

Hi! 我是比特幣創造者中本聰，
跟著我一起了解去中心化的商業新規則！



300秒

區塊鏈麻瓜
大變身!

一起來解鎖



區塊鏈夯什麼？

分散式帳本？

“ 以人工智慧、量子資訊、行動通訊、
物聯網以及區塊鏈為代表的
新一代訊息技術，正在加速突破應用。 ”
—— 習近平

改變記帳方式的新技術？

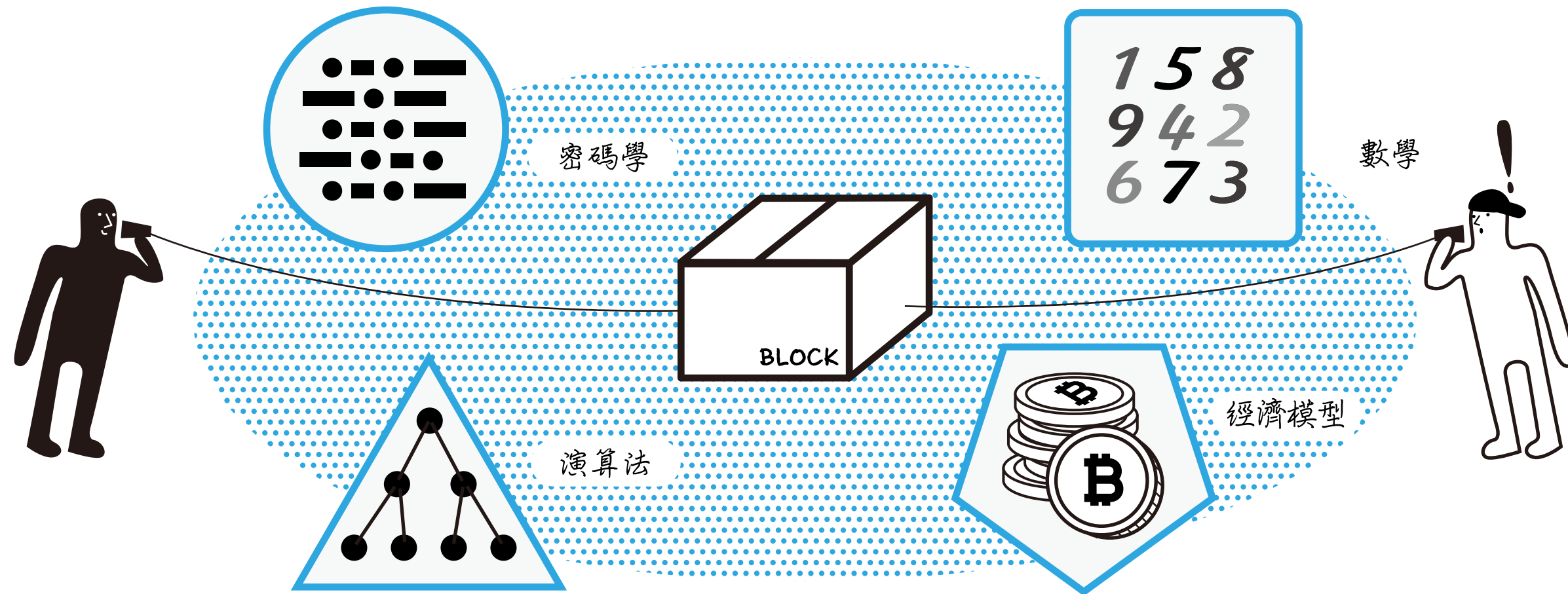


數位貨幣是甚麼？

智慧合約？

“ 區塊鏈將帶動繼蒸氣機、電力和電腦
發明而來的第4次工業革命。 ”
—— 世界經濟論壇創辦人施瓦布

區塊鏈夯什麼？



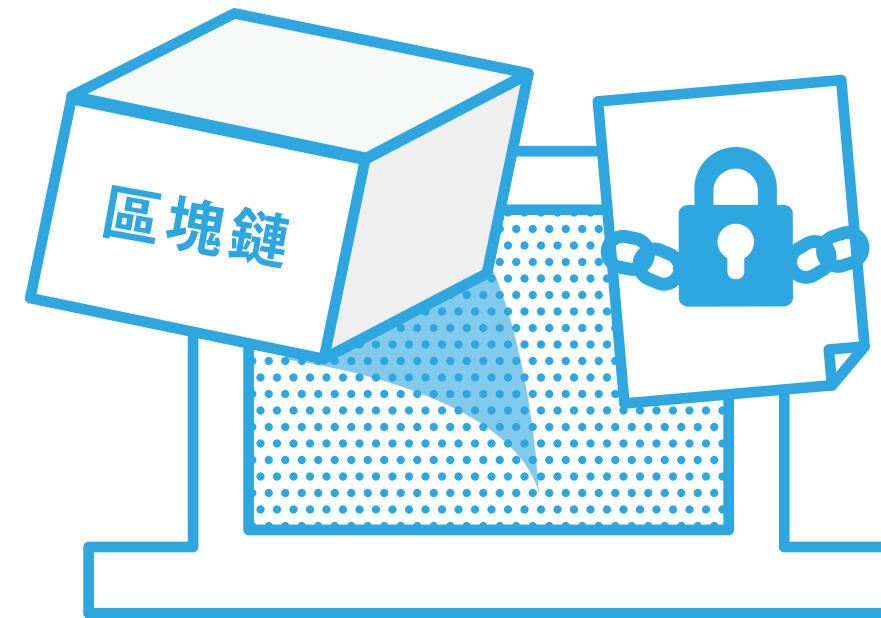
區塊鏈是將許多跨領域技術湊在一起，並結合點對點網路關係，建立信任效果。
成為一個不需基於彼此信任基礎、也不需仰賴單一中心化機構就能夠運作的分散式系統。

區塊鏈夯什麼？

以貨幣交易為例



傳統貨幣交易方式，需要第三方機構，
例如銀行、政府、央行等當作中介。



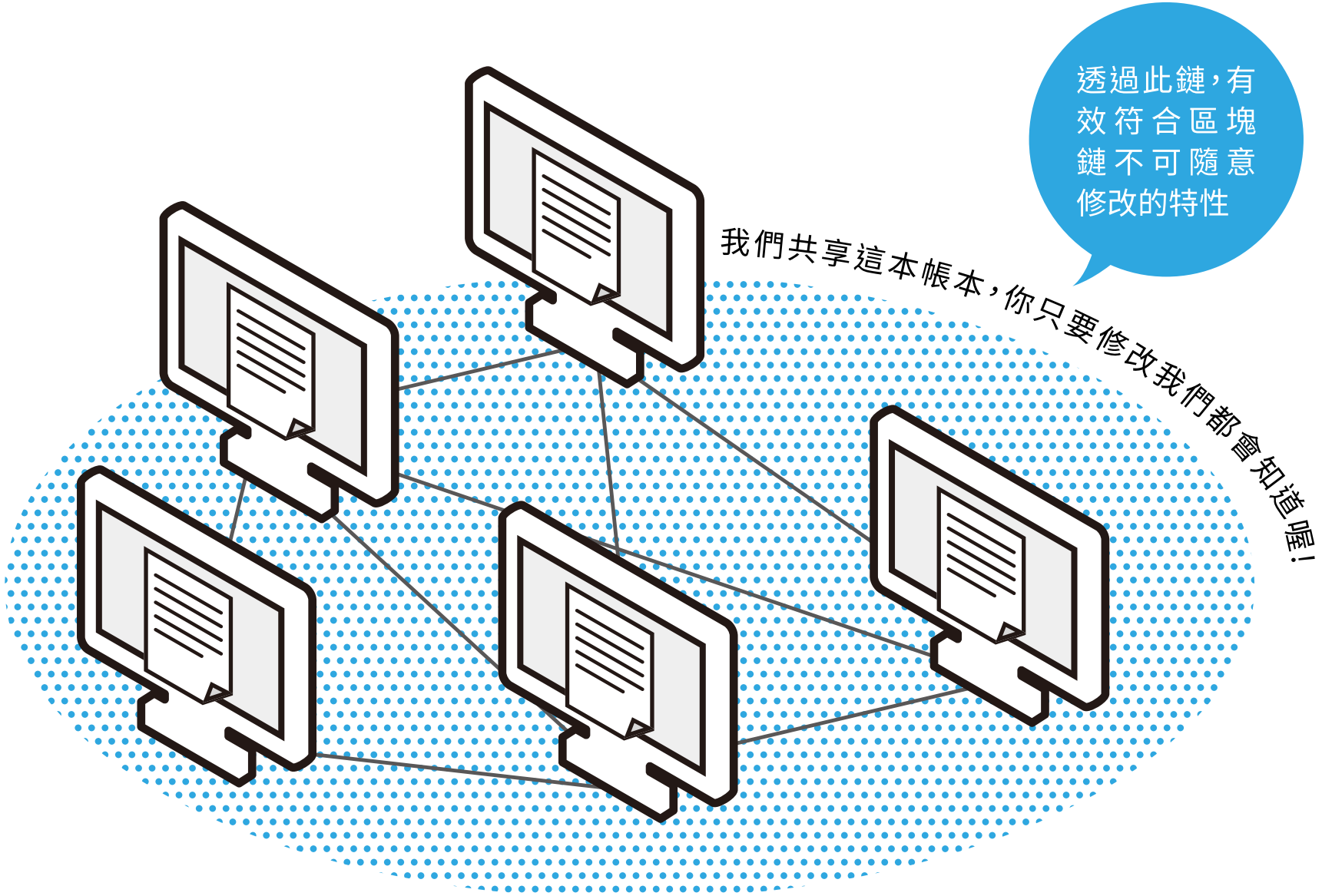
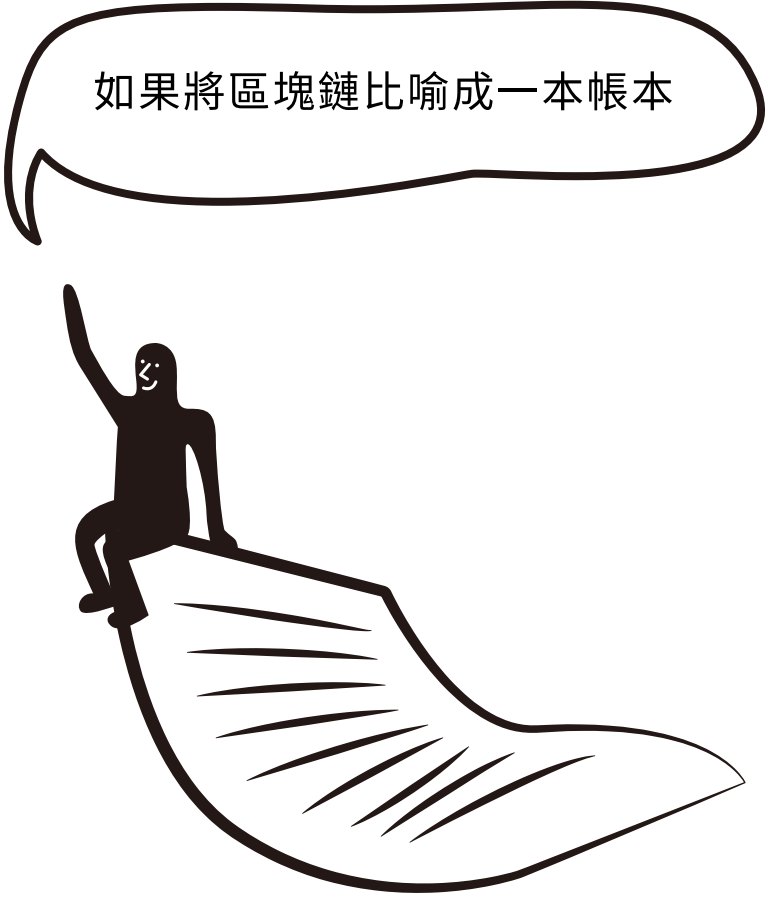
透過區塊鏈技術可以實現：

1. 不需第三方機構，即可於網路上進行有價資產轉移。
2. 以P2P完成跨國匯兌

區塊鏈包含6個核心技術



區塊鏈技術大拆解

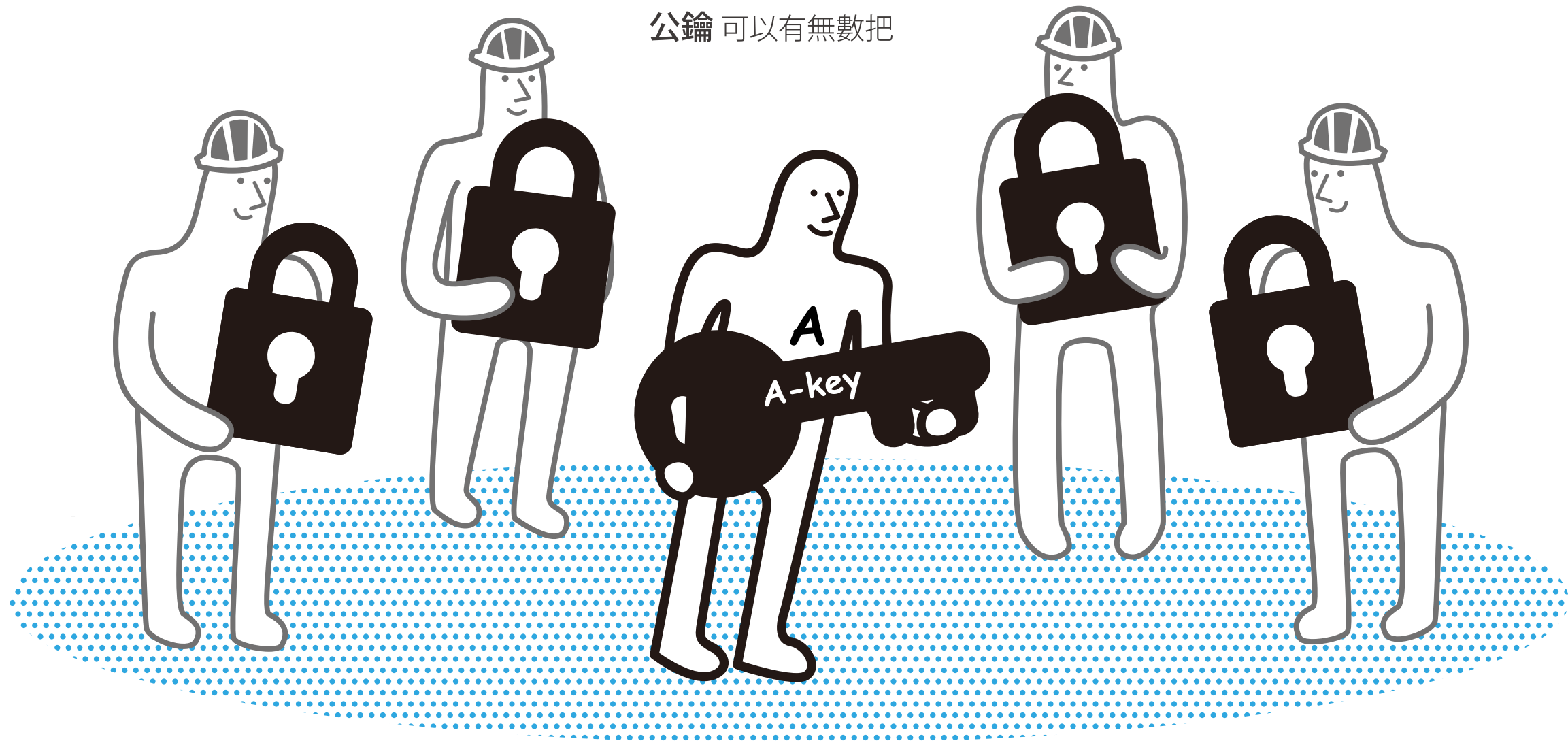


區塊 就是帳本的內頁用來記錄交易，且標有頁碼以確保區塊的前後相連。

鏈 是在多位記帳者（礦工）電腦內，保存同一份帳本。每一筆交易都必須由記帳者彼此達成共識，才能確保帳本內容完全同步。

區塊鏈技術大拆解

公鑰 可以有無數把

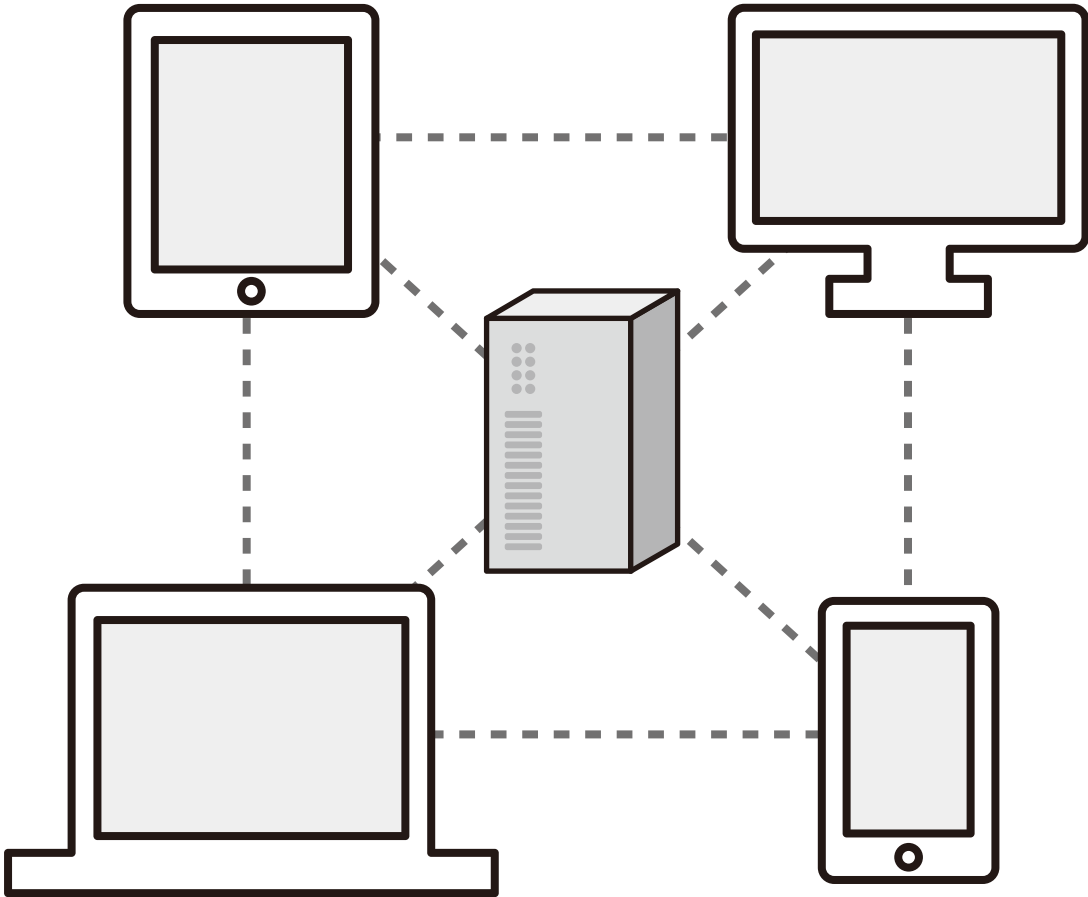


私鑰 代表對該帳戶有所有權跟使用權, 並且只有一把

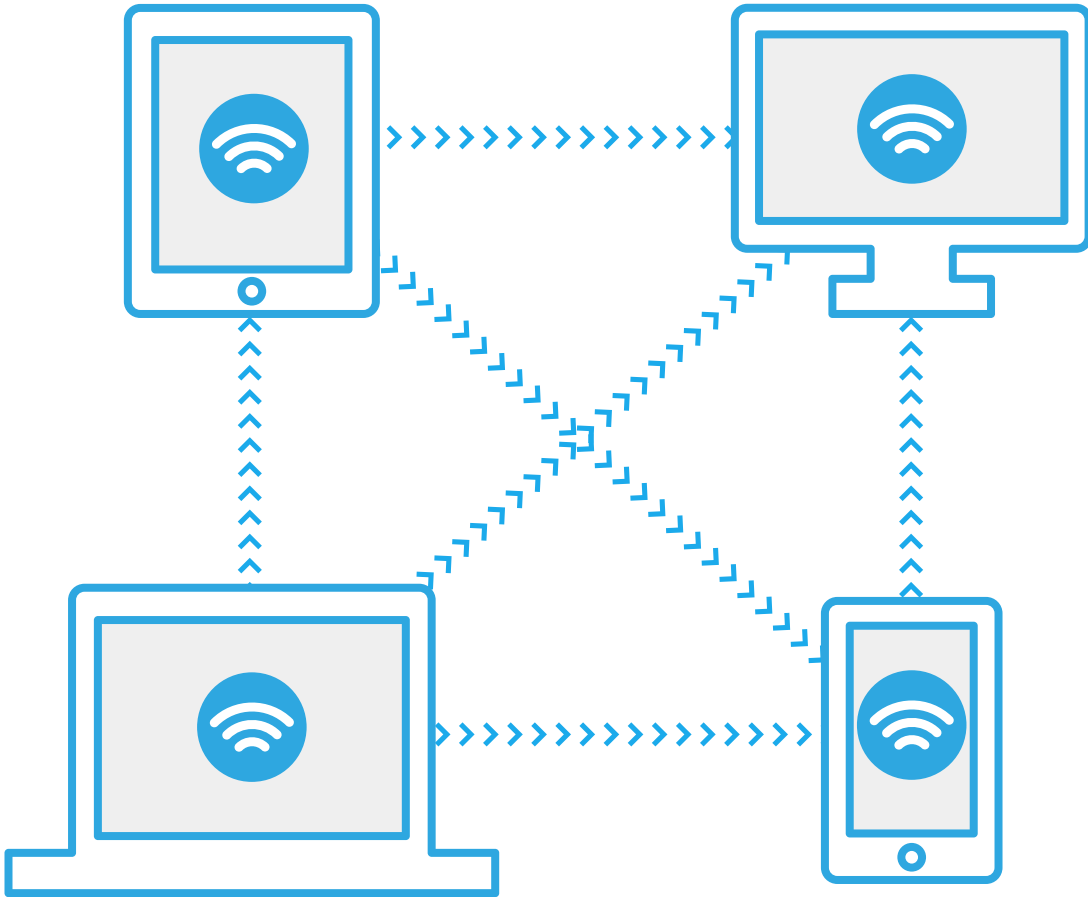
數位簽章

當A發起一筆交易, 會用私鑰進行簽章, 協助驗證的節點只要能用A的公鑰配對成功就能確認該筆交易由A發起。

區塊鏈技術大拆解



傳統網路運輸方式
傳輸必須透過伺服器

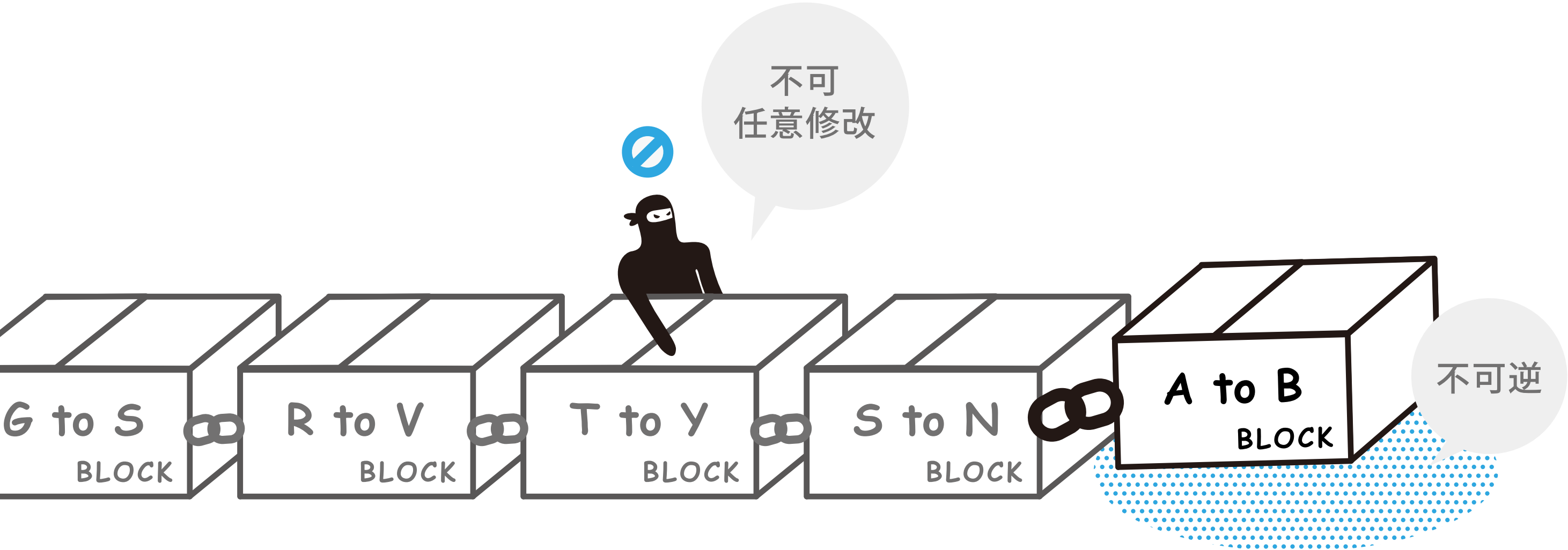


P2P網路技術
電腦間可以自動組網傳輸

P2P網路技術

讓區塊鏈具備自動組網功能，讓交易訊息可以一傳十、十傳百在網路中擴散。就像BT、eMule這類P2P下載軟體，是一種無中心伺服器的網路傳輸方式，依照用戶群交換資訊的網路系統，可減少傳輸中的節點，降低資料遺失風險。

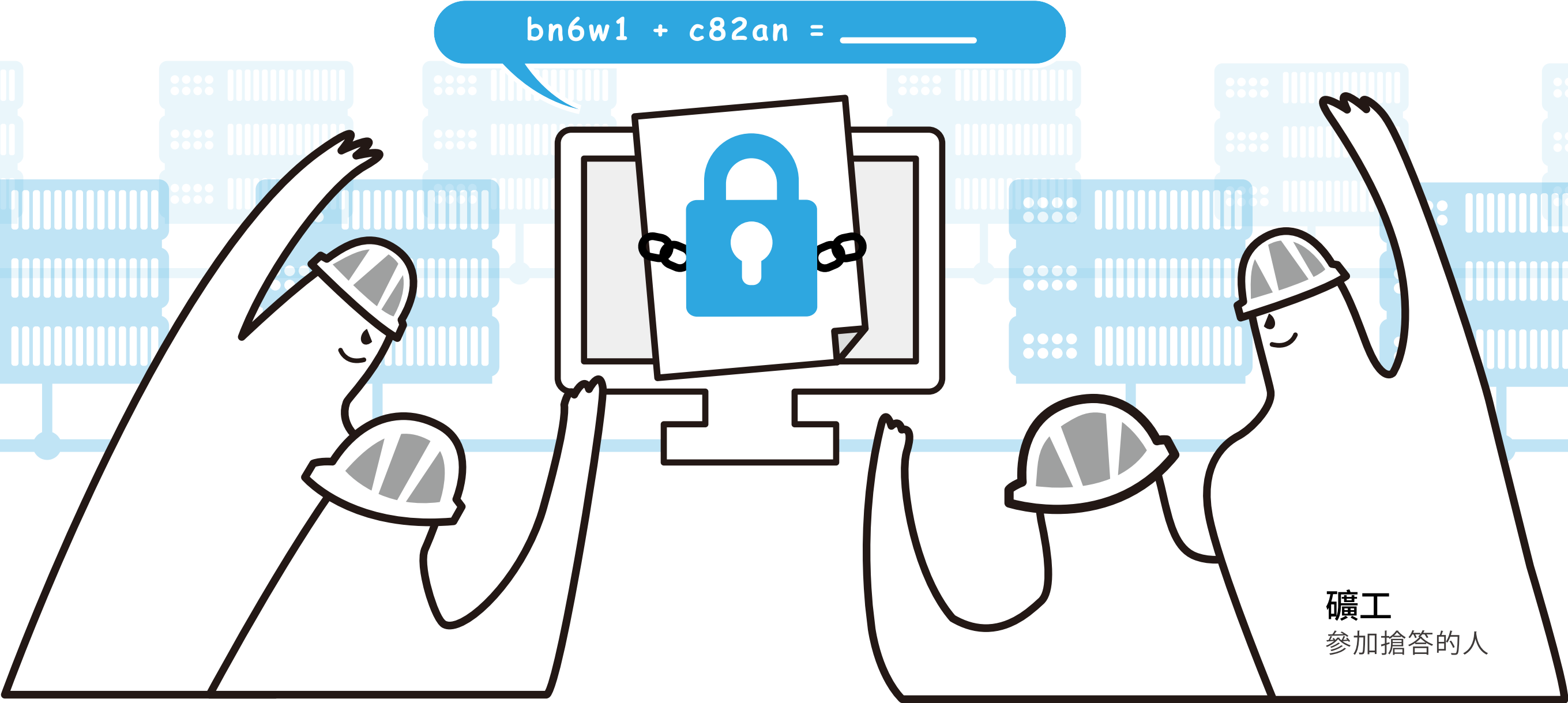
區塊鏈技術大拆解



雜湊演算法

區塊鏈中保證交易訊息不被篡改的單向密碼機制。
實現區塊鏈的特性：1.不可任意修改 2.不可逆

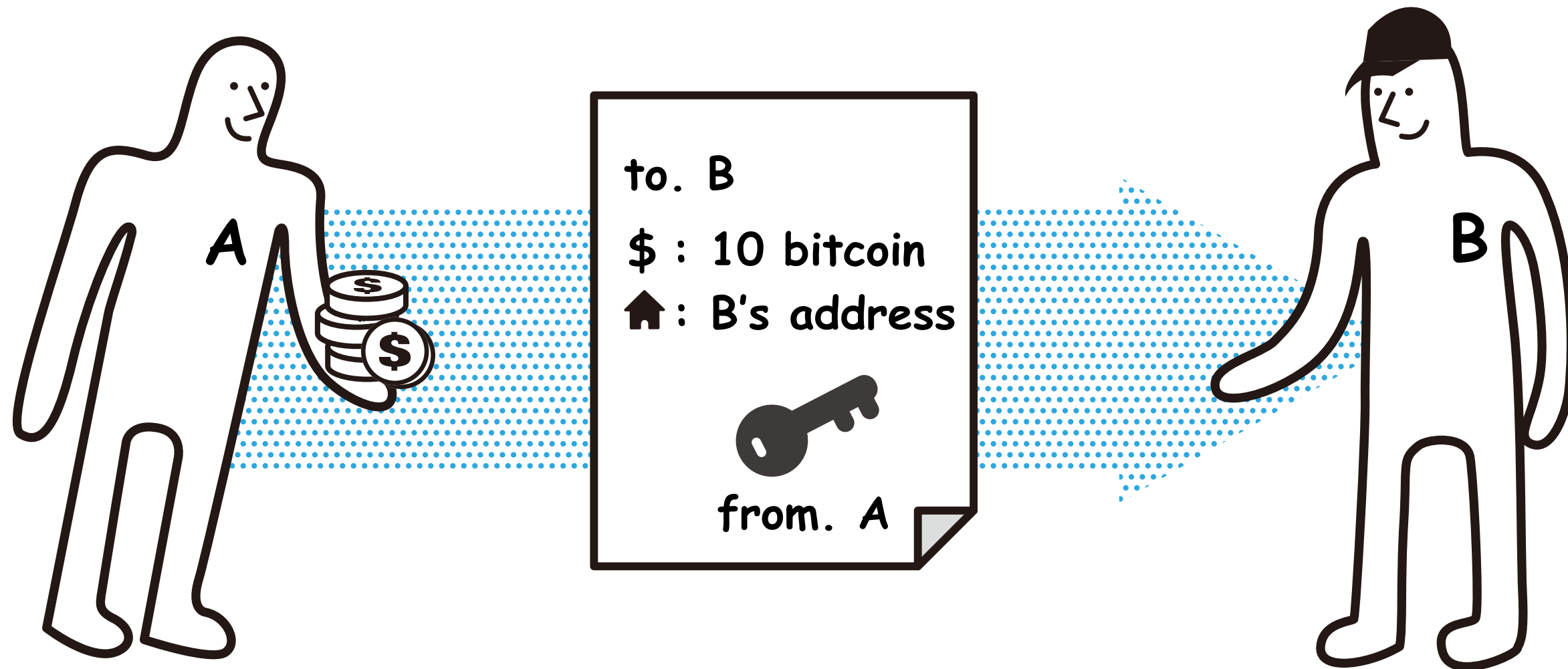
區塊鏈技術大拆解



挖礦

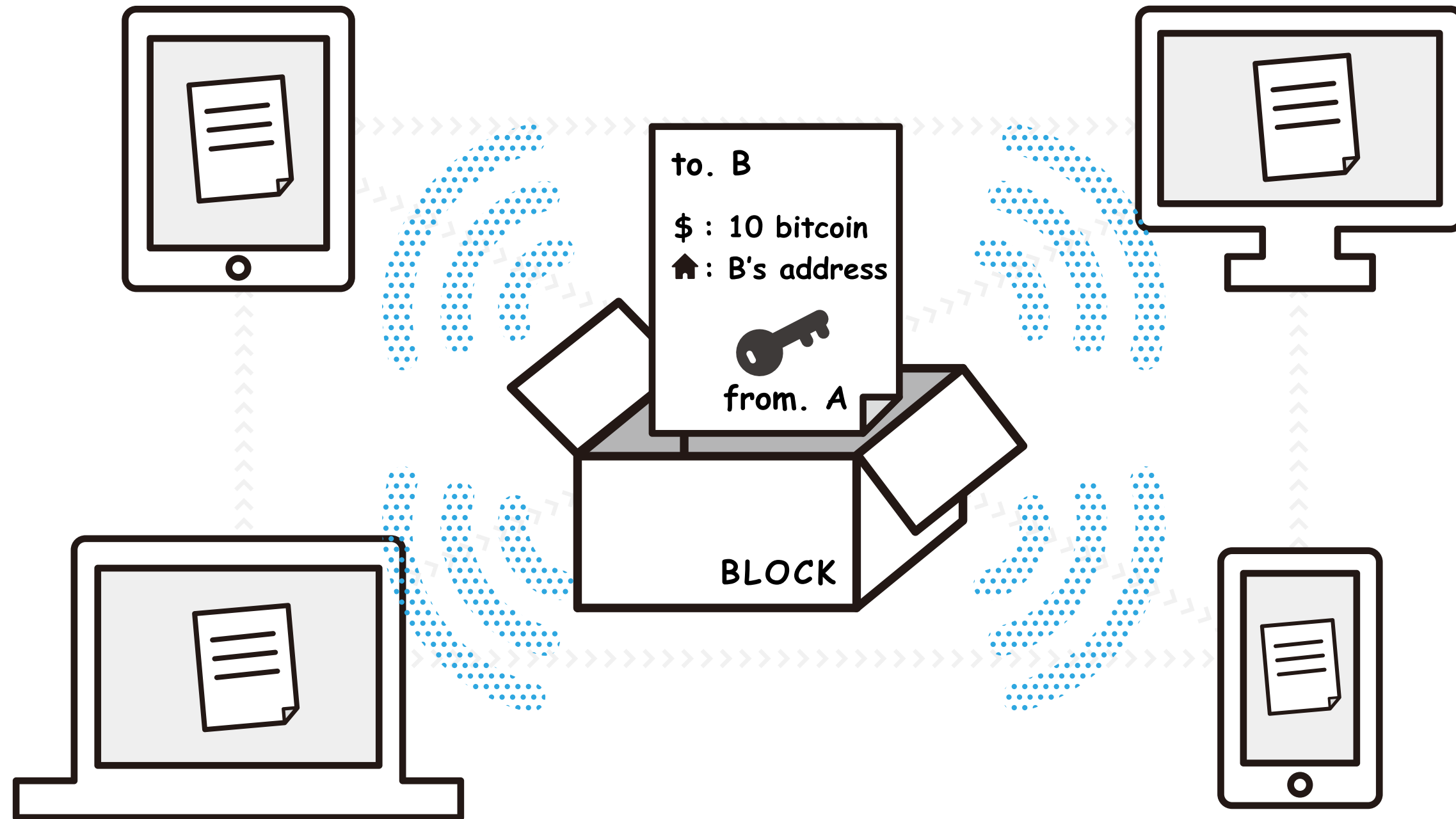
以比特幣網路為例，為了取得交易記帳權，共同維護帳本的人或電腦必須比賽解出一個複雜的運算問題，通常最先解出的人所記錄的交易記錄才能被視作有效、即獲得記帳權，此過程即稱為挖礦。

一筆比特幣交易如何進行？



A先發起一個請求：我想要建立一個新的區塊，在A的錢包中輸入交易金額和B的比特幣地址，並用私鑰在交易訊息上簽章

一筆比特幣交易如何進行？



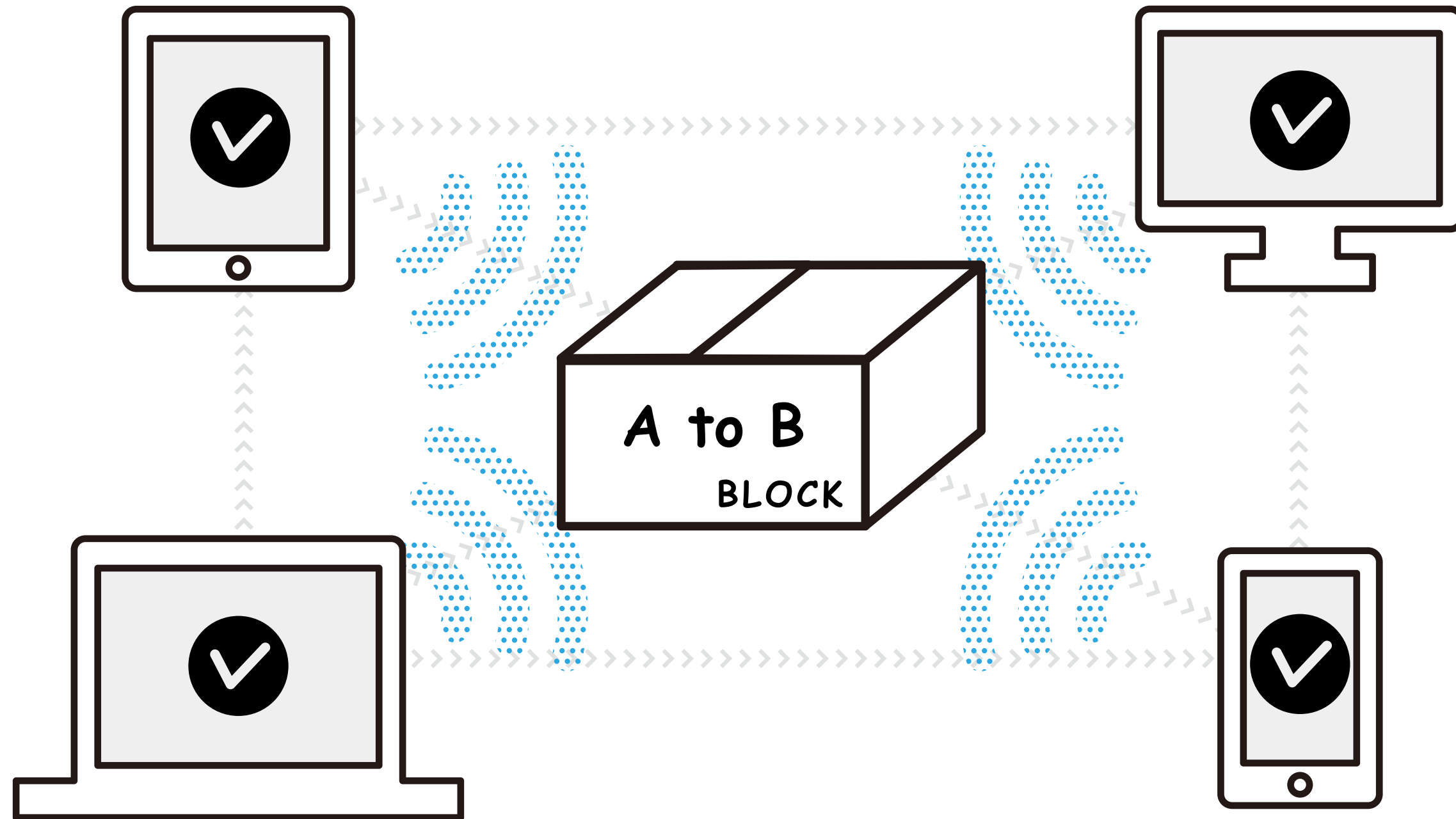
這筆交易會被包裹在區塊中，存在於網路上，
此區塊就會透過P2P網路，被廣播到區塊鏈上的各個節點

一筆比特幣交易如何進行？



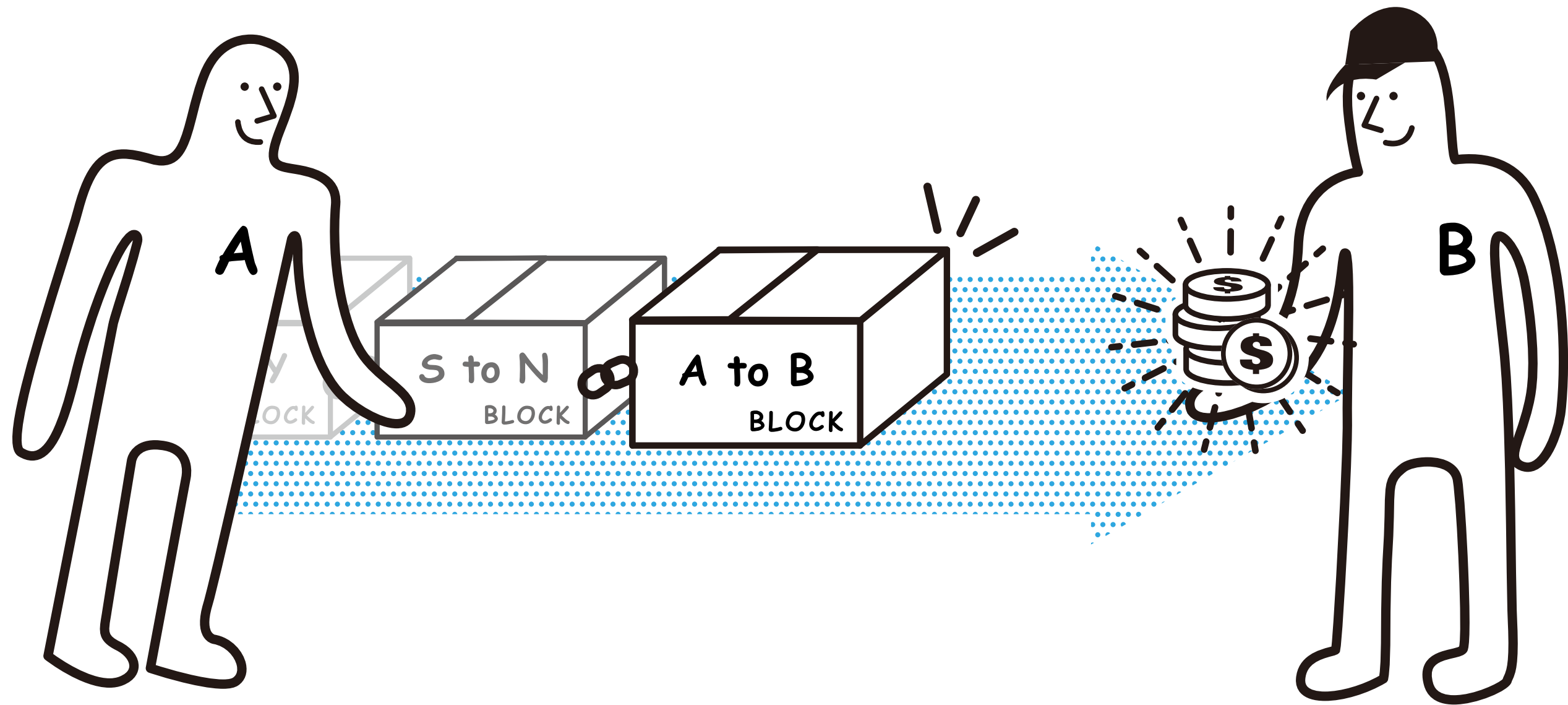
節點(礦工)收到訊息後，運用公鑰驗證發起人身分、
檢查交易地址有效、檢查帳戶餘額充足後，獲得記帳權的礦工記錄交易

一筆比特幣交易如何進行？



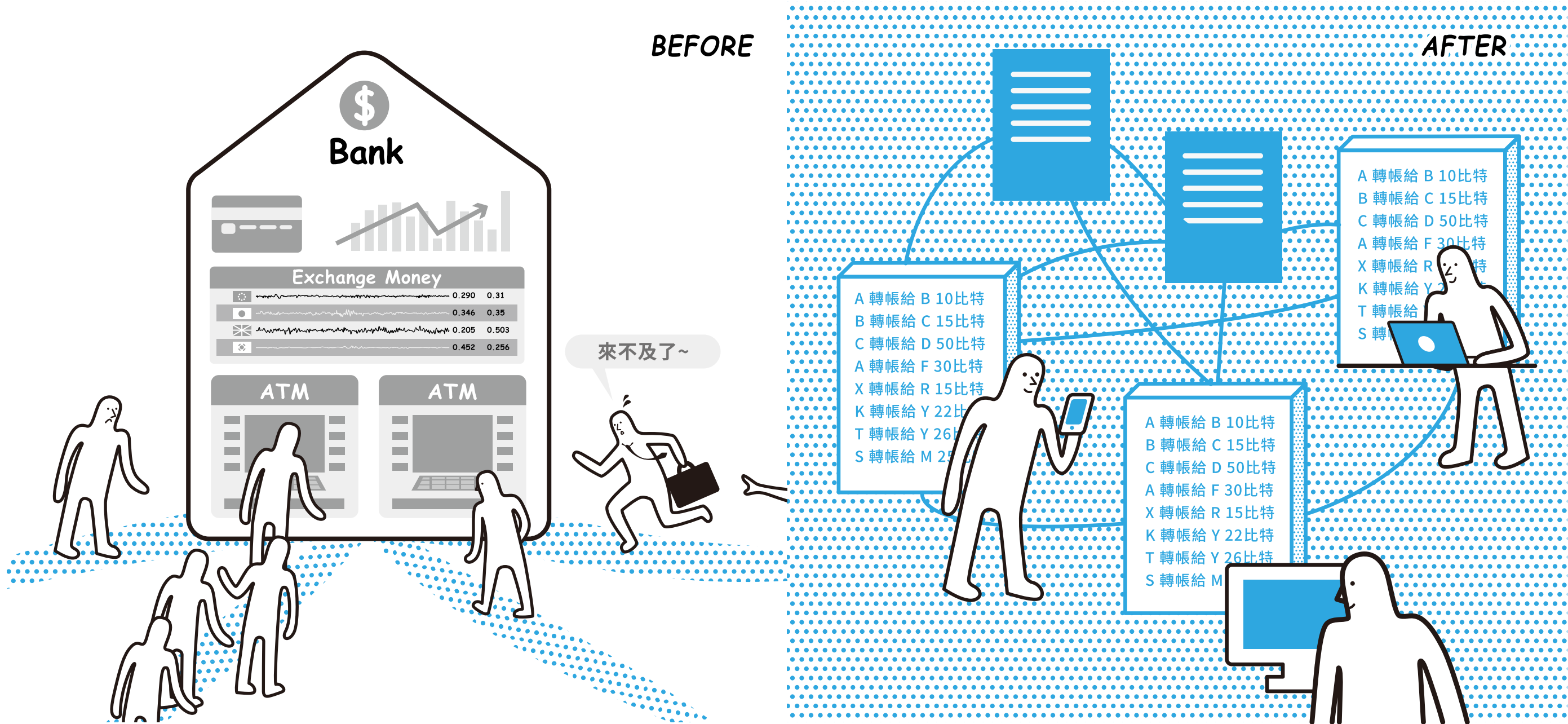
各節點確認這筆交易後，此交易成立

一筆比特幣交易如何進行？



區塊就會被添加到主鏈上，錢就會從A轉移到B身上

區塊鏈五大應用場景



銀行業－降低營運成本及弊端發生

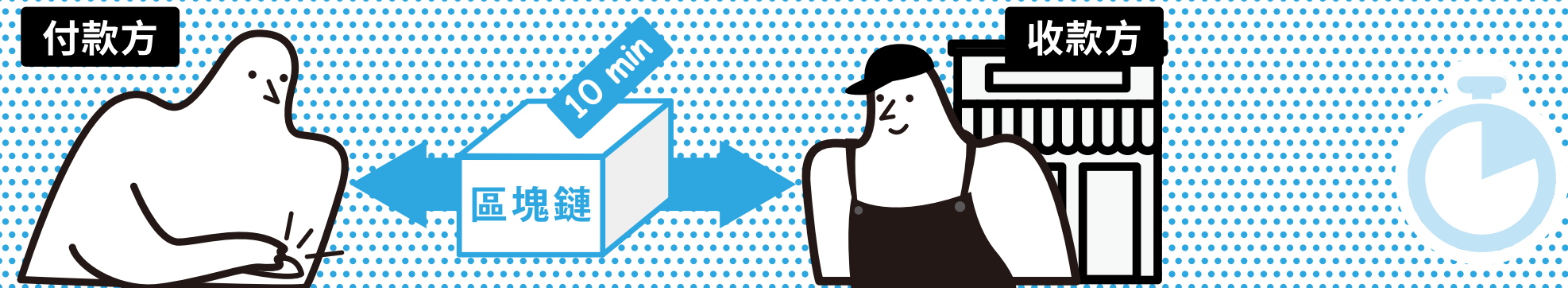
- 1.減少銀行維護中央電子帳本資料庫的營運成本
- 2.讓交易資訊透明，避免金融弊端發生

區塊鏈五大應用場景

BEFORE



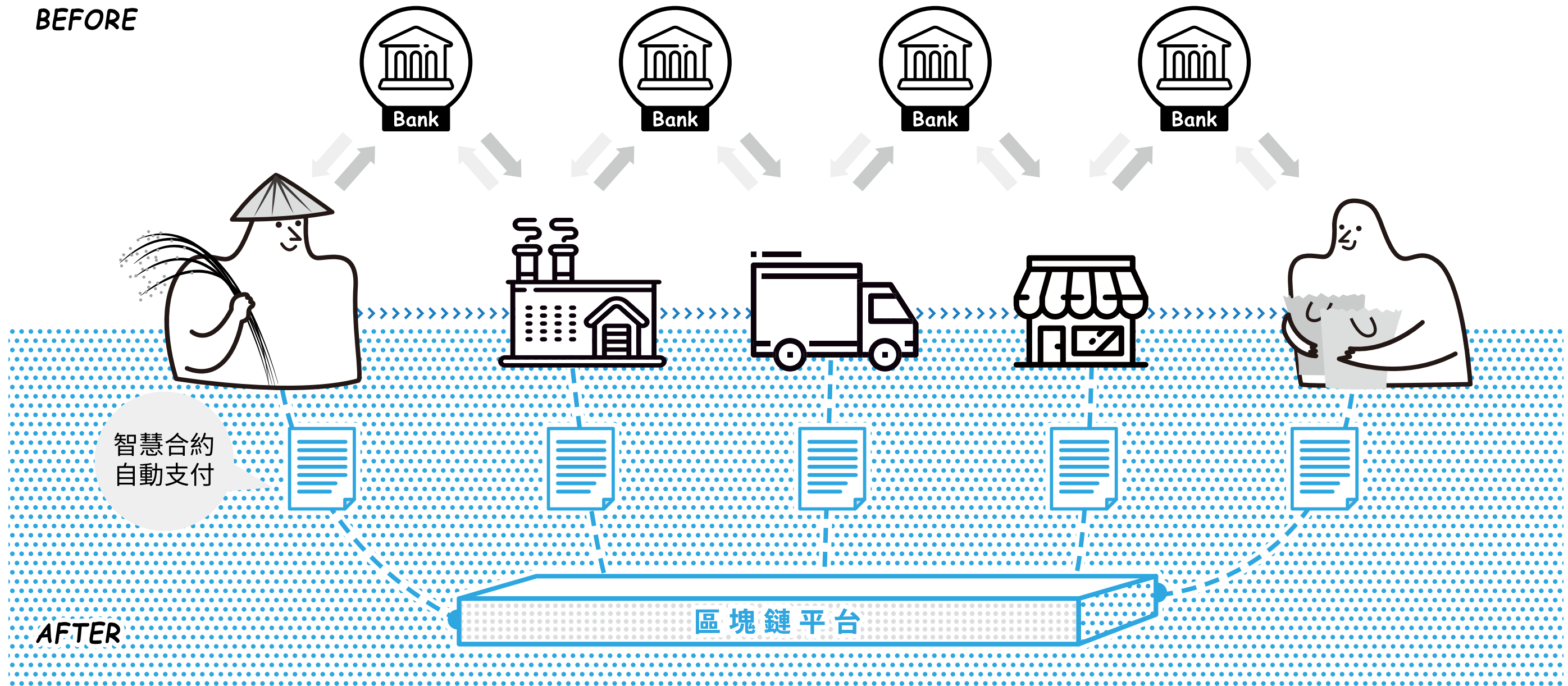
AFTER



跨境支付－縮短時間及隱性成本

1. 收款方，可快速收到款項，無須再等3-5天
2. 付款方，可以減少高額匯款手續費的支出

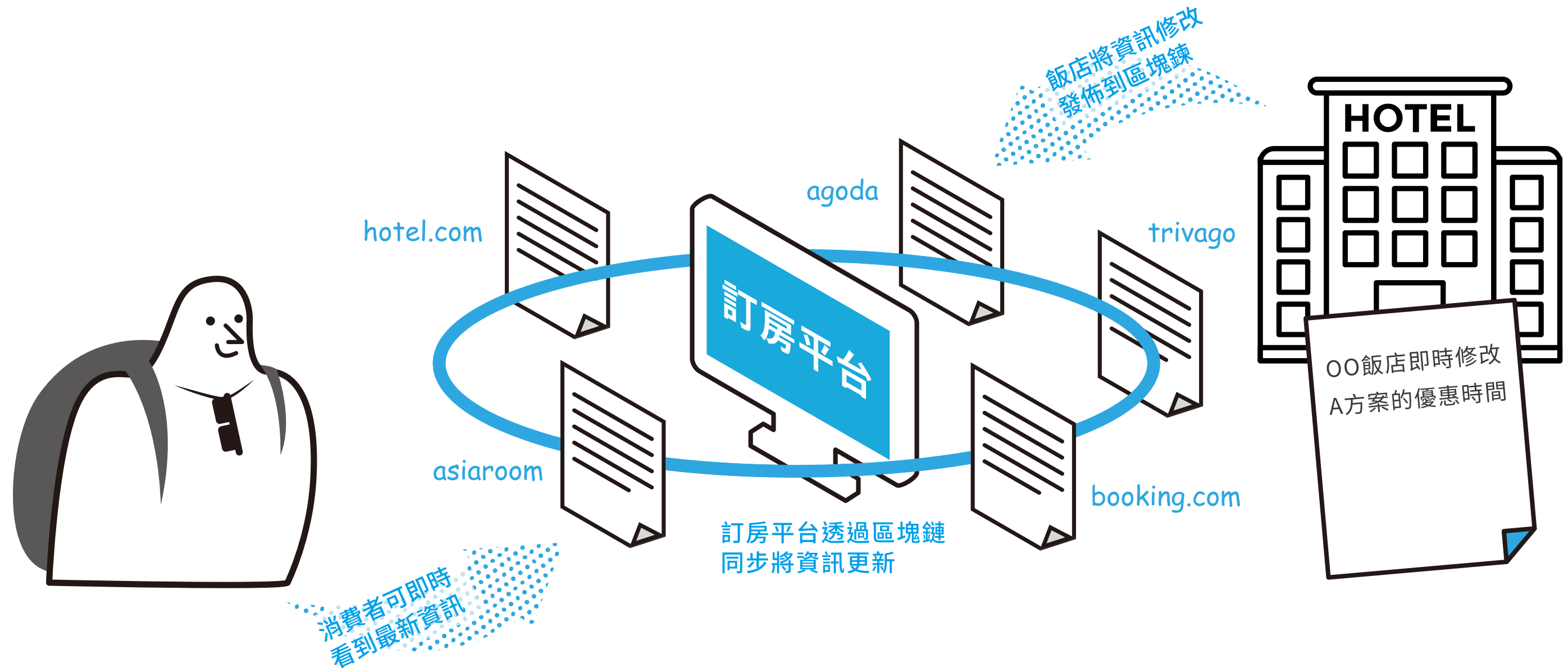
區塊鏈五大應用場景



供應鏈管理—流程簡化及交易透明

1. 簡化供應鏈交易繁複流程
2. 透過智慧合約，買賣交易條件透明，帳款可以準時支付。

區塊鏈五大應用場景



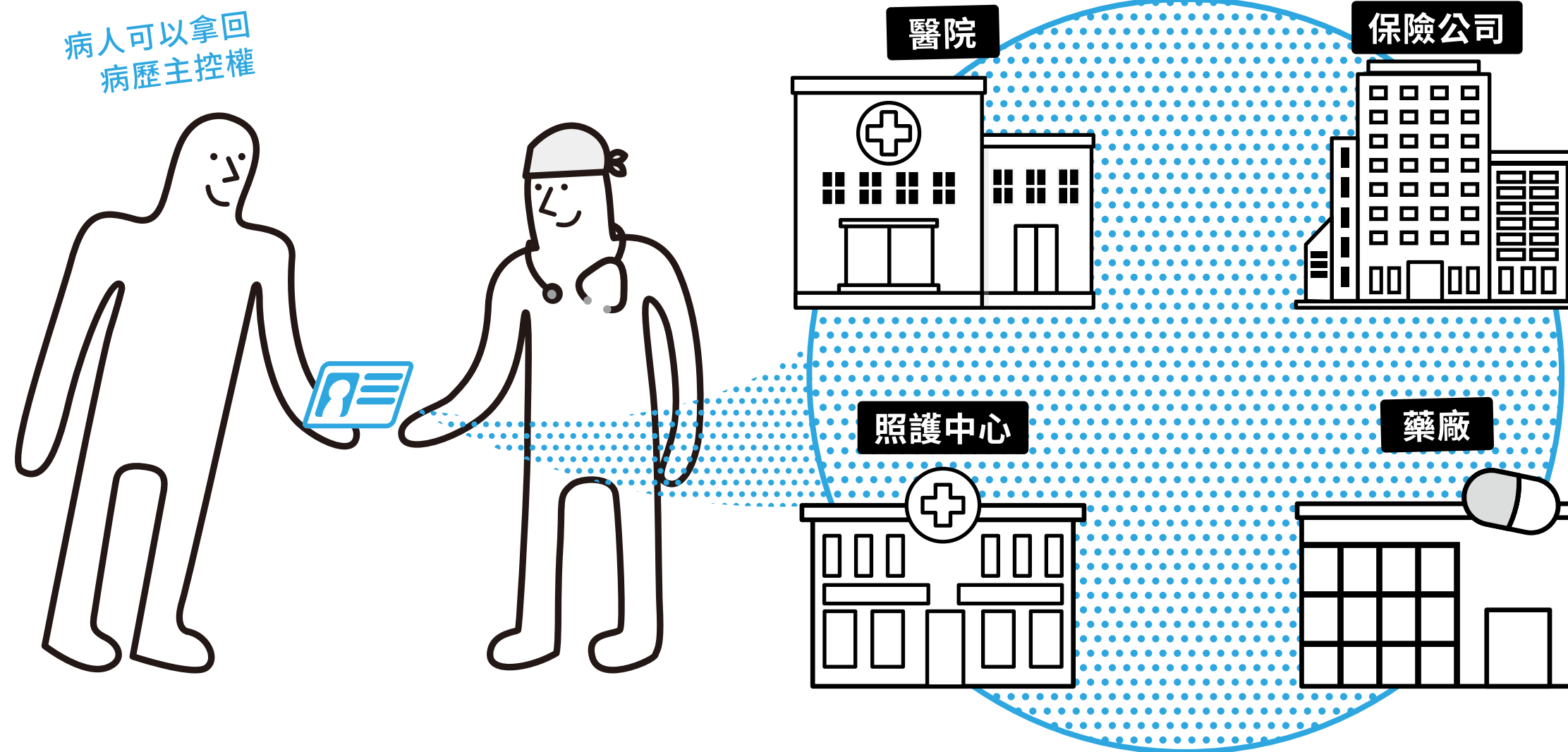
飯店業－資訊同步，減少資訊不對稱

1. 飯店業者：確保於所有訂房平台資訊準確即時。

優惠訊息可透過智慧合約，自動於所有訂房平台生效，減少人工管理成本。

2. 消費者：不會發生重複訂房窘況。

區塊鏈五大應用場景



醫療業—大幅提升病歷安全性，共同打造醫療系統生態圈

1. 打破醫療封閉體系，病人可以拿回病歷主控權，自行決定資料要分享給誰。
2. 結合智慧合約，病人申請保險僅需線上作業，即可自動給付保險費。
3. 醫院可與不同產業整合，包含保險業、照護機構、藥廠等，共同開發生態系統應用。