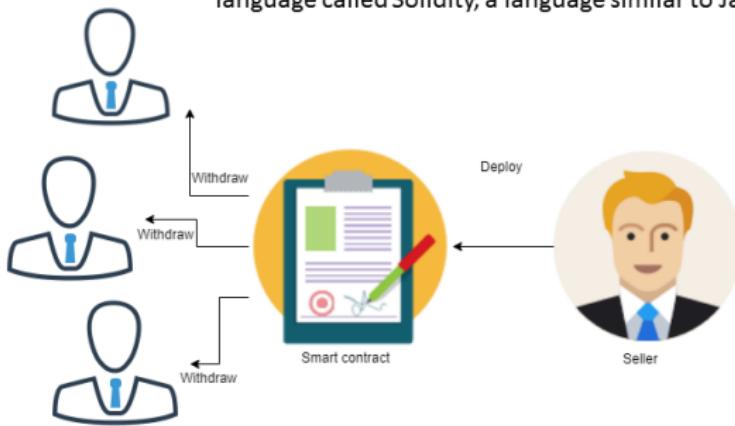
- 智能合約(Smart Contract)一詞是由學者尼克·薩博(Nick Szabo)於1990年代初期提出可以將交易的條款透過電腦化來落實；但是，當時並沒有得到太多的回響，直到這幾年，智能合約才隨著區塊鏈(Blockchain)技術的興起，逐漸在金融業中流傳開來。
- 2016年區塊鏈平台—以太坊(Ethereum)的推出，其白皮書名為「新一代智能合約與分散式應用平台」(A Next-Generation Smart Contract and Decentralized Application Platform)，強調智能合約為其平台特色，一舉將智能合約這個名詞推到一個新的層次，讓大家開始注意到智能合約的重要性，甚至視其為「區塊鏈2.0」的主要技術與應用。

智能合約：執行於EVM的程式

- 智能合約是一個運行在區塊鏈 VM 上面的 instance。更精確說，在 Ethereum Blockchain 上的 Smart Contract是指能運作在 Ethereum Virtual Machine (EVM) 上面的程式碼。
- 此程式碼可以把它當作是一個類別 (class)，它必須被部署 (deploy) 到區塊鏈上，此程式會被創造出一個 instance，而這個 instance 將會被放在區塊鏈上。一旦合約部署成功時會得到一個地址，它就像記憶體位置一樣，取得這個位置後搭配正確的 interface 資訊就可以執行這個合約。

Solidity : smart contract **on line**

This smart contract will be written in a programming language called Solidity, a language similar to JavaScript.



```
pragma solidity ^0.4.4;

contract SplitIt {

    address[] employees = [address01,address02,..];
    uint totalReceived=0;
    mapping (address => uint) withdrawnAmounts;

    function SplitIt() payable {
        updateTotalReceived();
    }

    function () payable {
        updateTotalReceived();
    }

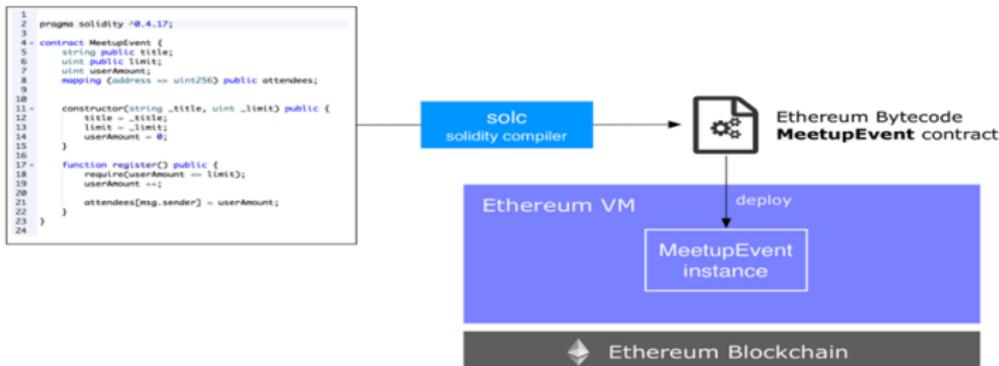
    function updateTotalReceived() internal {
        totalReceived += msg.value;
    }

    modifier canWithdraw() {
        bool contains = false;
        for(uint i = 0; i < employees.length; i++) {
            if (employees[i] == msg.sender) {
                contains = true;
            }
        }
        require(contains);
    }

    function withdraw() canWithdraw {
        uint amountAllocated = totalReceived/employees.length;
        uint amountWithdrawn = withdrawnAmounts[msg.sender];
        uint amount = amountAllocated - amountWithdrawn;
        withdrawnAmounts[msg.sender] = amountWithdrawn + amount;

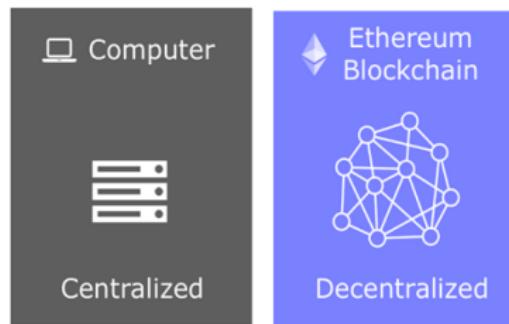
        if (amount > 0) {
            msg.sender.transfer(amount);
        }
    }
}
```

運作在 Ethereum Virtual Machine (EVM) 上面的程式碼



去中心化架構。

- 在區塊鏈 VM 上跑的程式（也就是 Smart Contract）跟一般 VM 上跑的程式，最不一樣的地方就在於去中心化架構。



區塊鏈技術-小結

- 區塊鏈是由密碼學的加密函數及分散式資料庫所組成的點對點交易系統，比特幣的底層技術，是一種解決方案，是人工智慧下個人隱私與資訊安全的解決方案。
- **使用電子錢包，如: Ethereum Wallet可以很快了解區塊鏈的運作機制。**
- 區塊鏈的貢獻在於可以傳遞價值，例如資產等。這是現今網路僅能傳遞訊息所無法做到的，所以區塊鏈也被視為新一代的網路協定。
- **挑戰利用 PoW(工作證明)使區塊間無法竄改的共識機制。**目前有以太坊的 PoS(權利證明)、PoA (認證證明)。因為PoW機制需高算力且耗電，所以以太坊提出PoS, PoA希望避免使用者利用ASIC礦機挖礦，及改善耗電的問題。另外，最大亮點在於可於EVM上執行智能合約。
- 目前除了有挖礦的區塊鏈，還有不需挖礦的IOTA 以 Tangle分散式技術及 IBM + Linux 所合作的Hyperledger Project為主，交易時間更短，解決規模化大量使用點對點交易的問題。

素養、智能合約、區塊鏈技術

舉例：線上學習智慧素養教育合約

- 所謂「素養」，就是「**知識、技能、態度**」。
 - 「知識」指的是學生對一套理論的理解，**比如知道平均數、中位數**。
 - 「技能」指的是學生學習到的實作能力，**比如可以使用平均數、中位數解釋目前年輕人薪資水準**。
 - 「態度」指的是對前兩者的價值判斷和個人感受，比如說，**學生知道如何正確解釋全球世界年輕人薪資水準，並且對現今台灣社會職場新鮮人薪資水平提出建議與解釋**。
- 檢測學生對一套教材的「素養」掌握到什麼地步：
 - 你學到了什麼？
 - 你覺得這東西可以怎麼用？
 - 你對這東西有什麼感覺？

例子 :線上學習智慧素養教育合約

- 統計學概論 - 第一章

授課教材：謝邦昌教授 / 統計學概論 數據資料的解讀者 / 華立圖書

授課教師：林億雄 Email : yhslin@tsu.edu.tw

- 請展開完成網路自我學習測試

- Step 1 : 線上學習與閱讀

0:19 問題一 出處：何謂統計學？

0:25 問題二 出處：請問你有哪四種資料尺度？

0:36 問題三 出處：請問你有哪二種資料型態？

1:04 問題四 出處：請問你母體參數包括哪四類？

1:13 問題五 出處：請問你何謂樣本統計量？

Step 2 : 網路學習測驗 <http://ppt.cc/ZaCq>

Step 3 : 自我檢測 統計學概論第一章 習題 <http://ppt.cc/65Ks>



統計學第01章網路學習測驗 By Leo



*必填

請輸入受測者系級 *

請輸入受測者姓名 *

請輸入受測者學號 *

請輸入受測者性別 *

請輸入受測單元代碼 *

問題一：請問何謂統計學？

統計學概論第一章習題

*必填

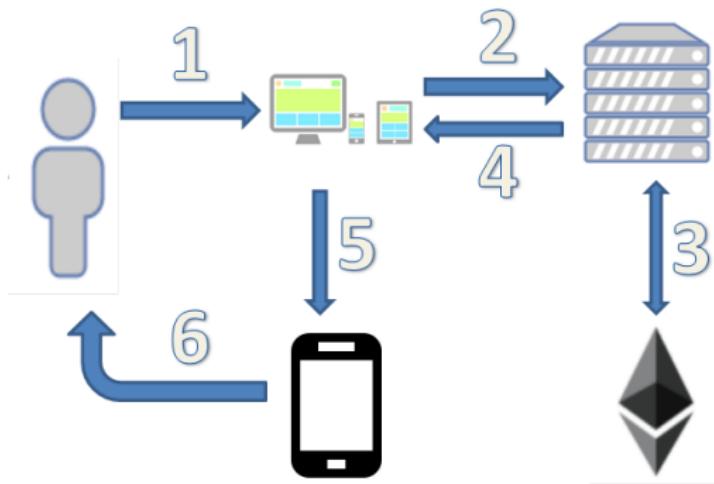
1.下列何者敘述最符合統計學的意義？*

- (a) 統計學是利用數字來推論統計的科學
- (b) 統計學主要是規劃資料的蒐集、整理與分析
- (c) 統計學主要是利用樣本的訊息來推論母體的資訊
- (d) 統計學主要是研究概率的問題解決不確定性
- (e) 統計學是一種抽樣及問卷設計的學科

2.在變數的型態中通常可分成名目變數、順序變數、區間變數和比例變數四類型，試寫出下列變數應為何種變數型態？*

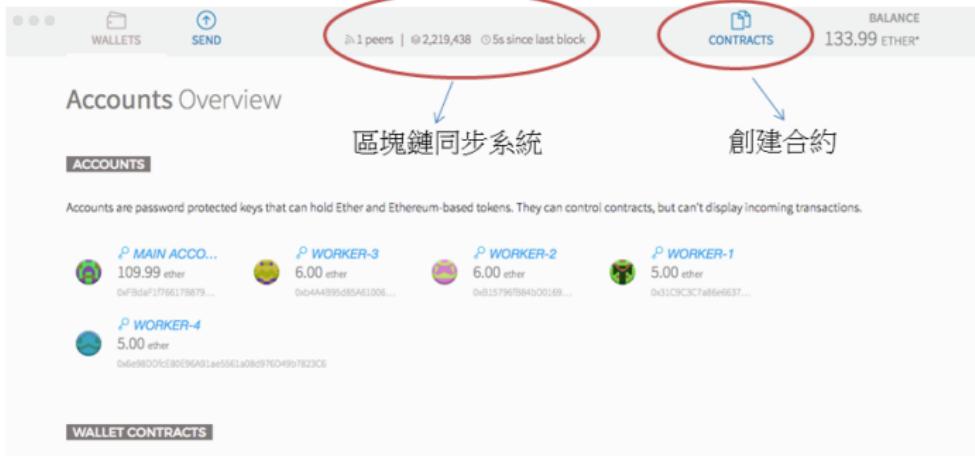
	名目變數	順序變數	區間變數	比例變數
(a)學生的學號	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(b)成績單上的成績 排名	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(c)軍隊軍官職位資 料	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(d)年齡在19歲以 下、20歲到64歲、 65歲以上	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(e)某產品銷售金額	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

基於區塊鏈2.0智慧素養教育合約流程圖



- 1 : 進入網頁輸入 Ethereum Address 。
- 2 : 後端伺服器認證，進行使用者學習歷程紀錄，如：Moodle 、 Moocs 。
- 3 : Ethereum 雲端認證，智能合約於區塊鏈執行，預期結合 Moodle 或 Moocs 。
- 4 : 將智能合約所產生的 JSON 檔和 QR Code ，傳至網頁供使用者保存。
- 5 : 將所產生 JSON 檔和 QR Code ，傳送至使用者手機下載保存。
- 6 : 使用者可由手機查看教育合約執行內容。

創建者：發布智能合約



交易確認：PoA 認證證明

LATEST TRANSACTIONS

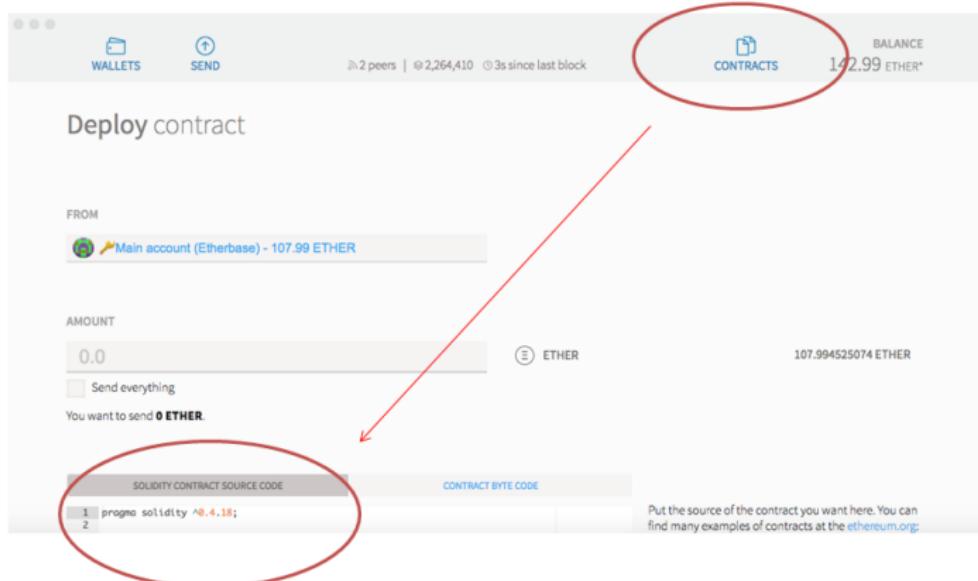
Filter transactions

Date	Type	Description	Confirmations	Value	Actions
May 13	Contract execution	Worker-1 → :Split03	0 of 12 Confirmations	-0.00 ETHER	
May 13	Contract execution	Worker-2 → :Split03	1 of 12 Confirmations	0.00 ETHER	
May 13	Contract execution	Worker-1 → :Split03	4 of 12 Confirmations	-0.00 ETHER	
May 13	Created contract	Main account (Etherbase) → Created contract at :Demo-Split2018	6 minutes ago	-0.00 ETHER	
May 5	Sent	Main account (Etherbase) → 0x62ca05a2E7CA852b21D203cc90F0979E31B881B3A		-1.00 ETHER	

Show More



創建者 : Solidity程式碼佈署



創建者 : Smart Contracts

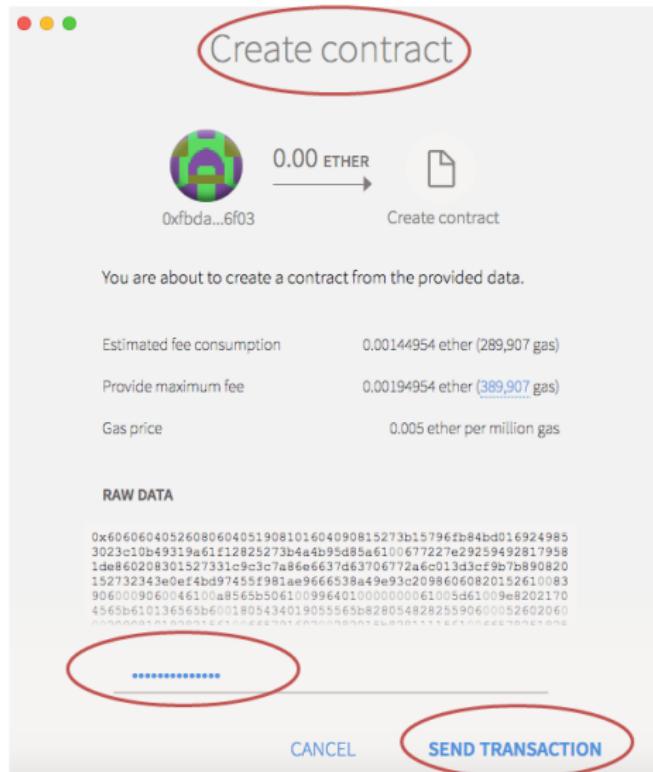
The screenshot shows the Etherbase wallet interface. At the top, it displays network status (1 peers), transaction count (2,271,671), and time since last block (2s). It also shows the user has 142.99 Ether. Below this, the 'WALLETS' tab is selected, showing the main account with 107.99 Ether.

In the 'SEND' section, the amount is set to 0.0 Ether. There is a checkbox for 'Send everything' which is unchecked. A note below says 'You want to send 0 Ether.'

The main area shows the 'SOLIDITY CONTRACT SOURCE CODE' for a 'SplitIt' contract:

```
1 pragma solidity ^0.4.4;
2
3 contract SplitIt {
4     address[] employees = [0x815796fB84b00163749853023C10b49319A61f12, 0xb4A4895d85A6100677];
5
6
7
8     uint totalReceived;
9     mapping (address => uint) withdrawnAmount;
10
11     function SplitIt() payable public{
12         updateTotalReceived();
13     }
14
15 }
```

A red circle highlights the first few lines of the Solidity code. To the right, the 'CONTRACT BYT CODE' and 'SELECT CONTRACT TO DEPLOY' sections are visible, though they are currently empty.



創建者:智能合約發布成功

1

May 13	Created contract	6 minutes ago	-0.00 ETHER
May 5	Sent		-1.00 ETHER

2

智能合約產生
Contract Address、
JSON Interface

The interface includes sections for Wallets, Send, Contracts, and a detailed view of the deployed contract. The detailed view shows the contract address (0x08e72190377002091B01112F01136E7E) and its balance (193.98 ETHER*). It also provides options to transfer ether/tokens, copy the address, show a QR code, or show the JSON interface.

WALLETS SEND CONTRACTS 193.98 ETHER*

智能合約產生
Contract Address、
JSON Interface

0x08e72190377002091B01112F01136E7E 193.98 ETHER*

Transfer Ether & Tokens

Copy address

Show QR-Code

Show Interface

HIDE CONTRACT INFO

READ FROM CONTRACT WRITE TO CONTRACT

創建者：Watch Smart Contract

- **Contract Address :** 0x08e721903770082083B04F24FfDF90523e2EE0f9
- **JSON :** [{ "constant": false, "inputs": [], "name": "withdraw", "outputs": [], "payable": false, "stateMutability": "nonpayable", "type": "function" }, { "inputs": [], "payable": true, "stateMutability": "payable", "type": "constructor" }, { "payable": true, "stateMutability": "payable", "type": "fallback" }]
- 使用者取得創建者發布的 **Contract Address**，及 **JSON**，就可以執行智能合約。

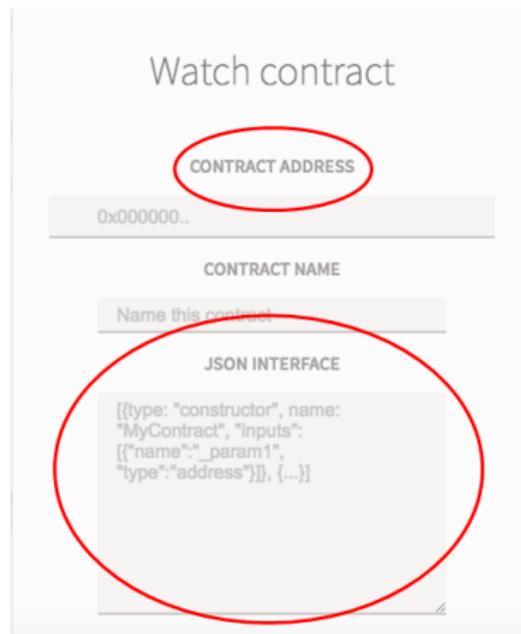
使用者：**WATCH CONTRACT**

使用者 : Watch Contract

The screenshot shows a blockchain wallet interface with the following elements:

- Top Bar:** Includes icons for close, minimize, maximize, and exit; tabs for "WALLETS" and "SEND"; a progress bar; "CONTRACTS" tab; and a balance of "182.98 ETHER*".
- Section Header:** "CUSTOM CONTRACTS"
- Contract List:** A grid of 15 contract entries, each with a small icon, name, ether balance, and address. The contracts listed are:
 - 2018-DEMO (6.00 ether)
 - 2018-SMAR... (0.00 ether)
 - :01-智能合... (0.00 ether)
 - :DEMO-SP... (0.00 ether)
 - :GREETER ... (0.00 ether)
 - :SAMPLE O... (0.00 ether)
 - :SIMPLE ST... (0.00 ether)
 - :SPLIT IT 5... (0.00 ether)
 - :SPLIT IT E... (0.00 ether)
 - :SPLIT01 (0.00 ether)
 - :SPLIT03 (0.00 ether)
 - :GREET-KILL (0.00 ether)
 - :LEO SMAR... (0.00 ether)
 - :LEO SMAR... (0.00 ether)
 - GREET-01 (0.00 ether)
 - :LEOCOIN (ADMIN PAGE) (0.00 ether)
- Bottom Left:** A blue button labeled "WATCH CONTRACT" with a white plus sign, which is circled in red.

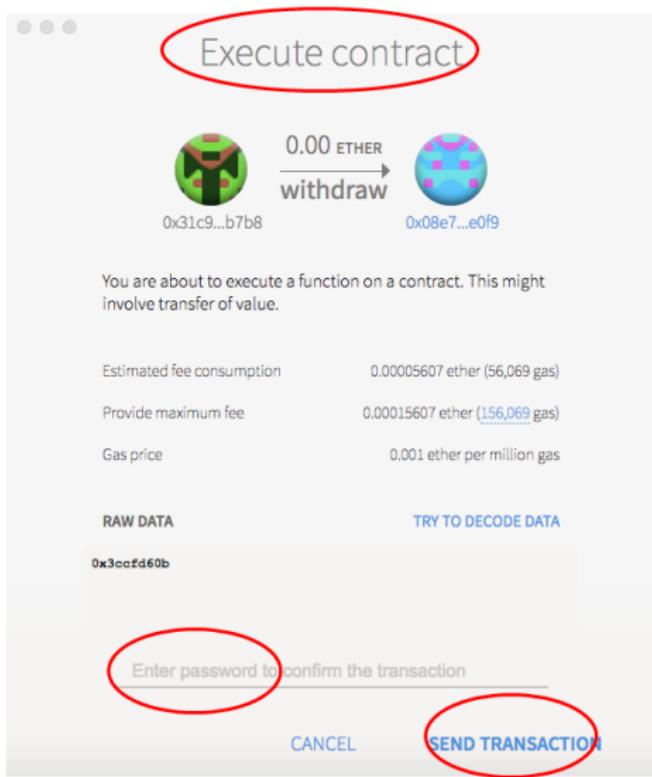
使用者 : Watch Contract



使用者 : Watch Contract

The screenshot shows a blockchain wallet interface with the following elements:

- Top Bar:** Includes tabs for **WALLETS** (circled in red), **SEND**, network status (1 peers, 2,363,109 blocks, 17s since last block), **CONTRACTS**, and account balance (193.98 ETHER* and 6.00 ETHER*).
- Wallet List:** Shows a single wallet entry: **2018-DEMO**.
- Buttons:** **HIDE CONTRACT INFO** (blue button) and two large buttons at the bottom: **READ FROM CONTRACT** and **WRITE TO CONTRACT**.
- Function Selection:** A dropdown menu titled "Select function" with "Withdraw" selected.
- Execution Context:** A section titled "Execute from" showing "Worker-1 - 3.02 ETHER".
- Execute Button:** A large blue button labeled **EXECUTE** (circled in red).



執行智能合約成功

LATEST TRANSACTIONS

Filter transactions

Date	Type	Description	Status	Value	Actions
May 13	Contract execution	Worker-1 → :Split00	0 of 12 Confirmations	-0.00 ETHER	
May 13	Contract execution	Worker-2 → :Split00	1 of 12 Confirmations	-0.00 ETHER	
May 13	Contract execution	Worker-1 → :Split00	4 of 12 Confirmations	-0.00 ETHER	
May 13	Created contract	Main account (Etherbase) → Created contract at :Demo-Split2018	6 minutes ago	-0.00 ETHER	
May 5	Sent	Main account (Etherbase) → 0x62ca05a2E7CA852b21D203cc90F0979E31B881B3A		-1.00 ETHER	

Show More

Etherscan：透過API使用網頁查詢

The screenshot shows the Etherscan interface for the Rinkeby (CLIQUE) TESTNET. At the top, there is a navigation bar with links for Home, Blockchain, Token, Chart, and Misc. Below the navigation bar, there is a search bar and a Go button. A banner for the SLX TOKEN PRE-SALE MAY 11 - 45% DISCOUNT is displayed, stating "Unrestricted global entertainment access. SLATE powers future entertainment".

Blocks:

- Block 2263073 Mined By 0x663f83421bf059... > 24 secs ago
- Block 2263072 Mined By 0x42eb768f244c88... > 39 secs ago
- Block 2263071 Mined By 0xfc10cbc391de84d... > 54 secs ago

Transactions:

- TX# 0XP9CC56EC8E5EACBDCD2714... From 0x9e282642a4ca1... To 0x8190c2cbf65381a... Amount 0.04597832 Ether > 24 secs ago
- TX# 0X0BA0BB9D8DC27D18D2F94E... From 0xd4d0de9370eff1... To 0x02daaaed56413c... Amount 0.1 Ether > 24 secs ago
- TX# 0XF1D2ECB2CB362D843D51D0... From 0x31b98d14007bde... To 0x52c3a960f293cac... Amount 18.75 Ether > 24 secs ago

<https://rinkeby.etherscan.io/>

Etherscan : 查詢交易內容

The screenshot shows a detailed view of a Ethereum transaction on the Etherscan interface. The transaction hash is 0x2e3a318ae25c01a8a961ae346f1ae4de680758502942585a83d219837dd4542. The status is Success, and it has 2208512 confirmations. The transaction was timestamped at 13 hrs 10 mins ago (May-01-2018 06:02:19 PM +UTC). The recipient address is 0x8d593ec80c9541e1fd4376796292f56e9c659601, and the value sent is 1 Ether (\$0.00). The gas limit was 129500, and the gas used was 29500. The gas price was 0.00000003 Ether (3 Gwei). The actual transaction cost/fee was 0.0000885 Ether (\$0.000000). The nonce was 20. The input data field contains a large hex string: 0x4c656f20536179203a20e4bc... (truncated for brevity). A 'Convert To UTF8' button is visible below the input data.

Transaction Information	
TxHash:	0x2e3a318ae25c01a8a961ae346f1ae4de680758502942585a83d219837dd4542
TxReceipt Status:	Success
Block Height:	2208512 (3162 block confirmations)
TimeStamp:	13 hrs 10 mins ago (May-01-2018 06:02:19 PM +UTC)
From:	0x8d593ec80c9541e1fd4376796292f56e9c659601
To:	0x8d593ec80c9541e1fd4376796292f56e9c659601
Value:	1 Ether (\$0.00)
Gas Limit:	129500
Gas Used By Txn:	29500
Gas Price:	0.00000003 Ether (3 Gwei)
Actual Tx Cost/Fee:	0.0000885 Ether (\$0.000000)
Nonce:	20
Input Data:	0x4c656f20536179203a20e4bc... [Truncated]

Account 0xFBdaF1f76617B879714f3b1a227E661f416a6f03

The screenshot shows the Etherscan interface for the RINKEBY (CLIQUE) TESTNET. The address `0xFBdaF1f76617B879714f3b1a227E661f416a6f03` is entered in the search bar. The page displays the following information:

- Overview:** Balance: 91,24461805 Ether, Transactions: 29 txns.
- Transactions:** A table showing the latest 25 transactions from a total of 29. The table includes columns: TxHash, Block, Age, From, To, Value, and [Tx fee]. The data is as follows:

TxHash	Block	Age	From	To	Value	[Tx fee]
0x2ea3a318ae25c0...	2208512	13 hrs 13 mins ago	0xfbdaaf1f76617b879...	0xdad593ec80c9541...	1 Ether	0.0000088
0xfbad03ef53cd350...	2208436	13 hrs 32 mins ago	0xfbdaaf1f76617b879...	0xdad593ec80c9541...	1 Ether	0.0000084
0x2ad02fa52116ad...	2184738	4 days 16 hrs ago	0xfbdaaf1f76617b879...	0xContract Creation	0 Ether	0.00032013
0xddb2aaacf20a36a...	2184697	4 days 16 hrs ago	0xfbdaaf1f76617b879...	0xContract Creation	0 Ether	0.00028467

Contract 0x65F69D82Ed403adE1478f563957C22b1a7B03A81

The screenshot shows the Etherscan interface for the Rinkeby Testnet. The URL in the address bar is <https://rinkeby.etherscan.io/address/0x65f69d82ed403ade1478f563957c22b1a7b03a81>. The page title is "Rinkeby Accounts, Address...". The navigation bar includes links for HOME, BLOCKCHAIN, TOKEN, CHART, and MISC.

Contract Overview:

- Balance: 3 Ether
- Contract Creator: 0xfbda1f76617b879... at bn 0x133cb0ff58b459fd...
- Transactions: 11 txns

Transactions: Shows the latest 11 transactions for the contract.

TxHash	Block	Age	From	To	Value	[TxFee]
0x215425c4373908...	1999737	36 days 19 hrs ago	0xfbda1f76617b879...	IN 0x65f69d82ed403ad...	3 Ether	0.000026278
0x604bf9ef894ec54...	1999725	36 days 19 hrs ago	0xb15796fb64bd016...	IN 0x65f69d82ed403ad...	0 Ether	0.000074458
0x707cf0444edd5e0...	1999720	36 days 19 hrs ago	0xb4a4b95d85a610...	IN 0x65f69d82ed403ad...	0 Ether	0.000074458
0x48590847d6937b9...	1999708	36 days 19 hrs ago	0x31c9c3c7a86e66...	IN 0x65f69d82ed403ad...	0 Ether	0.000074458

待解問題與未來推廣

區塊鏈可促進大數據預測任務的自動化

- 區塊鏈可將大數據預測行為透過智能合約轉變成具體行為。
- 區塊鏈可以是探索人工智慧潛在途徑之一，可使系統自動化，並賦於系統運作權限。
- 區塊鏈中的共識機制有可能促使產生友善的人工智慧。
- 區塊鏈可以促成一種自動交易，讓系統上的多方參與，這是過去人類未曾企及通用交易方式

智能合約的戰場

- Hyperledger Fabric的智能合約叫做Chaincode，所用的程式語言是Go語言，使用Docker容器來執行。
- 以太坊使用以太坊虛擬機器（Ethereum Virtual Machine，EVM）來執行智能合約程式，開發用的程式語言則是Solidity。
- 未來Fabric可能會接受以太坊的EVM執行環境
(2017/08 Hyperledger 發布「Sawtooth Ethereum」，該計畫目標為支援以太坊智能合約 <https://www.youtube.com/watch?v=tjrvWvX4diA>)

相關應用 - 區塊鏈整合醫院病人數據與病歷

- 未來推廣：醫療機構也能夠妥善運用區塊鏈技術，醫院中病人的數據、病歷等等都需要隱私，**區塊鏈的不可竄改性能讓病患資料被保障**，甚至未來能夠結合人工智慧，將病歷更進一步的導向智能諮詢、智能抓藥等功能。
- 醫療需求需要大量的、可靠的安全資料，這樣的需求可以透過區塊鏈技術來滿足，在醫療費用越來越高的此刻，**結合人工智慧區塊鏈的醫療保健服務非常值得我們期待**。
- **健康區塊鏈填補全民健保缺口**
<http://www.chinatimes.com/realtimenews/20161027001811-260410>

待解問題

- Moodle、Moocs 結合 Ethereum 將具有保護個人隱私，資訊透明的功能，但雙方協調軟體API仍需改善。
- Ethereum為**圖靈完備平台、具有腳本語言Solidity**，但交易確認需依靠礦工及獎勵。
- IOTA擁有**不用挖礦**分散式帳本 Tangle技術。但，因不具備圖靈完備的功能，所以暫時不能執行智能合約。
- **未來重點：創造(或使用)一個不用挖礦的區塊鏈平台，並擁有能執行智能合約的功能**，將可成為紀錄學習歷程最佳工具，進而促成人工智能大數據分析自動化。**(類似：Hyperledger) (影片4)**
- 期待大家參與，讓這概念技術可以獲得真正突破。**(截至目前已經提供超過 50 顆測試幣供有興趣的夥伴測試)**

