



作者：

Matt Kunke
研究分析師

日期：2021年11月10日
主題：數碼資產



GLOBAL X ETFs研究

比特幣：基礎資訊

2008年10月，密碼學郵寄列表中出現一份吹捧潛在革命性貨幣概念的神秘白皮書。中本聰（一個人或可能是一群人的化名）以此長達九頁的白皮書有條理地介紹全球第一個去中心化點對點貨幣系統。該文章聲稱任何有互聯網連接的人都可使用這個完全開放的系統，這些參與者將可隨時在全球範圍內交換價值，而無需可信的中介。

幾個月後，在2009年1月，比特幣軟件的第一個版本正式標誌著比特幣網絡的創建，在該報告中以大寫“B”引述。該網絡是**區塊鏈技術**的第一個應用，它是一個完全透明、共享和持續協調的分散式賬本，用於記錄交易和追蹤資產。該網絡的推出也標誌著比特幣的誕生。該報告以小寫“b”引述比特幣，它是一種可分割、可互換且易於轉移的數碼貨幣，可通過程序化定義的貨幣政策確保其稀缺性。

比特幣發展成熟：從個別化到主流

比特幣來得正是時候。它的推出適逢全球金融危機(GFC)的高峰期，當時許多人對持有他們資金的大型銀行和制定貨幣政策的政府失去了信任。比特幣代表一種「硬通貨」的新形式，無法由任何中心化實體進行調整或控制。這個特徵以及比特幣的稀缺性在金融危機之後引發了共鳴，因為世界各國政府實施大規模的量化寬鬆計劃，增加法定貨幣的供應。

在全球金融危機之後的幾年，比特幣的可信度穩步上升，但它在很大程度上仍然是一種個別化資產，容易出現波動和遭受懷疑。然後，新冠肺炎大流行及其所需的聯邦刺激措施使比特幣最顯著的特徵重新成為大眾焦點。熱切的投資者抓住這個機會更廣泛地參與比特幣和加密貨幣社區。雖然其價格仍大幅波動，批評者亦依然存在，但比特幣變得前所未有地主流，並正在鞏固其立足點。

今天，全球共有1,885萬個比特幣，總市值達1.23萬億美元。鏈上每天約進行280,000筆交易，平均交易量約達48億美元。¹



比特幣價格（對數尺度）

資料來源：Blockchain.com。截至 10/21/2021。



關於比特幣、其關鍵組成部分及其運作方式的知識

由於其不斷攀升的地位和潛在的投資影響，本報告將回答有關比特幣及其運作方式的基本問題。

- **什麼是比特幣？** 更可轉移的數碼版本黃金。
- **什麼是比特幣網絡？** 第一個真正開放、無需許可且信任最小化的金融生態系統。
- **什麼是節點？** 運行比特幣軟件並幫助保護網絡的電腦。
- **挖礦如何運作？** 以特殊節點解決數學難題，以在鏈中創建下一個區塊。
- **為什麼定義主區塊鏈是關鍵的？** 這可解決網絡延遲帶來的問題。
- **真正的結算何時進行？** 當交易獲得足夠數量的確認時。

本報告還會關注三個廣泛的問題，以討論比特幣在經濟環境中的定位。

- **比特幣提供什麼？** 獨立的信任來源和金融包容性。
- **我們該如何看待比特幣的監管環境？** 看為故事不斷發展的部分。
- **為什麼現在該投資比特幣？** 比特幣是專為如今這種經濟時期創建的資產。

比特幣：更可轉移的數碼版黃金

作為一種貨幣，比特幣是用戶網絡中一種供應有限的資產，用戶同意作為一種貨幣形式，其價值無法由單一實體控制或改變。比特幣是區塊鏈技術的第一個應用，在比特幣區塊鏈上以賬本餘額的形式存在。有別於傳統的支持法定貨幣，比特幣沒有實體紙幣或硬幣。

相反，比特幣用戶擁有私鑰，可以將其視為帳戶密碼。用戶還擁有公鑰和地址，是以加密方式從私鑰推算而來並與私鑰連接的。私鑰不可透過公鑰或地址查出，這是重要的。用戶地址類似於用於識別比特幣交易目的地的公共用戶名。從本質上來說，要使用比特幣，用戶需要與公鑰相關聯的私鑰和持有比特幣的地址。接收比特幣的用戶只需向發送人提供他們的比特幣地址。

公鑰和地址的推算

資料來源：Global X ETF, Mastering Bitcoin Programming the Open Blockchain。



不過，公開出示您的私鑰似乎會產生問題。比特幣是一種不記名的數碼資產，這意味著任何持有私鑰的個人都可以使用它。可以想像，被要求出示私鑰可能會讓任何人竊取相關地址中的比特幣。然而，使用比特幣實際上並無向網絡透露私鑰。使用比特幣會顯示一個數碼簽名，可以通過加密方式驗證簽名者擁有私鑰。

數碼簽名源自用戶的私鑰和擬議的交易資訊。由於公鑰和地址源自私鑰，高階數學可以驗證創建數碼簽名的私鑰與用於創建公鑰的私鑰是否相同。這種加密關係允許數碼簽名獨立驗證網絡上的比特幣所有權，為比特幣用戶提供使用他們比特幣的自由，同時防止不良分子使用他人的比特幣。

比特幣網絡：第一個真正開放、無需許可和信任最小化的金融生態系統

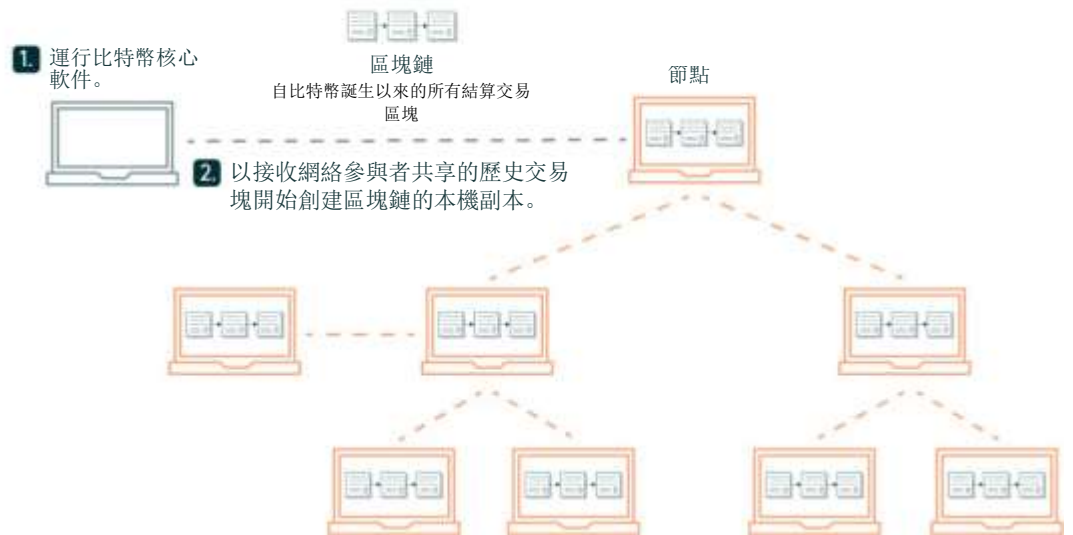
比特幣網絡允許在沒有金融機構等中介的情況下以點對點的方式轉移比特幣。該網絡利用完全透明的區塊鏈技術進行交易記錄和比特幣追蹤。網絡參與者可以通過遵循協議規則，並根據規則獨立驗證交易和區塊找到共識狀態，在該狀態下就區塊鏈的分散式賬本達成共識。

該網絡使用比特幣核心——一個包羅萬有的軟件包，允許完全自主的參與。當一台電腦運行該軟件時，它會連接網絡中的其他電腦，這些電腦稱為節點。

然後電腦開始接收自網絡創建以來出現的所有交易塊。電腦可以創建自己的分散式交易數據庫完整副本，稱為比特幣區塊鏈。比特幣核心內置一個錢包應用程式，讓參與者直接通過該軟件進行比特幣交易。錢包處理密鑰對的管理，追蹤比特幣餘額，並允許以創建數碼簽名使用比特幣。

運行比特幣核心軟件的電腦節點網絡

資料來源：Global X ETF。



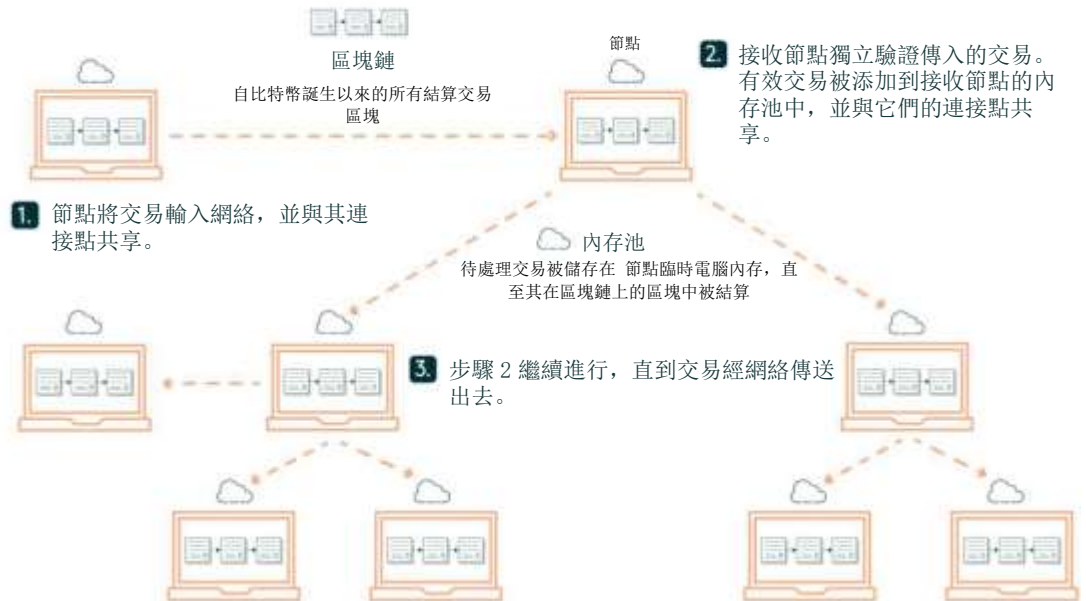
節點：運行比特幣核心的電腦，幫助保護網絡

在創建自己的區塊鏈副本後，節點會維護區塊鏈的最新副本，並在新交易和新區塊出現時實時聽取其對等點的訊息。節點根據協議規則獨立驗證所有交易和區塊，以幫助保護網絡，僅將有效的交易和區塊發送到其連接點。每個節點持續更新已驗證但待處理的交易池，稱為內存池。

當節點從其連接點之一接收新交易時，該軟件會根據一套綜合標準獨立驗證該交易的有效性，包括評估數碼簽名。如果交易有效，接收節點會將其儲存在其臨時電腦內存中，並將交易發送到它被連接的其他節點。此後，這個循環重複：另一個節點聽取、接收、驗證這筆交易，然後將交易發送到它們的連接點。這個循環是資訊如何在點對點基礎上經網絡傳送的方式。

通過比特幣網絡傳送交易

資料來源：Global X ETF。



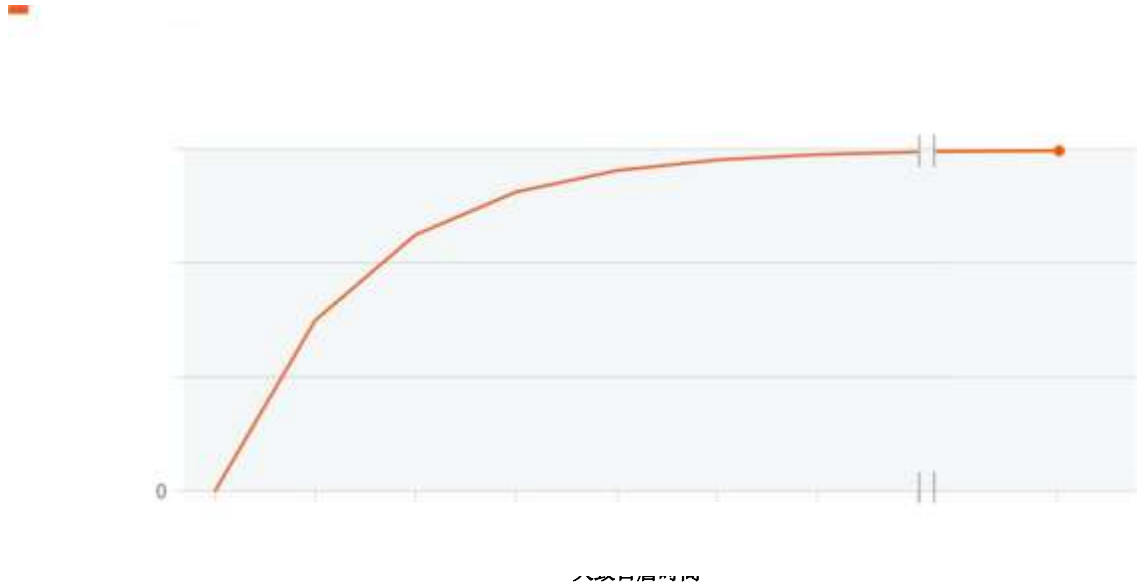
挖礦節點：解決數學難題以創建下一個區塊的特殊節點

所有比特幣節點都獨立驗證交易，但挖礦節點是一種特殊類型的節點，將交易聚合到在區塊鏈上被記錄的區塊中，以進行結算。從這個意義來說，挖礦節點是與別不同的，因為它們在鏈上創建區塊。區塊可以被視為交易的結算層。交易在節點之間被接續發送，並被儲存在臨時內存中。此時，當礦工將交易納入一個區塊時，它們基本上是待處理交易，直到在區塊鏈上被結算。

挖礦節點在競爭中投入大量計算資源，以成為第一個解決具挑戰性數學難題的節點。這個難題的解決方案被稱為工作量證明。這個難題是以原力計算解決的，礦工通過加密哈希函數迭代不同的輸入，以搜索稀有輸出或哈希。工作量證明很難找到，但任何節點都可以瑣細地驗證礦工是否投放了計算資源，以找到解決方案。只有具有有效數碼簽名的交易才被視為有效交易，同樣，候選區塊需要工作量證明才能成為有效區塊。

第一個解決這個難題的礦工可獲經濟激勵。首先發送具有有效工作量證明新區塊的礦工可獲區塊獎勵和該區塊內的所有交易費用。區塊獎勵是一種特殊交易，允許礦工向自己發送固定數量的新創造比特幣。這個過程被稱為挖礦，因為區塊獎勵代表第一次產生新的比特幣，類似於從地下開採的新黃金。

目前，區塊獎勵會創造6.25個新比特幣，現時相當於超過400,000美元。⁹然而，區塊獎勵每210,000個區塊或大約每四年減少50%，直至大約2140年，區塊獎勵將不再存在。這些減半事件推動比特幣的通貨緊縮貨幣政策。下一次減半預料將在2024年發生，每個區塊的獎勵將減至3.125個比特幣。



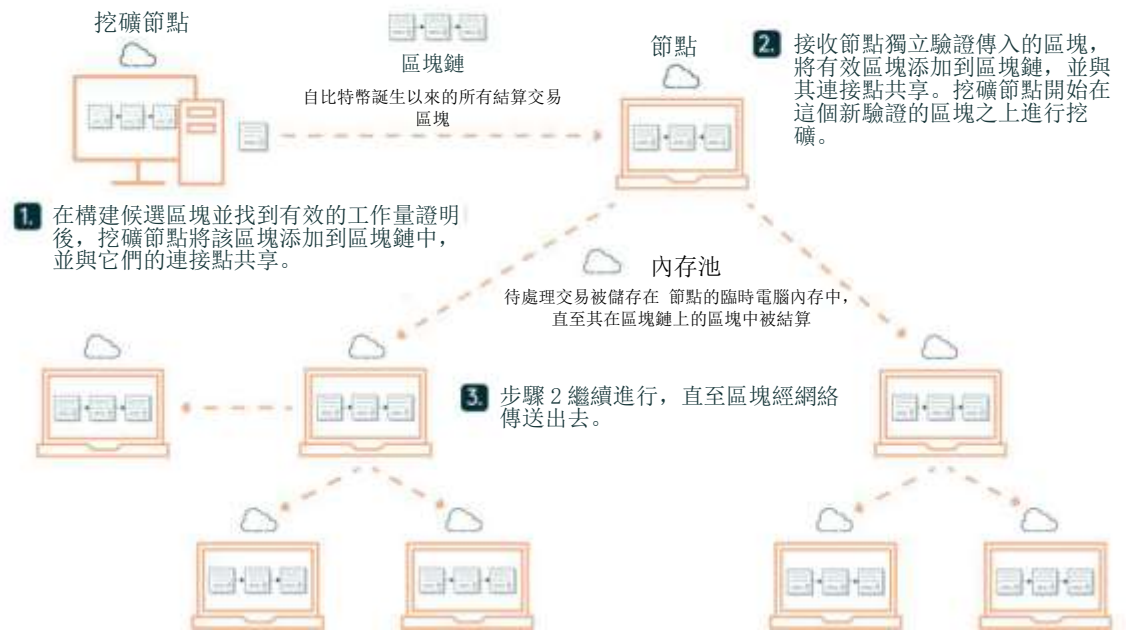
此外，當用戶在比特幣網絡上進行交易時，他們通常會支付少量交易費用，以激勵礦工將他們的交易納入區塊中，以進行結算。在網絡需求強勁的時期，交易費用可能會大增，因為它們代表比特幣消費者爭相讓其交易被結算。例如，2021年9月的平均交易費用僅為2.50美元，但在2021年4月的10天時間裏，平均交易費用達20-65美元，當時比特幣首次突破60,000美元，且網絡非常擁擠。³區塊中通常有1,500-2,500筆交易，交易費用通常只佔礦工解決區塊總報酬的一小部分。

一旦礦工解決了一個區塊，他們就會通過網絡傳送該區塊。每個節點驗證新收到區塊的有效性，然後將其添加到他們的區塊鏈副本中。收到新的有效區塊會重置挖礦遊戲。所有礦工創建一個新的候選區塊，並嘗試第一個解決與新收到區塊相關的難題。



經比特幣網絡阻止傳送

資料來源：Global X ETF。



比特幣核心軟件的設計讓這個挖礦難題平均每10分鐘被解決一次。為了達以上目標，隨著試圖解決難題的哈希率上升（下降），該軟件約每兩週調整難題的難度，以增加（減少）其挑戰性。因此，有別於開採貴金屬，比特幣的開採速度無法加快。換句話說，比特幣供應的增加是固定的，與比特幣的需求無關。對更多挖礦設備增加投資只會導致解決難題的計算量更大，從而保持比特幣發行率不變。

主區塊鏈：解決網絡延遲帶來的問題

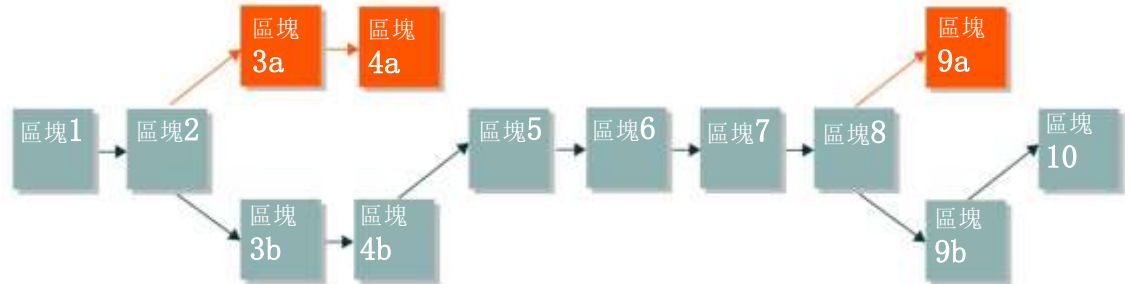
有一個問題可能會出現，就是兩個礦工幾乎同時解決工作量證明，並發送有效區塊。由於全球網絡的性質，資訊經其進行點對點流通，網絡延遲無可避免地導致各個節點接收資訊的時間稍有不同。該協議要求每個節點將最長的鏈標識為主區塊鏈，或更準確地說，將累積工作最多的鏈標識為主區塊鏈，以解決這種動態問題。例如，如果我們假設礦工甲和礦工乙幾乎在同一時間生產有效區塊，則礦工丙可能會先收到礦工甲的區塊，而礦工丁可能會先收到礦工乙的區塊。

這種情況可以在區塊鏈中創建一個臨時分叉，這意味著兩個區塊鏈都是暫時有效的，並且只有在未來區塊被添加到其中一個鏈之後，主鏈才能被識別。但是當礦工選擇在哪條鏈上形成後續區塊後，這種情況就可以很快被解決。在默認的情況下，礦工從他們收到的第一個有效區塊開始工作。所以礦工甲和礦工乙從一個區塊鏈中挖礦，而礦工乙和礦工丁則從另一個區塊鏈挖礦。

隨著更多區塊的生產，分叉鏈的雙方繼續同時解決工作量證明的概率迅速變為零。一旦一方先於另一方找到下一個區塊，生產這個區塊的鏈就會被視為主區塊鏈，而鏈的另一方將會根據協議規則被放棄。該協議規則允許節點找到共識，並就區塊鏈的狀態和進行的交易達成一致。下圖中的橙色區塊是有效的，但事後可見它們不是主鏈的一部分。主鏈以藍色表示。

區塊鏈中的臨時分叉

資料來源：Global X ETF。



真正的結算和不變性：當交易獲得足夠數量的確認時

當交易被納入一個區塊中時，它通常被視為已結算。但是由於某些情況會導致區塊鏈在短期內暫時分叉和重組，因此必須滿足某些條件才能實現真正的結算和不變性。

只有在獲得足夠數量的確認後，即在包含特定交易區塊之上在鏈中添加區塊，才能實現真正的結算和不變性。一個獲得六個確認的區塊通常被視為不可改變或不可更改。對於小額交易，一至三個確認通常被視為安全。由於區塊以引用前一個區塊哈希的每個新挖礦區塊被連接在一起，隨著被埋在下面區塊數量的增加，交易變得更加安全和不可改變。

例如，一個惡意分子想撤銷一個獲得六個確認的交易，他需要將六個區塊送返包含他們欲操縱交易的區塊。然後他們需要對該區塊以及分叉鏈上其他五個後續區塊重新挖礦，並分別找到這六個區塊的有效工作量證明。同時，所有遵守協議規則的良好參與者都正在挖礦和擴展先前定義的主區塊鏈。惡意分子需要控制整個網絡超過50%的計算能力，並持續足夠長的時間，才可克服與主鏈相比六個區塊的不足。

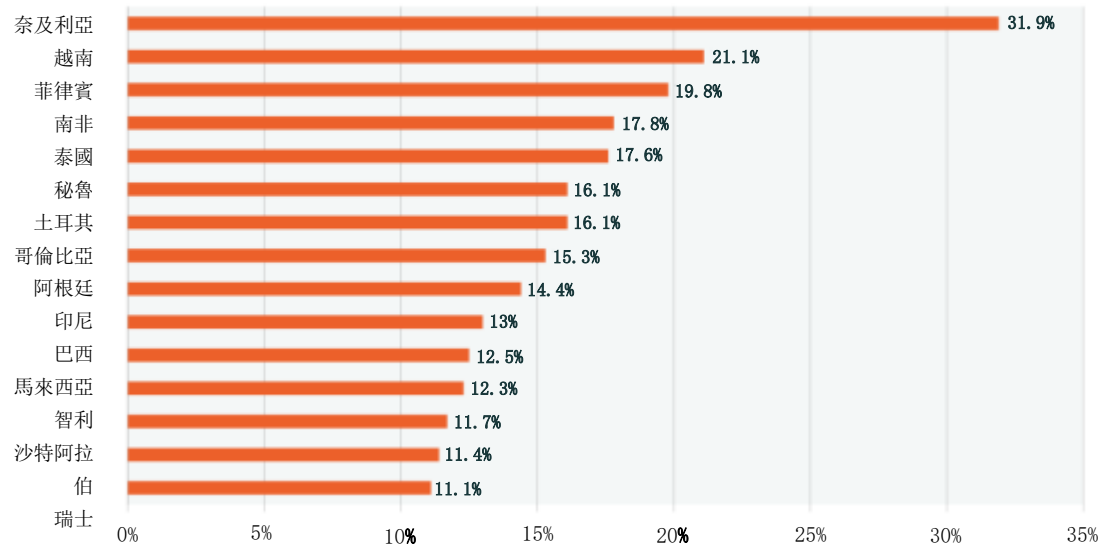
比特幣提供什麼：獲取和信任的獨立來源

比特幣網絡是一個金融生態系統，參與者不需要信任一個政府，以支持貨幣或負責任地管理貨幣供應。對於發達國家來說，這個特徵的重要性可能特別難以明白，儘管最近的經濟危機可能有助於理解。在保護投資者的強大監管框架內營運可信賴金融機構並不是全球平等享有的特權，尤其在新興經濟體。

比特幣網絡為沒有銀行賬戶和銀行賬戶不足的人群提供一種金融包容性機制，特別是在政治不穩定、腐敗或嚴重通貨膨脹的國家。市場和消費者數據公司Statista 2021年2月的一項調查表明，民眾使用加密貨幣頻率最高的前10個國家都是新興市場國家。尼日利亞領先，有32%的受訪者表示他們更廣泛地使用比特幣或加密貨幣，其次是越南（21%）和菲律賓（20%）。⁴

各國加密貨幣使用情況

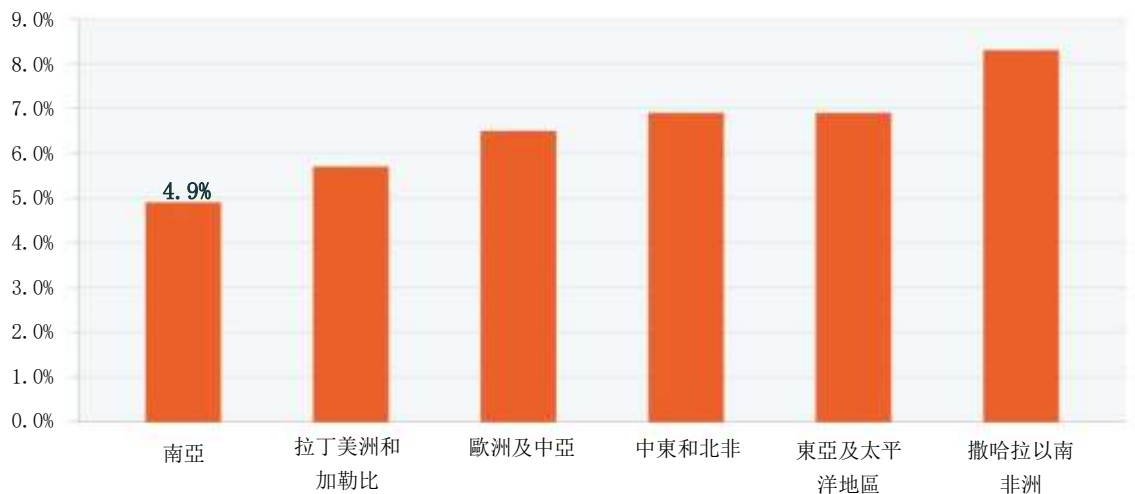
資料來源：全球消費者調查，截至 2021 年 2 月 28 日。



匯款市場是比特幣的另一個關鍵用例。與較發達的國家相比，匯款佔新興市場國家國內生產總值的比重不成比例。根據世界銀行的數據，交易費用導致全球平均匯款減少了6.4%。部分成本較高匯款渠道的費用可增加至10%以上。⁵

各地區平均匯款成本

資料來源：可在 <http://remittanceprices.worldbank.org> 查閱世界銀行的《全球匯款費用》。截至 3/31/2021。



對於某些新興經濟體來說，利用比特幣在國際上轉移財富可能是一種重要的成本節約措施。例如，薩爾瓦多是一個約有70%人口接收匯款的國家。政府決定成為第一個採用比特幣作為法定貨幣的國家，可能是一個值得注意的測試案例。據估計，比特幣每年可為該國節省4億美元的匯款費用。⁶

監管環境：故事不斷發展的部分

比特幣仍處於起步階段，與其他數碼資產一樣，在充滿不確定性而且錯綜複雜的監管環境中運作，該環境因國家和國家內的司法管轄區而異。例如在聯邦層面，美國的加密貨幣法規仍然很少，但各個州都有自己的規定，有些州比其他州更嚴格。紐約州金融服務部 (NYDFS) 的規定明顯比美國任何其他地方都嚴格。

由於世界各地的法規、分類和稅收待遇各不相同，因此很難評估比特幣的監管格局。隨著時間的發展，我們期望更明確的監管框架將被制定。更清晰的監管制度可降低風險，可能有利於比特幣發展，並鼓勵更多的參與。隨著比特幣的接受度不斷提高，未能實施審慎監管可能會在企業決定如何最好地利用比特幣運營方面扼殺本地創新。例如，美國最大加密貨幣交易所之一 Kraken 於 2015 年 BitLicense 框架實施後停止在紐約運營。⁷

過度監管的風險是一個考慮因素，但比特幣網絡的去中心化和全球性質可減緩監管過度的影響。我們認為 2021 年 9 月中國全面禁止加密貨幣只輕微干擾價格就是一個例子。⁸

為什麼現在該投資比特幣：比特幣是專為如今這種經濟時期創建的資產。

要了解比特幣吸引力日益增長的一個重要考慮因素，是它的形成年代適逢兩次具有深遠政治和社會影響力的歷史性經濟危機。這些危機凸顯了傳統金融生態系統的兩個最大問題：不獲信任和無法獲取。但比特幣的主要原則解決了以上問題。

- 比特幣是一個去中心化的網絡，允許參與者在全球範圍內交換價值，而無需可信的監管機構或金融中介。
- 區塊鏈技術允許網絡參與者遵循一套完全透明的協議規則，在分散式賬本上找到共識狀態。
- 數碼貨幣易於分割、可替代和可轉移，並通過程序化定義的貨幣政策確保其稀缺性，
- 只需互聯網連接即可參與。

這些屬性越來越能引發個人投資者的共鳴，尤其是在主流金融界。投資銀行和對沖基金現在紛紛對比特幣投入財務和人力資本，企業亦開始將比特幣納入資產負債表，投資者甚至包括大學。一個蓬勃的受監管比特幣衍生品生態系統也有助提升該領域的可信度。

2008 年 10 月最大的謎團不是中本聰的身份，而是比特幣最終可能在全球經濟中佔據的份額。十三年後，中本聰的身份仍然未明，但隨著人們對其越來越熟悉，比特幣相繼獲得合法性。畢竟，比特幣帶來擁有可驗證稀缺資產的潛力，加上日益擴張的全球用戶網絡，通常都能吸引投資者。

詞彙表

術語按出現次序列出。

密碼學：對在敵對行為存在的情況下安全傳送資訊技術的廣泛研究。請參閱公鑰密碼學。



比特幣網絡：運行比特幣核心軟件的電腦點對點網絡。比特幣網絡允許在無需可信中介的情況下轉移價值（比特幣）。

區塊鏈（鏈）：點對點共享和持續協調的分散式賬本，可進行交易記錄和資產追蹤，而無需可信的中介。網絡中的參與者稱為節點，根據網絡規則傳送交易和區塊，以供其他節點驗證。交易被聚合到記錄交易時間和順序的區塊之中。區塊與前一個區塊連接在一起，形成一個鏈，隨著每個後續區塊的加入而線性增長。區塊平均每10分鐘被添加到鏈中。

比特幣：一種在比特幣區塊鏈上完全作為賬本餘額存在的不記名數碼資產，是比特幣網絡的原生加密貨幣。

加密貨幣：一種數碼貨幣，其中交易會被驗證，並由依賴密碼學的去中心化系統維護記錄，而不是獲信任的第三方。

鏈上：指出現在實際區塊鏈上的交易。例如，當在中心化加密貨幣交易所進行交易時(如Coinbase)，中心化方只需將比特幣在他們為所有客戶維護的賬本上進行轉移。在資產從平台中被提取之前，這些交易實際上不會在區塊鏈上產生交易。

私鑰：代表不記名數碼資產比特幣的所有權；類似於帳戶密碼。私鑰用於創建數碼簽名，以驗證比特幣所有權。如果要找到相關的私鑰，任何人都可以獲取一個地址的比特幣。

公鑰：以數學方式從私鑰推算出來。要使用與之相關的比特幣，必須公開私鑰。數碼簽名根據公鑰進行驗證，以驗證潛在消費者是否控制與公鑰關聯的私鑰。另外，公鑰用作加密哈希函數的輸入，以生成地址。

地址：以數學方式從公鑰推算出來；類似於用於識別比特幣交易目的地的公共用戶名。

數碼簽名：以數學方式從私鑰和交易的哈希值推算出來。數碼簽名證明私鑰和相關公鑰的所有權，而無需透露私鑰。數碼簽名允許獨立驗證網絡上的比特幣所有權，為比特幣所有者提供使用比特幣的自由，同時防止不良分子使用他人的比特幣。

比特幣核心：執行比特幣協議和比特幣網絡所有方面工作的共享資源電腦軟件。

節點：運行比特幣核心以維護自己區塊鏈副本的電腦。節點以根據協議規則獨立驗證所有交易和區塊參與網絡的安全，只將有效的交易和區塊發送給其連接點。

公鑰密碼學：也稱為非對稱密碼學，使用兩個不同但數學上相關的密鑰，一個用於加密，另一個用於解密。這是比特幣網絡中使用的特定密碼學，其中公鑰用於接收比特幣，私鑰用於簽署交易，以使用比特幣。

點：網絡中相互直接連接的節點。



內存池：也稱為mempool，指節點在於區塊結算之前儲存在其本機電腦內存上已驗證但待處理交易的池。

挖礦節點：一個特殊的節點子集，將交易聚合到在區塊鏈上被記錄的區塊中，以進行結算。挖礦節點基於加密哈希函數爭相成為第一個解決具挑戰性數學難題的節點。礦工將大量計算資源投放於通過加密哈希函數盡快以原力計算不同輸入的結果。

工作量證明：基於礦工爭相解決加密哈希函數的具挑戰性數學難題解決方案。由於加密哈希函數的特性，要找到工作量證明非常困難，但任何節點都可以瑣細地驗證礦工是否投放了計算資源，以找到解決方案。當兩個區塊被同時開採時，工作量證明有助於解決分歧，並以使人望而卻步的歷史區塊高操縱成本保護網絡。

加密哈希函數：一種單向函數，可用於將任意長度的數據繪制成決定性的固定長度結果。加密哈希函數包括以下關鍵特性：1)它們是可重複的；對於任何輸入，結果輸出（哈希）始終相同。2)它們是單向函數，不可從給定的輸出推算出輸入。3)函數具有光學隨機特性，不可通過對輸入進行小幅調整來定制輸出。挖礦過程依賴盡快重複計算加密哈希函數的結果，以達到特定的輸出。這些函數還用於從公鑰推算地址。

哈希：加密哈希函數的輸出。

候選區塊：礦工試圖通過找到有效的工作量證明來添加到區塊鏈中的待處理交易區塊。找到工作量證明後，候選區塊會成為有效區塊，並被添加到鏈中。此時，礦工形成一個新的候選區塊，他們嘗試第一個解決與新收到區塊相關的難題，並將下一個有效區塊添加到鏈中。礦工通常以選擇內存池中交易費用最高的交易形成候選區塊。

區塊獎勵：一種特殊的交易，允許礦工向自己發送固定數量的新創造比特幣，作為解決區塊的經濟獎勵。目前，區塊獎勵為每區塊6.25比特幣。區塊獎勵是創造新比特幣的唯一途徑。

交易費用：用於激勵礦工將其交易納入一個區塊以進行結算的小額交易費用。交易費用通常很少，但在網絡嚴重擁擠的時期會變得相當可觀。

減半：將區塊獎勵減少50%。每210,000個區塊或大約每四年發生一次減半事件。下一次減半預料將在2024年發生，每個區塊的獎勵將減至3.125個比特幣。

難度：在特定時間點挖礦比特幣區塊難度的衡量。比特幣網絡設計為區塊平均每10分鐘被開採一次，隨著礦工背後的計算能力增加（減少），難度也會增加（減少），以確保區塊繼續平均每10分鐘被開採一次。難度每2,016個區塊被調整一次，或平均約每兩週調整一次。該軟件僅計算挖礦2,016個區塊所需預期分鐘（20,160分鐘）與挖礦最後2,016個區塊所需實際分鐘的比率，並按此比率向上或向下調整先前的難度。

哈希率：對在某個時間點保護比特幣網絡總計算能力的估計。它以網絡中所有礦工每秒匯總計算的哈希數量衡量。比特幣網絡哈希率在2021年達到峰值，每秒約180百京個哈希。



主區塊鏈（主鏈）：根據底層區塊的難度累計工作量最多的區塊鏈。主鏈通常擁有最多區塊。

分叉：從一條鏈分叉成兩條不同鏈的區塊鏈。這些鏈共享相同的歷史，但達到了它們新區塊不再相同的一個點。當兩個礦工同時挖礦一個區塊時會出現臨時分叉，但協議規則會令它們重回單個主鏈之上。協議規則被更改或社區對協議規則存在分歧時往往會出現更多的永久性分叉，導致運行軟件出現多個分叉版本。

不變性：不可改變的狀態或條件。

確認：在特定交易被納入一個區塊中之後添加到區塊鏈的區塊數量。第一次確認是當交易被納入一個區塊中時。每次新的有效區塊在鏈上被挖礦，都會添加一個確認。

1. Blockchain.com, 截至2021年10月21日。
2. Coinmarketcap.com, 截至2021年10月21日。
3. lockchain.com, 截至2021年10月21日
4. Statista 全球消費者調查, 截至2021年2月28日
5. Remittance Prices Worldwide, “Remittance Prices Worldwide Quarterly” (全球匯款費用季刊), 截至2021年3月31日
6. CNBC.com, “El Salvador’s new bitcoin plan could cost money providers like Western Union and others \$400 million a year, says President Bukele” (薩爾瓦多的新比特幣計劃可能使西聯匯款等貨幣供應商每年少賺4億美元, 納伊布·布格磊總統表示), 截至2021年9月9日
7. Blog.kraken.com, “Farewell, New York” (再見, 紐約), 截至2015年8月9日
8. Coinmarketcap.com, 截至2021年10月21日

比特幣和比特幣期貨是相對較新的資產類別。它們面臨獨特而重大的風險，並且以往一直受顯著價格波動的影響。以上投資的價值可能會在沒有警告的情況下大幅下跌，甚至跌至零。閣下應為失去全部投資作好準備。

投資涉及風險，包括可能損失本金。多元化並不能確保盈利或免遭虧損。此資訊無意作為個人或個性化的投資或稅務意見，並且不得用於交易目的。有關您的投資及 / 或稅務情況的更多資訊，請諮詢財務顧問或稅務專家。

本材料代表對特定時間點市場環境的評估，並非對未來事件的預測，亦非對未來結果的保證。此資訊無意作為個人或個性化的投資或稅務意見，並且不得用於交易目的。有關您的投資及 / 或稅務情況的更多資訊，請諮詢財務顧問或稅務專家。

比特幣在很大程度上不受監管，比特幣投資可能比受監管的投資更易受到欺詐和操縱。比特幣和比特幣期貨受價格快速波動的影響，包括由網紅和媒體行動和聲明帶來的波動。

