**比特幣（Bitcoin）：一切的起源**

什麼是比特幣？

* 比特幣是由中本聰（Satoshi Nakamoto）於 2008 年提出的概念，包含比特幣區塊鏈（Bitcoin）這套轉帳系統，以及比特幣（BTC）這個數位貨幣。這套系統開發至今將屆滿 10 年。[[解讀中本聰的比特幣論文]](https://blocktrend.today/08-22-2017-satoshi-nakamoto-bitcoin-a-peer-to-peer-electronic-cash-system)
* 比特幣為什麼會漲價？
* 比特幣總量固定（2,100 萬枚）供給有限，若越多人想買（需求越多），價格就會越高。道理和股票漲跌相同，是簡單的供需法則。 [[穩定價格：數位貨幣的經濟難題]](https://blocktrend.today/04-17-2018-cryptocurrency-problem-stable-coin)
* 有兩種人想買比特幣：想使用比特幣區塊鏈（Bitcoin）這套轉帳系統的使用者、預期比特幣（BTC）未來會漲價的投資者。

如何獲得比特幣？

* 兩種方式：組電腦挖礦、到交易所買幣。
* 用挖礦獲得比特幣，就像是自己養牛來喝牛奶。到交易所買比特幣，就像是到超市買牛奶。兩種方式花費的時間、金錢成本各不相同。
* 「挖礦」是一套吸引大家貢獻自己電腦運算資源的獎勵機制，電腦運算資源會幫助比特幣區塊鏈運作。挖礦獎勵是每 10 分鐘提供 12.5 枚比特幣（時價約 10 萬美金）。透過「挖礦」賺取比特幣的人，就稱為礦工。
* 「買幣」得透過數位貨幣交易所，道理就像是買賣美金、日幣也得透過匯兌所一樣。雖然一枚比特幣價值數千美金，但是你也可以用 100 元台幣到全家、萊爾富，買等值的零點幾枚比特幣。

比特幣常常被駭嗎？

* 比特幣區塊鏈這套轉帳系統，將近 10 年來還沒有成功被駭過。被駭客入侵並損失資金的是交易所。這就像是匯兌所發生搶案， 與銀行轉帳系統是否安全是兩回事。

比特幣跟區塊鏈的關係是？

* 比特幣區塊鏈（Bitcoin）是一套仰賴「存簿記帳」的轉帳系統。就像你可以透過 ATM 轉帳新台幣一樣，你也可以透過比特幣區塊鏈轉帳比特幣（BTC）。
* 存簿上記錄的是誰在什麼時候轉了多少錢。差別在於 ATM 是由「銀行」來確保轉帳紀錄的正確性，而比特幣是由「區塊鏈技術」擔保轉帳紀錄正確性。
* 簡單來說，區塊鏈就是比特幣（數位貨幣）的防偽（tamper proof）機制。

我要怎麼跟長輩解釋比特幣？

* 只要牢記比特幣有三大特性：實用性、投資性以及投機性。[[比特幣的三種特性]](https://blocktrend.today/05-04-2018-buffett-said-bitcoin-is-not-an-investment)
* 從實用性來說：持有比特幣的人，才能使用比特幣區塊鏈的轉帳服務，將交易紀錄寫在比特幣區塊鏈上。就像是帳戶裡有新台幣的人，才能使用 ATM 的轉帳服務，將交易紀錄寫在銀行的存簿上。用比特幣做跨國轉帳，理論上會比使用銀行轉帳更便宜，且收款方能更快收到錢。
* 從投資性來說：因為比特幣供給總量有限，所以市場需求越大，比特幣的價格就會上漲；相反的市場需求越小，價格就會下跌。各國政府、企業是否接受以比特幣付款，就直接影響市場對比特幣的需求大小，是造成價格波動的因素之一。
* 從投機性來說：比特幣的價格並不理性。例如今年 5 月時以比特幣轉帳的速度，已經比今年 1 月時更快，但是比特幣的價格卻只有當時的一半。也就是說，比特幣的價格高低與產品好壞並沒有絕對關係。比特幣價格並不理性。

**區塊鏈（blockchain）：讓數位資產無法造假**

區塊鏈的顛覆性？

* 區塊鏈就像是當年的網路一樣，會改變許多行業的運作規則。政府、金融、物流、創意產業都積極投入，研究區塊鏈。區塊鏈的重要功用是數位資產的防偽，這是電腦、網路普及之後，全球才開始面臨的新問題。
* 現在有很多法規、業界慣例，是只承認實體文件的有效性，但電子文件卻沒有同等地位。因為實體資產的防偽，是很早就開始發展的技術。但是，數位資產的防偽卻遲遲沒有好解法，區塊鏈填補了這個空缺。而且，實體鈔票上的浮水印技術很難應用到精品皮包上，但是區塊鏈的防偽技術卻能在各種數位資產間通用。[[防偽需求有多大，區塊鏈潛力就多大]](https://blocktrend.today/06-07-2018-how-blockchain-can-disrupt-the-world)

區塊鏈如何防偽？

* 研究區塊鏈這套防偽機制，就像在研究鈔票的浮水印、雷射技術，是技術門檻最高的部分。
* 假設大家的交易紀錄都像是存簿一樣。「區塊」就是存簿的內頁，用來記錄誰在什麼時候轉帳多少錢。「鏈」就像在存簿內頁標註頁碼，以確保彼此前後相連。
* 礦工負責保管存簿、驗證交易和記帳。比特幣區塊鏈上有將近 1 萬名礦工，他們彼此獨立且互不相識，但各自都有一份相同版本的存簿。因此，駭客竄改其中一份存簿，並沒有效果。因為大家的版本都跟他不一樣，很快就知道這是偽造的存簿。

區塊鏈有哪些常見的應用？

* 區塊鏈才剛開始發展，沒有常見的應用，更沒有非區塊鏈不可的應用。最常見的是比特幣（Bitcoin），它將區塊鏈當成是數位貨幣的防偽技術，但使用過比特幣的人還是相對少數。
* 我曾經寫過區塊鏈在[網路文章](https://blocktrend.today/04-13-2018-matters-social-media-for-nice-contents)、[數位圖片販售](https://blocktrend.today/01-26-2018-kodaks-great-idea-and-a-bet)、[音樂授權](https://blocktrend.today/01-26-2018-kodaks-great-idea-and-a-bet)、[數位廣告](https://blocktrend.today/03-22-2018-brave-payments-change-digital-ads-market)、[綠電交易](https://blocktrend.today/02-09-2018-trade-green-electricity-instead-of-certification)、[公益捐款](https://blocktrend.today/02-23-2018-pain-points-of-donation)、[線上開戶](https://blocktrend.today/03-01-2018-moni-account-on-blockchain)、[數位身份](https://blocktrend.today/05-03-2018-lanyu-digital-id-tao-coin)上的應用。

區塊鏈好像很完美，它有什麼弱點？

* 交易速度太慢：比特幣每秒只能交易 3 到 5 筆交易，相對於 Paypal 每秒數百筆交易、VISA 每秒數千筆交易都慢得多。
* 沒有隱私性：比特幣的交易內容都是匿名公開在網路上，就像是全球的 Email 內容被完全公開一樣，只是大家不知道付款者、收款者實際上是誰。
* 安全性可能不足：比特幣的安全性仰賴多少礦工願意加入，並貢獻電腦運算能力。因此「挖礦」這套誘因機制必須吸引到足夠的礦工。如果礦工不足，其實區塊鏈並不一定多安全。[[區塊鏈該如何兼顧安全、效率及開放性]](https://blocktrend.today/03-27-2018-blockchain-trilemma)

**ICO（Initial Coin Offering）：新的募資模式**

什麼是 ICO？

* 現在全球共有 1,600 多種數位貨幣，再新發行一種幣，就叫做 ICO。這就像是 IPO 是在股市列表上，再新增加一支可以交易的股票一樣。
* ICO 很像群眾募資的概念，都是「先收錢，再辦事」的運作邏輯。募資方發行一種新的數位貨幣，拿來向市場上的投資者換取比特幣（BTC）或以太幣（ETH）。
* 募到錢之後，再由開發團隊依照當初在 ICO 白皮書上的承諾，讓服務、應用上線。所以，ICO 是一種新的募資方式。[[圈錢不是 ICO 的最終目的]](https://blocktrend.today/01-30-2018-ico-value-and-defect-analysis)

ICO 是詐騙嗎？

* 有很多團隊收了錢但不做事或乾脆落跑，這就是詐騙。
* ICO 白皮書不需遵守任何法令規範，製作門檻比大學生的期末報告還低。也沒有人對發起 ICO 的團隊進行實質審查。因此 ICO 就像是一種人人都可以公開募資的管道，只不過募的是數位貨幣，而不是新台幣。[[美國政府發起的 ICO 詐騙專案]](https://blocktrend.today/05-24-2018-sec-ico-project-howeycoins)

為什麼這麼多 ICO 案？

* 對發起者而言，是「先收錢，再辦事」的運作邏輯。可以用低成本的代幣，向市場上換一筆資金，和一群持有代幣的人。這相較於傳統得先自掏腰包燒一筆錢，但市場大小、顧客是誰都未知。相對來說，發起者透過 ICO 募資的風險更低。

為什麼大家搶著參與 ICO？

* ICO 專案經常會有類似群眾募資的早鳥優惠價，吸引投資者儘早購買。投資者只要預期 ICO 的幣未來會漲價，因為優惠的數量或期間有限，就會搶著購買。
* 但是，並沒有人能保證 ICO 的幣未來是漲還是跌，這就像是 IPO 的股票在上市之後，也會上漲或下跌一樣。

ICO 和區塊鏈的關係是？

* 採用區塊鏈技術，作為新發行數位貨幣的防偽機制。換句話說，在區塊鏈上發行新的幣。
* 將兌幣的智慧合約（兌幣機）保存在區塊鏈上，確保大家都可以在公開透明的規則下，公平的發行、兌換新幣，杜絕私下交易。

**以太坊（Ethereum）：用區塊鏈打造的應用平台**

什麼是以太坊？

* 以太坊和比特幣區塊鏈一樣，都是一個獨立運作的區塊鏈，但兩者有層次上的差異。比特幣是區塊鏈、應用相互綁死的轉帳系統。以太坊是用區塊鏈打造的應用平台，可以讓很多不同的應用程式，建立在以太坊平台上。
* 用手機來比喻，以太坊像是智慧型手機的作業系統。軟體工程師可以直接使用以太坊的既有資源，建立基於區塊鏈的應用（Decentralized App），但不需要自己從頭建構新的區塊鏈。這就像是 Google 已經建構好了 Android 手機作業系統，因此 LINE 只需要基於 Android 提供的資源開發 LINE App 即可，而不需要自己從頭開發一整套手機作業系統。

以太幣（ETH）有什麼用途？

* 不同於我們使用 LINE 不需要支付使用費給 Android，使用以太坊（Ethereum）上的應用，使用者必須付以太幣給以太坊。
* 以太幣與比特幣（BTC）最大的差別，就是能作為以太坊運行時的「燃料」。除此之外，以太幣同樣可以用作轉帳交易的數位貨幣，幣價會隨著需求漲跌。以太坊也有自己的「挖礦」機制吸引礦工加入，只不過礦工挖的是以太幣。

以太坊如何運作？

* 以太坊運作就像一台自動販賣機，必須投入以太幣才能幫你執行區塊鏈上的程式碼。是使用者付費的概念。
* 區塊鏈上的程式碼，統稱為智慧合約。以太坊上的應用，就是由多個智慧合約組合而成的。有別於用中文寫成的紙本合約，智慧合約的智慧之處在於將合約條件轉成程式碼，交由區塊鏈上的電腦執行。透過區塊鏈上的電腦執行程式，達成資產交換自動化，也因此無法人為干預。
* 使用者要支付多少以太幣，取決於智慧合約所需要執行的運算數量多寡、單價決定。

以太坊有應用商店（app store）嗎？

* 目前有[網站](https://dappradar.com/)根據應用的使用量、以太幣交易量排序，但以太坊並不像 iOS 和 Android 有審查機制，決定應用程式是否能夠上架，因此也不會出現統一管理的應用商店。
* 以太坊的優點是？
* 用以太坊執行智慧合約，有別於用企業的雲端運算平台（例如 Amazon Web Service）執行程式碼。以太坊能夠確保程式被貫徹執行，而不受到政府要求下架或企業審查的限制、干預。例如中國有不少被官方禁止的翻牆軟體，之前就想從 Amazon 搬家到以太坊上。

以太坊的缺點是？

* 交易速度慢：以太坊每秒只能處理 10 到 15 筆交易。
* 成本昂貴：將以太坊拿來與 Amazon 的雲端服務比較，Amazon 的 CP 值比以太坊高了 100 萬倍。

該如何入門以太坊？

* 如果你是工程師，想從寫程式的角度切入。可以學習用以太坊內建的程式語言 Solidity 來撰寫智慧合約，它的語法類似 JavaScript，因此入門門檻不高。
* 如果你要從區塊鏈概念的角度切入，我建議你[訂閱區塊勢](https://blocktrend.today/member-plan)。區塊鏈難的不是技術，而是反直覺的「去中心化思維」。