

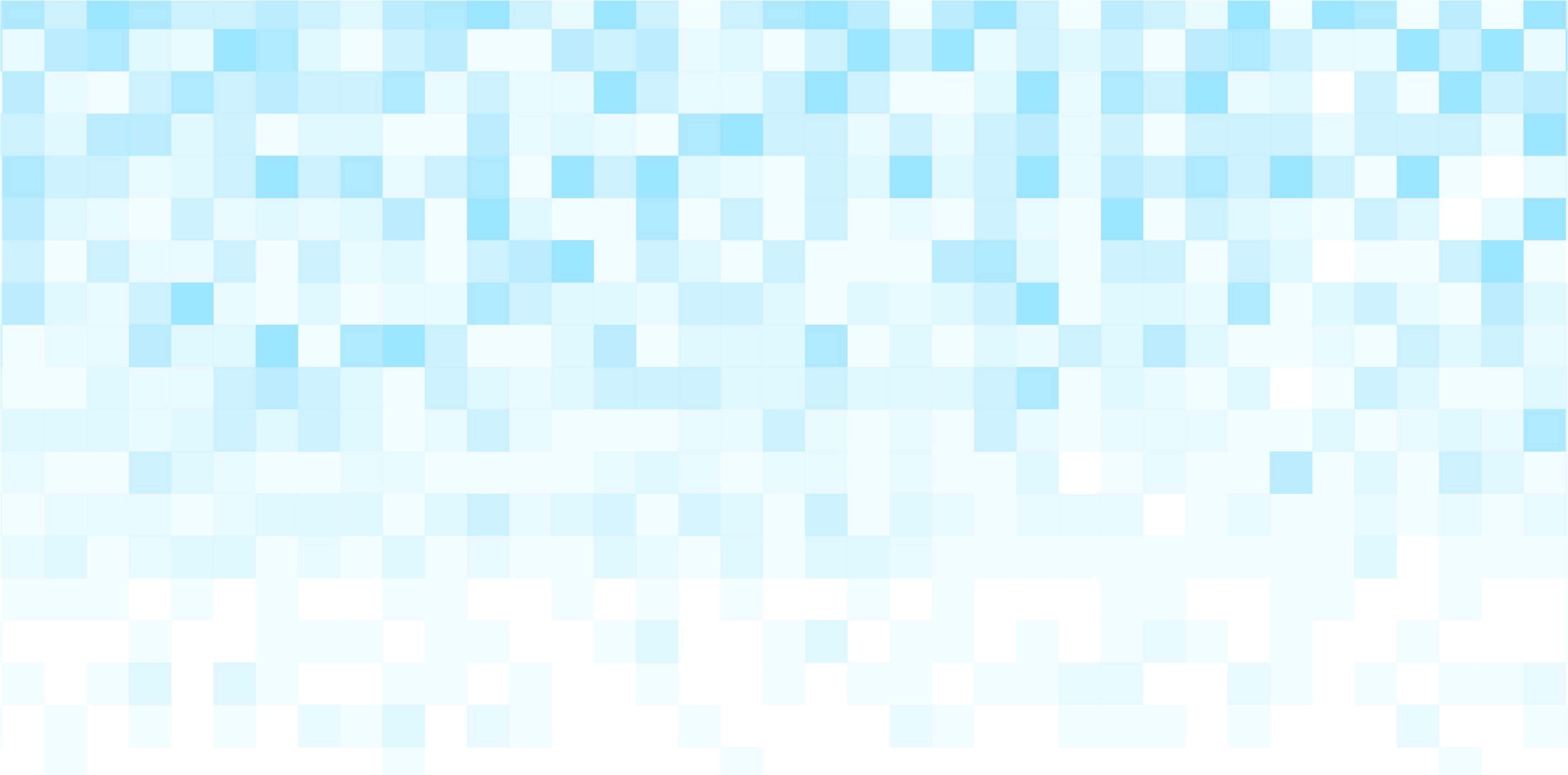
資訊素養與倫理 高中職 5 版

編撰：臺北市立建國高級中學 王鼎中 老師
臺北市立景美女子高級中學 孫晉忻 老師

虛擬世界任遨遊

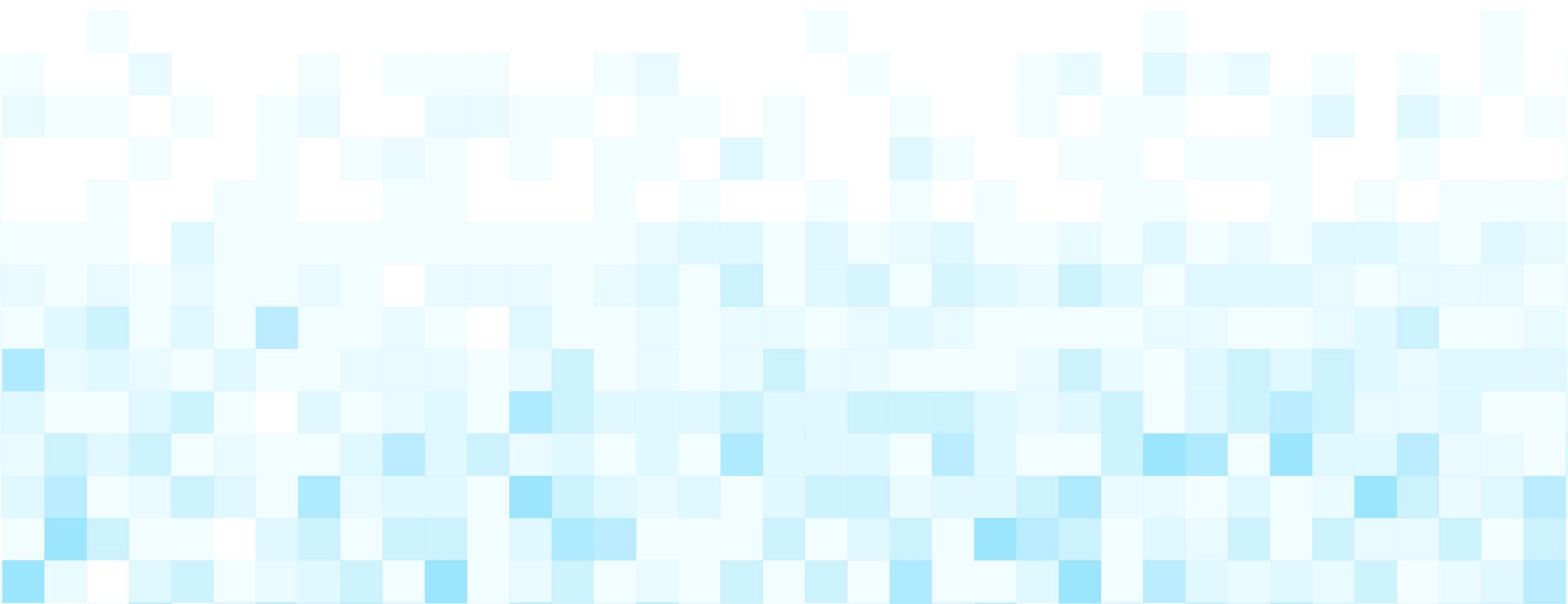
虛擬社會的運作與治理





虛擬世界任遨遊

虛擬社會的運作與治理



01 ▶ 一葉知秋 學思並進

1-1 學習目標

- 理解架構：認識構成虛擬世界的基本要素與運作邏輯。
- 信任型態：認識動態信任架構的概念並能應用在生活情境中。
- 去中心化：瞭解去中心化與區塊鏈的概念如何形塑虛擬世界的交易方式。
- 自治共好：學習自我保護與遵守規範的重要原則，成為虛擬世界的優質公民。

▶ 核心素養

- 科 S-U-A1 具備應用科技的知識與能力，有效規劃生涯發展。
科 V-U-A1 / 科 C-U-A1 具備應用科技的知識與能力，有效規劃個人生涯發展朝向自我精進。
- 科 S-U-A2 運用科技工具與策略進行系統思考與分析探索，並有效解決問題。
科 V-U-A2 / 科 C-U-A2 具備系統思考與分析探索的能力，並能整合科學、科技、工程、藝術與數學等方法及工具，有效處理與解決問題。
- 科 S-U-B1 合理地運用科技符號與運算思維，表達思想與經驗，有效地與他人溝通互動。
科 V-U-B1 / 科 C-U-B1 合理的運用科技符號與運算思維進行表達，並能有效進行思想與經驗的表達，與他人溝通並解決問題。
- 科 S-U-B2 理解科技與資訊的原理及發展趨勢，整合運用科技、資訊及媒體，並能分析思辨人與科技、社會、環境的關係。
科 V-U-B2 / 科 C-U-B2 理解科技與資訊的原理及發展趨勢，具備科技、資訊、媒體的整合運用能力，並能分析、思辨、批判人與科技、社會、環境之關係。
- 科 S-U-C1 / 科 V-U-C1 / 科 C-U-C1 具備科技與人文議題的思辨與反省能力，並能主動關注科技發展衍生之社會議題與倫理責任。
- 科 S-U-C2 妥善運用科技工具以組織工作團隊，進行溝通協調，合作完成科技專題製作。
科 V-U-C2 / 科 C-U-C2 妥善運用科技工具以組織工作團隊，並進行溝通協調，以進行合作共創。

▶ 學習表現

- 運 t-V-1 能了解資訊系統之運算原理。
- 運 p-V-1 能整合資訊科技進行有效的溝通表達。
- 運 a-V-3 能探索新興的資訊科技。
- 運 c-V-3 能整合適當的資訊科技與他人合作完成專題製作。
- 設 k-V-3 能分析、思辨與批判人與科技、社會、環境之間的關係。

▶ 學習內容

- 資 H-V-3 資訊科技對人與社會的影響與衝擊。
- 資 S-V-2 系統平台之未來發展趨勢。
- 資 T-V-1 數位合作共創的概念與工具使用。
- 生 N-V-2 工程、科技、科學與數學的統整與應用。
- 生 S-V-1 工程科技議題的探究。

►學習重點

- 學生能分辨「帳號」與「可驗證身分」差異，並能說明以DID與VC的關係與實際應用範例。
- 學生能理解虛擬世界的構成要素「身分、資料、資產、規則」，並能舉例說明各組成要素。
- 學生能分辨傳統網路驗證與零信任架構的差異。
- 學生能解釋「授權無上限」風險並完成一份個人撤權清單。
- 學生能理解去中心化的概念並說明去中心化的優點及限制。
- 學生能了解區塊鏈區塊結構與不可竄改的意義。
- 學生能說出 DeFi（去中心化金融）/ NFT（非同質化代幣）的合理用途與常見詐騙手法，並提出防範策略。

1-2 引言：阿俊的一天

阿俊是一個大學生，平日除了念書，也熱愛打球和搖滾樂。他是網路上「街頭籃球咖」社群的管理員之一，負責受理成員的申訴。同時他也參加幾個熱門音樂與搖滾樂的線上團體，認識各種搖滾流派並學習創作。阿俊最近開始將自己創作的音樂打包成NFT，放在平台上，期待遇見欣賞他音樂的收藏家。

7:50 捷運上 / 空投(Airdrop)

阿俊在捷運上收到兩個空投，其中一則寫著「專案上市，小額以太幣限時免費領取」。他認為這是接觸加密貨幣投資的好機會，就依指示輸入錢包的位址，並點擊授權讓網站「讀取與轉移特定代幣」。

8:40 課堂簽到 / 可驗證憑證

到教室後，阿俊拿出手機，使用學籍系統DID提供的「本班學生」驗證憑證簽到。點名系統只記錄了阿俊簽到的時間，不會額外蒐集其他資料。

10:05 上課中 / 區塊鏈健康護照

今天早上的3堂課是傳染病與防疫專題，老師講到接種疫苗的重要性。阿俊和同學們紛紛打開健康護照，上面用區塊鏈技術記錄了個人出生到現在已完成接種的各種疫苗項目，大家各自對照紀錄完成課程中的申論練習題。

12:00 午餐／加密貨幣

中午用餐時，阿俊收到上個月打工的薪水。店長選擇以穩定幣發薪，因為穩定幣幣值相對穩定，且轉帳迅速又免手續費。阿俊把一半的穩定幣換回新臺幣，用來支付日常生活花費，另一半保留在加密錢包。

14:00 購物 / 智慧合約

阿俊早就在線上二手市集看中一款編曲的效果器，他利用剛領到的薪水買下。市集平台使用智慧合約：先把阿俊付的款項鎖在合約中，賣家寄出、買家確認收貨後，系統會自動放款給賣家。整個過程僅授予「一次、限額、限時有效」的最小權限。

18:00 音樂會 / NFT票證

晚上阿俊參加他最愛的樂團新歌發表會。這次門票採NFT形式，避免門票偽造與遺失的風險，而且獨一無二的門票圖卡還可以收藏。年底樂團的線上演唱會也可憑同一張NFT入場，十分划算。

21:00 線上會議 / 社群自治

回家後阿俊很疲倦了，但他必須參加「街頭籃球咖」的定期自治會議。本次會議室僅接受「管理員」憑證進入。主要內容是討論社群成員糾紛：成員A因為不滿成員B反對自己的發言，刻意搜索並洩漏成員B的真實姓名、所在國家與相關隱私。成員B收集相關證據後向社群管理員提出舉報，管理群討論後達成共識，解除成員A的社群資格，以後成員A不能再優先使用與社群簽約的籃球場，他原本持有的社群代幣也失效。這些解除資格的動作將由智慧合約自動執行。

23:30 深夜 / 授權風險與補救

上床睡覺前，阿俊收到2則通知：一則是有人下標了阿俊的NFT音樂作品，讓他十分開心；但另一則卻顯示早上的空投其實是釣魚詐騙。由於他授予了「不限額度」的代幣轉出權限，錢包餘額已被掏空。吃驚的阿俊立刻開啟「授權管理」撤銷所有不必要授權，並且將交易證據留存下來，準備明天早上向加密貨幣平台舉報，並且到警察局備案。

阿俊的一天，敘述了與以往不同的生活模式，也包含很多陌生的名詞，例如DID、NFT、穩定幣…等。看不懂也不用擔心，請繼續往後面閱讀，接下來我們將為你介紹許多新觀念，在第6頁也有完整的名詞解釋，邀請你和我們一起探索虛擬世界的組成。



02 ▶ 兩全其美 觸類旁通

2-1 主題探索

2-1-1 進入虛擬世界

阿俊的一天就是未來真實世界與虛擬世界雙重運作的縮影：搭捷運、上課、打工、參加演唱會等都是真實的生活，而參與社群組織、網路交易、投資加密貨幣是在虛擬世界發生的，在那裡我們甚至可以擁有不同的人生。但如同真實世界的運作，要在虛擬世界通行一樣需要證明身分、遵守規則、尊重他人。而各種危機例如詐騙、隱私外洩、受人身攻擊等，也會在虛擬世界發生。

一、虛擬世界運作的四個要素

（一）你是誰：身分

在虛擬世界通行，確認合法身分是最重要的事，與可信任的人交流比較能降低風險。以往談到網路的世界，大家直覺會想到「身分」就是自己的帳號密碼。然而隨著虛擬世界快速擴張並趨於複雜，身分認證不能只靠密碼，而是更完整的驗證系統。未來發展的趨勢是由去中心化識別（Decentralized Identifier，簡稱DID）提供憑證來證明我們的身分。例如由學校DID提供阿俊個人在校證明，可以讓課程點名系統記錄並完成阿俊上課簽到的動作。

（二）你揭露什麼：資料

隨著使用時間越久，我們在網路上儲存的資料與留下的紀錄也越多。如果沒有適當的保護，我們在虛擬世界的一切足跡可能都公開在大家面前。真實世界中都有個人資料保護法來保護大眾的隱私，而在虛擬世界中保護個資的原則是「最小揭露」與「最小授權」。例如：健康護照DID可以只證明阿俊是否已接種疫苗，而不會透露阿俊的完整病史；加密貨幣平台應該只能獲得轉入貨幣的帳戶授權，不應該有匯出或轉帳的授權。

（三）你擁有什麼：資產

虛擬世界交流充滿各種機會，「虛擬經濟」興起讓人們不再被限制只能在真實世界賺錢。例如：非同質化代幣讓使用者買賣非實體化物品的權利，例如票券、音樂作品。而使用智慧合約進行第三方託管，收貨後自動放款，也可以增加買賣的透明度與保障。



（四）如何安全運行：規則與信任

僅有資料與技術還不夠，虛擬世界的參與者必須遵循某些規則，才能做到公平與安全。這些規則包含了身分驗證的流程、資產使用的權限控制、資料交換的安全標準，甚至交易與合約的自動化規範。例如「零信任架構」要求每一次操作都需經過驗證，以降低入侵風險；「最小揭露原則」提醒我們只提供必要的資訊，以保護隱私；「去中心化概念」避免集中化管理的壟斷，提供使用者更多自主的權利。這些設計增加了虛擬世界的安全與穩定性。

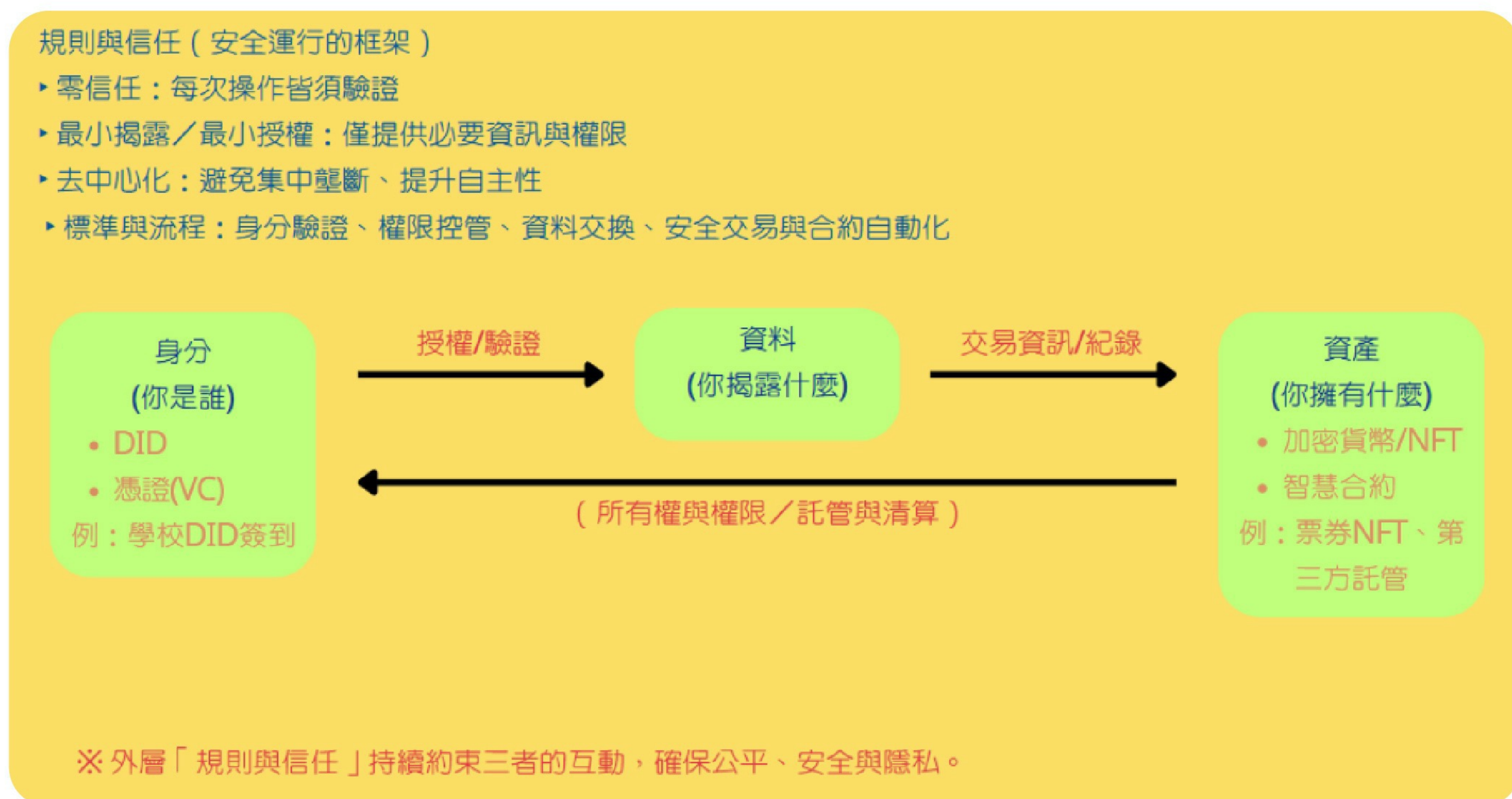
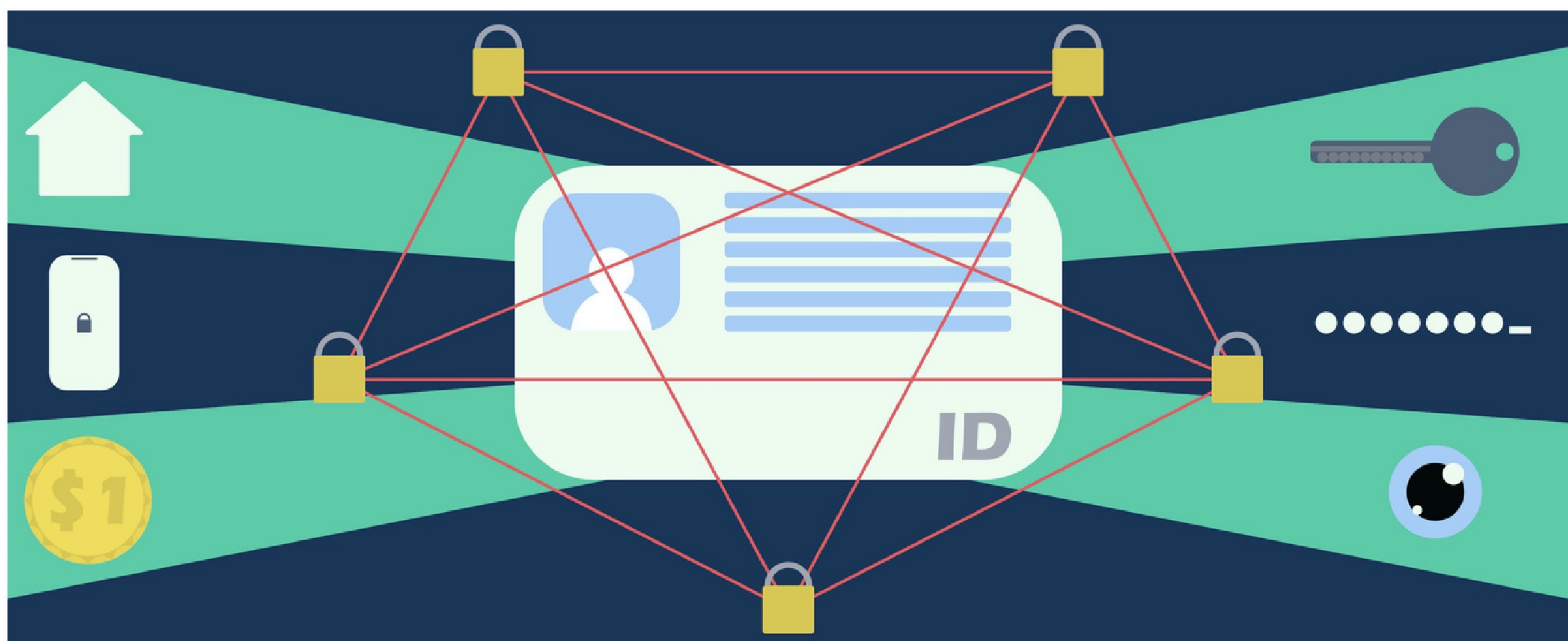


圖1 虛擬世界的基本要素與對應關係

圖 1 顯示了以上這些基本要素及其對應關係，具備了以上這些基本要素，人們在虛擬世界彼此交流、結成組織，開始共同管理與自治，這樣的世界可以跨越性別、年齡、種族與國界，未來虛擬世界仍有超乎想像的發展空間。



二、認識「阿俊的一天」中的專有名詞

前面我們提到了一些專有名詞，這些名詞是由不同領域的科學家累積發展的技術，從而構成現在虛擬世界運作的根基，我們先簡單說明它的定義，在後面的各單元會為大家一一詳細解釋。

- **加密貨幣 (cryptocurrency, 簡稱crypto) :**
是一種使用虛擬交易媒介，沒有實體貨幣，只能透過密碼學的方式證明所有權與進行交易。
- **NFT (非同質化代幣, Non-Fungible Token) :**
是不可分割、不可互換的代幣，虛擬世界中票券、收藏品、藝術創作常使用NFT形式做交易或保存。
- **加密貨幣錢包 (Cryptocurrency Wallet) :**
不是指真的錢包或帳戶，而是一種數位工具，用於儲存和管理加密貨幣的私鑰和公鑰。
- **空投 (Airdrop) :**
平台免費發放代幣或其他數位資產，以吸引使用者注意的行銷方法。
- **DID (去中心化識別, Decentralized Identifier) :**
用去中心化方式記錄的身分資料，不靠單一平台管理就能進行驗證。
- **可驗證憑證 (Verifiable Credentials, 簡稱VC) :**
由DID發出的證明資料，提供其他系統進行驗證。
- **區塊鏈 (Blockchain) :**
從去中心化具體發展出來的技術，是加密貨幣、NFT底層運作基礎。



- **穩定幣 (Stablecoin) :**
依據法定貨幣價格設計的加密代幣，和投資型加密貨幣比較起來幣值相對穩定。
- **智慧合約 (Smart Contracts) :**
以區塊鏈為技術基礎發展的自動交易程式。
- **最小授權 (Least Privilege) :**
應用系統只開放給外界足以完成任務、最小的操作權。
- **去中心化社群自治 (Decentralized Autonomous Organization, 簡稱DAO) :**
利用區塊鏈與智慧合約的自治組織，無中央領導的組織形式。
- **釣魚詐騙 :**
一種網路犯罪手法，透過網路溝通管道，誘騙受害者點擊惡意連結或提供個人敏感資訊。
- **授權管理 :**
由個人決定對外開放帳戶的存取權限，應該定期檢查與撤銷不必要的授權以維護帳戶安全。

2-1-2 虛擬世界的信任機制

在真實世界中，我們透過見面互動、檢查資料、法律授權等人為方式來確認身分。網際網路興起後，資訊防護技術則是採用帳號密碼與信任邊界（Trust boundary）來確認使用者身分與權限。帳號密碼像一組固定的門鎖與鑰匙，而信任邊界像一道圍牆：牆內的人與裝置是受信任、安全的，範圍外則不受信任。舉兩個實際的例子：學校設有門禁機制，能通過警衛檢查並進入學校的人就是可信任的師生，可以進出校內的辦公室與教室；或者像臺北市政府教育局的線上資料庫知識管理平臺，透過帳號密碼或校內IP登入的就是可信任的使用者，能查閱各種資料庫的內容。

然而現在網路環境變得更複雜，虛實交錯的各種情境下，不僅帳號密碼的安全性不足，可信任的邊界也更難定義。例如突破門禁進入校園的陌生人，可能竊取校內資料或騷擾師生；因為生病或參加教育旅行不在學校的同學，卻是可信任的使用者，要有權限進入課程或參與校內活動等等。在虛擬世界亦是如此，所以網路的信任機制也有新的發展。

一、「零信任」的概念

零信任架構（Zero Trust Architecture, 簡稱ZTA）的概念是：不管是誰、不管在哪裡，預設不信任任何使用者與裝置。在零信任架構下，存取資料或服務一定要驗證身分，通過驗證後也只能獲得最小授權，使用者登入後的動態也會持續被監控。

這個概念應用在真實世界中，像一位非常多疑的警衛，而且要求很嚴格，非常麻煩。然而在虛擬世界，我們不應該追求便利，安全與信任才是首要原則。透過嚴格驗證確認身分的合法性之後，我們才能安心做更多交流，因此零信任架構是目前組織與企業推動的資訊安全方向。國家資通安全研究院也在113年推出「機關導入零信任參考指引」，提升國家資安防護能力。透過表1，更能了解傳統的驗證與零信任架構的差異。

表1 傳統驗證與零信任架構的差異

面 向	傳統驗證	零信任架構
基本概念	預設「通過一次驗證進入內部者，都是安全的」。	預設不信任任何使用者與設備，每次都必須重新驗證。
信任假設	內部皆可信，攻擊者通常來自外部。	外部與內部皆可能有風險。
驗證方式	帳號密碼為主，或搭配雙重驗證。	使用多因子驗證（MFA）、行為分析、生物特徵辨識、動態驗證。
授權原則	只要進入系統，通常可存取所有資源。	每次只授權完成任務所需的最少權限。
保護目標	重視於入口與邊界的安全防護。	重視資料與服務的防護，持續監控使用者存取動態。

二、動態信任相關機制

在零信任架構下，若想登入系統、存取資訊、參與活動，都必須完成最重要的身分驗證。現在與未來的身分驗證不再只是單一帳號密碼，將會是多因子鑑別（Multi-Factor Authentication，簡稱MFA）。多因子鑑別就是同時要通過2種以上認證方向，包括密碼、指紋或臉部生物特徵、動態簡訊驗證碼、數位簽章、智慧卡片、信任平台憑證等。

在網路上活動，我們會使用很多系統，例如一面播放音樂一面在線上與其他人對話，再連到購物網站等。如果每一個系統都需要進行多因子鑑別來登入，會有大量繁瑣的申請與查驗工作。為了改善這個問題，現在已經發展出我們熟悉的單一帳號登入（Single Sign-on，簡稱SSO）服務：只需要在一個入口建立身分並通過驗證，就可以用這個身分登入其他不同的系統。例如現在想申請一些網站的會員，除了直接提供個人資料外，也可以選擇使用Google帳號或某些大型社交平台帳號登入。這樣做的優點是方便而且簡化重複申請的工作，缺點是集中管理問題：驗證身分的入口將擁有管理權與大量使用者的資料。如果入口平台突然撤銷某人的許可、不合理的加收費用，或是濫用個人隱私資料，受害的是我們一般使用者。

為了避免集中管理可能發生問題，目前發展出不同的架構，就是「去中心化識別DID」。它是一個Web標準制定組織W3C所提出來的數位身分識別的標準。你可以想像DID是一個記錄著個人完整資料的檔案，可以提供給不同平台做身分驗證。它聽起來有點像一組SSO的帳號，但最大的差別是DID不在網路服務商的手上，而是我們自己擁有，而且我們自己可以決定要提供哪些資料進行驗證。舉個例子，在真實世界中去便利商店買一瓶可樂，我們只需要出示會員編號來累積消費點數，但不需要向店員出示身分證字號。在虛擬世界也是，我們只需要選擇DID中最少的資訊，足夠讓系統認證身分即可，其他內容不會被公開。這也是零信任架構下資訊安全的另一個原則「最小揭露（Least Disclosure）」。

面對不同的系統詢問，DID發出最小的對應證明資料，這個證明資料稱為可驗證憑證（Verifiable Credentials，簡稱VCs）。例如我們想買的筆記型電腦有學生優惠價，就可以向學校DID系統申請在學憑證，以驗證我們的學生身分；如果想向某個組織申請獎學金，則是向學校DID系統申請成績憑證，以顯示我們的在校分數是符合獎學金要求。這樣可以避免向外部平台揭露個人全部資料，可以同時達到認證與保護隱私的目標，有關DID與憑證證明的關係請參考圖2。

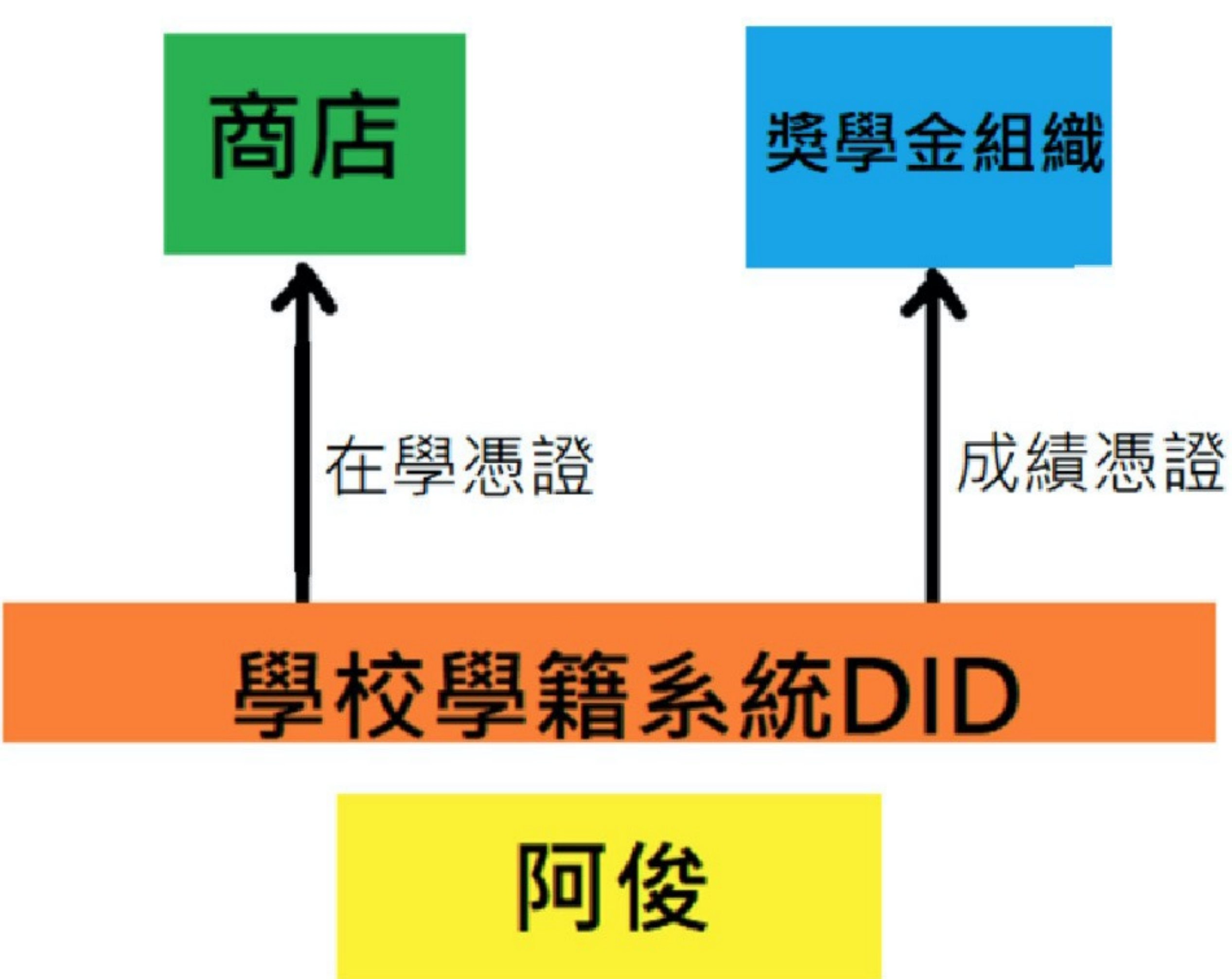


圖2 使用者、DID與憑證的關係

除了最小揭露，還有一個類似的概念是「最小授權」。有時候我們必須允許某些服務存取我們的資料，例如社群軟體要能存取我們的相簿才能上傳照片，或是行動支付軟體要能存取我們的銀行帳戶，才能用手機進行電子支付。如果一不小心開放過多的權限，不法份子就有可能利用漏洞竊取我們的資料或資產。因此「注意授權」和「定期撤權」是保護自己的好習慣，要清楚開放的對象、內容、時間、上限，並且固定時間檢查授權清單。

圖3呈現動態信任架構，它不是單一工具，而是將零信任架構、DID、可驗證憑證、最小權限、最小揭露等拼成一套可自主調整的系統。它讓阿俊在虛擬世界裡安全、快速、合規地完成一天的學習、工作與娛樂。

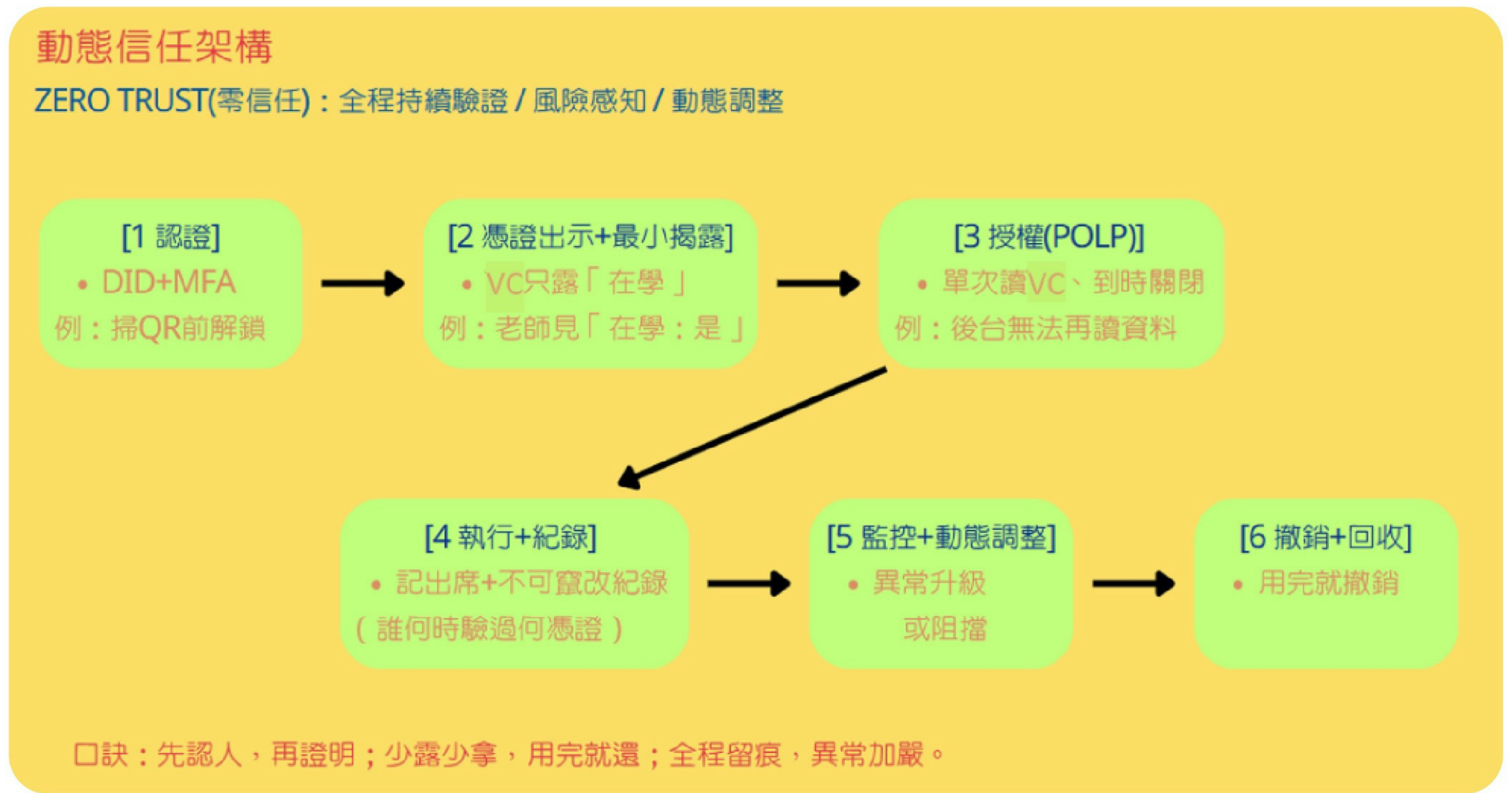
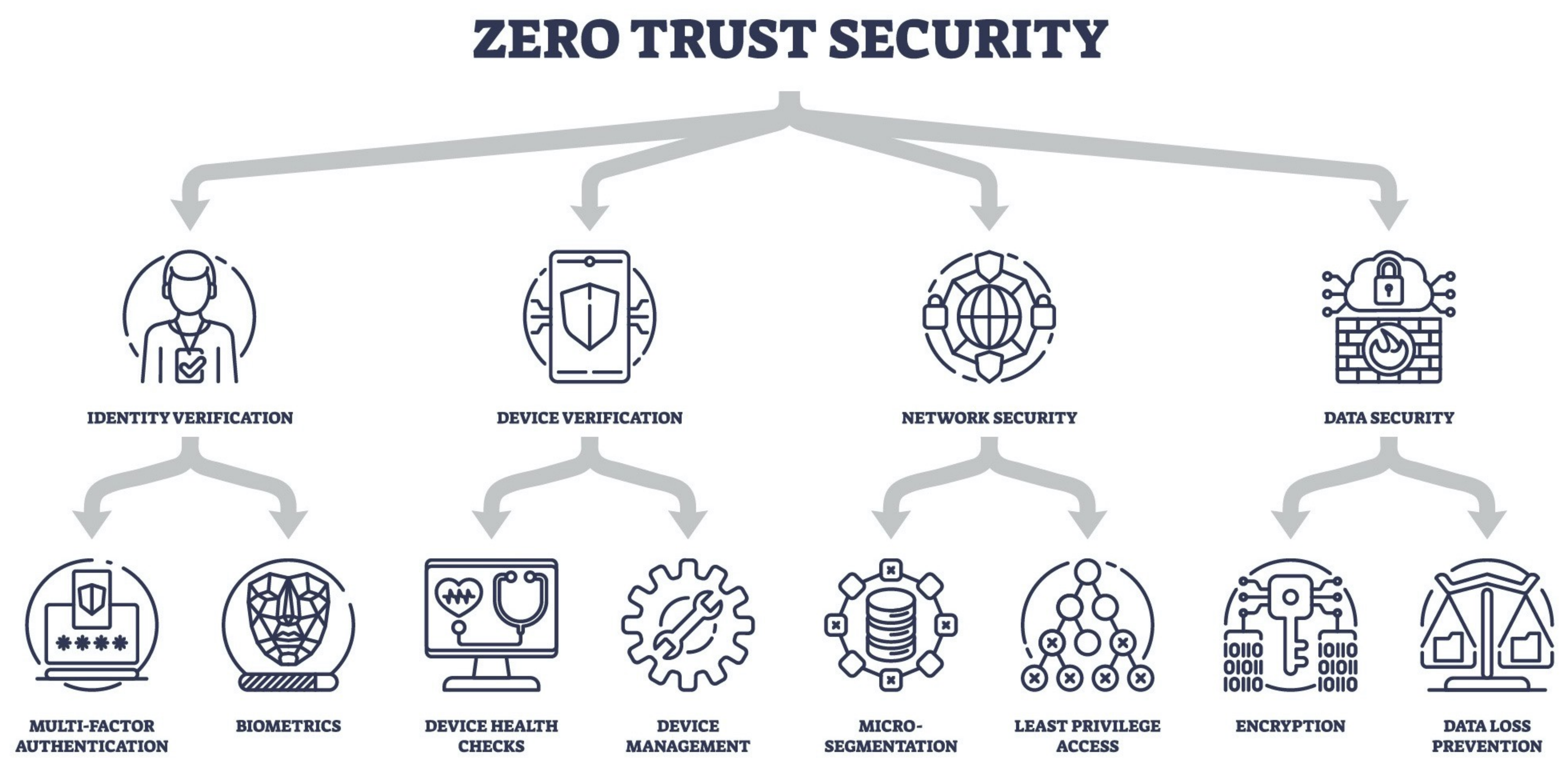


圖3 動態信任架構



● 從阿俊的一天看動態信任的實際應用

◆ 課堂簽到

- 流程：登入學籍系統→學籍DID確認身份→發出合格憑證→報到系統檢驗憑證→完成簽到。
- 重點：1. 阿俊不需要重複在學籍系統與報到系統註冊帳號。
2. 學籍DID只提供「認證此人是本班學生」資料，不揭露其他訊息。
3. 此憑證可控制1分鐘內有效，避免濫用。
- 素養提醒：學籍系統發出的憑證不要隨意在別處使用。

◆ 線上會議

- 流程：使用DID登入社群→社群確認為阿俊為管理者→發出合格憑證→允許進入線上會議室。
- 重點：1. 進入線上會議的權限不需要人為審核，憑證可自動檢核參與成員。
2. 成員可以透過憑證獲得投票權，並限定投票的次數與使用時間。
- 素養提醒：線上會議時，背景與聲音會透露你所在的實際地點

◆ 空投詐騙與授權管理

- 流程：阿俊接到空投→依指示開啟帳戶授權→帳戶中的加密貨幣全部被轉出→阿俊晚上發現後立即撤銷授權。
- 重點：1. 阿俊認為開啟的授權只是提供個人姓名與錢包位址，讓平台可以轉入免費代幣，沒有仔細確認所有權限清單。
2. 零信任架構中「最小授權」的目標就是要防止類似惡意入侵。
- 素養提醒：養成每天「檢查權限」的數位好習慣，保護自己的權益。



2-1-3 去中心化的虛擬世界

經過信任驗證登入虛擬世界後，我們也會像身處真實世界一樣，與其他人們進行交流互動。在虛擬世界我們交流的對象跨越國籍、年齡、性別，如何進行金融相關的交易？彼此的權益又該如何保障呢？

一、去中心化的概念

在真實世界中，我們的權益受損時，可以依據政府法律或規定進行追討或要求賠償。但是在虛擬世界我們可能連對方真實姓名、住在哪一個國家都不知道，此時想透過傳統的中央機構保障自己的權益，難度會變得更高。「去中心化」架構就為虛擬世界中的交易提供了不同的運作模式。

去中心化的概念是：廢除或降低集中管理機構的權力，取而代之的是讓每一位參與者共同管理資源。上面我們提過「零信任概念」、「去中心化識別」也是一樣的原則，努力降低依賴單一機構的狀況，讓使用者有更多自主權。

我們用真實例子來說明這個概念（參見圖4）：真實世界中，銀行是大家信任的機構，所以每個人的金融交易都是透過銀行進行，例如昱昱用ATM轉帳1,000元給阿泰，這筆交易能不能成功執行、記錄在哪裡、收取多少手續費，都是由銀行決定，這是中心化結構。「去中心化」則是沒有銀行存在，但是每位參與者都擁有管理的權力。今天昱昱使用去中心化架構下轉帳1,000元給阿泰，這筆交易會同時由昱昱、阿泰、小其、比比、阿俊，小珍…等參與者一起同意與記錄，因此每個人不需要依賴中央單位，也不必受其控制，想進行交易或查詢紀錄有更高的自主權。

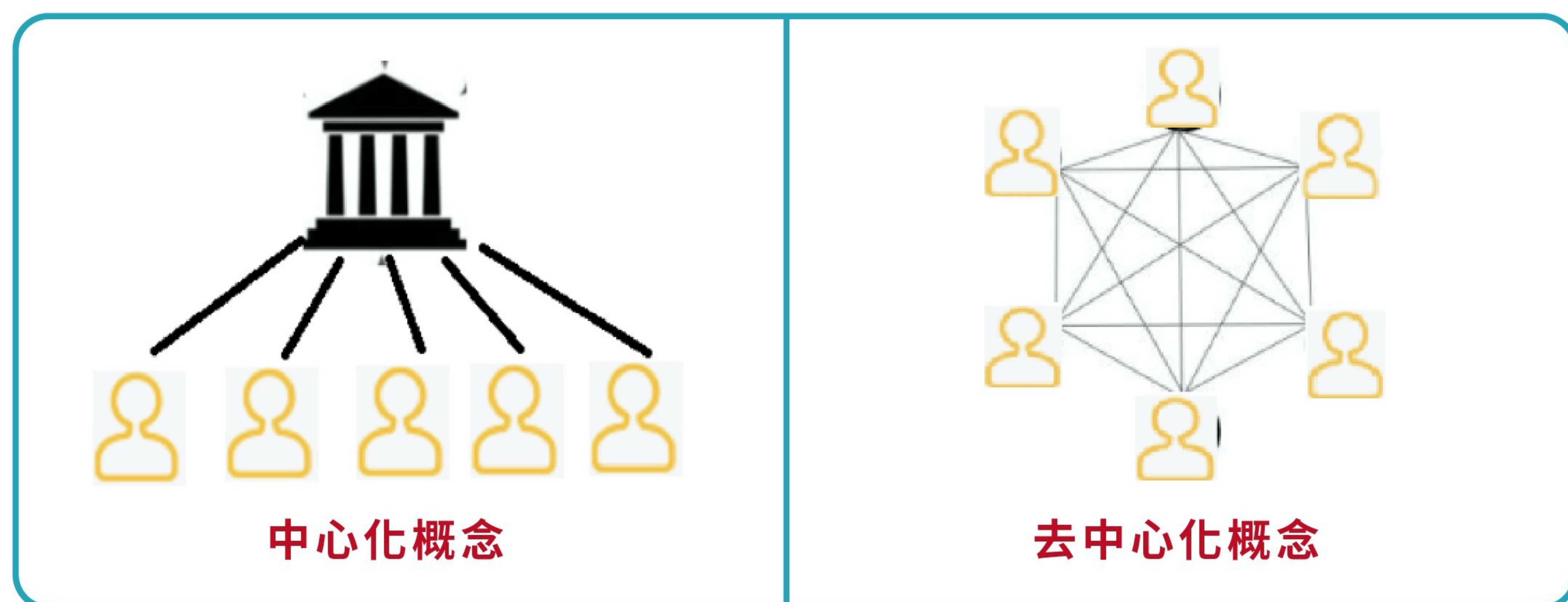


圖4 中心化與去中心化概念不同的架構

為什麼要設計去中心化的機制呢？主要是避免權力集中可能造成的腐敗，以及減少中心系統崩潰時引發的危機：當中央權力擴大，大眾相對就被削弱了個別的權利與自由度；如果集中管理單位發生貪污、惡意倒閉或資料損毀等危機，受影響的也是一般大眾。因此降低中央管理單位的權力，透過系統化的方式讓眾多使用者共同管理資源，可以避免上述的缺點，也能增加公平性、透明度、安全性與韌性。

二、去中心化的設計原理

那麼去中心化是怎麼運作的呢？我們用一個簡單的故事來說明（如圖5）：4個好朋友共同出錢買了一套哈利波特全集，他們會彼此交換閱讀。為了管理這套書，每個人都有一本筆記本，記錄這套小說每一本在誰的手上。

某天比比從小其那裡拿第2集來看，此時4個人會各自在筆記本寫下這個移動紀錄，並且彼此確認筆記內容是一致的。假設一個月後阿俊想看第2集，他不用一個一個詢問朋友，只要去查筆記本就知道應該跟比比拿書。

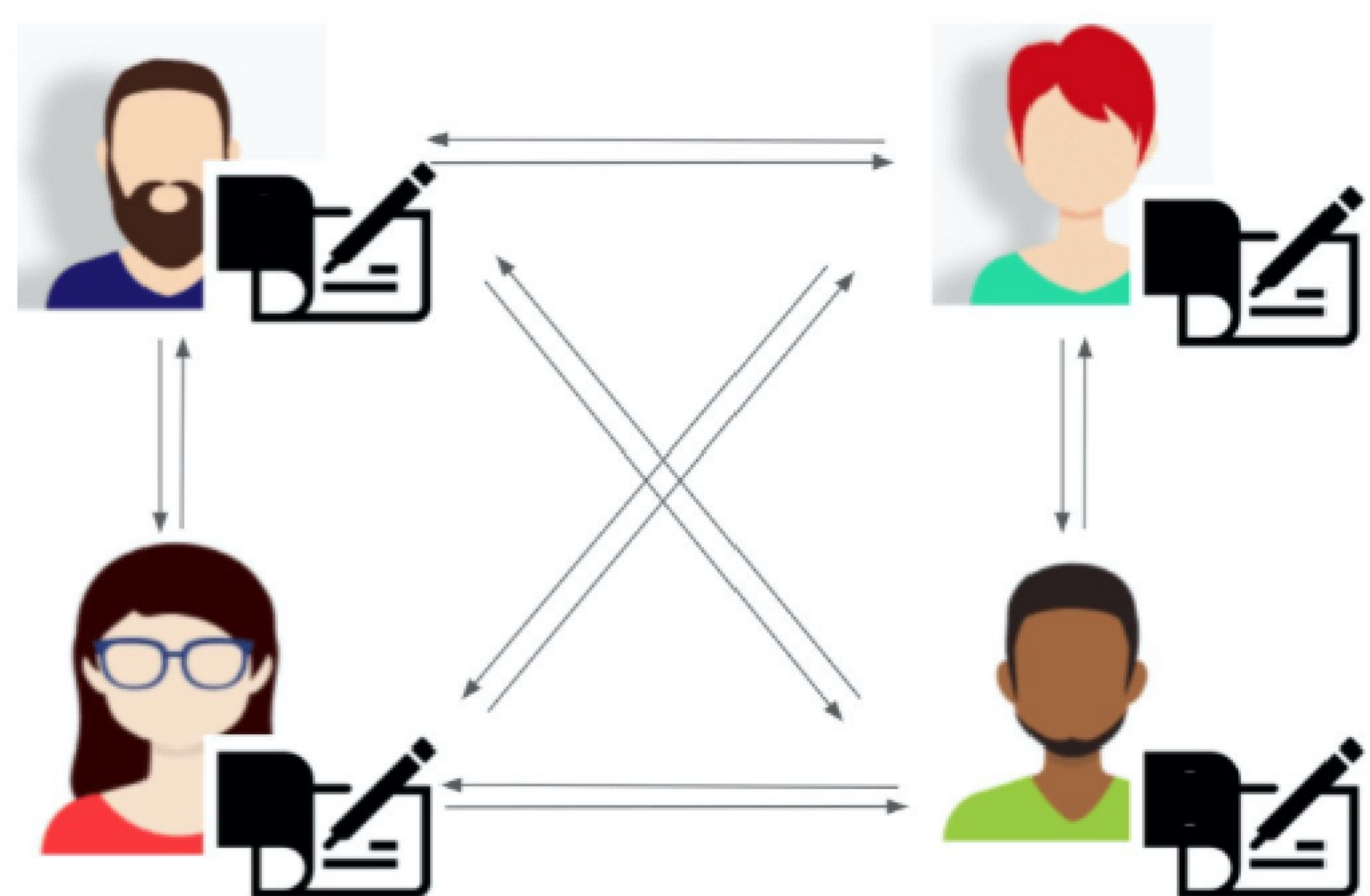


圖5 去中心化架構下，每個人有自己的交易紀錄

某天比比從小其那裡拿第2集來看，此時4個人會各自在筆記本寫下這個移動紀錄，並且彼此確認筆記內容是一致的。假設一個月後阿俊想看第2集，他不用一個一個詢問朋友，只要去查筆記本就知道應該跟比比拿書。

今天阿俊拿到了第2集，大家同時更新筆記本上的紀錄。此時小珍發現只有自己的筆記和其他人不一樣：大家都記錄第3集在小珍手上，但小珍的筆記上沒有這項紀錄，而且她身邊也沒有第3集。大家努力追查後，發現原來是小珍的弟弟意外把第3集弄丟了，情急之下偷偷修改姐姐的筆記想掩蓋事實。但由於其他人都有相同的紀錄，因此大家很快就發現問題在哪裡，並且想辦法解決問題。發生此事後，大家決定以後一律用密語寫紀錄，避免再被外人竄改筆記內容。

上面這個故事列出了去中心化設計的重點：

- 分散式帳本技術（Distributed ledger Technology）

不依賴中心單位管理，分散式帳本技術讓將資料庫分散於平等的參與者身上，每一個參與者都有各自的交易紀錄。如同上述例子中每個人都有一本內容相同的筆記一樣。

- 共識機制（Consensus Mechanism）

當一筆新的交易出現，因為沒有中心單位負責審核紀錄，因此採用「大家同意」的方式做出最新最正確的紀錄版本，這就是共識機制。一旦達成共識，所有參與者都會更新成相同的複本。在上面買書的故事中，大家每次交換書籍時都會檢查筆記內容是否相同，就是類似共識機制。

- 不可更改（Immutable）

因為帳本分散在多處，帳本內容被竄改的機會也增加，就像上面的故事中，小珍的筆記就被弟弟偷偷修改了。要保護每個帳本的安全性，去中心化系統必須加入更多數學運算，例如難以還原的函數、加密方法，或是只加不改（Append-only）的設計，以保障資料的不可更改性。

透過適當的設計，我們就有機會實現平等而不需要依賴中央管轄的運作模式。但是去中心化只有好處嗎？下一節我們討論它的優勢與問題。

三、去中心化的優點與限制

去中心化機制十分符合虛擬世界的交易需求。在網路上若要跨國進行金錢或物品交易。如果採用中心化實體金融，可能曠日廢時並受到許多限制。舉個例子：住在紐西蘭的小珍創作網路動畫，阿國是他的粉絲。某天阿國請小珍製作一支動畫，雙方也談好價格，但是小珍發現阿國住在越南。如果採用傳統金融交易，從越南匯款到紐西蘭必須雙方都要有銀行帳戶，還要申請國際匯款並且支付高額手續費，再花費幾個工作日才能完成（參見圖6）。



圖6 傳統國際轉帳流程

但如果他們採用去中心化的方式轉帳（如圖7），只要參與管理帳本的使用者共同承認這筆交易，那麼轉帳立即成立，省了手續費，交易也會被記錄下來。

- 整體來說，去中心化的優點包括：
- （一）自主性：資料或交易不需要透過中央單位管理與審核，自主空間更大，使用者彼此直接交易的效率也較好。
 - （二）透明度：交易內容由參與者共同記錄，而且可以事後查證與追蹤過程，不必擔心黑箱或做假的狀況發生。
 - （三）安全性：資料不是集中儲存而是分散在參與者手上，並且有加密機制，能抵抗攻擊也可降低單點故障風險，具備較高的復原能力，更具有安全性與韌性。



圖7 去中心化的轉帳流程



去中心化的設計理念很理想，但是「公平自主」與「簡單方便」難以兼顧，去中心化也有一些限制，例如：

- （一）沒有中央單位審核使用者與交易內容，因此風險要由使用者自己承擔。例如操作過程發生錯誤，交易內容有爭議等，很有可能無法反悔取消。
- （二）去中心化系統要顧及共識機制與資料安全等，操作上比較複雜，使用的門檻較高，不易普及。
- （三）分散式帳本的做法需要複製多筆資料，每次交易時還要進行共識檢查與加密演算，因此系統非常耗費能量，當資料量變大時，交易的效率也會降低。

去中心化是一個創新的概念，雖然有其限制，但可以嘗試修改架構或設備來改善。區塊鏈（Blockchain）就是從去中心化具體發展出來技術。因為區塊鏈的誕生，我們現在有加密貨幣、數位履歷等具體的應用。下一節一起認識區塊鏈技術。

四、認識區塊鏈技術

區塊鏈（Blockchain）顧名思義，是由一個個區塊（Block）組成，並且像鏈條（Chain）一樣彼此相連，形成完整的資料系統（參見圖8）。

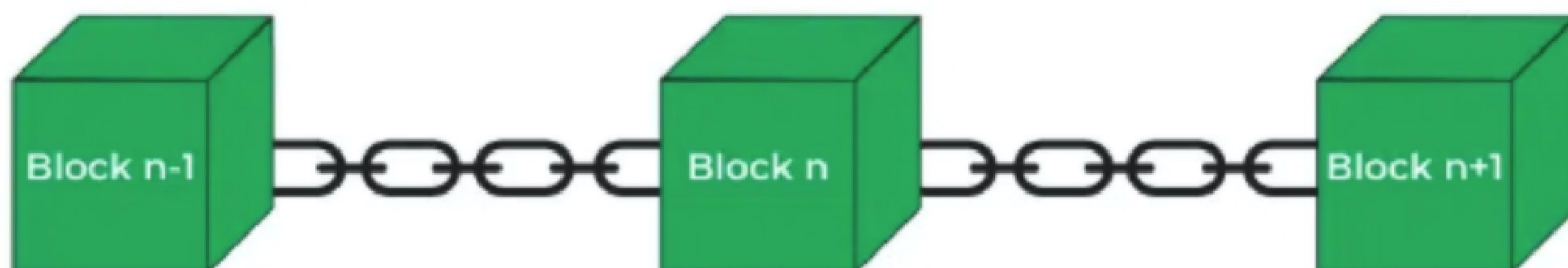


圖8 區塊鏈架構

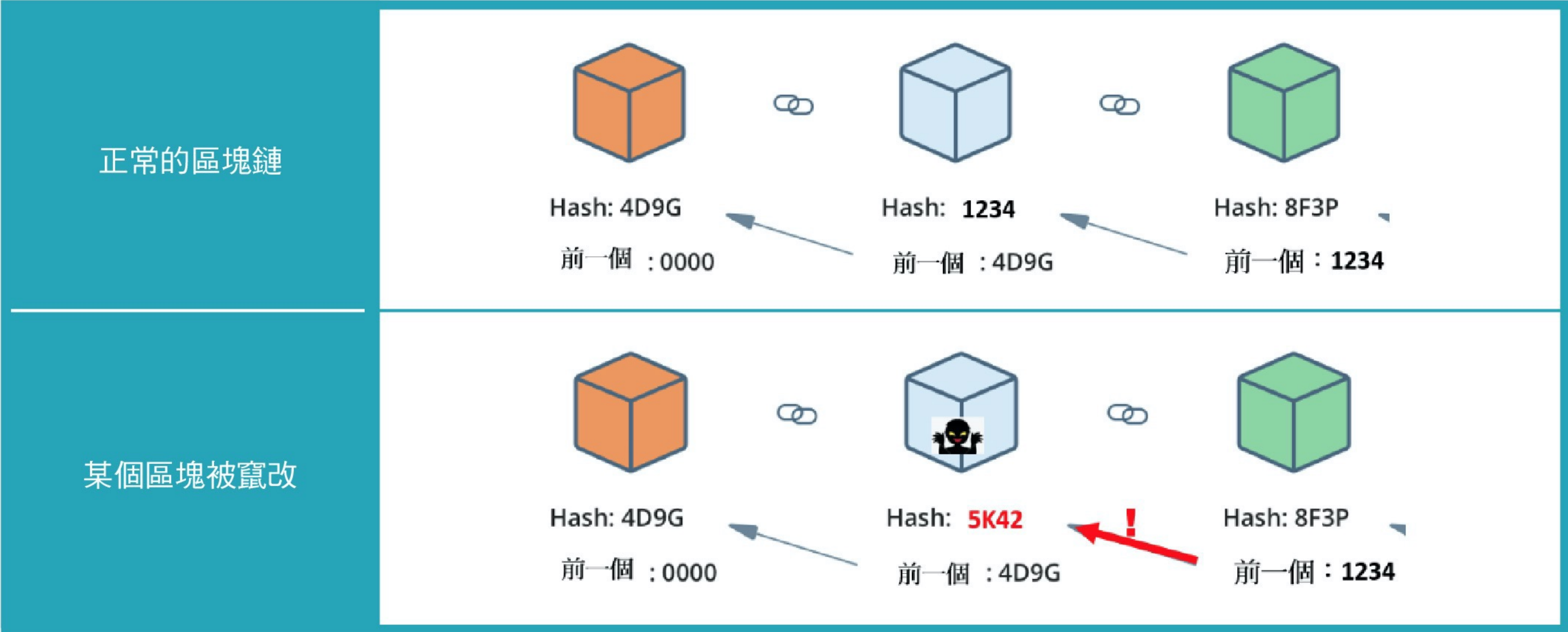
一個區塊就像一本筆記本，裡面通常記錄了以下內容：

- （一）交易資料：例如交易雙方的身分，交易詳細內容等。
- （二）時間戳記：記錄交易發生的時間。
- （三）自己的雜湊值（Hash）：為了識別區塊，系統會使用雜湊函數將交易內容計算出一組獨特的「雜湊值指紋」。如果交易內容改變，雜湊值也會跟著變化。
- （四）前一個區塊的雜湊值：這是區塊能串成「鏈」的重點。

前三項內容用來描述區塊本身，最後一項則讓區塊能夠相互連接。假設現在有一個新的區塊生成，系統會先找出目前已存在的區塊鏈末端，取得末端區塊的雜湊值，並將它寫入新生成的區塊中。這樣一來，新生成的區塊就能掛在這條鏈的最末端，更新整條鏈。

鏈的結構能有效防止資料被竄改（參見表2），舉例來說，區塊B串在區塊A的後面，區塊B會記錄區塊A的雜湊值（假設是1234）。如果駭客竄改了區塊A的交易資料，區塊A的雜湊值會發生變化，不再等於1234。此時A和B記錄雜湊值產生矛盾，整個系統就能立刻發現並阻止竄改行為。

表2 區塊鏈如何偵測到某一個區塊資料被竄改

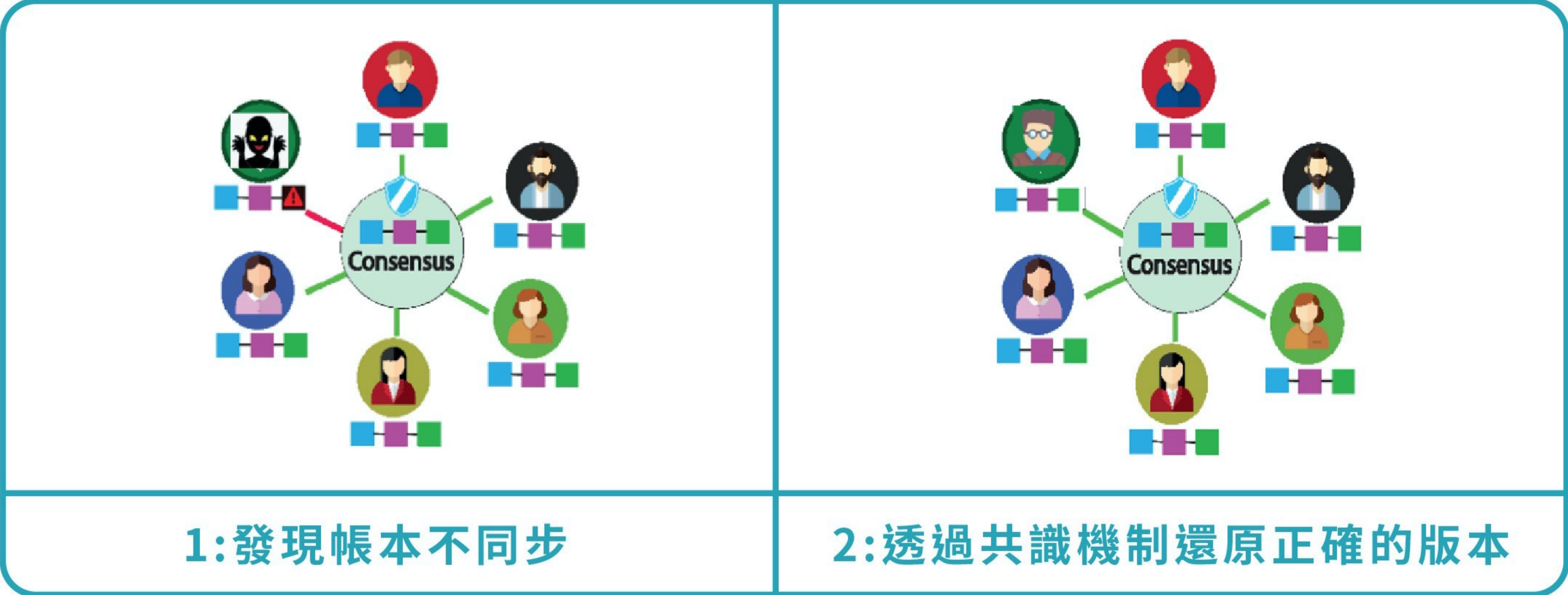


除了上述的基本結構，區塊鏈還結合其他技術來實現去中心化的運作。

（一）共識機制

共識機制（參見表3）能讓分散在各處的帳本維持一致的內容，它是一種演算法，例如比特幣採用工作量證明（PoW）演算法來維持共識，我們又稱PoW為「挖礦」。PoW機制是公平的，但是礦工大量計算會拖慢效率與耗損能源，因此又有權益證明（PoS）和提名權益證明（NPoS）等改良後的共識機制。未來應該還會創造出更多新的演算法，讓整體機制變得更好。

表3 區塊鏈偵測與還原帳本資料不同步的步驟



（二）加密

為了防止帳本或交易被攻擊，區塊鏈採用非對稱式加密技術來保護資料。這種加密技術的使用者擁有一組對應的公開金鑰與私密金鑰（Public Key / Private Key）。公開金鑰可以提供給外界，用於加密訊息與驗證簽名，私密金鑰則只能自己保存，用於解密訊息或進行數位簽名。透過非對稱式加密技術，使用者得以安全的進行交易，同時也能保障紀錄不被竄改。

2-1-4 區塊鏈的應用與挑戰

許多人聽到區塊鏈，第一想到的是比特幣（Bitcoin），但實際上區塊鏈不是只應用在加密貨幣，還有NFT（非同質化代幣）、Defi（去中心化金融）、履歷認證、自治運作等應用情境，提供虛擬世界一種新的信任模式。以下我們來認識區塊鏈的應用、它造成的影響與區塊鏈的挑戰。

一、區塊鏈核心應用：加密貨幣與NFT

在眾多區塊鏈應用中，加密貨幣與 NFT 最為人熟知。前者開啟了去中心化金融的新局面，後者則讓數位資產得以自由流通。這兩者不僅改變了傳統的交易模式，也為虛擬世界奠定了新的經濟基礎。

加密貨幣是由一組網路代碼所組成的虛擬交易媒介，不是真實錢幣，也沒有法律上的發行機構，表4列出法定貨幣、虛擬貨幣與加密貨幣的相異點。

表4 法定貨幣、虛擬代幣與加密貨幣比較

	法定貨幣	虛擬代幣	加密貨幣
發行者	國家中央銀行	平台或遊戲公司	區塊鏈系統
形式	紙鈔、硬幣、帳戶	遊戲點數、平台代幣	比特幣、以太幣等
價值基礎	國家信用與法律保障	平台規則與使用需求	區塊鏈共識機制
使用範圍	國內外	限特定平台或遊戲	線上交易、跨境支付
交易方式	銀行、金融機構	平台內部轉帳或兌換	去中心化網路驗證
安全性	受法律保障，可防偽	依平台管理，可能遭竄改	透過加密技術確保，不易竄改

第一種加密貨幣是比特幣（Bitcoin），於2009年問世，發展至今市面上已經出現上萬種加密貨幣，大部份有其特殊的用途。我們在新聞上看到價格大漲大跌的比特幣屬於公鏈幣，風險較高。此外還有與法定貨幣連結的穩定幣、與去中心化金融系統結合的Defi代幣、類似公司股票的平台幣等不同種類的幣別。

加密貨幣擁有區塊鏈最大的特色，包括去中心化、透明、不可竄改。此外，不論種族、性別、年齡、經濟或政治狀況，只要使用者擁有一個加密貨幣錢包，都能在任何時間地點操作加密貨幣。而且加密貨幣的交易紀錄中記載的是錢包位址，不是交易人姓名。因此加密貨幣還具有全球化與匿名的特性。

隨著加密貨幣流通盛行，陸續有了加密貨幣交易所、支付系統、借貸、保險、資產管理等類似真實世界的金融服務系統，我們稱之為去中心化金融（Decentralized Finance，簡稱DeFi）。DeFi為虛擬世界提供一種更安全的經濟運作模式，使用者可以在DeFi上完成大部份與傳統銀行類似的服務，而且不必經過書面審核、速度更快、手續費更低、也具有全球化與匿名的特色。

另一種使用區塊鏈技術的數位商品稱為非同質化代幣NFT。你可以想像一個NFT是一枚代幣，但是它獨一無二、無法拆分。NFT可以是一幅畫作、一首音樂、一張卡片、一個虛擬寶物。它和加密貨幣相同之處是都可以在去中心化金融市場中交易，最大的不同是NFT無法被取代與切割，例如我可以買0.1個比特幣，或是拿其他同值貨幣來交換，但是我無法買0.1幅圖畫，也無法拿2首不同的音樂做替換。

過去數位世界中的「非同質化」創作時常不被重視，例如一張苦心創作的數位圖畫可能被他人輕易下載、修改、冒用等，但是以NFT發行的創作具有「身分證」，記錄在區塊鏈的身分證讓他人能確認此作品是原版或複製品。發行NFT的創作者可以用自動化的方式收取使用與轉手交易的版稅，收藏者則是能擁有一個獨特的作品，並且可以透過區塊鏈保證它的真實性，圖9顯示非同質化代幣（NFT）創作者與收藏者的關係。



圖9 非同質化代幣（NFT）創作者與收藏者的關係

NFT從2021年開始在市場上爆紅，當時許多商品都炒作至天價進行買賣。現在NFT已經不再是熱門討論話題，但它仍然持續發展中，包括虛擬資產、音樂專輯、票券、會員憑證等都可見到NFT的相關應用。

二、區塊鏈延伸應用：智慧合約與驗證服務

上一節提到去中心化金融，從加密貨幣延伸出來的保險、借貸等金融服務是使用「智慧合約」來提供安全且即時的交易。你可以想像智慧合約類似自動販賣機，是利用區塊鏈技術發展的程式，當條件符合時即自動執行合約訂定的工作。真實世界中也有利用智慧合約進行的應用，包括物件租賃、小額理賠、自動媒合買賣方的服務，可減少人為的詐欺與人力維護的成本。例如新加坡有TADA媒合計程車服務，國內有奧丁丁區塊鏈旅宿訂房服務等。

除了金融交易外，區塊鏈的自主、透明、不可竄改等特性還可以用在防偽與建立信任機制，包括：

（一）資料驗證

利用區塊鏈儲存個人學歷、證書、執照，或土地房屋所有權資料等，可以防止偽造。例如我國法務部提供律師證書區塊鏈驗證功能，內政部也提供電子產權憑證查詢服務，讓民眾檢索資料更方便也更安心。



（二）醫療紀錄

個人醫療病歷一向是重要隱私，但是在轉院、健檢、理賠、就業、施打疫苗等狀況下時常需要調閱個人健康紀錄。利用區塊鏈建立與管理健康資料，可以兼顧隱私與便利性。國外在疫情後推出Digital Health Pass，國內如臺北醫學大學也推出智鏈護照服務。

（三）記錄與徵信

利用區塊鏈儲存公益捐款金流、群眾募資狀況，可以增加透明度與可信任度。例如國際的Giveth組織、國內的度度客募資，都應用區塊鏈技術打造透明的金流平台。

（四）供應鏈管理

製造商與企業都需要管理商品或零件供應鏈，而區塊鏈技術提供商品的透明度和可追溯性，可以用來驗證產品真偽、追蹤從來源到目的地的足跡，管理庫存數量與物流狀況，讓企業與使用者可以更有效率的掌握商品資訊，國外企業如Walmart、DHL、Nestle、IBM等皆應用區塊鏈管理商品供應鏈。



三、區塊鏈的困境與挑戰

讀到這裡，你可能會覺得區塊鏈是不錯的創新技術，但許多人一聽到區塊鏈就會聯想到詐騙、泡沫化等負面名詞。這樣的印象並不是源於技術本身，而是因為從2019年開始，加密貨幣與 NFT 市場的炒作過度，導致價格大幅波動，也成為不肖人士進行詐騙與投機的工具，因此社會大眾逐漸將區塊鏈與「風險」劃上等號，忽略了它正向應用的潛力。從2022年開始這波熱潮開始減退，區塊鏈技術雖然仍在發展中，NFT的創作能量也十分豐沛，但是相關的討論度已經變少。

除了金融交易外，區塊鏈的自主、透明、不可竄改等特性還可以用在防偽與建立信任機制，包括：

（一）能源消耗太大

要運作去中心化的共識機制，例如PoW工作量證明演算法會需要大量運算設備來計算數學難題。這種激烈的「算力競賽」造成巨大的電力與水力浪費。這不僅帶來環保疑慮，也使得區塊鏈難以被視為永續發展的技術。雖然後續有不同的改良演算法出現，但是仍需要時間推廣與改善現況。

（二）執行效率低落

區塊鏈的去中心化設計保障了自主性與透明性，但是與傳統的中心化資料庫相比，在交易速度與效率上比較落後。中心化系統只需一個伺服器確認交易即可完成，但區塊鏈卻需要分散在世界各地的許多節點共同驗證，尤其當交易量增加時，網路容易壅塞，將導致等待時間過長，這使得區塊鏈難以立即取代日常消費支付系統，還需要發展新技術來彌補理想與現實中的落差。

（三）不法人士利用

區塊鏈具有全球化與匿名特性，雖然可以保障使用者隱私，但也被不法份子濫用。例如加密貨幣交易不需要經過銀行或政府審查，一些非法活動如毒品交易、勒索病毒贖金支付、洗錢等，會透過加密貨幣進行，讓執法機關難以追查犯罪者的身分。此外，去中心化市場也因為沒有中央機構監管，出現許多假冒NFT或詐騙案件，導致社會大眾對區塊鏈有許多負面印象。

（四）法律監管問題

區塊鏈是一個跨國界、分散式的技術，但現行法律多數仍以國家為單位設計，無法完全因應它帶來的新挑戰。以加密貨幣為例，有國家已將比特幣當成法定貨幣，一些國家正在制定相關監管規則，也有部分國家仍然嚴格禁止加密貨幣流通。如何在「保障社會安全」與「維持創新動能」之間取得平衡，並且與世界並進，是未來各國必須面對的重要課題。

總結來說，區塊鏈是一項創新而充滿潛力的技術，但是涉及法律、倫理與公共政策，需要跨國的討論與合作，還要克服對環境的長期影響，同時使用者也要培養良好的數位素養，避免陷入人為詐騙的陷阱中。只有當技術逐步成熟、制度逐漸完善，區塊鏈才能真正發揮它「新型態信任基礎」的價值。

● 從阿俊的一天看區塊鏈的實際應用

◆ 區塊鏈健康護照

- 流程：施打疫苗→醫療院所上傳紀錄→以區塊鏈方式記錄在個人健康護照中→使用者自行管理。
- 重點：
 1. 個人健康護照可包含病歷、健檢報告、疫苗接種紀錄等資訊。
 2. 透過區塊鏈技術整合，健康數據的所有權集中屬於使用者，不是分散儲存在各家醫療院所中。
 3. 因應不同情境，使用者可以自行決定揭露哪些健康資料。
- 素養提醒：同學除了保護自己的醫療紀錄，也要尊重他人隱私。

◆ 穩定幣

- 流程：店長將穩定幣所有權轉讓給阿俊→阿俊透過交易所出金→交易所依當時匯率轉成新臺幣存入阿俊帳戶。
- 重點：
 1. 穩定幣是加密貨幣的一種，幣值與法定貨幣連結，波動性較小。
 2. 加密貨幣移轉時只有小額交易費，銀行則是收取固定手續費。
- 素養提醒：在不熟悉的交易所進行兌換時，建議先從小額兌換開始測試，以免轉出加密貨幣後，台幣帳戶卻沒有收到錢。

◆ 智慧合約交易

- 流程：買家下標付款→付款金額鎖在合約中→賣家寄出物品→買家確認物品沒有問題→智慧合約放款給賣家。
- 重點：
 1. 智慧合約是一段自動執行的程式，沒有人為介入。
 2. 授權智慧合約執行時，應該注意授權的範圍與時間。
- 素養提醒：智慧合約優點是透明準確，而且有紀錄。缺點是如果合約內容有漏洞或邏輯錯誤，可能造成無法補救的錯誤。

◆ 票卷NFT

- 流程：阿俊購買門票→主辦單位將門票NFT所有權轉讓給阿俊→入場時檢查本人有門票所有權→入場。
- 重點：
 1. 可以設定門票NFT轉讓的次數，避免黃牛轉賣獲利。
 2. 門票NFT非實體且難以複製，可以避免票券遺失或偽票流通。
- 素養提醒：NFT也是加密貨幣，購買時要注意價值波動的風險。

◆ NFT創作

- 流程：原著者創作音樂→在NFT平台將音樂所有權轉換為代幣→收藏家在平台挑選喜歡的作品→採用競標或直接購買的方式投資。
- 重點：
 1. NFT的價值在於其「所有權」的獨特性，而作品本身是數位檔案，是可以被複製的。
 2. NFT形式多元，區分為購買作品所有權、著作權或是使用權等。投資前一定要詳細閱讀合約，並且留存賣方承諾，以保障權益。
- 素養提醒：將自己的創作轉成NFT，屬於公開傳輸行為，因此要注意創作內容必須是原創，不能重製或改作別人的作品，避免觸法。

2-1-5 虛實整合新未來



動態信任機制與區塊鏈的誕生，挑戰了傳統中心化的制度，改變了資訊驗證、保存與流通的方式，也讓虛擬世界不再只是娛樂或交流的平台，而逐漸具備治理與經濟的特徵。放眼未來，隨著技術進步，我們可以從以下幾個方向想像可能的發展：

（一）AI與去中心化結合

AI擅長分析資料並做出預測，區塊鏈則能保障資料的真實性與不可竄改，而零信任架構確保驗證安全性。三者結合後，能透過各自的優勢，建立更透明、安全、高效的系統。例如，未來醫療AI若能利用區塊鏈記錄的病例，就能確保資料的準確性，診斷結果更具信任度；相對的區塊鏈也能透過去中心化的方式分享與管理醫療數據，保障AI模型不被壟斷；而動態信任機制能確保醫療資料的存取權限，避免資料被濫用。

（二）更自由的共享環境

目前普及的雲端服務與社交平台多半仍是由特定服務商提供系統，使用者隱私資料都由服務商主導，要不要收費也取決於服務商，屬於中心化結構。如果未來能結合區塊鏈與動態信任架構，使用者可直接掌握自己的資料與隱私，透過去中心化的網路進行交換與驗證，不必依賴單一平台的允許。這將使資訊共享更自由，也能降低資料被濫用的風險。

（三）虛擬經濟的展望

隨著加密貨幣與去中心化金融發展，未來在虛擬世界，人們不僅能購買商品，支付服務費用，甚至可以在虛擬世界工作賺取收入。區塊鏈讓這些資產擁有清楚的歸屬權與交易紀錄，零信任的安全設計則能防止帳號資料外洩或是被冒用，使虛擬資產可以像現實世界的資產一樣被管理與流通。這樣的經濟模式，將使「虛擬」與「現實」的界線越來越模糊，形成一個雙向互動的新社會。

（四）數位誠信與隱私保護

虛擬世界的挑戰之一，是如何在公開透明與個人隱私之間取得平衡。區塊鏈可保障資料不被竄改，但其透明可追蹤的特性也有隱私疑慮。零信任架構強調「必要驗證、最小揭露」，搭配新興的零知識證明（Zero-Knowledge Proof），能讓人們在不揭露完整資料的情況下，證明自己符合資格。只要妥善運用這些技術，就能同時建立數位誠信與隱私保護。

（五）永續發展

目前部分區塊鏈運作仍需消耗大量能源，這與全球追求的永續發展目標有所衝突。目前一些新的共識機制如權益證明（PoS）能大幅降低能耗；同時，也有區塊鏈專案嘗試結合再生能源，打造「綠色區塊鏈」，例如再生塑膠市場、時尚循環平台、碳足跡管理。虛擬世界若要成為長期存在的社會，就必須讓其底層技術符合環境永續的需求。

（六）全球治理與數位公民

零信任與區塊鏈的結合，挑戰傳統的國家治理模式，也帶來跨國界的新可能。未來，透過去中心化自治組織（DAO），人們能以「數位公民」的身份參與社群決策，不再完全依賴國家或企業。這些治理模式雖仍在實驗階段，但已經展現出一種新的「全球治理」方向。未來，我們可能同時是現實國家的公民，也是虛擬社群的參與者，活躍於雙重社會之中。

動態信任架構、區塊鏈與人工智慧，不僅是技術的演進，也在塑造虛擬社會的運作方式。當這些發展趨勢交織在一起，虛擬與真實的界線逐漸模糊，最終可能形成一個全新的虛實整合的社會，而你我都將是其中的一份子。讀完本單元後，未來同學在虛擬世界活動時，記得不要只停留在娛樂與使用的層面，而是理解背後的運作模式，觀察並思考它們如何影響自己的生活與環境。同時，也希望大家能想像並積極參與未來世界的建構，成為塑造新世代數位社會的重要一員。



2-2 概念統整

一、整體圖像：從「我是誰」到「如何被信任」

虛擬世界的運作主要由以下要素構成「身分 → 資料 → 資產 → 規則與信任」。人先能被辨識，才有後續的資料互動與價值流動；而這些互動必須在可被檢查的規則之下，才會形成穩定的社會秩序。這四個要素彼此牽動，最終構成具有「社會性」的數位空間與日常情境。

二、核心原則：不預設信任、只給必要、隨情境調整

現代網路把「一次進門、內部皆可信」的做法，轉向不預設信任的零信任：每次請求都重新驗證、授權以最小必要為準則，並接續發展為持續觀察行為，以動態調整風險的動態信任架構，讓「新裝置、異地、大額」等場景能即時升級驗證或限縮權限。

三、可驗證的身分與憑證：從「我說我有」到「可被查驗我有」

去中心化的身分標識連結可驗證的憑證（VC），在需要時組裝成一次性可驗證展示（VP），並可限制時效與欄位，達到「只出示必要、可追溯可撤銷」的效果。這使得像「課堂簽到」或「健康出入」等場景，能快速完成核驗，而不外洩多餘個資。

四、價值交換的安全模型：從轉帳到交易託管

當互動觸及價值交換，託管（escrow）與條件式釋放就成為降低爭議的關鍵：款項先被鎖定，確認收貨後才自動放款；同時，對合約與應用的授權設定一次、限額、到期，完成任務即失效，避免「無上限授權」帶來的風險。

五、規則與治理：把「誰能做什麼」說清楚，並能被驗證

以虛擬社群運作為例：誰能進來、能做什麼、怎麼決策要寫清楚並可驗證；當出現異常（如同票多地同時驗證、短時間大量提案），系統能自動要求更高強度驗證或暫停流程，以維持公信力。

六、技術底層：為何能「可查、可驗、不可竄改」

前述概念得以實現，主要仰賴以下幾個重要技術：

- 分散式紀錄與共識：當不同節點出現版本差異，系統透過共識機制回復到唯一正確的帳本，避免單點篡改。
- 非對稱金鑰與數位簽章：公開金鑰用於驗證、私密金鑰用於簽章或解密，確保訊息來源可信與內容完整，支撐「可驗證」的基礎。
- 身分 / 裝置 / 信任推斷三層鑑別：同時看「是誰」、「用什麼裝置」、「處在怎樣的風險情境」，來決定能否、以及在何種限制下存取資源。

不論是簽到、出示健康憑證、薪資入帳、二手交易，或票務與社群投票，它們都遵循同一條主軸：先可驗證地確認人與裝置 → 依任務給最小揭露與最小權限 → 依情境動態升降風險 → 完成即關閉或撤銷。這條主軸把身分、資料與資產的互動規範化，讓虛擬社會得以在安全與便利之間取得平衡。

2-3 觀念釐清

進入虛擬世界，最重要的事情就是好好保護自己。然而技術進展快速，各種陷阱也層出不窮，想保護自己最好的辦法就是具有正確的觀念與好習慣。以下介紹一些大家常陷入的錯誤認知，並且提出對應的修正行為與正確的習慣，希望能幫助同學能更安全的在虛擬世界探索與遨遊。

① 截圖≠憑證

- 情境 | 演唱會入口，工作人員要阿俊出示票證。
- 對話 | 「我有截圖啊！」阿俊的朋友說。
- 常見誤解 | 只要畫面長得像，就能當作證明。
- 釐清 | 截圖只是影像，無法被驗證真偽、是否過期、是否已被使用；真正的憑證需能被讀取與核驗，並回應「現在確實有效」。
- 一句話記住 | 看得到不等於驗得到。

② 帳號≠身分

- 情境 | 社團投票開放，系統要求登入與核驗。
- 對話 | 「我有帳號就代表我是社員。」小雅說。
- 常見誤解 | 登入某平台就代表身分真實、資格正確。
- 釐清 | 帳號表示「你在這個系統裡有一個容器」，不代表你擁有某些資格；身分是「你是誰」，資格是「你具備什麼權限」，兩者都要能被核驗。
- 一句話記住 | 身分與資格才是門票。

③ 驗證≠授權≠監控

- 情境 | 阿俊用手機進入校務系統。
- 對話 | 「既然登入過，就該能做所有事吧？」
- 常見誤解 | 一次登入等於所有權限開通。
- 釐清 | 驗證是「你是誰」、授權是「你能做什麼」、監控是「做了什麼要被記錄」，三者相互獨立；登入不等於無限權限。
- 一句話記住 | 先認人，再定權，過程要留痕。

④ 一次登入≠一直可信

- 情境 | 深夜異地，多次下載成績資料。
- 對話 | 「我早上驗證過了，為何又被擋？」
- 常見誤解 | 進了門就一直安全。
- 釐清 | 環境在變（時間、地點、行為、金額），信任也要跟著變；高風險場景應提升驗證或臨時限縮權限。
- 一句話記住 | 信任是動態，不是一次終身。

⑤ 加密≠簽章

- 情境 | 阿俊把報名名單寄給承辦人。
- 對話 | 「我用加密寄出，就能證明是我傳的。」
- 常見誤解 | 加密就等於能證明來源。
- 釐清 | 加密是「讓內容看不懂」，簽章是「讓來源可信、內容完整可驗」；要保密用加密，要證明誰送的與有無竄改用簽章。
- 一句話記住 | 保密靠加密，可信靠簽章。

⑥ 「授權一次」≠「永久有效」

- 情境 | 阿俊上午點了空投連結，晚上錢包被扣款。
- 對話 | 「我只是按一次允許，怎會一直扣？」
- 常見誤解 | 同意一次=只影響當下那次。
- 釐清 | 若授與的是「無上限或長期」權限，對方可在之後持續動作；理想作法是設定一次、限額、到期，並定期撤銷不必要授權。
- 一句話記住 | 授權要可過期、可限額、可撤回。

⑦ 擁有代幣≠擁有著作權

- 情境 | 朋友轉手賣出一張限量數位收藏NFT。
- 對話 | 「我有代幣，當然可以重製販售原圖。」
- 常見誤解 | 擁有「代表物」就擁有作品所有權與授權。
- 釐清 | 代幣通常代表「持有某項權益或紀錄」，不等於作品的複製、改作、公開傳輸等權利；權利範圍以發行規則與法律為準。
- 一句話記住 | 持有代表物，不等於持有權利。

⑧ 免費空投≠免費禮物

- 情境 | 阿俊在社群收到「限時領取」訊息。
- 對話 | 「反正免費，點了不虧。」
- 常見誤解 | 不付錢就沒有風險。
- 釐清 | 多數釣魚仰賴貪快與好奇；只要連接錢包或同意可疑授權，就可能付出更大代價。
- 一句話記住 | 免費的最貴。

⑨ 託管交易≠拖慢流程

- 情境 | 二手市集，賣家催促直接轉帳。
- 對話 | 「走託管太麻煩，先匯款比較快。」
- 常見誤解 | 安全與效率必然對立。
- 釐清 | 託管把風險前置管理：款項先鎖住、條件達成才放款，避免貨款與商品不對等；多一步核驗，少十步追討。
- 一句話記住 | 多一步託管，少十步麻煩。

⑩ 共享票碼≠共享權益

- 情境 | 演唱會當天，兩個入口同時有人驗到同一張票。
- 對話 | 「我只是借朋友進場一下。」
- 常見誤解 | 票是檔案，複製就能共用。
- 釐清 | 正規票務驗的是「此刻是否持有與未使用」，若偵測同時使用，系統應封鎖與升級驗證；共享等於破壞公平，也可能導致雙方都被拒。
- 一句話記住 | 票是當下的持有權，不是可複製的圖片。

⑪ 內網／熟悉裝置≠自然可信

- 情境 | 校園 Wi-Fi 下，阿俊借用同學筆電處理帳務。
- 對話 | 「都是學校網路，應該安全吧？」
- 常見誤解 | 在「熟悉的地方」就不用擔心。
- 釐清 | 信任不是看位置，而是看「使用者、裝置狀態與當下風險」；陌生或未管控的裝置應降權或避免高敏感操作。
- 一句話記住 | 安全看情境，不是看地點。

2-4 延伸學習

- 政府零信任架構說明文件（國家資通安全研究院 NICS）
取自：https://download.nics.nat.gov.tw/api/v4/file-service/UploadFile/zerotrust/政府零信任架構說明_V2.1_1131017.pdf
- 電子簽章的相關技術介紹（數位發展部 MODA）
取自：<https://moda.gov.tw/press/multimedia/blog/12794>
- AI時代的數位識讀與挑戰（台灣事實查核中心）
取自：<https://tfc-taiwan.org.tw/ai-era-digital-literacy/>
- 去中心化身份 DID 的應用發展（臺灣大學計中電子報）
取自：<https://www.cc.ntu.edu.tw/chinese/epaper/home/001/Upload/354/reIfile/26962/246431/12fed7c2-42f9-4d12-99a7-9f0e19493daf.pdf>
- 從NFT內涵、應用談相關法律爭議（經濟部智慧財產局）
取自：<https://www.tipo.gov.tw/wSite/public/Attachment/0/f1748336976119.pdf>
- 資訊學科中心增能講座：新興科技技術發展與趨勢應用-區塊鏈
取自：<https://www.youtube.com/watch?v=oHroK0o9efY>
- 鏈習生自學入門
取自：<https://chaine.io/what-is-cryptocurrency-virtualcurrency/>



03 ▶ 三絕韋編 鑑往知來

3-1 中文參考資料

- 數位發展部。（2024年5月15日）。電子簽章法。數位發展部主管法規共用系統。
取自：<https://law.moda.gov.tw/LawContent.aspx?id=FL011349>
- 國家資通安全研究院。（2024年12月31日）。政府機關導入零信任架構參考指引－身分與設備鑑別（V1）。
取自：https://download.nics.nat.gov.tw/api/v4/file-service/UploadFile/zerotrust/政府機關導入零信任架構參考指引-身分與設備鑑別_V1_1131231.pdf
- 經濟部智慧財產局。（2022）。發行 NFT 需要取得授權嗎？
取自：<https://www1.tipo.gov.tw/tw/cp-51-906909-7e992-1.html>。2025年8月27日檢索。
- 國立臺灣大學計算機及資訊網路中心。（2024年12月20日）。去中心化身份 DID 的應用發展（PDF）。
取自：<https://www.cc.ntu.edu.tw/chinese/epaper/home/001/Upload/354/reIfile/26962/246431/12fed7c2-42f9-4d12-99a7-9f0e19493daf.pdf>
- 李沛鐸、林姿妤（2023）。區塊鏈技術應用於健康資料治理之效益、困境與挑戰。圖書資訊學研究，18(1)，129 - 174。
取自：[https://doi.org/10.30177/JLISR.202312_18\(1\).0004](https://doi.org/10.30177/JLISR.202312_18(1).0004)
- 中央銀行（2022）。DeFi 及 NFT 之發展與風險議題。存款保險資訊季刊，35(3)。
取自：https://www.cdic.gov.tw/upload/cont_att/35-3-3.pdf
- 資訊科技學科中心（2024 年 1 月 5 日）。112 學年度新興科技微課程教師增能講座：新興科技技術發展與趨勢應用－第一場（區塊鏈）〔影片〕。
YouTube。<https://www.youtube.com/watch?v=oHroK0o9efY>。2025年6月1日檢索。
- 鏈習生（2025 年 6 月 11 日）。虛擬貨幣是什麼？加密貨幣六大特性、種類、實際應用。鏈習生。<https://chaine.io/what-is-cryptocurrency-virtualcurrency/>。2025年8月17日檢索。
- 每日幣研（n.d.）。加密小白教學（分類頁）。2025年8月17日檢索，
取自：<https://cryptowesearch.com/categories/Crypto-Beginner-Tutorials>
- Ju, Yuren. 從 Facebook 無端封鎖帳號來看數位身分的問題與 DID 解決方案。YurenJu Blog。
取自：https://yurenju.blog/posts/2023-08-21_fb-ban-and-did-solution。2025年9月6日檢索
- 鄭凱恩（2025）。去中心化身分驗證的隱私強化技術：基於指定驗證者簽章及泛用環簽章的可驗證憑證（碩士論文，國立政治大學資訊安全碩士學位學程）。國立政治大學學術集成。
取自：https://ah.lib.nccu.edu.tw/item?item_id=178347

3-2 英文參考文獻

- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.
from <https://doi.org/10.6028/NIST.SP.800-207>
- National Institute of Standards and Technology. (2025). Digital identity guidelines (SP 800-63-4). National Institute of Standards and Technology.
from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf>
- World Wide Web Consortium (W3C). (2025, May 15). Verifiable Credentials Data Model v2.0.
from <https://www.w3.org/TR/vc-data-model-2.0/>
- World Wide Web Consortium (W3C). (2022, July 19). Decentralized Identifiers (DIDs) v1.0.
from <https://www.w3.org/TR/did-core/>
- Cybersecurity and Infrastructure Security Agency. (2023, April). Zero trust maturity model (Version 2.0).
from https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
- Nakamoto, S. (2008, October 31). Bitcoin: A peer-to-peer electronic cash system.
from <https://nakamotoinstitute.org/library/bitcoin/> ◦ 2025.9.5檢索 ◦
- National Institute of Standards and Technology. (2020, October 28). Zero trust cybersecurity: “Never trust, always verify.”
from <https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify> ◦ 2025.9.5檢索 ◦
- Cybersecurity and Infrastructure Security Agency. (2024, August). Connected communities guidance: Zero trust to protect interconnected systems.
from <https://lihi.cc/65zl7>



04 ▶ 四通八達 小試身手

4-1 主題探討



請以一個日常的數位情境（例如線上購票或校務系統資訊查詢），說明你所知的虛擬世界樣貌。



如果某個活動僅限「本校在學學生」報名。請說明：

- (1) 為何「有平台帳號」不等於「身分 / 資格符合」？
- (2) 你會要求對方出示哪些「事實」來證明（只描述必要事實，避免洩露多餘資料）。



以「登入校務行政系統下載成績單」為例，請分別說明：

- (1) 「驗證」在做什麼？
- (2) 「授權」在界定什麼？
- (3) 為何需要「監控」？



請簡要說明邊界信任與零信任這兩種做法的差異。



以下兩個情境，請各列出你會出示的必要事實（而非完整原始資料）：

(a) 看電影時，電影分級的年齡檢核。

(b) 社團投票僅限本屆幹部參與。

（提示：用「已滿 xx 歲」「屬於某角色」等事實描述，避免曝光生日、學號、電話等細節。）



請以「二手交易」為例，說明安全交易的託管流程（含：鎖款、寄送、驗收、放款、申訴備援）。



請判斷下列敘述的觀念是否正確並各用一句話說明理由：

() 「截圖」可以當做憑證。

() 加密就等於能證明訊息來源。

() 在內網或熟悉的Wi-Fi就自然可信。

() 持有代幣就等於擁有作品著作權。

() 一次登入就代表一直可信、什麼都能做。



資訊素養與倫理 高中職 5 版

出 版 / 臺北市政府教育局

召 集 人 / 湯志民 臺北市政府教育局局長

副召集人 / 卓育欣 臺北市政府教育局資訊教育科科长

張麗萍 臺北市立大直高級中學校長

指導委員 / 盧東華 臺北市立大學助理教授

李啟龍 國立台灣師範大學附屬高級中學資訊室主任

總 編 輯 / 林芸欣 臺北市立大直高級中學圖書館主任

執行編輯 / 魏仲良 臺北市立大直高級中學資訊組組長

編審委員 / 王鼎中 臺北市立建國高級中學老師

朱德清 臺北市立中山女子高級中學老師

侯莉莉 臺北市立內湖高級中學資訊組組長

孫晉忻 臺北市立景美女子高級中學老師

陳佳宜 臺北市立麗山高級中學老師

陳哲雋 臺北市立南港高級中學資訊組組長

陳 晉 臺北市立復興高級中學老師

陳瑞宜 臺北市立大同高級中學研發處主任

楊喻文 臺北市立第一女子高級中學資訊組組長

蔡志敏 臺北市立大同高級中學老師

蔡明男 臺北市立內湖高級中學圖書館主任

賴和隆 臺北市立中正高級中學老師

韓君尹 臺北市立和平高級中學資訊組組長

羅玕貞 臺北市立內湖高級中學老師

(按姓氏筆畫排列)

承辦單位 / 臺北市立大直高級中學

出版日期 / 中華民國114年9月

虛擬世界任遨遊

虛擬社會的運作與治理



臺北市政府教育局

DEPARTMENT OF EDUCATION
TAIPEI CITY GOVERNMENT