

談比特幣

驊達科技 程正孚 整理

很多人一定都聽過新聞媒體報導的 比特幣 (Bitcoin)，比特幣也可以說是各種虛擬貨幣的代名詞，比特幣 (Bitcoin) 是最早推出的虛擬貨幣 (也稱加密貨幣)，也是目前市值排名第一的虛擬貨幣，這種虛擬貨幣不由中央銀行、政府機構所發行，只能使用電子 (網路) 方式進行交易、轉移、儲存，它只是一串代碼，並沒有實體，比特幣使用區塊鏈技術來記載交易資料，每筆資料有安全性高、匿名的特性，不易被竄改資料。如今虛擬貨幣已經不是只有比特幣，而是有非常多種類特性的數字貨幣，如雨後春筍一直冒出來，但比特幣在眾多虛擬貨幣之中，重要性上目前仍是有著不可動搖的地位。但相信許多人可能依然不太了解比特幣是如何運作的，比特幣交易所是不是詐騙、如何投資？有甚麼風險？以下是簡略介紹！

比特幣是什麼？

比特幣 (英語: Bitcoin, 縮寫: BTC 或 XBT) 是一種基於去中心化，採用點對點網

路與共識主動性，開放原始碼，以區塊鏈作為底層技術的加密貨幣，比特幣由日本中本聰 (網名) (Satoshi Nakamoto) 於2008年10月31日發表論文，2009年1月3日，創世區塊誕生。在某些國家、央行、政府機關則將比特幣視為虛擬商品，而不認為是貨幣。

任何人皆可參與比特幣活動，可以通過稱為挖礦的電腦運算來發行。比特幣協定數量上限為2100萬個，以避免通貨膨脹問題。使用比特幣是透過私鑰作為數位簽章，允許個人直接支付給他人，與現金相同，不需經過如銀行、清算中心、證券商、電子支付平台等第三方機構，從而避免了高手續費、繁瑣流程以及受監管性的問題，任何使用者只要擁有可連線網際網路的數位裝置皆可使用。

但是由於比特幣區塊鏈在一定時間內能接受的交易量有限，約每10分鐘能接受最多2,500筆交易，交易手續費也會隨著比特幣交易量而波動，在2017年6月，小於1毫比特的交易，交易手續費已遠遠大於交易金額；在2017年12月，Steam宣布停止接受比特

幣，理由是「交易費用高昂，且波動性大」，在2018年2月，平均交易手續費從2017年第四季度的34美元，下降至約1美元，而此問題，正在試圖以閃電網路之類的技術來解決，擴充比特幣一定時間內的交易量。2021年1月8日，比特幣交易價格升至41,616美元；2月21日，再創58,238美元，繼3月13日，比特幣交易價格衝破60,000美元；2021年3月14日盤中，比特幣交易價格曾一度升至61,669.88美元歷史天價。

比特幣和一般法定貨幣有何不同？

比特幣（Bitcoin）和一般傳統貨幣（一般稱為法定貨幣、法幣）不同，它可以在全世界通用，不需要兌換、不用支付高額的手續費，就能在全世界進行轉帳，也不用在許多銀行、不同國家貨幣之間來回兌換，可以說是一種能讓資產自由移動的貨幣。例如每次有跨國匯款，成本都至少要近千元，有些國家則是有跨境轉帳金額限制，但透過加密貨幣機制，有機會可以把成本降到相對更低、限制更寬鬆。

在某些國家（如奈及利亞）因為通膨嚴重、法幣貶值、國際匯款管制，因此比特幣幾乎變成他們最重要的貨幣工具。當然，比特幣目前的泛用性、交易速度、交易成本，還沒有完全達到如同美元一樣的水準，且比特幣作為貨幣本身它價值並不穩定，且仍有一定的風險，但在匿名、與傳統貨幣區隔、不易被竄改的特性上，則是有傳統法定貨幣無可取代的特性。

比特幣（Bitcoin）是如何運作的？

比特幣（Bitcoin）最主要的運作機制，是用區塊鏈技術、挖礦、礦工來運作，這邊所說的挖礦及礦工，是指用自己的顯示卡GPU運算取得，不是真的去礦山採礦。參與處理區塊的使用者端可以得到一定量新發行的比特幣，以及相關的交易手續費。為了得到這些新產生的比特幣，參與處理區塊的使用者端需要付出大量的時間和計算力（為此社會有專業挖礦機替代電腦等其他低配的網路裝置），這個過程非常類似於開採礦業資源，因此中本聰將資料處理者命名為「礦工」，將資料處理活動稱之為「挖礦」。這些新產生出來的比特幣可以報償系統中的資料處理者，他們的計算工作為比特幣對等網路的正常運作提供保障。

1. 區塊鏈技術：

這是一種由網路代碼所組成的網路點對點（P2P）形式，利用複雜的密碼學原理來控制交易安全、交易單位，像是一個具有資料寫錄功能的電子記帳資料庫，每一筆交易都會永久記錄在雲端區塊上面，有可追溯、不可逆、不可竄改的特性。有一個簡單的比喻是，區塊鏈技術就是一個分散式的帳本，透過多個不同帳本紀錄、核對資料，來做到這些功能。

區塊鏈技術不需要第三方單位（如傳統銀行）來監管發行，透過這種加密技術能將資料分散儲存在不同雲端上，代表權力不是一個單位說了就算，而是分給參與交易的每一個人，不會因為單一節點的資料出問題受影

響，這也是區塊鏈技術一直在強調的去中心化概念。

2. 礦工：

交易比特幣的各種資訊會儲存在區塊上，透過大量的電腦運算驗證來確認區塊中資訊的正確度，負責確認這些資訊正確度的人稱為礦工。

3. 挖礦：

中本聰在創造比特幣的時候，就已經設定好遊戲規則，限定比特幣總數為2100萬個，至2020年6月，比特幣已經發行了1840萬個。比特幣運作的設定裡，每10分鐘能找到一個新區塊，並且就能得到比特幣當獎勵，但是每發現21萬個區塊，獎勵就會減少，2009年的一個區塊獎勵為比特幣50個、2012年則降低為比特幣25個、2016年為比特幣12.5個、2020年只剩下6.25個比特幣。如今一般人已經很難參與作為比特幣礦工與挖礦，這其實也存在著過往比特幣分配不均的問題，但並不妨礙它總數量限定、匿名性等等特性，讓這世界上始終有一群人認定它的價值。

投資比特幣（Bitcoin）有什麼風險？

任何投資商品，談它好處，一定也要認識其風險。比特幣是一種虛擬貨幣、許多國家也不承認這是合法貨幣，因此在交易時可能不受法律保障，若是你想投資比特幣或其他虛擬貨幣，這些風險都要考量進去。

比特幣投資風險1：價格波動幅度大

比特幣發行數量有上限（2100萬個），

而且每年發行量逐漸遞減，取得不易、具稀少性的特性讓它成為炒作標的，價格很容易受到需求面因素影響而大幅波動，此外也容易受到政策、情緒面因素影響而有劇烈起伏，是一種投機性的商品。比特幣的報價在幾秒內波動數百美元，幾天內波動數千美元，在目前都是很常發生的事。因此雖然我們都稱它為貨幣，但實際上它並不像貨幣一樣具有穩定的價值可以用做日常買賣交易（穩定幣如USDT、BUSD價格波動小，才更適合當貨幣），更多人重視的其實是比特幣供給需求上的稀缺性，類似於黃金或原物料的存在，但價值來自於眾多人們的心理認可，而非實用價值，這也是一種風險。

比特幣投資風險2：交易過程風險

比特幣交易方式可以自行私下交易（稱為點對點交易），這種作法有點類似於網購面交，但自行交易不但成本高，可能買賣在比較差的價位、交易風險高，可能一買一賣時，對方收了幣卻不給錢，或者收了錢不給幣。因此人們大多會透過交易所來交易，買賣的價格更好、流動性更佳，但交易平台本身也有風險，例如某些品質不佳的交易所可能會被駭客入侵，或是惡意倒閉等因素影響造成投資人損失。對此其實目前的解決方案，是只用最大的一些平台，除了流動性好、交易成本低、對駭客攻擊有保險保障等等，在安全機制上才有足夠的保障。

比特幣投資風險3：可能淪為非法交易工具、政策風險

比特幣因為有匿名性、交易隱密性，很多犯罪者會用它作非法交易，例如成為販毒、洗錢等工具。這點的風險在於，一旦虛擬貨幣逐漸被更多人認可後，它就有可能會成為各國政府的攻擊目標。當然，也有些國家的做法是讓國內發行中心化的虛擬貨幣，簡單來說就是類似的機制，但是被一定程度受到監控管理。

比特幣 (Bitcoin) 要怎麼買？

想要交易比特幣 (Bitcoin) 有很多種管道，以下列出的是比較適合一般人的方式：

1. 透過虛擬貨幣交易所買賣

透過虛擬貨幣交易所，是目前一般人可以用最安全、最低成本買進並持有比特幣的方法。會比自己在網路上和陌生人交易安全許多，成本也更低。一般買進方式一般會分成買進“現貨”，也就是直接持有比特幣，也有買進“合約”，也就是比較類似於期貨，不實際持有比特幣，且允許以槓桿方式交易，做多或放空。選擇比特幣交易所也很簡單，就是從全球最大那幾間去選即可。

2. 透過外匯交易商買賣

透過外匯交易商的買賣，其實並不真實持有比特幣，而是持有比特幣的差價合約 (CFD)，一般交易成本、持有成本都略高一點，也可以支援槓桿交易。外匯交易商並非適合長期持有比特幣等虛擬貨幣的管道，它適合不想持有比特幣、但想投機操作買低賣高的人，來做短線操作。大多數外匯交易商都有提供比特幣的差價合約商品，可以用你自己慣用的交易商找到對應商品即可操作

。如果對外匯交易商不熟悉，也是建議選擇全球知名且規模大的外匯交易平台。

比特幣 (Bitcoin) 快速重點整理

1. 比特幣 (Bitcoin) 是最早推出的虛擬貨幣，透過區塊鏈技術來運作。
2. 比特幣 (Bitcoin) 的區塊鏈技術，主要用來記載交易資料，每筆資料有安全性高、匿名的特性，不會被竄改資料，符合了去中心化概念。
3. 比特幣取得不易、具稀少性的特性，讓它成為炒作標的，是一種投機性商品。
4. 比特幣有匿名性、交易隱密性的特性，但也有各種風險。
5. 如果要買進比特幣，記得選擇全球規模排名靠前的交易所去買賣，相對會比較安全。

資料來自 維基百科及<https://rich01.com/what-is-bitcoin-0/> (市場先生)

