區塊鏈的前世今生

主講人：李延浚 博士
lee0308@gmail.com

自我介紹

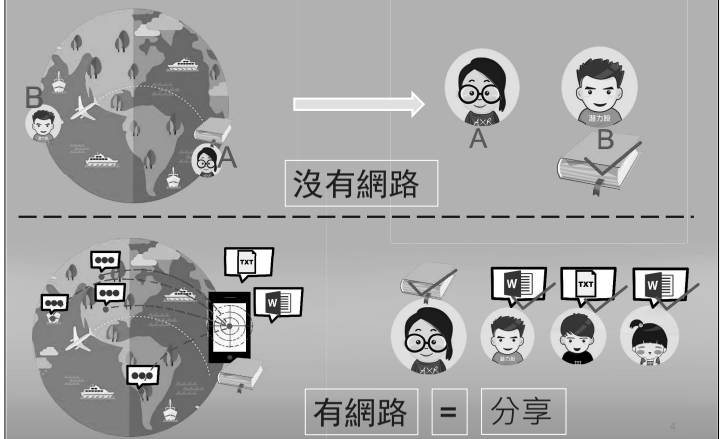
學歷	系所	
碩士	美國橋港大學	企管所
碩士	華梵大學	資管所
碩士	開南大學	法研所
博士	朝陽科技大學	資管所
博士後	南開大學	經濟學院

經歷			
廣西財經學院	副教授	維宇資訊	副總經理
天津南開大學	博士後研究員	廣西领傲信息科技	執行長
南寧東盟研究院	副主任	保險經紀人公會	資訊顧問

目錄

- 網路世界的便利與限制
- 區塊鏈的由來
- 區塊鏈的名詞概述
- 區塊鏈的應用
- 區塊鍊的限制

網路世界的便利與限制



區塊鏈的由來

- 分享 =? 交易

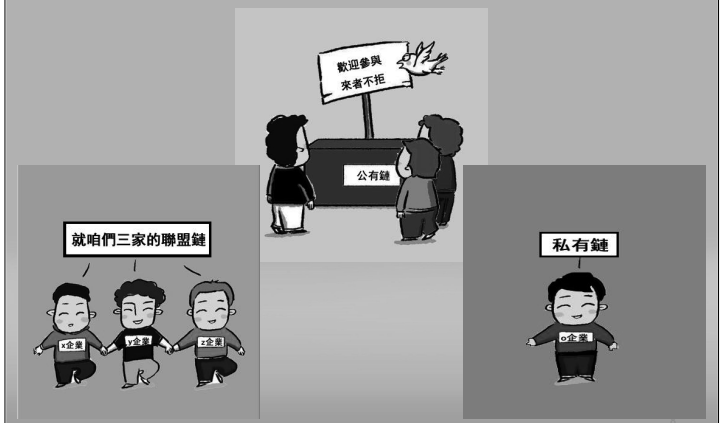
區塊鏈的由來

- 交易 =? 面對面 =? 即時

區塊鏈的由來

1. 去中心化
   去中心化是區塊鏈最突出最本質的特征。
2. 開放性。
   區塊鏈技術基礎是開源的，除了交易各方的私有信息被加密外，區塊鏈的數據對所有人開放，整個系統信息高度透明。
3. 獨立性
   基於協商一致的規範和協議(類似比特幣採用的哈希演算法等各種數學演算法)，整個區塊鏈系統不依賴其他第三方，所有節點能夠在系統內自動安全地驗證、交換數據，不需要任何人為的干預。
4. 安全性
   避免了主觀人為的數據變更。
5. 匿名性
   除非有法律規範要求，單從技術上來講，各區塊節點的身份信息不需要公開或驗證，信息傳遞可以匿名進行。

區塊鏈的名詞概述

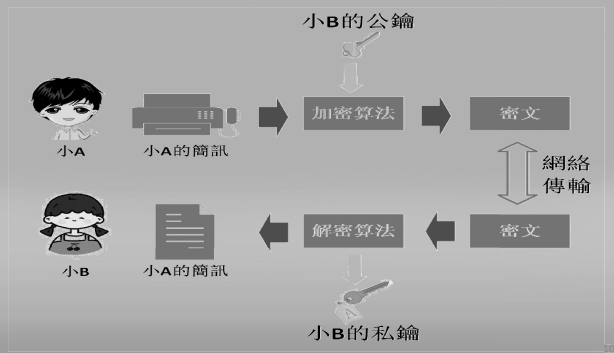


區塊鏈的名詞概述

	公有鏈	聯盟鏈	私有鏈
參與者	任何人自由進出	聯盟成員	鏈的所有者
共識機制	pow/pos	分散式一致性演算法	solo/pbft等
記帳人	所有參與者	聯盟成員協商確定	鏈的所有者
激勵機制	需要	可選	無
中心化程度	去中心化	弱中心化	強中心化
如初特點	信用的自建立	效率和成本最佳化	安全性高、效率高
承載能力	<100筆/秒	<10萬筆/秒	視組態決定
典型場景	加密貨幣	供應鏈金融、銀行、物流、電商	大型組織、機構
代表專案	比特幣、以太坊	R3、Hyperledger	

區塊鏈的名詞概述

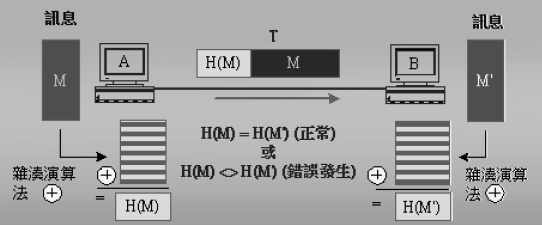
- 公鑰 & 私鑰



區塊鏈的名詞概述

雜湊函數

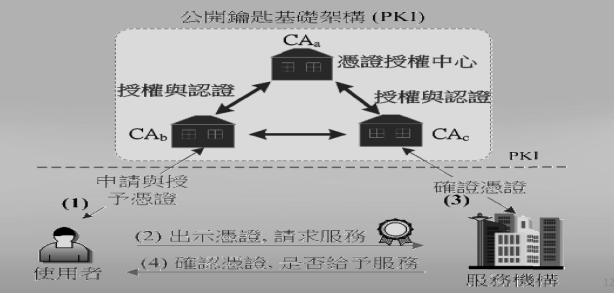
- 是將不定長度訊息的輸入，演算成固定長度雜湊值的輸出，且所計算出來的雜湊值必須符合兩個主要條件：
  (1) 由雜湊值是無法反推出原來的訊息
  (2) 雜湊值必須隨明文改變而改變



區塊鏈的名詞概述

數位簽章

- 是一種類似寫在紙上的普通的物理簽名，但是使用了公鑰加密領域的技術實現，用於鑑別數位信息的方法



區塊鏈的名詞概述

- 區塊

محمد بن سلمان بن امين الفارسى

Muḥammad ibn Salmān ibn Amīn al-Farsī

穆罕默德·本·薩勒曼·本·阿明·法爾西

本名：穆罕默德；

父名：薩勒曼；

祖父名：阿明；

族名：法爾西（「波斯人」）。

因此這一姓名體現的具體含義是「穆罕默德，阿明之子薩勒曼之子，波斯人」。

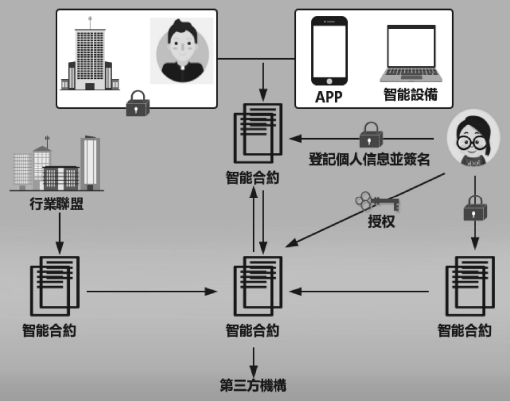
指稱此人時，應以「穆罕默德」為簡稱，或是以其長子的本名作匿稱稱呼之，如若其子名為卡里姆（Karīm），則可稱呼他為阿布-卡里姆（Abū Karīm，卡里姆之父）。

區塊鏈的名詞概述

- 鏈

區塊鏈的應用

區塊鏈的應用



區塊鍊的限制

工作量證明

區塊頭包含一個亂數，使得區塊的隨機散列值出現了所需的0個數。節點通過反復嘗試來找到這個亂數，這樣就構建了一個工作量證明機制。

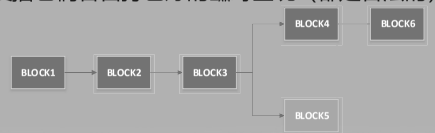
工作量證明機制的本質是一CPU一票，“大多數”的決定表達為最長的鏈，因為最長的鏈包含了最大的工作 量。如果大多數的CPU為誠實的節點控制，那麼誠實的鏈條將以最快的速度延長，並超越其他的競爭鏈條。如果想要修改已出現的區塊，攻擊者必須重新完成該區塊的工作量外加該區塊之後所有區塊的工作量，並最終趕上和超越誠實節點的工作量。

17

區塊鍊的限制

分叉

同一時間段內全網不止一個節點能計算出亂數，即會有多個節點在網路中廣播它們各自打包好的臨時區塊（都是合法的）。



某一節點若收到多個針對同一前續區塊的後續臨時區塊，則該節點會在本地區塊鏈上建立分支，多個臨時區塊對應多個分支。該僵局的打破要等到下一個工作量證明被發現，而其中的一條鏈條被證實為是較長的一條，那麼在另一條分支鏈條上工作的節點將轉換陣營，開始在較長的鏈條上工作。其他分支將會被網路徹底拋棄。

18

區塊鍊的限制

重複交易

- 指攻擊者幾乎同時將同一筆錢用作不同交易。

併發處理

- 區塊鏈系統面臨併發處理過低的問題。VisaNet在2013年的測試中，實現了處理每秒47000筆交易，相比之下比特幣每秒處理約7筆交易，乙太坊大約每秒處理30筆。

19

區塊鍊的限制

體積過大

- 隨著區塊鏈的發展，節點存儲的區塊鏈資料體積會越來越大，存儲和計算負擔將越來越重。

數據確認時間

- 目前的區塊鏈系統，尤其是金融區塊鏈系統中，存在資料確認時間較長的問題。

20

謝謝聆聽！