

區塊鏈基礎及其應用 講義

講師 陳在和

第一章 探詢區塊鏈的源頭-重回拜占庭

- 拜占庭將軍問題
- 古拜占庭位於土耳其伊斯坦堡.是東羅馬帝國首都.土地遼闊.保衛國土的將軍們之間的聯繫只能靠信差.戰爭期間所有將軍必須達成一致共識.若有贏的機會才進攻敵營.但軍隊裏可能有叛徒或間諜導致誤判.所以有些資訊未必是大家共識.如何不受間諜.叛徒的影響仍能達成共識.
- 叛變的將軍可視為:一個故障.不停發錯誤訊息的伺服器/一個為獲取暴利而做出的金融票據/一份失效的醫療合約糾紛/一份含糊不清的保單/一個可以發出信息.做出行動的錯誤訊節點

- 拜占庭將軍問題 解答者 - Satoshi Makamoto 中本聰
- 解決方案就是 - 工作量證明鏈(proof-of-work chain)
- 如何解決呢? (假設所將軍都有一部電腦供計算.聯繫)
- (1)引入一個困難的.需要10分鐘求解的工作量計算.限制了網路中每個時刻中被提出進攻時刻的數目
- (2)將所有求解出的”工作量證明“都逐一加入.形成一條越來越長的鏈條.一個紀錄所有:參與著攻擊時刻雜湊(Hash)計算的將軍.計算的”工作量證明”.關於“工作量證明”的計算總體名錄
- (3)基於這條長鏈.得出安全進攻時刻的答案

- **2008.11.1中本聰-比特幣P2P電子現金論文**
- 表達了比特幣五個主要的特性:
- (1)可以用點對點的網路解決雙重支付的問題
- (2)沒有鑄幣的協力廠
- (3)使用者可以匿名
- (4)可以用雜湊(Hash)現金形式的“工作量證明”來鑄造新貨幣
- (5)用於製造新幣的“工作量證明”機制.亦可用來預防雙重支付

圖 比特幣兌換美元價格

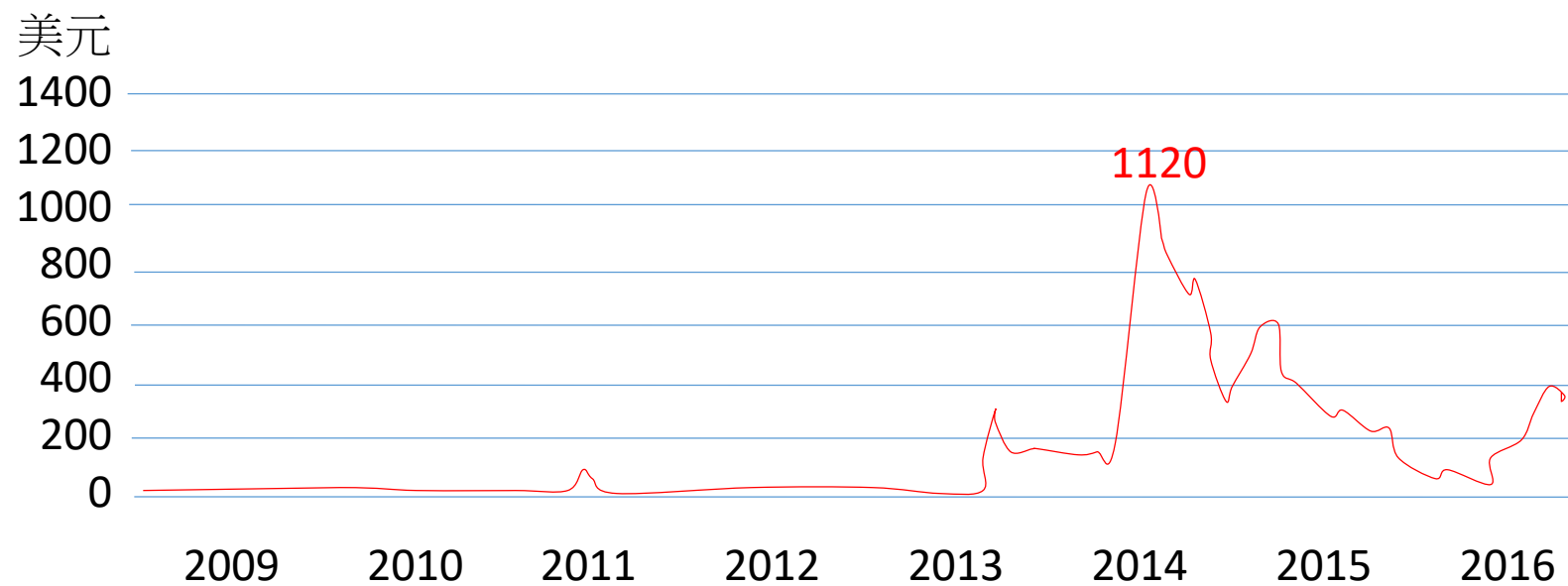
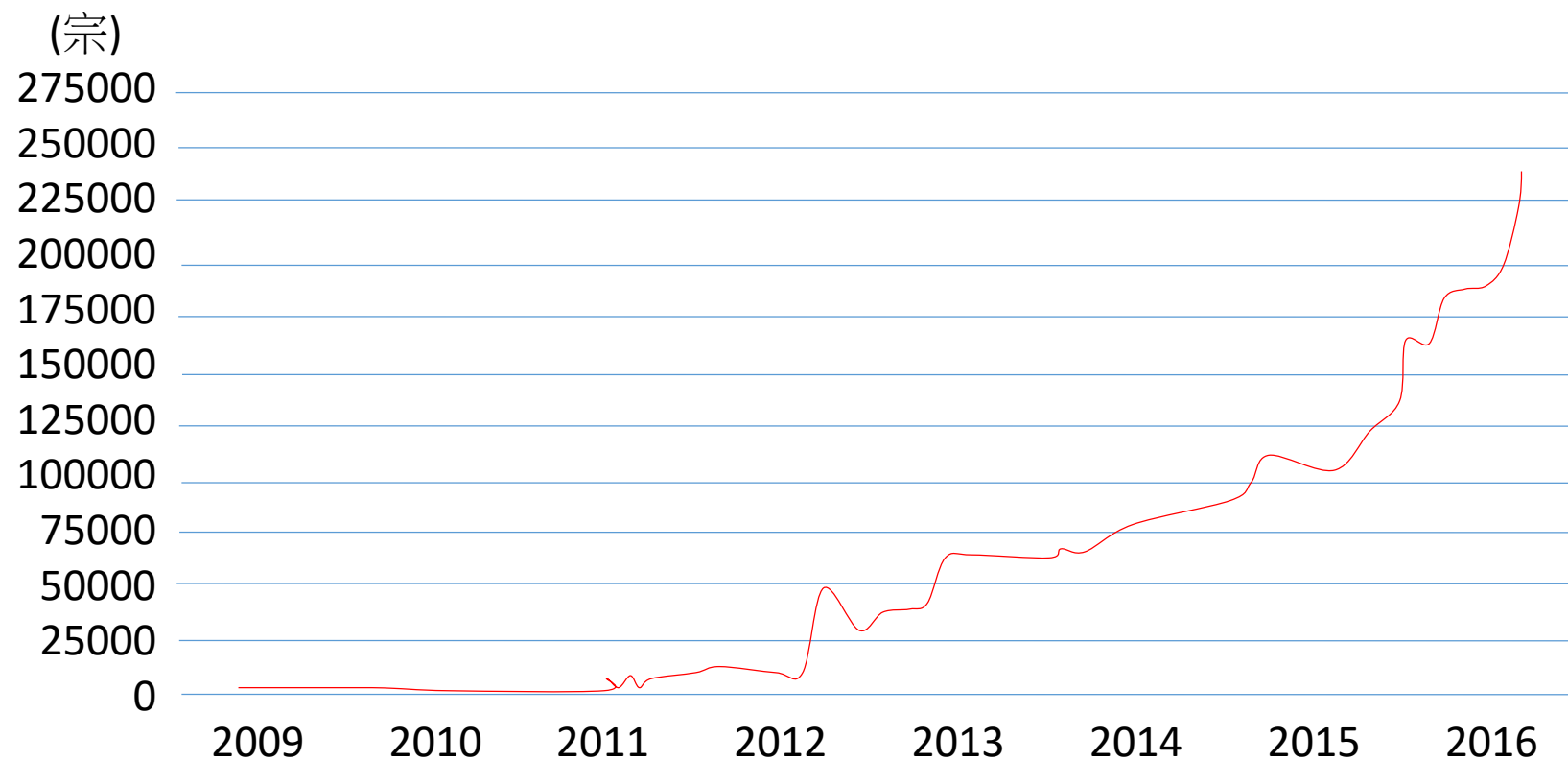


圖 比特幣每日交易數

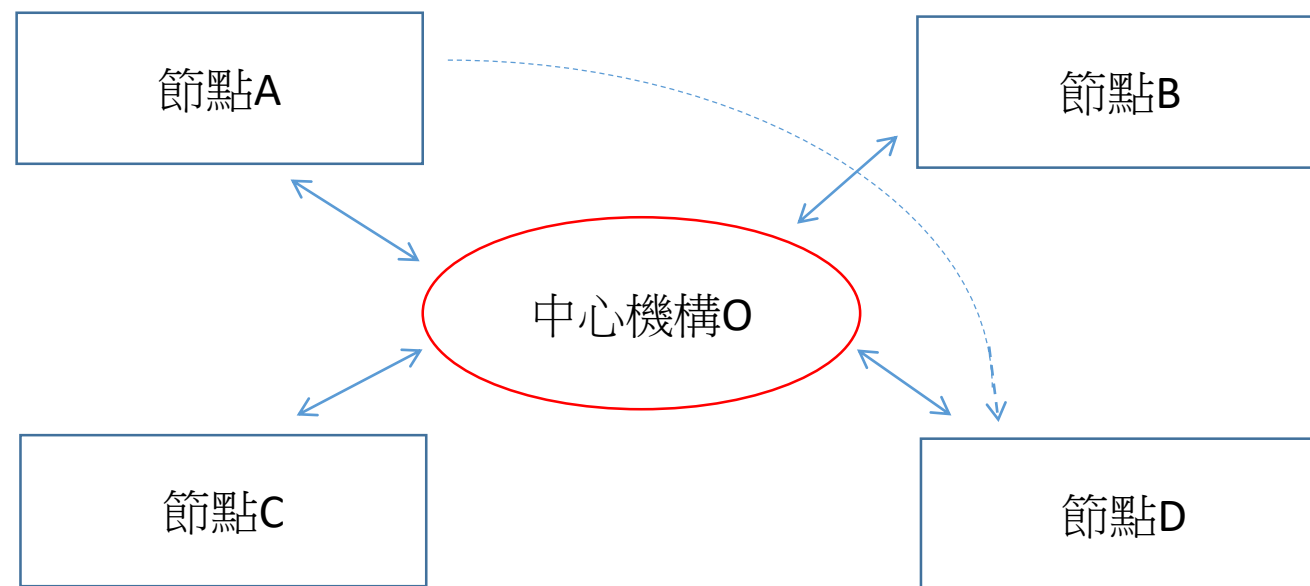


第二章 區塊鏈原理

- 一.區塊鏈的技術要素
- (一)區塊鏈
- 1.區塊
- **Header**:連結到前面的塊.並且為區塊鏈提供完整性
- **Body**:包含驗證了塊創建過程中比特幣交易的紀錄
- 2.鏈-目前分三類
- (1)公有區塊鏈(Public Block Chains)
- 世界上任何個體或團體都可以發送交易.且交易能夠獲得區塊鏈的有效確認.任何人都可以參與共識過程

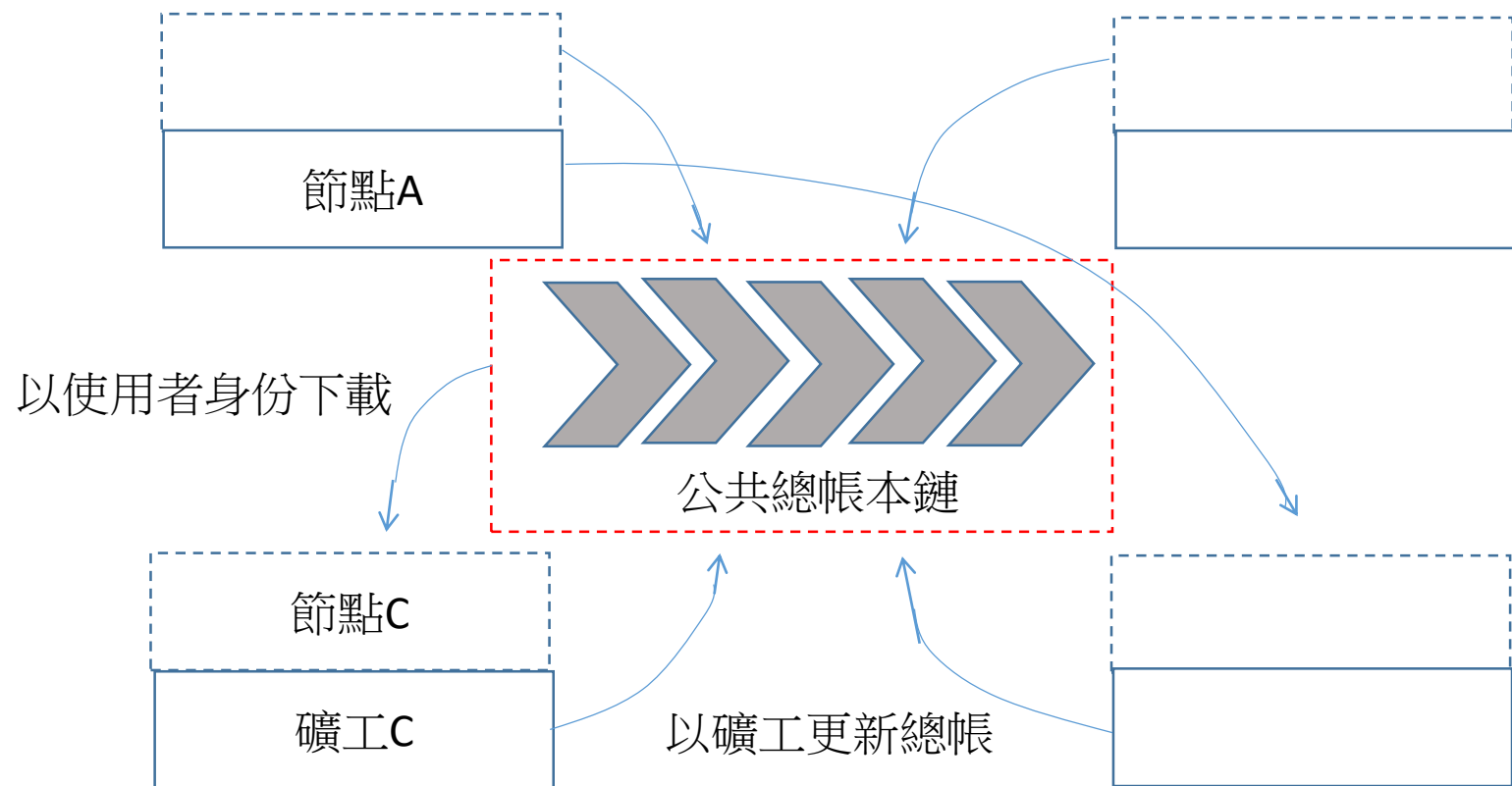
- (2)聯合(行業)區塊鏈(Consortium Block Chains)
- 由某群體內部指定多個預選的節點為記帳人.每個塊的生成由所有預選節點共同決定(預選節點參與共識過程).其他接入節點可以參與交易.但不問記帳過程
- (2)私有區塊鏈(Private Block Chains)
- 僅僅使用區塊鏈的總帳技術進行記帳.可以是一家公司或個人.獨享該區塊鏈的寫入許可權.本鏈與其他分散式儲存方案沒有太大區別

圖 區塊鏈原理介紹(1)



A借記一筆帳給D
需經過中心機構O
ABCD存款(準備金)在O處
ABCD日終都要和O對帳

圖 區塊鏈原理介紹(2)



- (二)分散儲存
- 分散儲存式比特幣的一個重要概念.它是一串使用密碼學方法相連產生的資料塊.每一個資料塊中包含了一次比特幣網路交易的資訊.用於驗證其資訊的有效性(防偽)和生成下一個區塊
- 1.分散式儲存系統
- 將資料分散儲存在多台的獨立設備上
- 2.集群檔案系統
- 是指運行在多台電腦上.相互之間透過某種方式通信.將集群內所有儲存空間資源整合.虛擬化.並對外提供訪問服務的檔案系統

- (三)共識機制
- 1.工作量證明(POW)
- 就是大家熟悉的挖礦.透過運算計算出一個滿足規則的亂數.即獲得本次的記帳權.發出本輪需要記錄的資料.全網其他節點驗證後一起儲存
- 優點:完全去中心化.節點自由進出
- 缺點:目前比特幣已經吸引全球大部分的算力.其他再用**POW**共識機制的區塊鏈應用很難獲得相同的算力來保障自身的安全.
- 挖礦造成大量的資源浪費.共識達成的週期較長.不適合商業使用

- 2.權益證明(POS)
- POS是POW的一種升級共識機制.根據每個節點所佔代幣的比例和時間.等比例地降低挖礦難度.從而加快找亂數的速度
- 優點:在一定程度上縮短了共識達成時間
- 缺點:還是需要挖礦.本質上沒有解決商業應用的痛點
- 3.股份授權證明機制(DPOS)
- DPOS是一種新的保障加密貨幣網路安全的演算法.其原理是給持股人一把對應表決權的鑰匙
- 優點:最大化安全與盈利.最小化成本與驗證時間
- 缺點:整個共識機制還是依賴代幣.但很多商業不須代幣

- 4.驗證池(Pool)
- 基於傳統的分散式一致性.加上資料驗證機制.是目前行業鏈大範圍在使用的共識機制
- 優點:不須代幣也能工作.秒級驗證共識
- 缺點:去中心化程度不如比特幣.更適合多方參與的中心商業模式

- 二.區塊鏈的核心特點
- (一)開放
- 比特幣的本質是一個互相驗證的公開記帳系統
- (二)分散式
- 分散式帳本式一個可在多個網站.不同地理位置或多個機構組成的網路裡進行分享的資產料庫

- (三)總帳本
- 1.公共帳本的特徵
- (1)去中心化
- (2)每次交易產生的帳本都記錄在區塊鏈的節點上.每個帳本都有完整的備份
- (3)每個帳本都記錄著本次交易&以前所有交易的資訊
- (4)區塊鏈實現了兩種記錄:交易與區塊
- (5)當你要發起一筆交易時.須把交易資訊廣播到區塊鏈網路中."礦工"將資訊收錄及驗證合法後.交易即完成
- (6)對於試圖修改或重寫交易記錄者.成本極高

- 2.關於公共帳本的三個問題
- 問題(1)如何保證用戶有足夠的餘額? 區塊鏈回溯你的交易歷史記錄即知
- 問題(2)如何保證你的帳本不被冒名頂替? 用數位簽章即解決
- 問題(3)那麼多礦工.該如何決定由哪個礦工生成下一個區塊鏈? 最長的哪一條鏈獲咥

- 三.區塊鏈的核心原理
- (一)點對點傳輸
- 點對點技術(Peer to Peer=P2P)又稱對等互聯網技術.依賴網路中參與者的計算能力和頻寬.而非少數的伺服器
- 1.點對點傳輸的優勢
- 讓所有用戶端都能提供資源-頻寬.儲存空間和計算能力
- 在多節點複製資料.防故障
- 2.點對點傳輸運用
- 讓不同參與者能共用資訊

- (二)分散式公共網路
- 分散式運算技術處於多種方案並存.其網路拓樸結構呈網格狀.與集中式網路結構不同
- 1.優點
- (1)電纜長度短.連線容易 (2)可靠性高 (3)易於擴充
- 2.缺點
- (1)複雜難管理 (2)故障診斷困難 (3)需更多的網路技術.管理人員

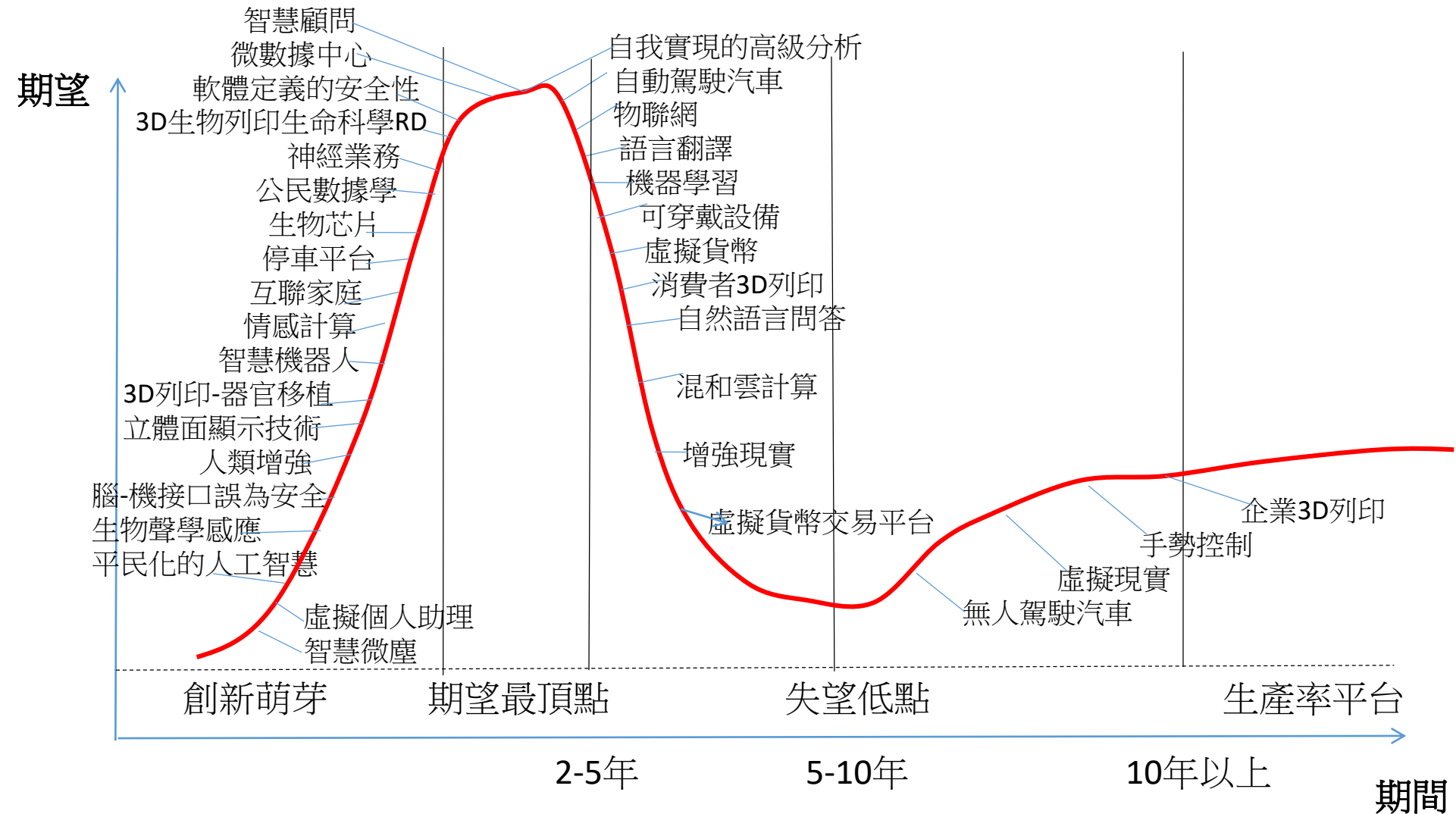
- (三)加密貨幣發行
- 1.虛擬貨幣分為加密貨幣和非加密貨幣
- (1)非加密貨幣由私人或公司自我固定發行.可無限發行.不需通過電腦的顯示卡運算程式解答方程式獲得.不具升值功能
- (2)加密貨幣不依靠法定貨幣機構發行.不受中央管控.依據全世界的電腦運算一組方程式開原始程式碼.透過電腦顯示卡.CPU大量的運算產生.基於密碼設定.只能被真實擁有者使用
- (3)非加密貨幣的數量無限.加密貨幣是有限的.具升值價值
- (4)加密貨幣是一串代碼

- 2.加密數位貨幣的核心是-能成為各國貨幣之間的媒介
- 它最終產生”國際物聯網.貿易之間的結算.結匯”作用
- 3.加密數位貨幣流通必須禁得起各國法律的推敲和考證
- 不可成為非法組織的工具.要登記納稅(=中心化).將輸給比特幣的去中心化之匿名發行
- 4.加密數位貨幣流通的發行是一種突破
- 增加融資管道.降低國際融資門檻.人人可參與
- 5.投資者.大眾消費者必須有貨幣戰爭的意識及全球視野

- (四)去中心化
- 去中心代表沒有中心.將”以人為中心(不可控)”外移至可控且中立的因素.其網路如同細胞組織.不受影響.更穩定
- 1.去中心化的優點
- (1)可適應性-即使失去部分.仍不影響整體
- (2)可進化性-不斷升級
- (3)無限性-這是一套併行運行系統.會有冗餘.自我延伸和自動繁衍是無止境的
- (4)彌補性-無規則產生無限可能.個體缺陷部不會導致整體之不足

- 2.去中心化的缺點
- (1)並非最優-亂中有序
- (2)不可控制
- (3)不可預測
- (4)不可知-項網路相互影響.橫向的因果關係
- (5)重啟效應差-點火系統好.但機械的預熱時間長.個體必須各就各才行

圖 高納德2015年新興技術成熟度曲線



- 什麼是區塊鏈?
- 中本聰第一版的比特幣區塊鏈的基礎協議:
- 通過蓋時間戳記.各方一同記帳.一同公證.每十分鐘確認一次.然後每合法的區塊形成一個鏈條.形成分散的.大家一致同意的帳本資料庫.這就是區塊鏈
- 它是一種資料庫.一種分散系統.也是一種網路底層協定

圖 區塊鏈示意圖



表 全球排名排名前**10**名的數位貨幣 - 2015年

	名稱	符號	單價
1	Bitcoin	BTC	427
2	Ethereum	ETH	6.4
3	Ripple	XRP	0.008
4	Litecoin	LTC	3.38
5	MaidSafeCoin	MAID	0.1
6	Dogecoin	DOGE	0.0002
7	Dash	DASH	4.0
8	Peercoin	PPC	0.5
9	Bitshered	BTS	0.004
10	Monerd	XMR	0.9

第二章 區塊鏈-顛覆世界的力量

- (一)去中心化
- 區塊鏈突出的特點-去中心化
- 鳥類飛行原則:彼此只看`6隻鳥.保持一致即可
- 沙丁魚群游.只盯住前後左右的魚.與他們保持一致的距離和方向
- 牠們沒有管理者(中心)一樣運作良好
- 人類學習”鳥群智慧“

- **2.為何去中心化會成功?**
- 類自古以來. 家族到王權都是中心化組織
- 但是當人個的能力越強時.中心化的需求越弱
- 網路連線就是去中心化.人人都是組成分子.沒有唯一的主角
- 因為去中心化.人人都是主角.積極性提高

- **3.區塊鏈去中心化技術意味著啥?**

- 區塊鏈的資料區塊取代了傳統的伺服器.使得每個參與區塊鏈系統的節點都是主機
- 所有的資料變更和所有的交易資訊都被記錄在系統上
- 它是一個證明與自證系統
- 以點對點的模式進行交易.可以略過去的中心化的模式

- (二)區塊鏈將建構完美的契約世界
- 1.智慧合約改變生活
- 即使互聯網已經經由各種方式改變了我們的生活.但是從來沒有一種方法能夠真正地在沒有中心化的權威機構的授權下讓你“擁有”某些數位產品
- 但是這種情況即將改變.因為密碼貨幣學的出現.智慧合約正走進我們的生活
- 智慧合約能自動執行合約條款的電腦程式.未來它可能取代律師.銀行.甚至能夠形成萬物皆聯網的智慧合約

- **2.智慧合約賦予物聯網”思考的力量“**
- 萬物互聯.徹底走入我們的生活的每個領域
- 但物聯網會有某些安全問題.ex汽車系統會受到無情攻擊.房屋進入系統需要加強等
- 區塊鏈的智慧合約技術有可能解決這些問題.因為每個人都是中心.大大減少了資訊流通的成本
- 在資訊安全上.智慧合約不會被超越.區塊鏈安全技術可確保資訊不被竊取.沒有垃圾訊息侵入

- **3.從智慧合約到智慧資產**

- 智慧合約可解很多法律難題
- 智慧合約可用在股票交易所.設定執行股票買賣
- 自動執行借貸款.自動管理個人的健康
- 未來的律師工作:製作至戶合約範本.而非執行合約
- 智慧資產的核心是控制所有.透過私密金鑰來隨時使用.不履行合約者將被收回金鑰
- 這就是有執行力的合約

- **4.區塊鏈率先顛覆金融領域**

- 由於區塊鏈來自比特幣.所以金融機構接觸與應用最早
- 2015年發起的區塊鏈聯盟-富國.花旗.德意志.匯豐.摩根史坦利..均參與
- 它為金融業帶來更高的透明度.高安全性.降低詐欺風險.更能提效率.節省開支(因為減少了中間環節.以及透過程式化記錄.儲存.傳遞.核實.分析資料)
- 區塊鏈本質上就是交易各方信任機制建設的一個完美的數學解決方案

- **5.區塊鏈將成為下一代的資料庫架構**
- 區塊鏈可以連接大數據
- 大數據預測分析可以和自動執行的智慧合約完美結合
- 區塊鏈技術加入經濟支付層.作為量化工具.海量地自動執行.可大量解放人的生產力
- 彼此互不信任的雙方亦可實現合作.區塊鏈類似一台“創造信任的機器“
- 分散式的區塊鏈開展了:分散式投票.分散式儲存.分散式信息平台

- (三)區塊鏈將如何顛覆我們的生活?
- 1.醫療去中心化
- 過去的個人醫療資料都在醫院.區塊鏈上的電子病歷.個人可自己保有.非常方便
- 用戶更有自主性
- 用戶保有隱私

- **2.智慧鎖**

- 基於區塊鏈的智慧鎖可連接物聯網.透過智慧合約進行控制
- 該鎖可一人或多人擁有
- 共享經濟得以去中心化.任何東西都方便租賃
- 隨時都可更換金鎖密碼

- **3.去中心化網域名稱系統**
- 區塊鏈可提供**DNS**系統替代方案.不被公司控制
- 它能让全世界任何人自由地在互聯網上發布資訊

- **4.數位藝術:區塊鏈認證服務**

- 數位藝術是區塊鏈加密技術能提供顛覆性創新的另一個舞台
- 區塊鏈技術可被用來註冊任何形式的智慧財產權.或將鑑證服務變得更加普遍.如合同公證
- 數位藝術還可透過區塊鏈來保護線上圖片.照片或數位藝術作品等數位資產的智財權

- **5.區塊鏈政府**

- 區塊鏈以去中心化.個性化.便宜高效的特點提供傳統服務.實現全新的.不同的政府管理模式和服務
- 區塊鏈能達成共識驅動.公開審計.全球性.永久性來保持所有檔案.成為全球性的資料庫.這將成為區塊鏈政府的基石.可重新分配公共資源.提高政府效率.節約成本.提高參與度.最終成為自治的經濟型態
- 未來不只是物理的互聯.人類大腦與電腦介面技術配合區塊鏈網路共同展開.如此知識.靈感.創意的交互鏈條能有序的形成與爆發性地演進

- **6.線上音樂**

- 區塊鏈技術可用來提升線上音樂分享的公平性
- 可透過直接付款給藝術家和利用智慧合約來自動解決許可的問題. 無需中間人
- 還可以協助將歌曲背後的藝術家和創作者進行分類

- **7.汽車租賃和銷售**

- 利用區塊鏈技術.以後的汽車租賃只要”點.簽.開”三步即完成
- 其步驟是:顧客想租賃汽車.交易將上傳到區塊鏈的公共帳戶 -> 顧客在駕駛座上簽一份租賃和保險協定.區塊鏈及時將資訊上傳 -> 把車開走
- 這種模式也將應用到汽車銷售和登記

- **8.全球公共衛生和慈善捐贈**
- 比特幣能為伊波拉病毒等傳染病危機提供高效.直接有針對性的資金援助.把資金迅速傳遞到公開且可以審計和跟蹤的地址
- 而傳統的銀行體系的處理過程會妨礙資金的急迫需求
- 透過比特幣.可籌集大量善款

- **9.區塊鏈基因測序**

- 當前個人獲得基因資料有二問題:一是法規限制.二是費用昂貴
- 區塊鏈可解決此二問題.其作法:全球分布的計算資源.低成本地完成測序服務.並以金鑰保存測序數據規避了法律問題
- 有了資料.若發現有潛在的高血壓.老年癡呆症.可改變生活習性以提前應對之

- **10.區塊鏈智慧城市**

- 生活在區塊鏈的智慧城市:我們可以為自己製造的麻煩付費.若發生交通阻塞則可支付延誤費給來往車輛
- 還可以公開透明地位好的服務.好的學校支付費用
- 如此.促進社會朝向自律.高效自治方向來發展

- **11.區塊鏈透明助學**

- 區塊鏈的智慧合約有無數用途.智慧文化合約就是其中一種
- 若有人提供孩子的上學資助.可透過智慧合約自動確認學習進度.滿足學習合約後.將自動觸發後續資金撥付
- 如此.促使贊助者和學習者展開點對點的聯繫.公開透明.正向激勵

- **12.數位身分證**

- 現在很多網站使用中心化的協力廠登陸
- 未來可使用區塊鏈技術.使用去中心化的協力廠登陸-可以姓名.地址或二維碼登陸.且和手機綁定.可以暢遊網路世界
- 在電商網站購買.無須繁瑣地綁定銀行卡.就可輕鬆地使用電子錢包來支付

- **13.區塊鏈身份認證**

- 區塊鏈具有人人可以查閱的特性.每個人都可以在有網路的地方查詢區塊鏈資訊
- 可想像.身份證和戶口名簿基本不需要.因為每個人的資料都可寫入區塊鏈.當你需驗證資訊時.查閱即可
- 無論是追查逃犯或“證明你媽是你媽”都OK

- **14.區塊鏈婚姻**

- 區塊鏈婚姻是區塊鏈作為公開檔案資訊庫的一個嘗試.若得到推廣.其好處有:
- 更加透明.公平.自由.能夠解決重婚.隱婚等各種情況
- 並通過智慧合約來改善贍養老人.生兒育女.購買房產等生活事宜

- **15.學歷證書**

- 區塊鏈技術可用來鑑定學歷證書.此舉可確保學生在課程認定上的真實性
- 若更多學校採此透明的成績單和學歷證書之方式.則學術界的腐敗將大幅減少
- 也省掉了人工核驗&紙本文件的成本

- **16.預測**

- 區塊鏈技術或將撼動整個研究.分析.諮詢和預測行業
- **Augur**線上眾籌平台有望在去中心化平台賺取利潤.它將提供一個博彩互換服務.還將提供選舉和自然災害博彩服務
- 這個想法已經創造了一個預測市場

- **17.網路安全**

- 雖然區塊鏈系統是公開的.但其核驗.發送等資料交流過程卻採用了先進的加密技術
- 此技術不僅確保資料的來源正確.也確保了資料在過程中不被攔截.更改.可有效降低傳統網路的安全風險
- 擋住了駭客攻擊與腐敗的可能性

- **18.人工智慧區塊鏈**

- 區塊鏈讓智慧設備設定時間進行自檢.會讓管理人員回到設備出錯的時間點去確認哪裡出錯
- 應用區塊鏈技術可以遠端實施人工智慧軟體解決方案
- 若設備有多個使用者.人工智慧區塊鏈可幫助提高安全性.區塊鏈會使各方共同約定設備狀態.基於智慧合約中的語言編碼做決定

表 各國對於比特幣的監督

主要手段	監管類型/國家示例
資訊/道德勸說	.公共警告 .投資方/買家資訊 .研究報告
具體利益相關者監督	
現有監管解讀	監管實施基於對現有框架(ex稅法處理)如何應用於數位貨幣或數位貨幣仲介機構的解讀(ex美國)
總體監督	涵蓋所有三個方面的專門法規(消費者權益保障.針對不同利益相關者的審慎的組織規則和支付系統的具體操作規則)
禁止	.禁止比特幣零售交易(或限制交易額) .禁止零售商接受數位貨幣付款 .禁止基於數位貨幣的金融工具ex中國.比利時 .封殺數位貨幣交易所 .禁止銀行間進行比特幣交易ex中國.墨西哥

- (四)區塊鏈與金融
- 1.商業銀行基於區塊鏈的應用領域
- (1)點對點交易.ex基於P2P的跨境支付.匯款
- (2)登記.作為可靠的資料庫來記錄各種資訊.ex反洗錢客戶資料
- (3)確權.如土地所有權.股權
- (4)智慧管理.ex利用智慧合約自動檢測與支付

- **2.貨幣的演變**

- 一階段:實物貨幣
- 二階段:實物貨幣->金屬貨幣
- 三階段:金屬貨幣->信用貨幣
- 四階段:貨幣的現在與未來-電子錢

- **3.金融科技**

- 區塊鏈對金融科技帶來最大的影響.是滿足了過去傳統金融及夠無法實現的金融需求.服務了過去未能服務的客戶.實質降低了金融服務的門檻
- 這使得**普惠金融**成為可能

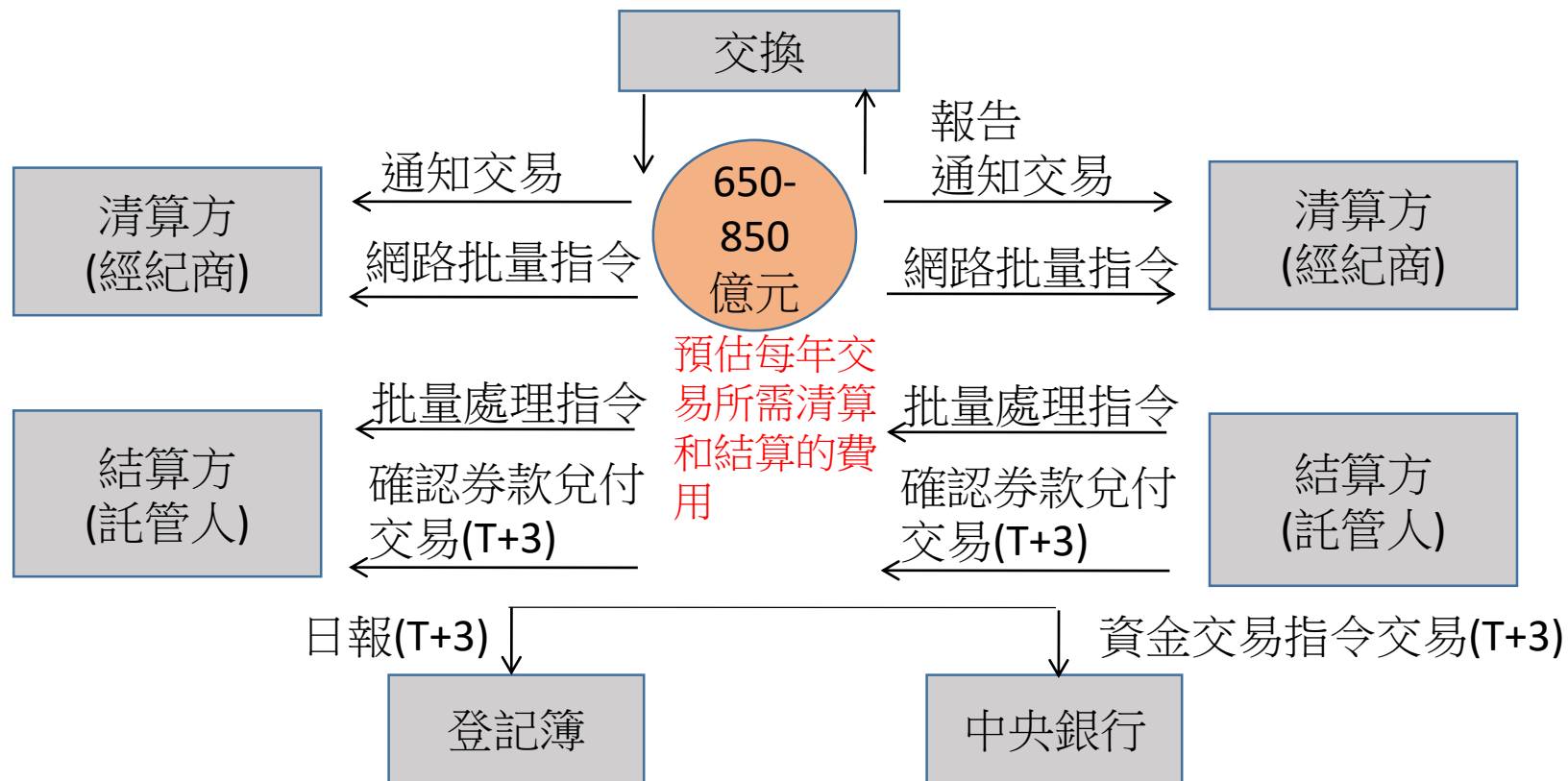
- **4.匯款**

- (1)電匯T/T-匯款人的錢給銀行->銀行通知國外分行匯給受款人
- (2)信匯M/T-進口人的錢給銀行.銀行以信件通知支行付款給出口人
- (3)票匯D/D-匯款人購賣銀行即期匯票.寄給受款人.受款人取款

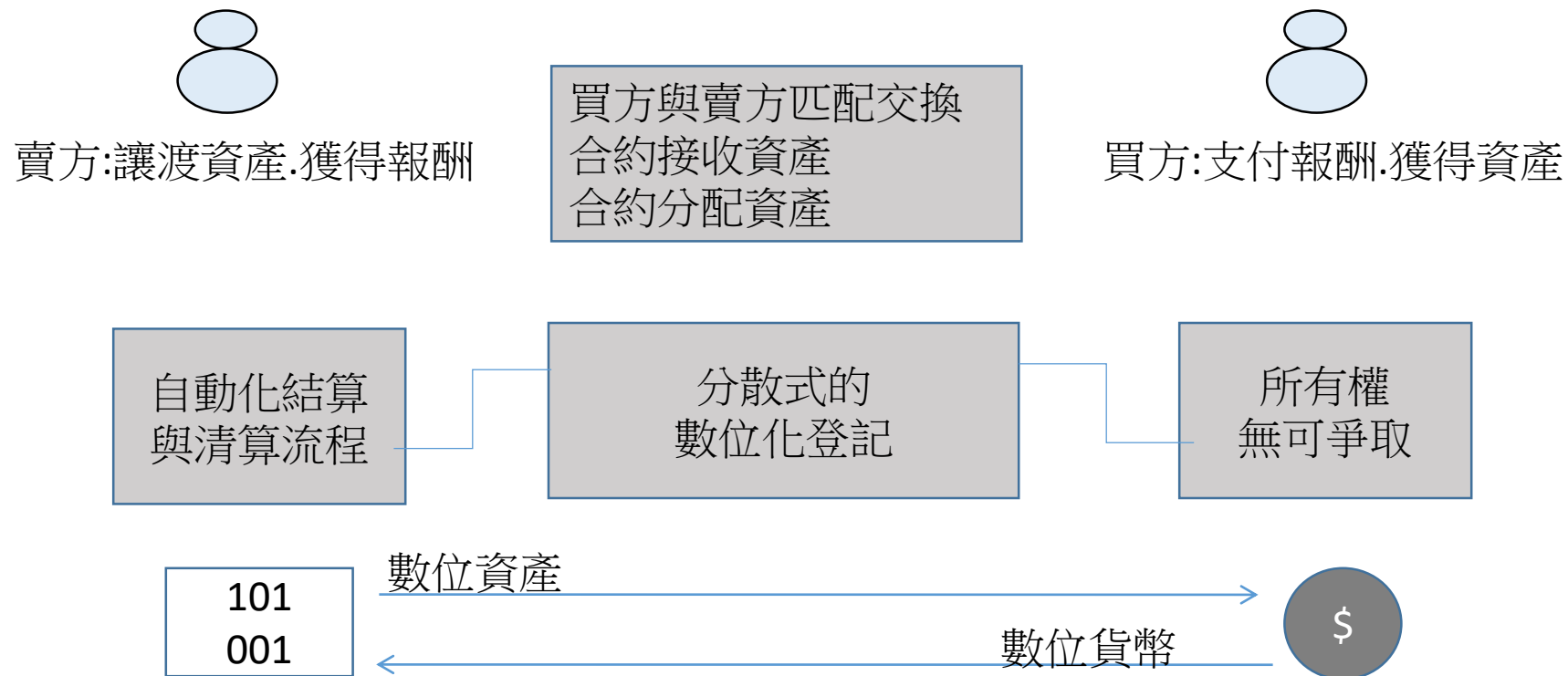


基於區塊鏈技術.以比特幣進行匯款

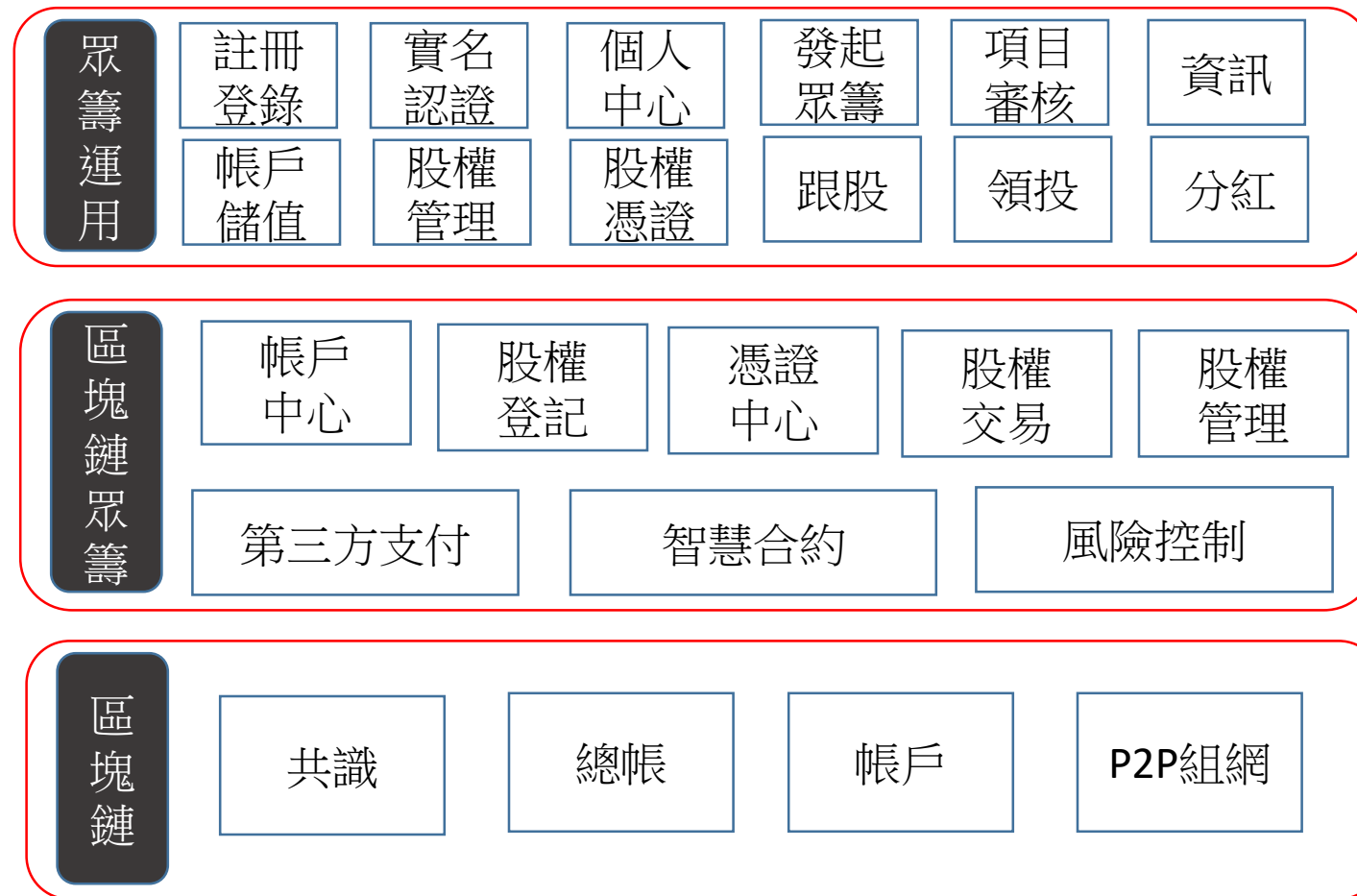
5.1 傳統的證券結算和清算系統(T+3天)



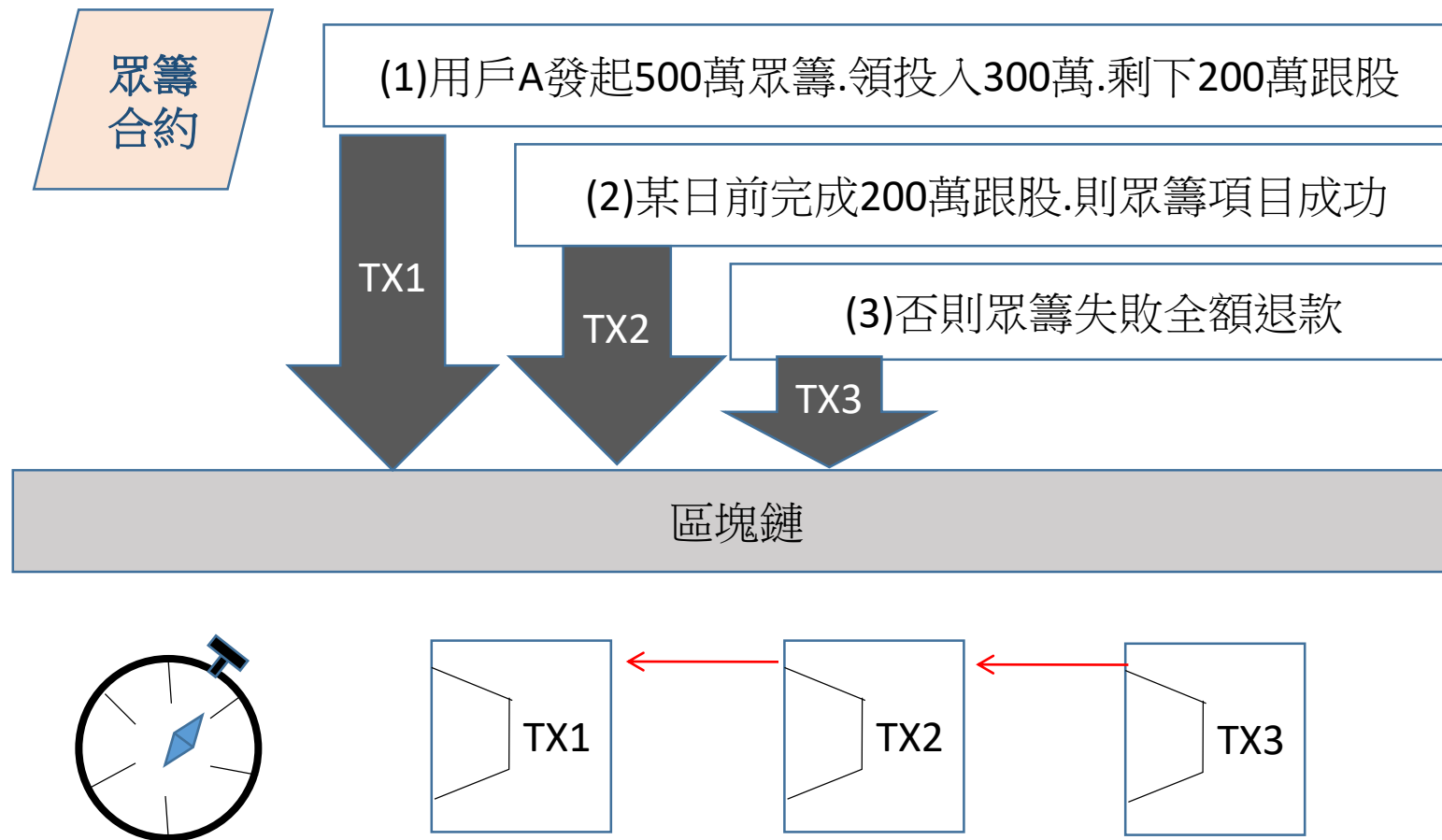
5.2 區塊鏈應用於證券結算和清算系統



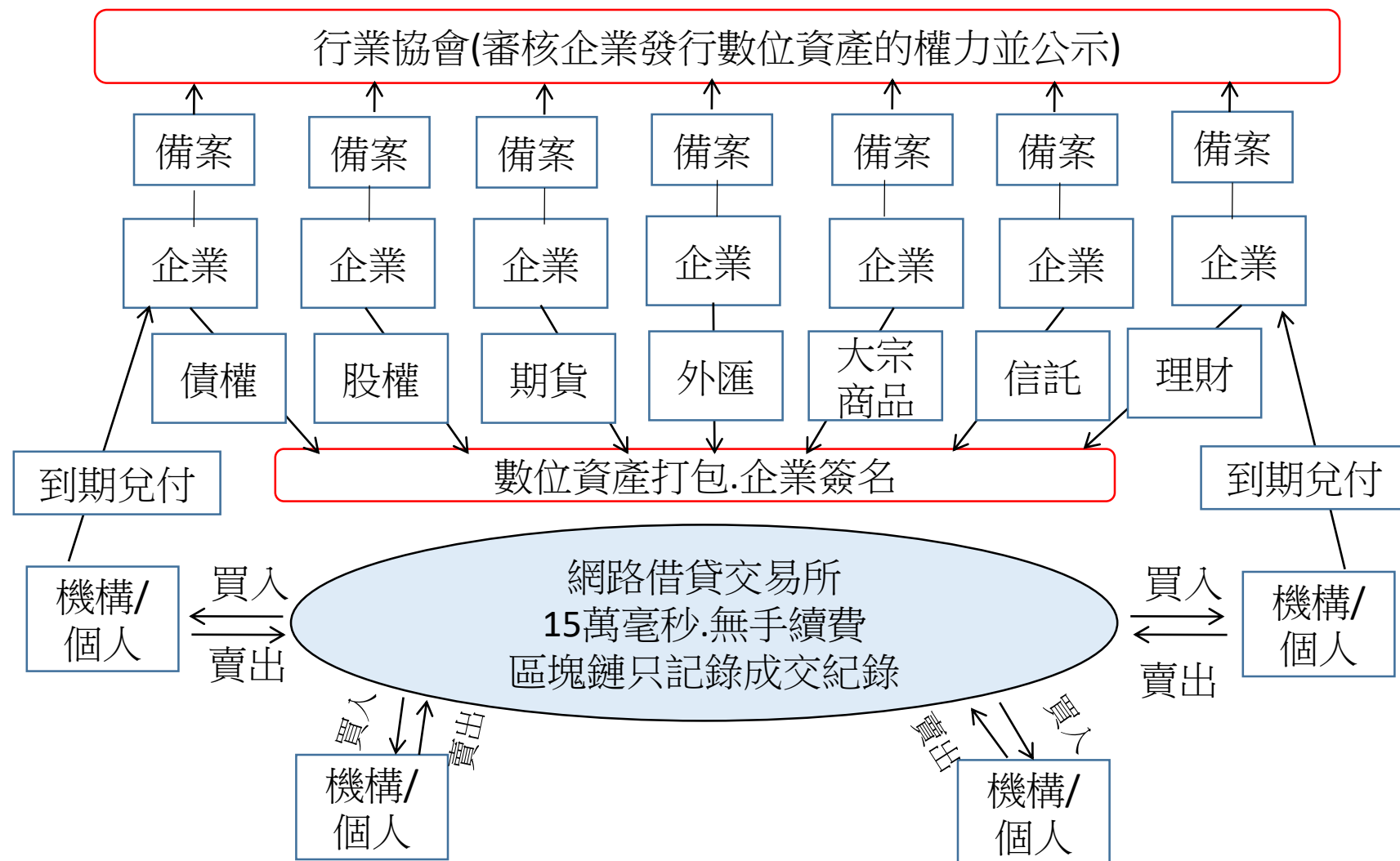
6.1 區塊鏈股權眾籌系統架構



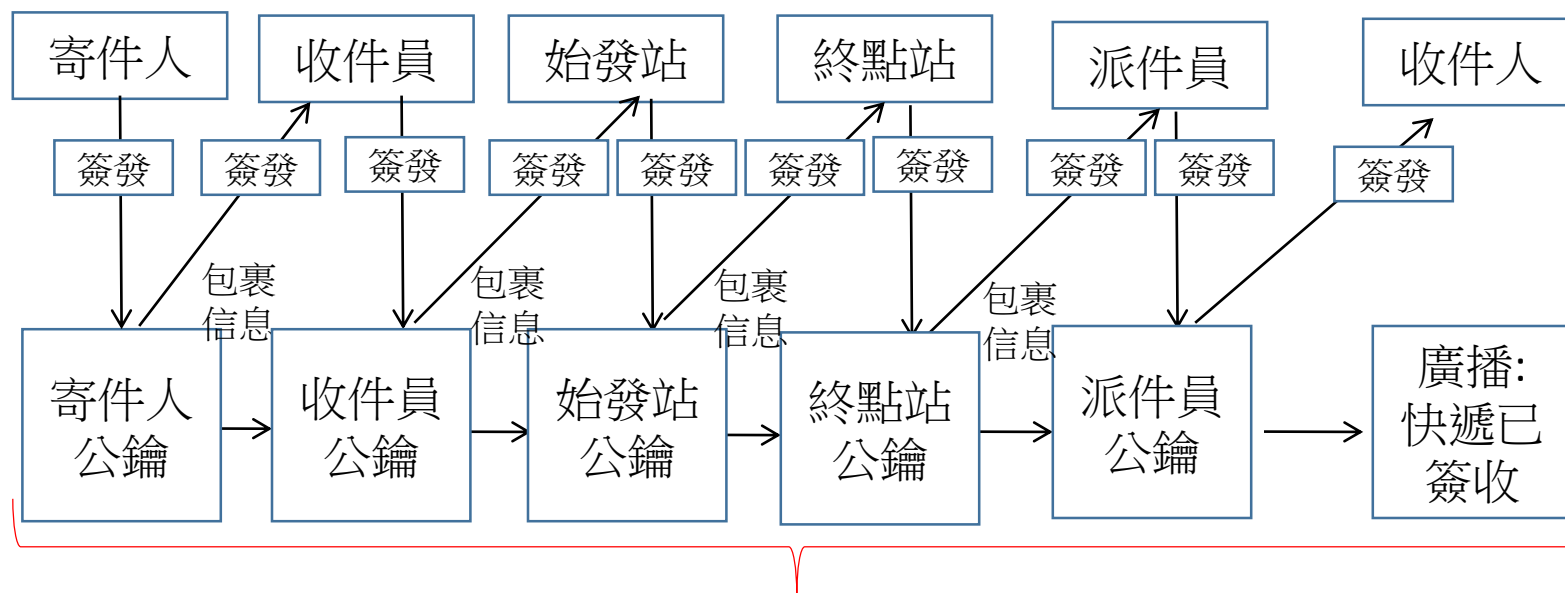
6.2 區塊鏈眾籌智慧合約示例



7. 美國區塊鏈研究中心基於以太坊的區塊鏈網路借貸票據交易所開源專案



8. 區塊鏈在物流行業的應用

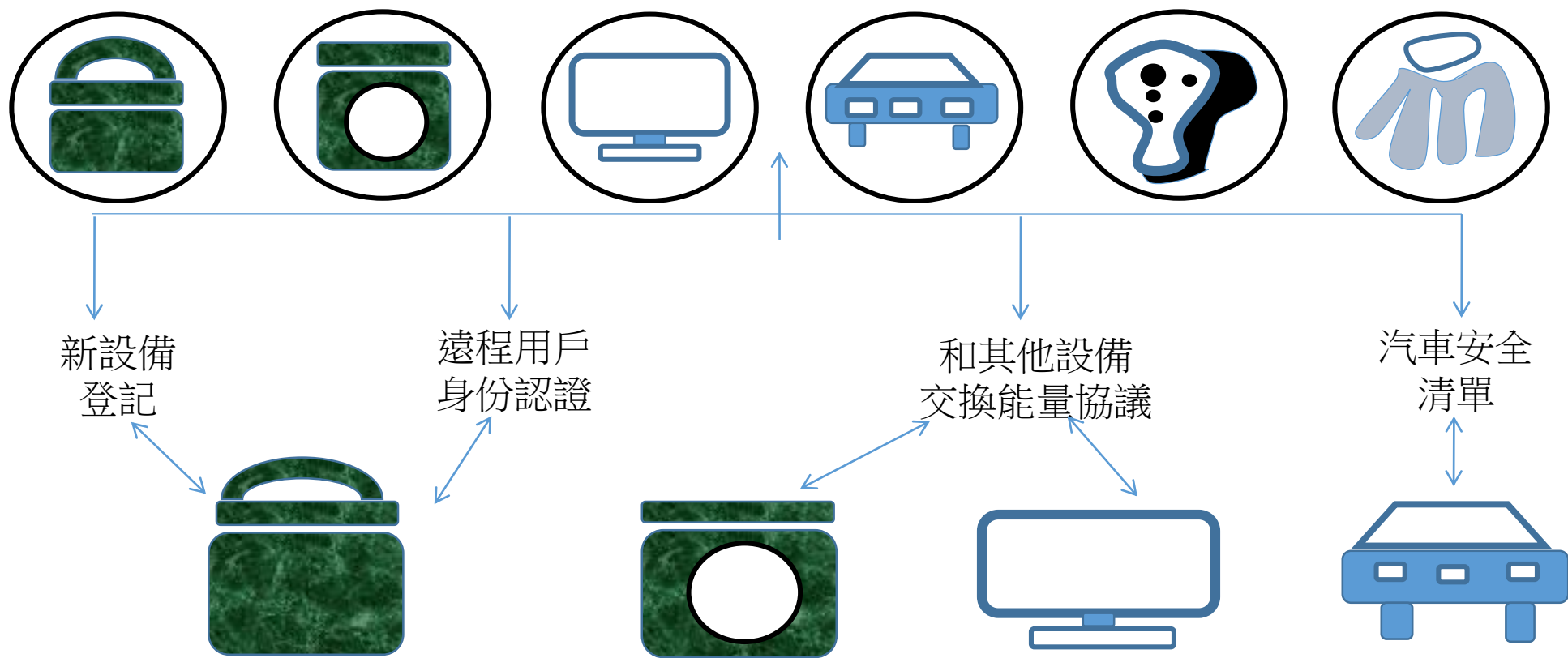


快遞物流實名制

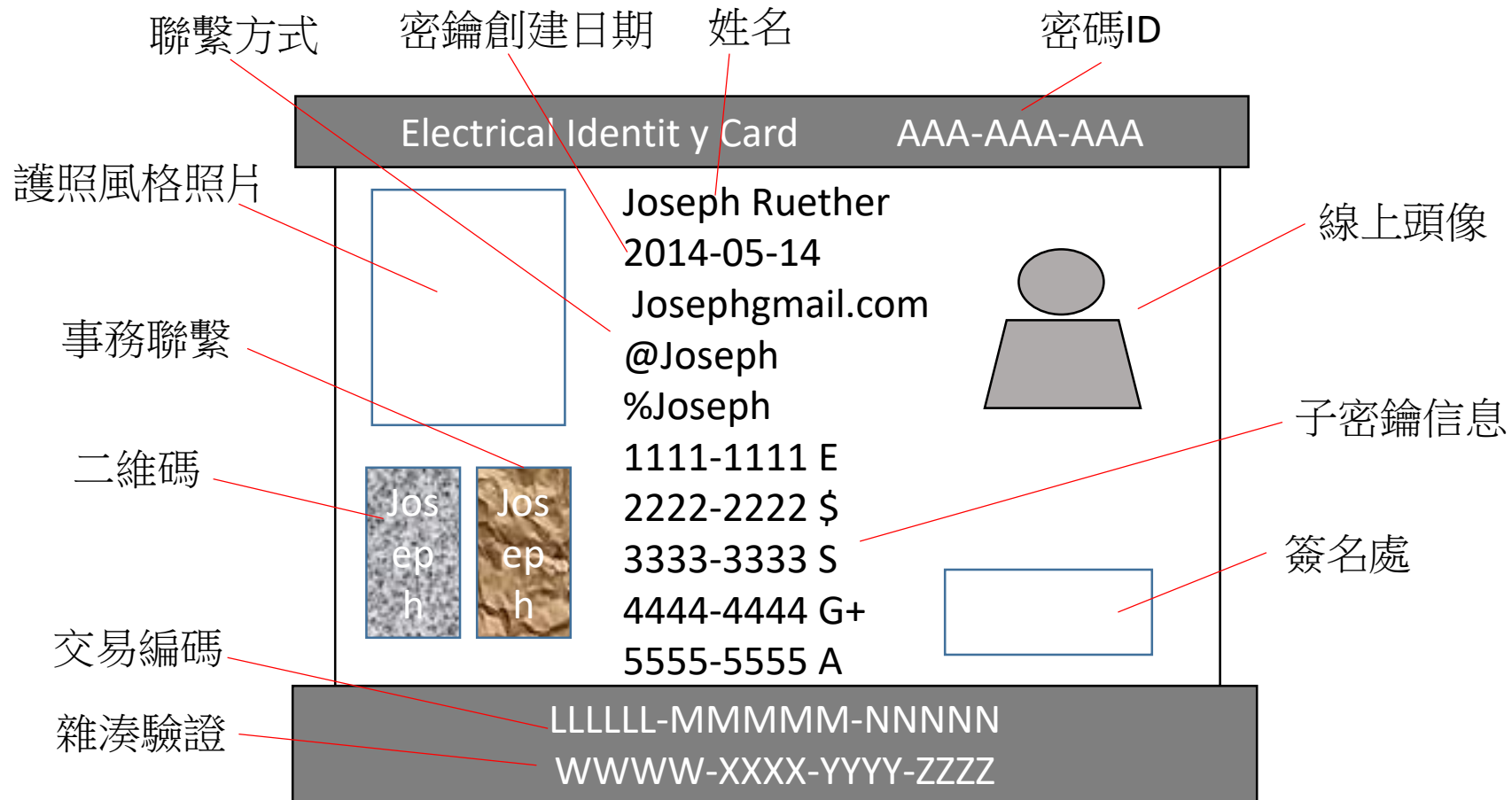
快遞相關各方及相關監管機構有權查詢

1. 包裹信息保留在快遞公司的服務器上. 將雜湊值保留在區塊鏈上
2. 包裹狀態的變化也保留在區塊鏈上. 且可追蹤歷史狀態

9. 區塊鏈充當一個通用的數位帳本. 促進物聯網設備間不同類型的交易



10. 智慧身份認證系統-區塊鏈身分證



Thanks