智慧財產。第三階段為智慧財產，可以將實體資產放置區塊鏈，並應用於各個領域，如：醫療、科學及藝術等，並探討如何將區塊鏈與物聯網進行結合。

Blockchain 4.0：智慧契約網路。目前已開始邁向第四階段，比特幣核心開發者Jeff Garzik認為「Blockchain 4.0是將所有的事情連結起來融進一個跨區塊鏈智慧契約網絡，對智慧資產進行保護。」達成金融市場交易清算、貿易金融、保險及跨境支付等服務。

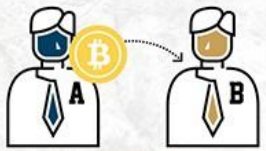
拆解區塊鏈

STEP 1

發起交易

STEP 2

驗證交易



B是一位網路賣家，最近開始接受比特幣付款。A是一位買家，想用比特幣付款買價值1聰比特幣的商品。整個流程會怎麼進行？

註：聰為比特幣最小單位，等於0.00000001比特幣。

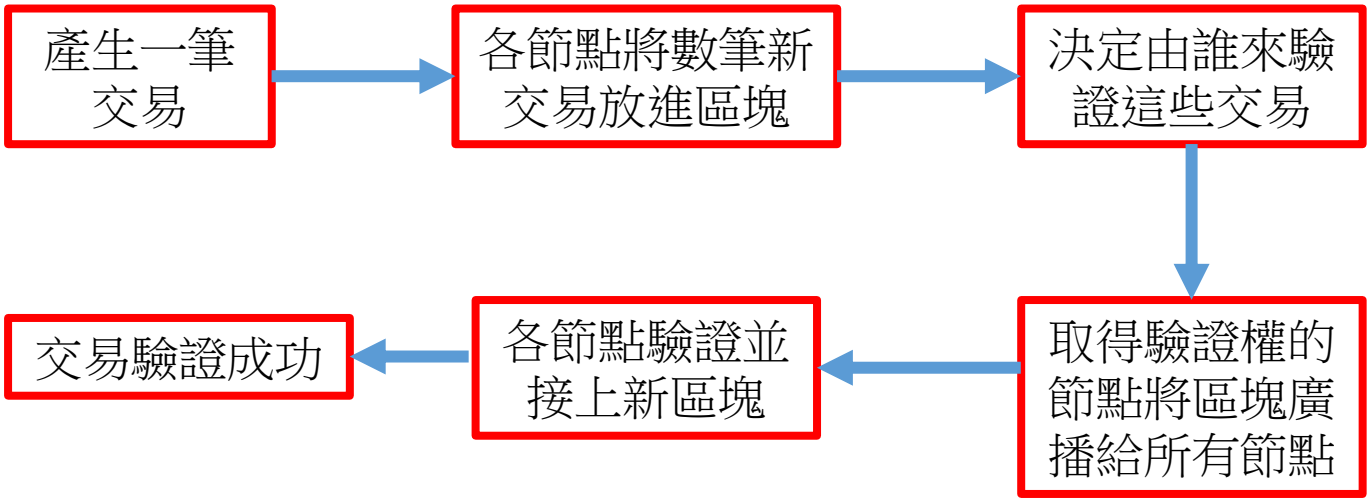
STEP 3

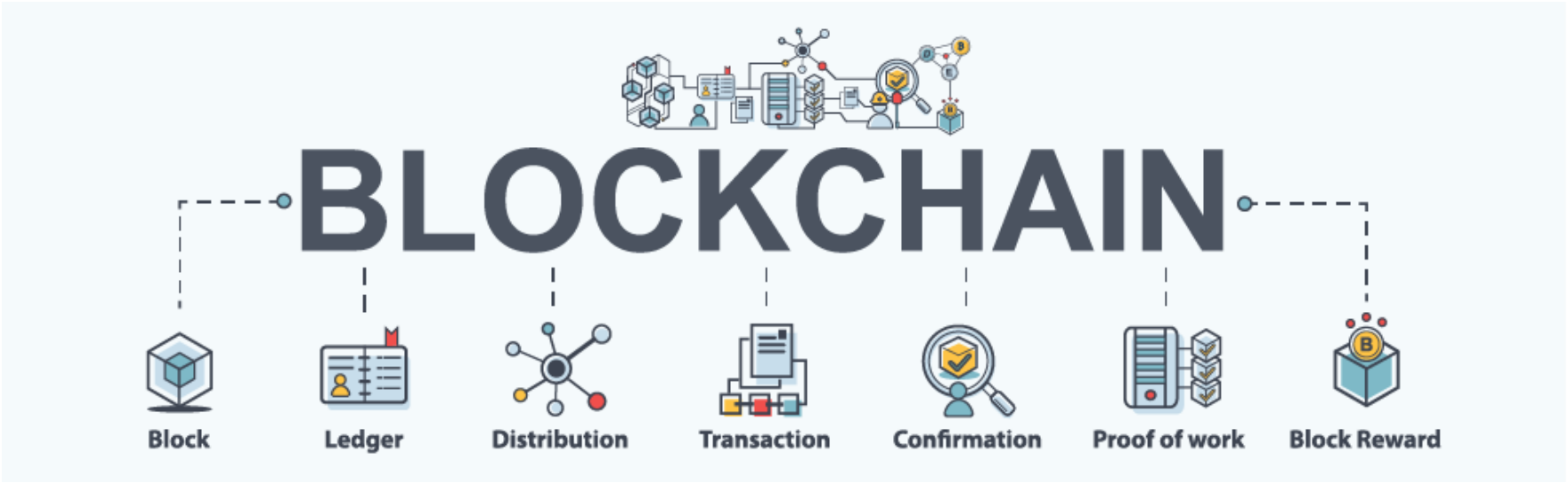
新增區塊

STEP 4

交易完成

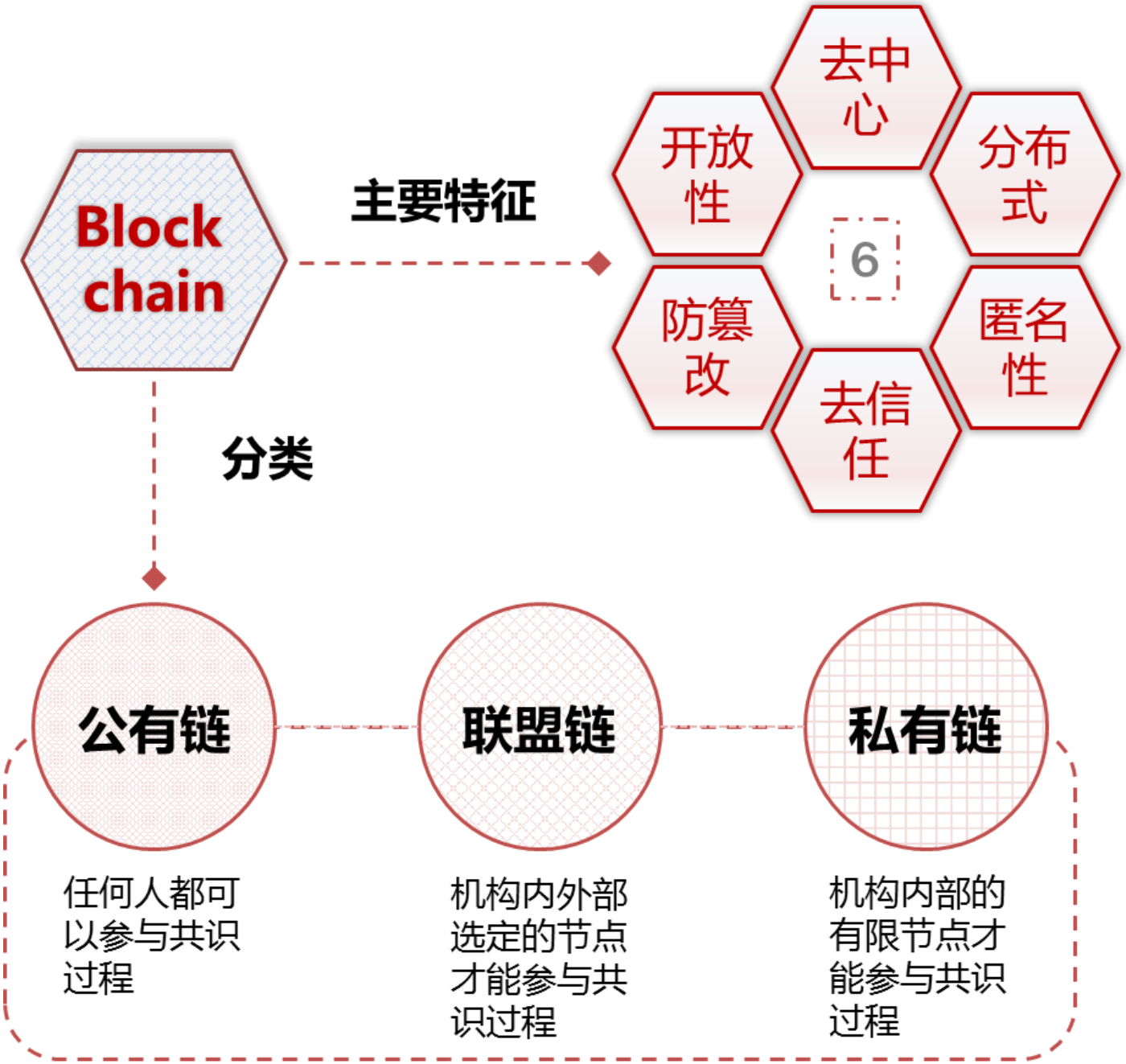
區塊鏈運作流程步驟


產生一筆交易
各節點將數筆新交易放進區塊
決定由誰來驗證這些交易
取得驗證權的節點將區塊廣播給所有節點
各節點驗證並接上新區塊
交易驗證成功


BLOCKCHAIN
Block
Ledger
Distribution
Transaction
Confirmation
Proof of work
Block Reward

特徵

- 區塊鏈技術是具有普適性的底層技術框架，可以為金融、經濟、科技甚至政治等各領域帶來深刻變革。在信息網絡化的大背景下，當需要進行信息交換的時候，如何防止遭遇惡意欺詐，從而做出正確決策？具有去中心化、可追溯性等特徵的區塊鏈技術正好解決了此類難題，區塊鏈的核心技術均圍繞此進行展開。


Block chain
主要特征
去中心
开放性
分布式
6
防篡改
匿名性
去信任
分类
公有链
联盟链
私有链
任何人都可以参与共识过程
机构内外部选定的节点才能参与共识过程
机构内部的有限节点才能参与共识过程

開放性

- 區塊鏈整體系統是開放的，除了節點的私鑰以外，網絡中的節點信息對所有人公開，區塊鏈中的數據對所有人公開，區塊鏈的源代碼對所有人公開。

自治性

- 區塊鏈採用基於預先設定好的規範或協議使得整個網絡中的所有節點能夠在自由、安全、無障礙的情況下的進行交互。
- 區塊鏈技術將原本人與人之間”的信任轉化為人對機器的信任，任何人為的行為都難以撼動機器計算的結果。

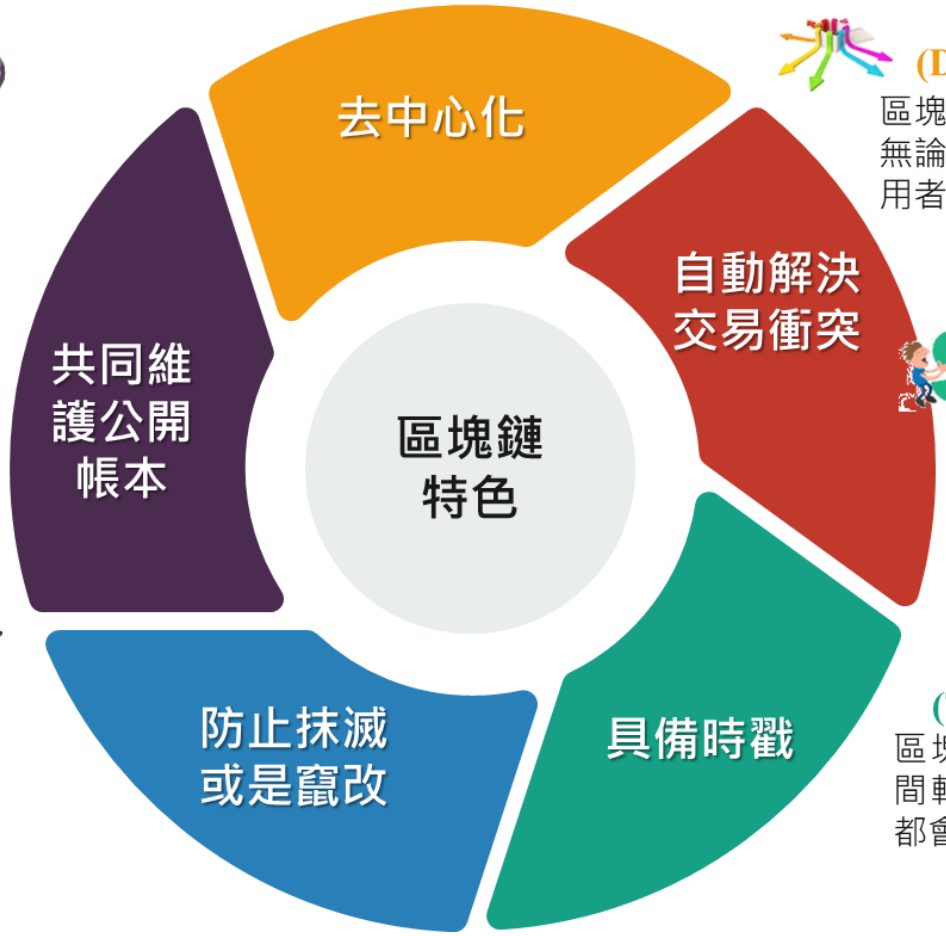
不可篡改性

- 在區塊鏈系統中，由於使用了哈希函數以及非對稱加密等先進的密碼學技術，在信息經過驗證後會被打包至區塊中，由於區塊鏈只做加法，所以區塊鏈上的區塊數據不可銷毀。由於它是分佈式的，所以單個節點對區塊的修改對於整個區塊鏈來說毫無影響，因此區塊鏈的數據穩定性和可靠性都是極高的。

可追溯性

- 儘管區塊鏈中的匿名性無法看到交易雙方的身份信息，但區塊+鏈的形式保存了從第一個區塊開始的所有歷史數據，連接的形式是後一個區塊擁有前一個區塊的HASH值，區塊鏈上任意一條記錄都可通過鍊式結構追溯本源，這樣從另一個方面保障了信息的安全性。

- 例如：電動車充電時，電動車、充電站可以自己驗證機器的身分。車子有自己的錢包，自動付錢給充電站，不假人工。
- 一般預測，IOTA適用於物聯網及微型支付。目前自駕車、智慧能源業者，也都在實驗IOTA技術。
- 例如透過區塊鏈連結同一社區住戶的太陽能板、電網及儲能設備，讓住戶可以直接向鄰居購買或販售多餘的太陽能電力；或應用在電動車充電站：自家電動車的充電樁可以共享。透過智慧合約（有交易，即付款）不需設專人收錢，可解決公共充電樁過少的問題。



共同維護公開帳本
(Public Ledger)
加入區塊鏈的各方，共同維護並享有同一份紀錄交易的帳本，在共同的資訊平台運作。

防止抹滅或是竄改
(Tamper Resistant)
以雜湊函數(hash function)為基礎，能保障資訊的完整性，若資訊被刪除或竄改，該區塊鏈的參與者必可察覺到資訊已被變更。

去中心化
(Decentraliztion)
區塊鏈以網路型態運作，無論是節點、數據或是使用者以點對點的方式連結。

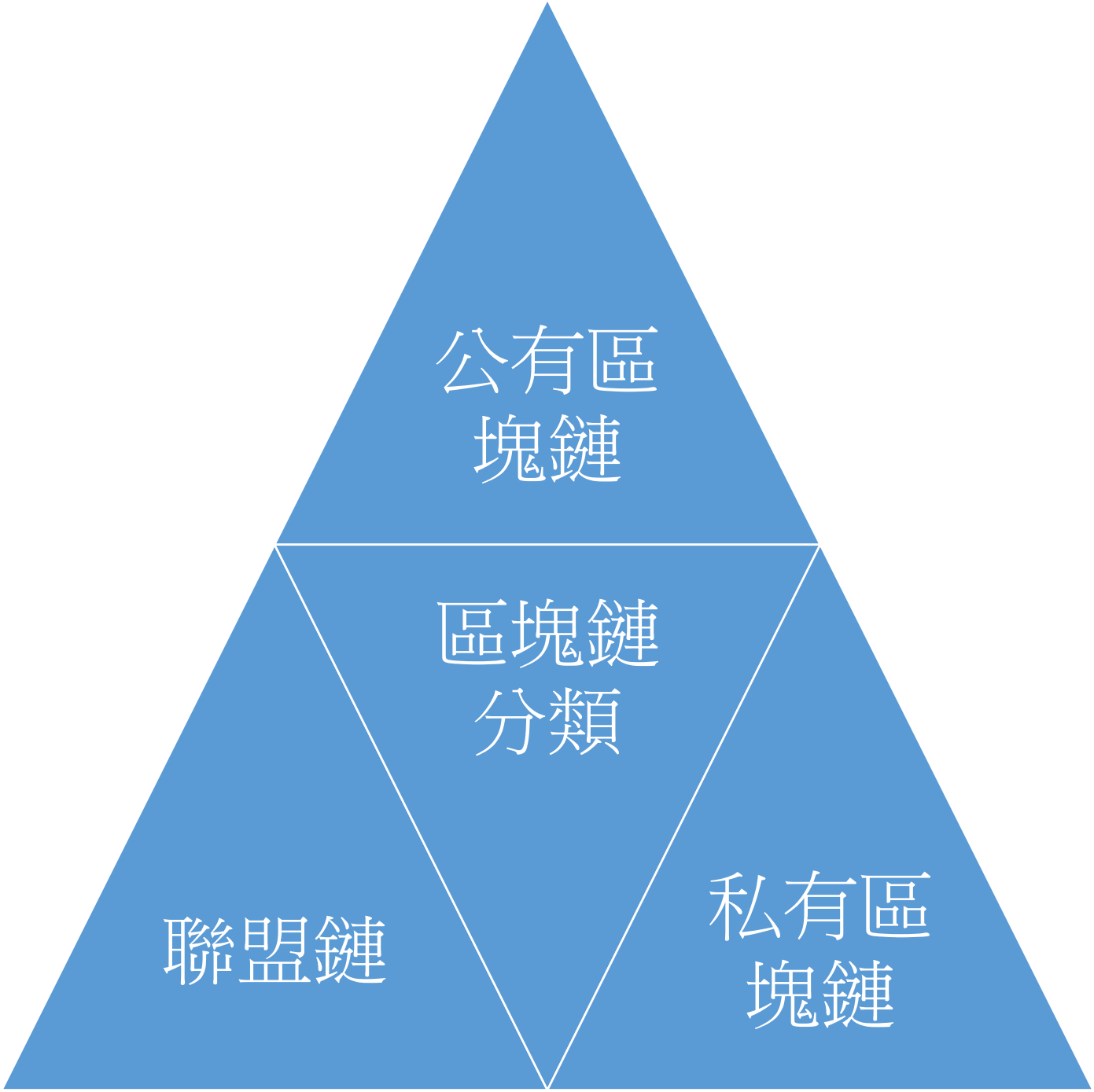
自動解決交易衝突
(Confliction Resolution)
當區塊鏈發生交易時，第二個使用同一批數位貨幣的交易即無法執行。

具備時戳
(Time Stamps)
區塊鏈參與者共用一時間軸，當資料變更時，都會註記時戳。


博弈
第三方托管
電子商務
全球支付
匯款
數位版權
智能合約
Smart contracts
數位貨幣
Digital currency
借貸
微金融
區塊鏈
股權
Securities
證券
Record keeping
數據記錄
醫療照護
私有市場
產權登記
債權
眾籌
金融衍生物
知識產權
投票
所有權
Google
葉峻樾醫師

區塊鏈分類

基於多種應用參與方式，區塊鏈目前主要分為公有區塊鏈、聯盟區塊鍊和私有區塊鏈。


公有區
塊鏈
區塊鏈
分類
聯盟鏈
私有區
塊鏈

公有鏈/私有鏈/聯盟鏈

公有區塊鏈

- 公有區塊鍊是指：
- 世界上任何個體或者團體都可以發送交易，且交易能夠獲得該區塊鏈的有效確認，任何人都可以參與其共識過程。公有區塊鍊是最早的區塊鏈，也是目前應用最廣泛的的區塊鏈。
- 是指像比特幣區塊鏈這樣的完全去中心化的、不受任何機構控制的區塊鏈。共識過程的參與者通過密碼學技術以及內建的經濟激勵維護數據庫的安全。

公有鏈

私有區塊鏈

- 私有區塊鍊是指存在一定的中心化控制的區塊鏈。僅僅使用區塊鏈的總賬技術進行記賬，可以是一個公司，也可以是個人，獨享該區塊鏈的寫入權限，本鏈與其他的分佈式存儲方案沒有太大區別。參與的節點只有用戶自己，數據的訪問和使用有嚴格的權限管理。聯盟鏈由於存在一定的中心化控制，所以也可以認為是屬於私有鏈範疇。

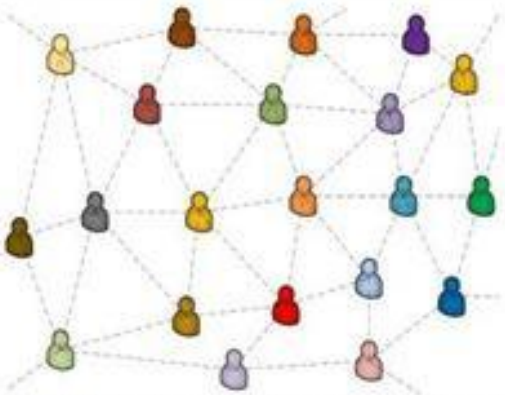
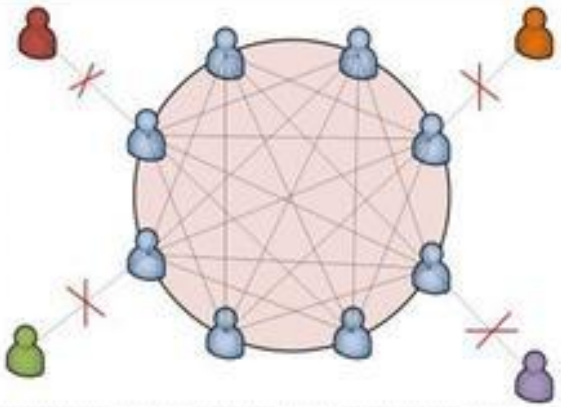
私有鏈

聯盟區塊鏈

- 聯盟區塊鍊是指：由某個群體內部指定多個預選的節點為記賬人，每個塊的生成由所有的預選節點共同決定，其他接入節點可以參與交易，但不過問記賬過程（本質上還是託管記賬，只是變成分佈式記賬，預選節點的多少，如何決定每個塊的記賬者成為該區塊鏈的主要風險點），其他任何人可以通過該區塊鏈開放的API進行限定查詢。
- 參與區塊鏈的節點是事先選擇好的，節點間很可能是有很好的網絡連接。這樣的區塊鏈上可以採用非工作量證明的其他共識算法，比如有100家金融機構之間建立了某個區塊鏈，規定必須67個以上的機構同意才算達成共識。

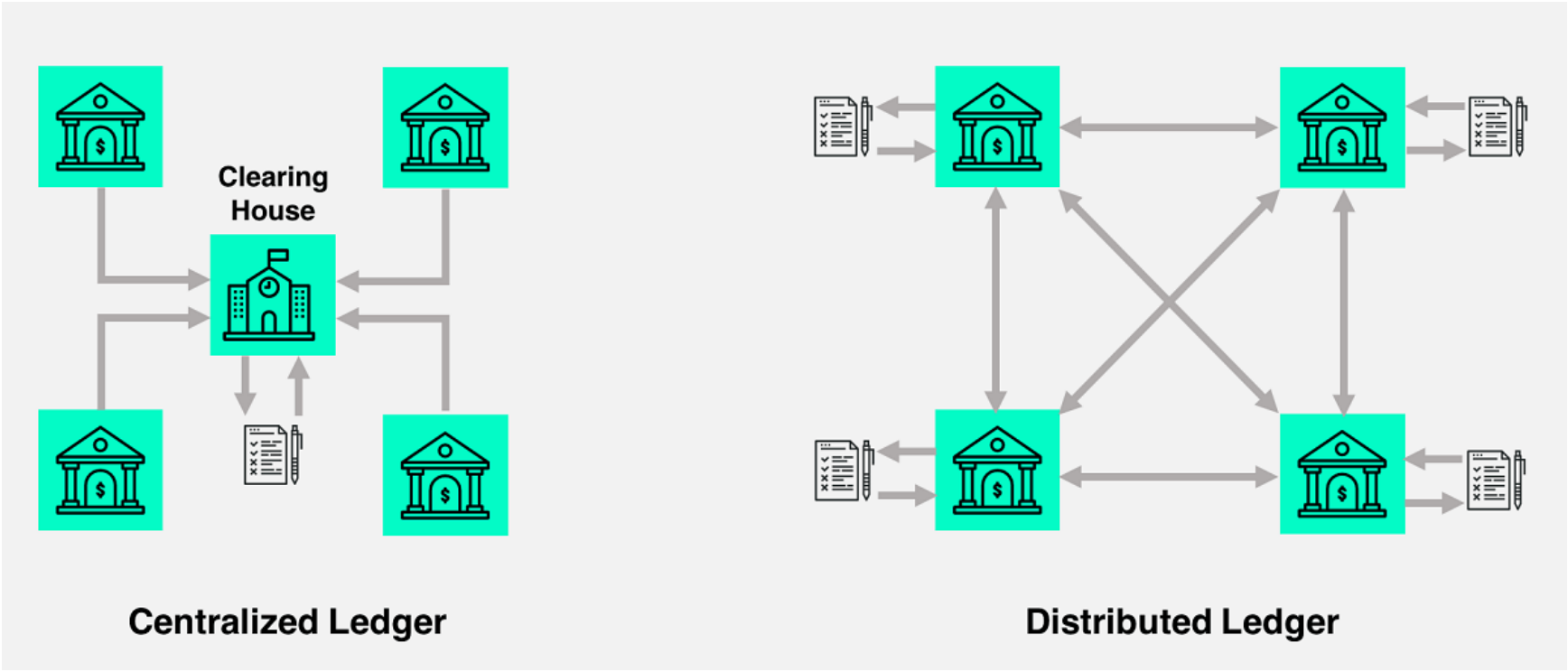
聯盟鏈

聯盟鏈 – 香港學歷證明

		
公有链（Public Blockchain）	**私有链**（Private Blockchain）	**联盟链**（Consortium Blockchain）
特点：去中心化程度最高，不受机构控制，整个账本对所有人公开透明。	特点：私有链的记账权不公开，信息不透明，去中心化最低，但具有记账速度快，记账成本低，隐私性高等优点	特点：多中心，以共识机制参与记账；交易处理快；通过私钥保护隐私；

去中心化

區塊鏈使用分佈式架構，在區塊鍊網絡中的節點同時扮演著“傳播者”和“驗證者”的角色，享受同等的權利、承受同等的義務，節點與節點之間可以自由通信，系統中的數據塊由具有存儲能力的節點共同存儲。



去中心化，如何顛覆世界？

區塊鏈演化三部曲

0

沒有區塊鏈之前

中心化的世界

1

區塊鏈1.0

比特幣：去中心化的開始

2

區塊鏈2.0

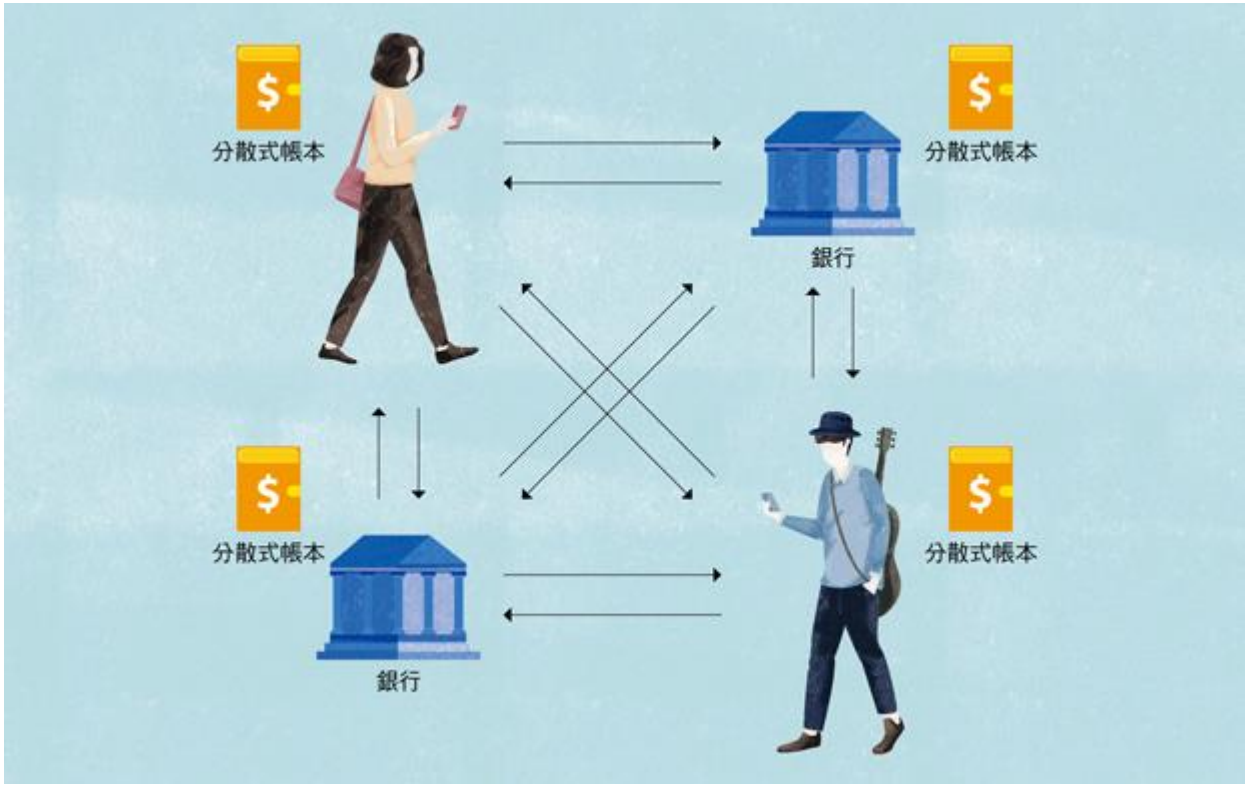
以太坊：智慧合約認證

3

區塊鏈3.0

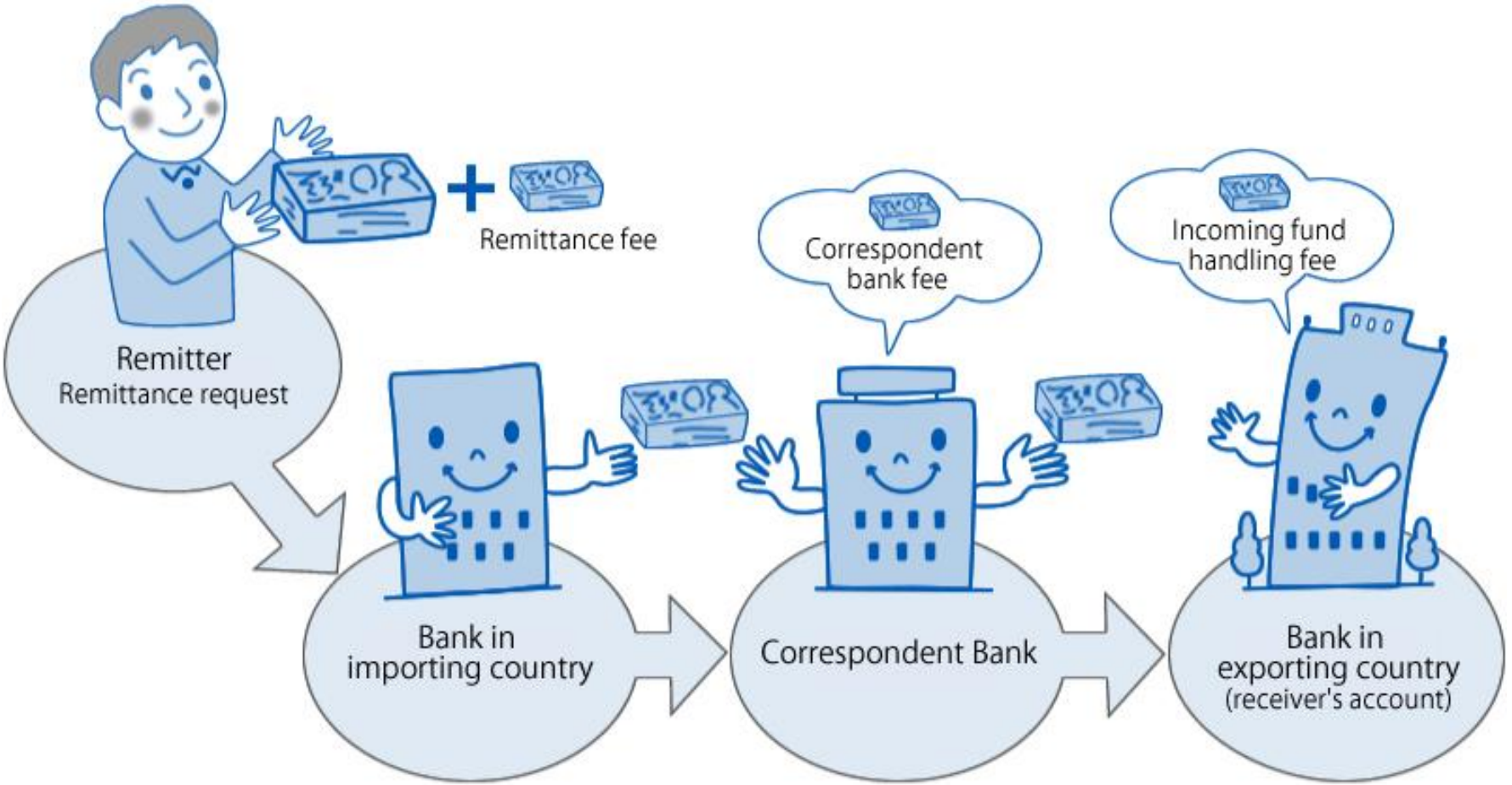
IOTA：連接實體生活、物聯網

區塊鏈1.0：
比特幣—去中心化的開始



比特幣（Bitcoin）開創了一種新的記帳方式，以「分散式帳本」（Distributed Ledger）跳過中介銀行，讓所有參與者的電腦一起記帳，做到去中心化的交易系統。

傳統貨幣交易方式

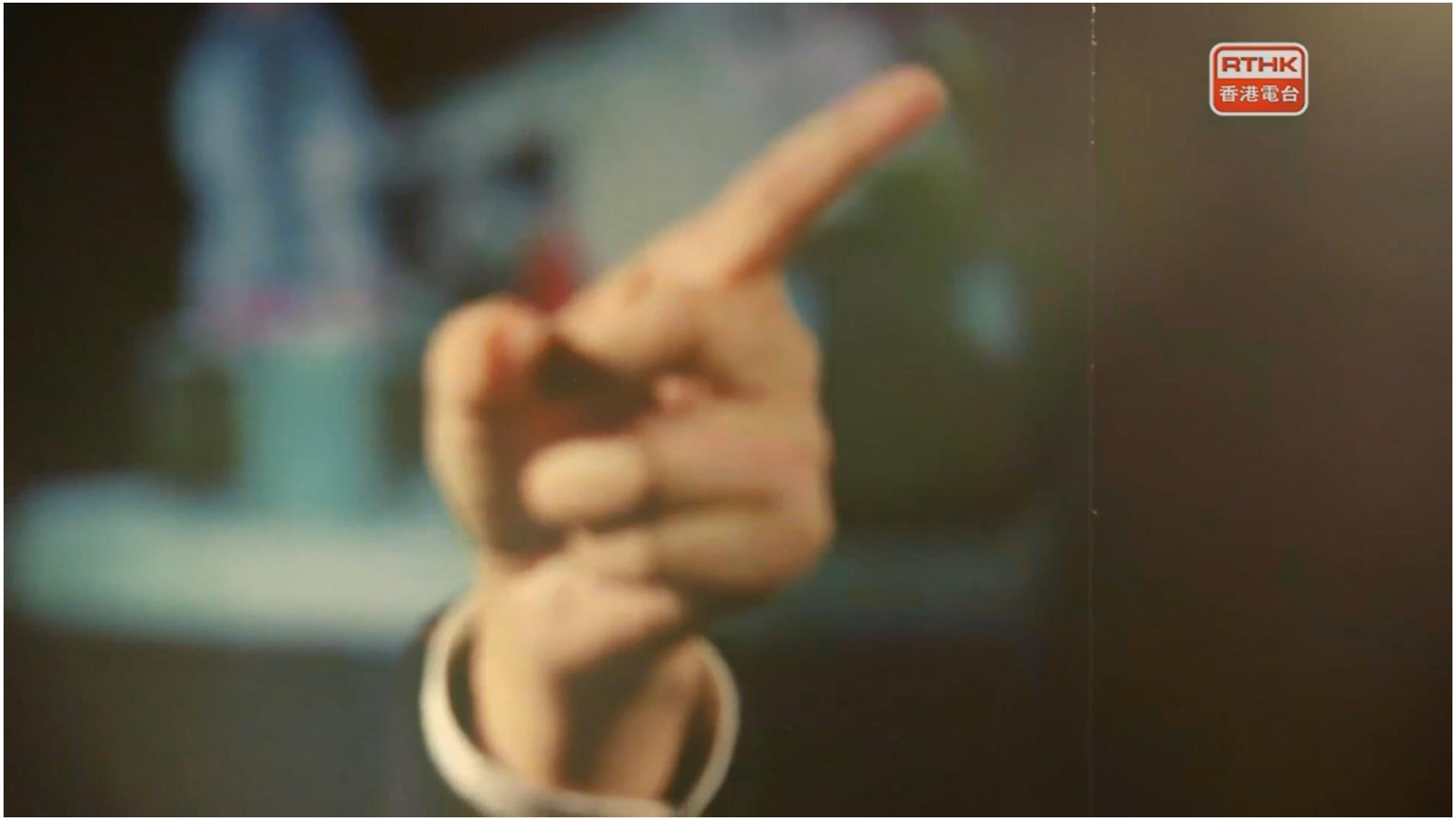

Remitter
Remittance request
Remittance fee
Bank in
importing country
Correspondent
bank fee
Correspondent Bank
Incoming fund
handling fee
Bank in
exporting country
(receiver's account)

	傳統貨幣交易模式
交易方式	-- 金融交易紀錄由中間金融機構負責管理 -- 中間金融機構負責查核金融往來交易資訊 -- 金融交易由付款人提出, 中間金融機構執行
優點	-- 中間金融機構之金融支付系統涵蓋面廣 -- 客戶對中間金融機構的接受度高 -- 可以與國際金融市場接軌
缺點	-- 金融交易過程透明度低 -- 個人基本資料容易隨著中間金融機構的管理不當而外流 -- 資產 (金) 轉移曠日費時 -- 金融交易成本高

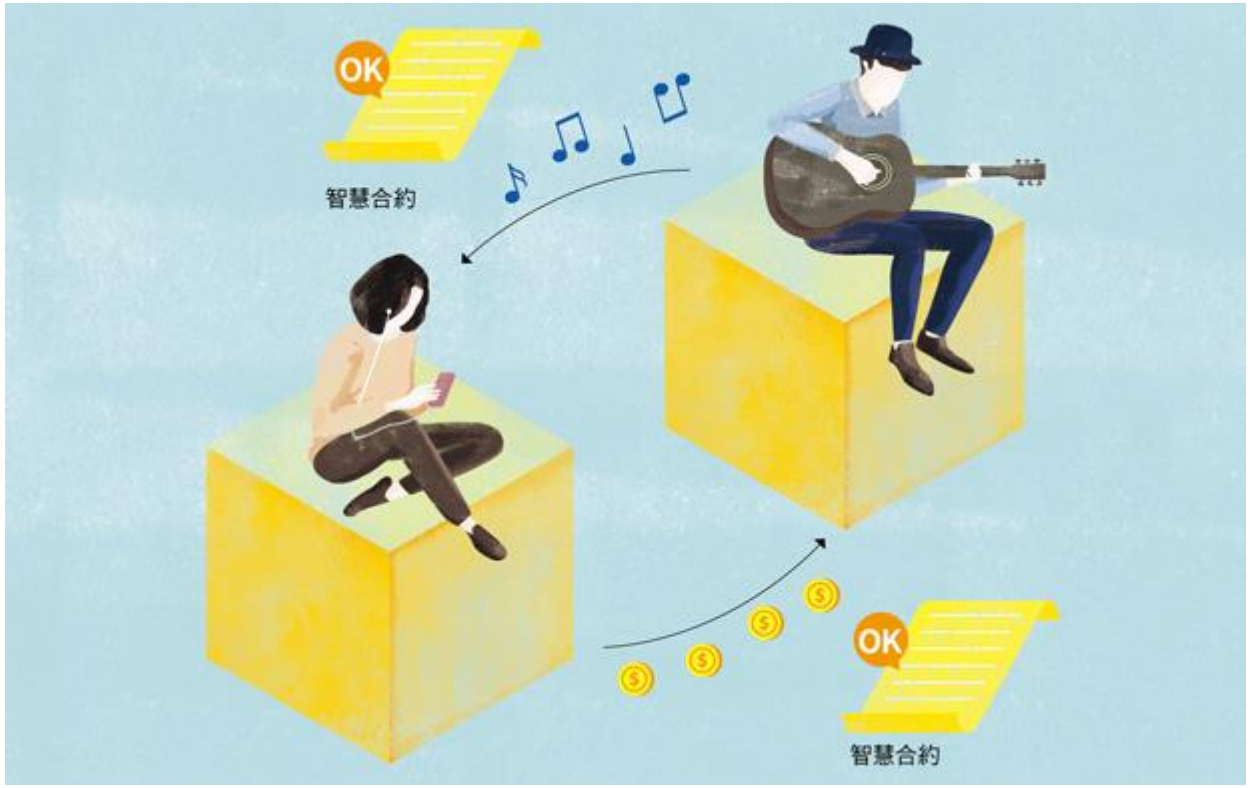
數位貨幣交易模式(區塊鏈)

	數位貨幣交易模式(區塊鏈)
交易方式	-- 數位金融交易紀錄採分散式記帳與儲存 -- 數位貨幣交易由分散式網路使用者進行驗證 -- 數位貨幣移轉由付款人啟動
優點	-- 數位貨幣交易紀錄資料透明, 但無法變更 -- 數位貨幣交易成本低 -- 數位貨幣交易風險低
缺點	-- 數位貨幣價值的穩定性低 -- 未受到貨幣法規限制 -- 數位貨幣交易無法變更或撤銷 -- 交易所容易受到網絡駭客的攻擊, 造成更大損失.

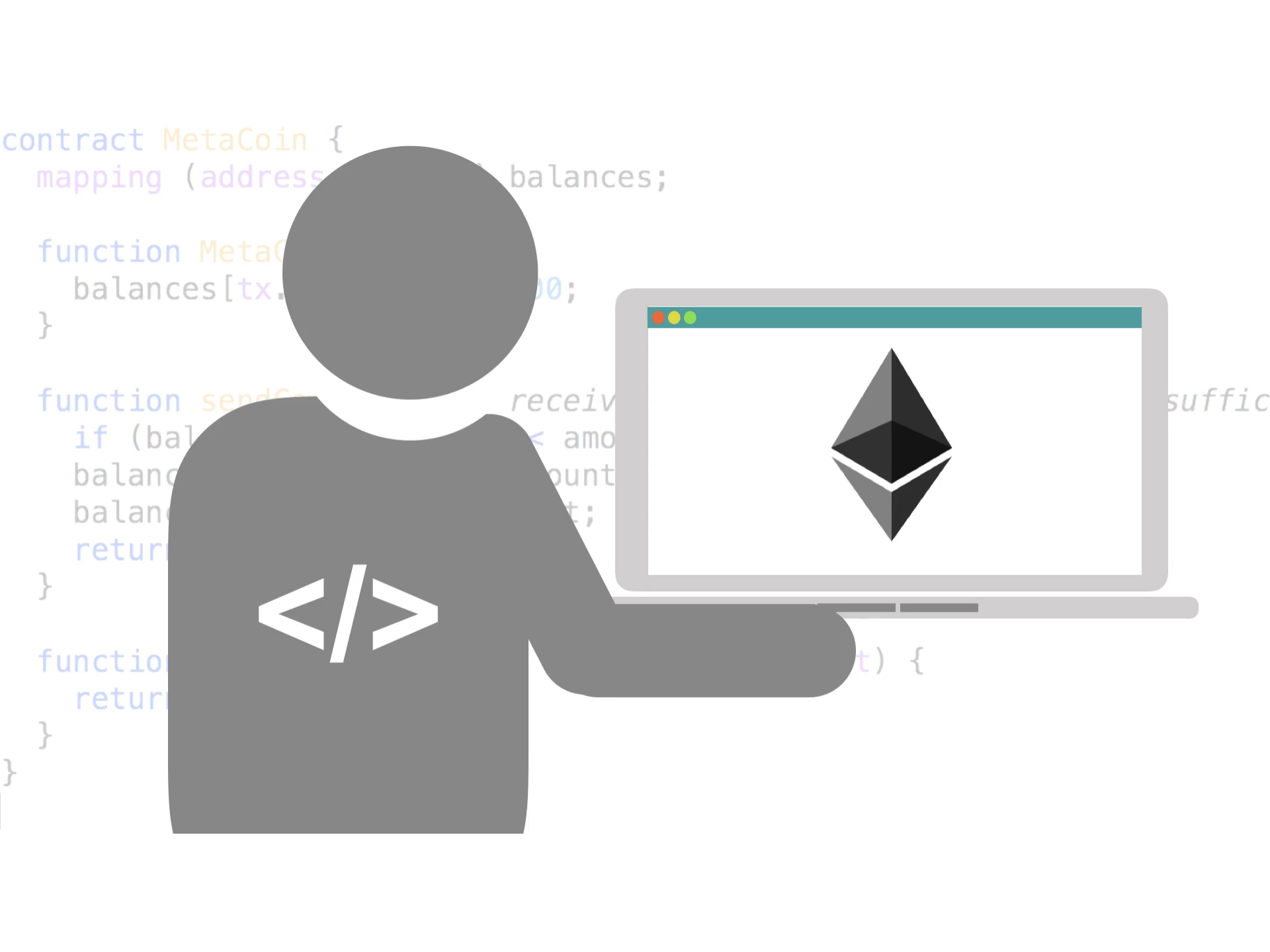
跨境支付寶



區塊鏈2.0：
以太坊—智慧合約認證



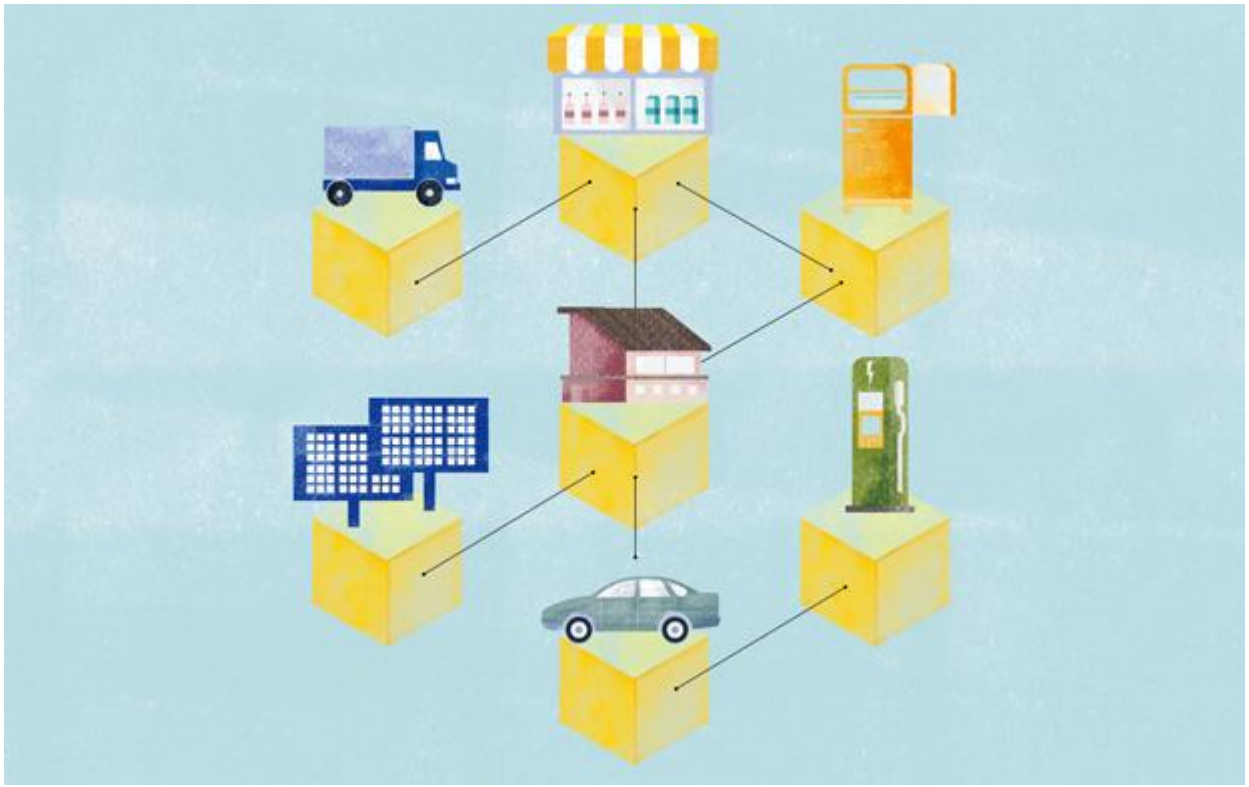
智慧合約是用程式寫成的合約，不會被竄改，會自動執行，還可搭配金融交易。因此，許多區塊鏈公司透過它來發行自己的代幣。



智慧合約

- 智慧合約可用來記錄股權、版權、智慧財產權的交易、也有人用它來記錄醫療、證書資訊。因此開啟比特幣等虛擬貨幣之外，區塊鏈應用的無限可能性。
- 例如食品產業的應用，從原料生產、加工、包裝、配送到上架，所有資料都會被寫入區塊鏈資料庫，消費者只要掃讀包裝條碼，就能獲取最完整的食品生產履歷；
- 在旅遊住宿方面，再也不需要透過Airbnb等中介平台，屋主直接在區塊鏈住宿平台上刊登出租訊息，就可以找到房客，並透過智慧合約完成租賃手續，不需支付平台任何費用。

區塊鏈3.0：
IOTA—連接實體生活、物聯網



IOTA透過較為簡單的演算法，讓每個鏈上的交易者都可以參與加密，且不需全體認證，不需礦工，可以加快加密時間。因此能進行物與物之間非常小、但頻率高的交易。

區塊鏈在商業上的6個使用場景

在一個行業裡，區塊鏈應用的主推動者可能有幾種：規模最大、最感受到痛點，或新進破壞者（disruptor）等。BCG整理了區塊鏈目前在商業世界的應用：

能源

去中間化有助於開闢小單位的能源市場，像是販售自家太陽能板的能源。

供應鏈管理

可追蹤貨品交易紀錄和產地，還能做為進出口的「信用狀」。

所有權證明

從交易紀錄上的資料，確認物品所有權轉移的過程。

身分認證

個人身分資料存於區塊鏈，可用於金融機構合法安全地確認客戶身分。

保險

串接航班資料，搭配個人身分驗證，一旦符合理賠條件，即自動申辦賠償。

醫療

不同醫療院所都可以藉由區塊鏈合法讀取病歷資料。