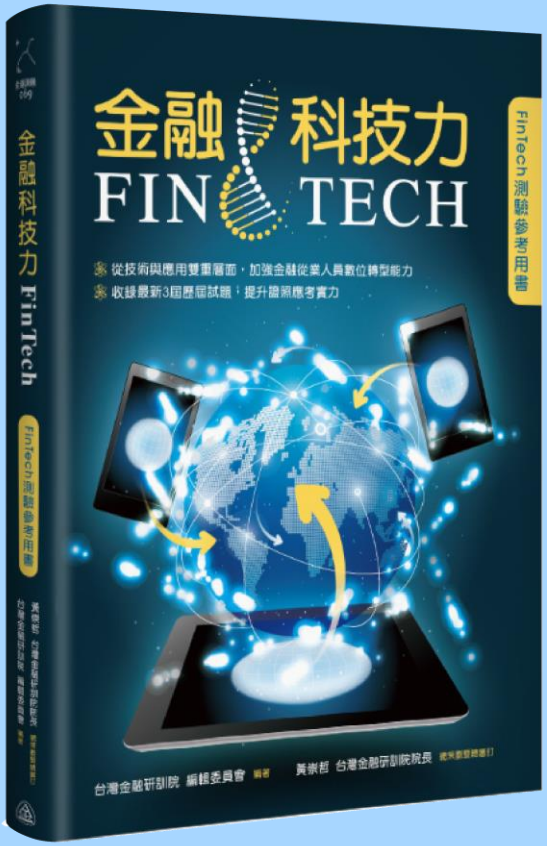

金融科技力
FIN TECH
FinTech測驗參考用書
從技術與應用雙重層面，加強金融從業人員數位轉型能力
收錄最新3屆歷屆試題，提升證照應考實力
台灣金融研訓院 編輯委員會 編著
黃崇哲 台灣金融研訓院院長

第五章
區塊鏈

本章架構

- 區塊鏈的緣起— 兼論數位貨幣
- 區塊鏈的運作機制— 以比特幣區塊鏈為例
- 區塊鏈的發展脈絡

本章重點

- 了解比特幣、數位貨幣與區塊鏈的關係：區塊鏈是承載比特幣交易的底層技術，比特幣是第一個去中心化的加密數位貨幣。
- 了解數位貨幣的分類與相關議題、初次代幣發行 (ICO)。
- 了解區塊鏈的運作，數位簽章與雜湊函數在區塊鏈的應用，以及挖礦的原理、共識機制、智能合約。
- 了解區塊鏈的特性：包括去中心化、不可竄改性、可追蹤性等。
- 了解區塊鏈應用的發展與可能場景：例如出現太多的中介參與，或是過高的中介成本，或者有低追蹤成本和高資訊安全的需求等。

區塊鏈的緣起— 兼論數位貨幣(1/6)

- 紐約時間2008年10月31日下午2時10分，中本聰在一個密碼學討論群組上發表了一篇論文，標題為「比特幣：點對點的電子現金系統」(Bitcion：A Peer-to-Peer Electronic Cash System)，文中闡釋了一種電子現金系統的基本框架。

區塊鏈的緣起— 兼論數位貨幣(2/6)

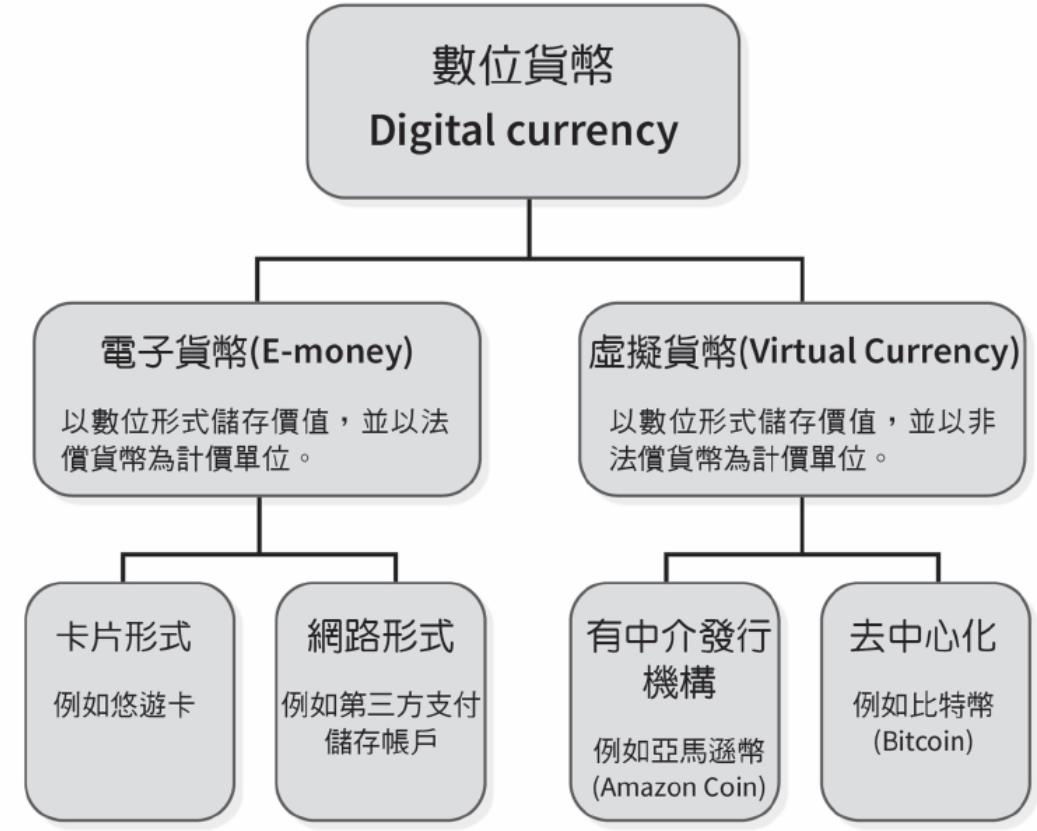
- 2009年1月3日，中本聰建立了序號為0的第一個比特幣區塊(俗稱創世區塊 (Genesis Block))，「挖掘」出第一批比特幣五十枚。
- 2009年1月9日，出現序號為1 的區塊，並與序號為0的創世區塊相連接，比特幣「區塊鏈」於焉誕生。

區塊鏈的緣起— 兼論數位貨幣(3/6)

- **比特幣與數位貨幣：**
  - 比特幣是數位貨幣的一種，也無法等同於所有數位貨幣。
  - 數位貨幣之下大別為兩類，一類稱「電子貨幣」，另一類稱「虛擬貨幣」，二者之區隔關鍵，在於是否以法償貨幣為計價單位。
  - 數位貨幣雖有「貨幣」之名，但依據目前的主流看法，以比特幣為首的加密貨幣，並不符合貨幣的功能性定義。

區塊鏈的緣起— 兼論數位貨幣(4/6)

- 中央銀行參照國際貨幣基金 (IMF) 的分類架構：



區塊鏈的緣起— 兼論數位貨幣(5/6)

- **首次代幣發行 (ICO)：**
  - ICO是指企業或非企業組織在區塊鏈技術的支持下，發行虛擬代幣給投資人，向投資人募集虛擬貨幣的一種籌資方式。
  - ICO 的名稱類比於IPO (Initial Public Offering，初次公開發行)，只是ICO不以股票換取鈔票，而是自己發行虛擬代幣換取其他具市場價值的虛擬貨幣。

區塊鏈的緣起— 兼論數位貨幣(6/6)

- 金管會對於ICO的態度：ICO發行方如有以虛偽不實的技術或成果，或有以不合理的高報酬，吸引投資人參與，則可能涉及詐欺或違法吸金等刑事案件，為維護金融秩序及投資人權益，將由檢調機關於查調具體事證後依法辦理。

區塊鏈的運作機制 (1/18)

- 比特幣在數位貨幣的譜系中，隸屬於「加密貨幣」(或稱「密碼貨幣」)，支撐比特幣的核心技術「區塊鏈」，便構築於密碼學(Cryptography) 之上。
- 區塊鏈涉及的密碼學技術：
  - 數位簽章(Digital Signature)
  - 雜湊函數 (Hash Function)

區塊鏈的運作機制 (2/18)

- **數位簽章：**

簽署人以其私鑰將訊息明文加密成「簽署文」

將明文與簽署文同時發送給對方，對方依據簽署人之公鑰解密簽署文

若解密的結果與明文一致，則對方可相信這則訊息是由簽署人所發

區塊鏈的運作機制 (3/18)

- **凱薩大帝時代「位移密碼 (shift cipher)」：**

  如傳送CAT這個單字，假設將26個英文字母平移五個位置，便可將CAT轉換為HFY。

位移前	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
位移後	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

明文 (Plaintext)： CAT

密文 (Ciphertext) ：HFY

加密鑰匙：「英文字母左移五個位置」

區塊鏈的運作機制 (4/18)

- **公鑰密碼術(Public-Key Cryptography)**又稱為「非對稱密碼術」，由Diffie and Hellman於1976年提出。

解秘方利用單向函數產生一對密鑰，分別稱作「公鑰 (Public Key)」與「私鑰 (Private Key)」

加密方獲取解密方的公鑰，利用公鑰為資訊加密

解密方得到加密的資訊後，利用私鑰解密

區塊鏈的運作機制 (5/18)

- **RSA演算法**
  - 最早的RSA 演算法採用因數分解
  - 橢圓曲線密碼術 (Elliptic Curve Cryptography, ECC) 安全性較高
  - 依據美國國家標準暨技術研究院 (National Institute of Standards and Technology, NIST) 的設定，對於最小密鑰長度的要求，RSA 是1024 位，ECC 只需160 位。
  - 比特幣區塊鏈使用橢圓曲線密碼術

區塊鏈的運作機制 (6/18)

- **雜湊函數：**
  - 是一種壓縮資料的演算法
  - 將輸入資料做「不可逆且不可重複的單向壓縮」，可使任何內容壓縮成一個固定長度的偽亂數
  - 沒有解密鑰匙
  - 比特幣區塊鏈所使用的雜湊演算法稱為SHA-256

區塊鏈的運作機制 (7/18)

- SHA-256：SHA 是「安全雜湊演算法 (Security Hash Algorithm)」的縮寫，256是指其雜湊值以二進位表示時長度有256 位，可用於查核文件是否遭到竄改，避免「從雜湊值逆推輸入資料」，此特性稱為「抗原像攻擊性 (Preimage Resistance)」。主要用途為產生區塊的「指紋」，做為區塊與區塊連結的依據。

區塊鏈的運作機制 (8/18)

- **區塊鏈的運作機制(以比特幣為例)：**
  - 每一個使用比特幣的參與者就是構成比特幣網路的一個節點，區塊鏈則是比特幣網路各節點間傳輸比特幣的交易記帳系統，而且各節點都可以擁有一份完整的總帳。

區塊鏈的運作機制 (9/18)

- **首次使用比特幣**：使用任一種類錢包軟體下載用戶端，自動生成「收帳帳號」位址及密碼。

位址 ➡ 以公鑰密碼術產生的公鑰再取其雜湊值

密碼 ➡ 與公鑰對應的私鑰

區塊鏈的運作機制 (10/18)

- **轉帳**：轉出錢包以私鑰加密交易內容，連同公鑰廣播到比特幣網路上(數位簽章)，節點自動傳輸驗證。
- **自動驗證**：

1.利用廣播所附的公鑰將交易訊息解密。

2.透過總帳本登載的歷史交易紀錄計算出該位址擁有足夠的 比特幣。

區塊鏈的運作機制 (11/18)

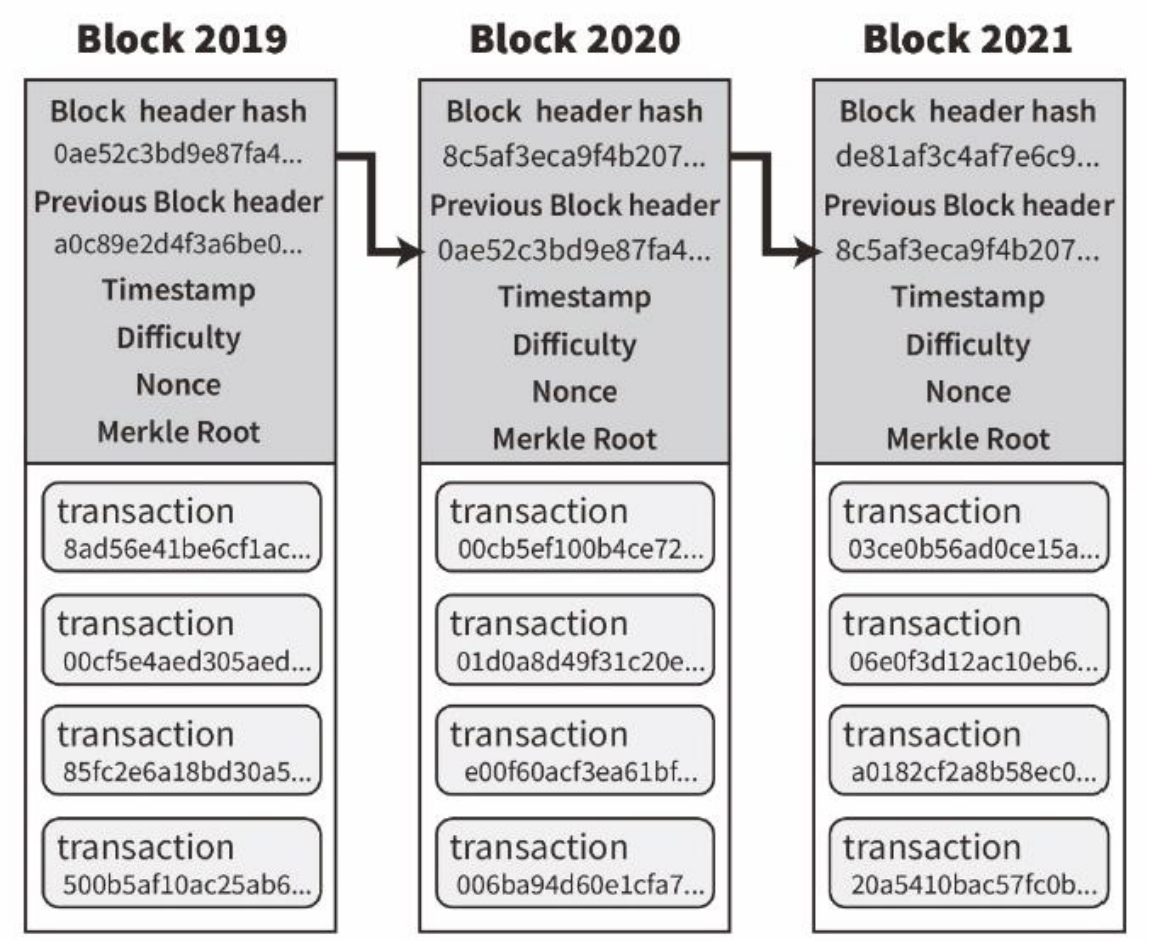
- **礦工**：爭奪「記帳權」的特殊節點稱為「礦工」。爭取到記帳權的礦工，有權將過去一段時間發生的交易紀錄打包成一個「區塊」，經其他節點驗證後，此一區塊即可附加在原本的「鏈」上；該礦工節點可獲得伴隨「記錄在該區塊內所有交易」的交易手續費，以及一筆額外的報酬。這筆額外的報酬，是隨著新區塊產生而創造出的新比特幣。

區塊鏈的運作機制 (12/18)

- **發行新比特幣的機制**：是最初每打包一個區塊可獲得50比特幣，隨後每生成二十一萬個區塊 (大約耗時四年)，釋出的新比特幣便減半，到了西元 2140 年左右，會存在約兩千一百萬比特幣，之後便不再發行新幣。

區塊鏈的運作機制 (13/18)

- **區塊的構造**：可分為區塊頭與區塊主體



區塊鏈的運作機制 (14/18)

- **挖礦**：「挖礦」的過程是由礦工節點競相解決一個與區塊頭雜湊值有關的題目。比特幣系統會依據系統設定的難度產生「目標數(target)」，礦工的任務就是尋找一個「隨機數」，使得區塊頭依SHA-256演算法取兩次雜湊後之雜湊值小於目標數。「算力」越強的礦工，取得「記帳權」的機會越大。

區塊鏈的運作機制 (15/18)

- **不可竄改性**：無法單獨竄改某一區塊的交易紀錄，一個區塊後面連接的區塊越多，這個區塊內的資料就越不易被竄改，在比特幣區塊鏈中，通常認為六個區塊就足夠安全了。在比特幣區塊鏈上進行51%攻擊的成本甚高，目前估計超過10億美元，實際上，比特幣問世以來還沒有遭遇過51%攻擊。

區塊鏈的運作機制 (16/18)

- **去中心化**：「挖礦」主要目的在於確保帳本的安全可信，「釋出新比特幣」則是鼓勵比特幣參與者獨立驗證交易的獎賞「誘因」，為了挖礦而消耗的資源則是維護可信任帳本的成本。「挖礦機制」是使得比特幣成為第一個去中心化數位貨幣的重要設計。

區塊鏈的運作機制 (17/18)

- **共識機制**：在去中心化的分散式網路中，協調所有參與者達成共識的方法，稱為「共識機制」。常見的共識機制有「工作量證明 (Proof of Work, PoW)」與「權益證明 (Proof of Stake, PoS)」。

區塊鏈的運作機制 (18/18)

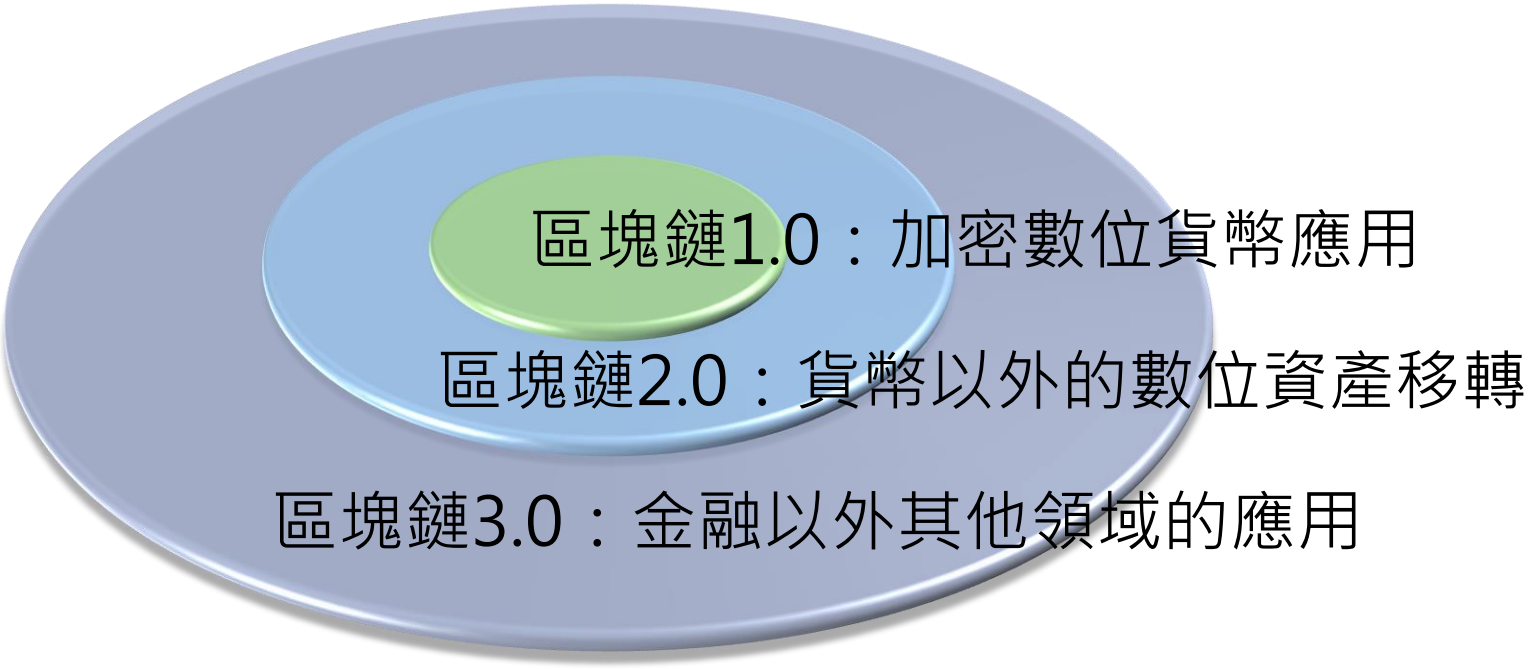
- **去中心化包含的層面：**

  1.藉由分散式共享帳本達成帳本資料存儲的去中心化。

  2.透過挖礦機制集體維護帳本，達成記帳行為本身的去中心化。

區塊鏈的發展脈絡(1/3)

- 區塊鏈應用的發展進程：



區塊鏈的發展脈絡(2/3)

- **區塊鏈的應用面向：**
  - 去中心化、不可竄改性、可追蹤性
  - 可任由所有人成為節點：公有鏈、私有鏈
  - 區塊鏈技術不一定能滿足複雜商業交易中較嚴格的保密要求和交易隱私的維護

區塊鏈的發展脈絡(3/3)

5個主要的區塊鏈平台

	Bitcoin	Ethereum	Hyperledger Fabric	R3 Corda (DLT)	Ripple
平台屬性	支付交易	通用型	通用型	金融業為主	支付交易
原生數位貨幣	比特幣	以太幣	無	無	XBR
網路參與限制	公開鏈	公開鏈， 私有/聯盟鏈	私有/聯盟鏈	私有/聯盟鏈	公開鏈 但有限制
交易者(使用者)	匿名或由鏈外AP 控管	匿名或由鏈外AP 控管	登記制(CA)	登記制	登記制
交易內容(隱私)	公開	公開	公開或限制	公開或限制	部分公開
共識機制	Mining 工作量證明 (PoW)	(1) Mining PoW, (2) PoA (3) 將加入 PoS	V0.6： PBFT/SIEVE V1.0： Kafaka/SBFT	Notary/RAFT	Ripple 協議
智能合約功能	無	有	有	有	無