GLOBAL X ETF 研究

# 以太坊：基礎資訊

作者：
數碼資產團隊
GLOBAL X 研究

日期：2022 年 3 月 1 日
話題：數碼資產

**編者按：**我們為所有以橙色標註的術語提供了一個詞彙表。

2009 年比特幣的誕生標誌著首次成功應用區塊鏈技術作為一種有限供應的去中心化貨幣。重要的是，它面向任何人開放。比特幣啟發了開發人員發掘更廣泛的、由區塊鏈技術提供的安全性、透明度和可擴展性支持的工具與應用。比特幣網絡為交易媒介提供了基礎，與此同時一位年輕程式編寫員將它視為一種能夠挑戰中心化經濟實體的方法。

2013 年，年僅 19 歲的 Vitalik Buterin 發表了以太坊白皮書，其中他介紹了一種新穎的通用區塊鍊網絡，允許開發人員構建可編程條件和應用程式。實質上，Buterin 創造了一個可編程貨幣系統，其徹底改變了人們思考、創造和佈署區塊鏈技術的方式。

## 關於以太坊、其關鍵組成部分及其運作方式的應知事項

由於其不斷攀升的地位和潛在的投資影響，本報告將回答有關以太坊網絡的基本問題。

- **什麼是以太坊？**具有智能合約功能的去中心化區塊鏈。
- **什麼是以太幣 (ETH)？**以太坊的原生貨幣。
- **什麼是節點？**運行以太坊客戶端以驗證交易及區塊的電腦。
- **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。
- **真正的結算何時進行？**當交易獲得足夠數量的確認時。
- **什麼是智能合約，它們為什麼重要？**基於預定義條件的可編程合約。
- **什麼是去中心化應用程式 (DApp)，它們為什麼重要？**使用智能合約構建的應用程式。
- **以太坊網絡前景如何？**向可以使網絡更具可擴展性和環境友好性的共識機制的過渡。
- **為什麼 ETH 有價值？**它決定了網絡的經濟。
- **為什麼現在是發展以太坊的好時機？**最大及最被廣泛採用的智能合約區塊鏈提供了價值潛力與增長。

## 以太坊：具有智能合約功能的區塊鏈。

2015 年 7 月以太坊的面世推出了一種新穎的區塊鏈，內置圖靈完備語言，它是可用於嵌入邏輯並完成比簡單支付更高階的交易的一種編程語言。這種語言的引入使開發人員能夠創建應用程式並將其整合到以太坊中，作為能夠寄存智能合約和去中心化應用程式 (DApp) 的開放生態系統的基礎層。

智能合約構成了以太坊的大部分價值主張。智能合約具有預定義的準則，可以根據編程條件自動執行回應，並將協議記錄在區塊鏈中。智能合約消除了對第三方中介的需求。

DApp 是以智能合約可編程性創建和配置的前端、面向用戶的應用程式。這些可編程合約用於創建去中心化金融服務應用程式 (DeFi) 和非同質化代幣 (NFT)，它們代表了獨特資產的數碼所有權。智能合約還用於創建和協調被稱為去中心化自治組織 (DAO) 的去中心化管治組織。在網絡內，去中心化應用程式的集合代表了以太坊生態系統。

以太坊網絡使用完全透明的區塊鏈技術在賬本上記錄交易和追蹤狀態。網絡參與者可根據協議規則獨立驗證交易和區塊找到共識狀態，也就是在該狀態下就區塊鏈的分散式賬本達成共識。區塊是由一連串交易聚合而成的獨立數據結構，包含對其父區塊或上一個區塊的索引。

以太坊虛擬機 (EVM) 是以太坊的分佈式狀態機器，負責維護網絡的數據結構與標準。實質上，EVM 定義了用於計算區塊之間狀態轉換的規則。狀態轉換可能是賬戶餘額的簡單變動，也可能是更複雜的智能合約交互產生的結果。

## 以太幣 (ETH)：推動以太坊網絡發展的原生加密貨幣

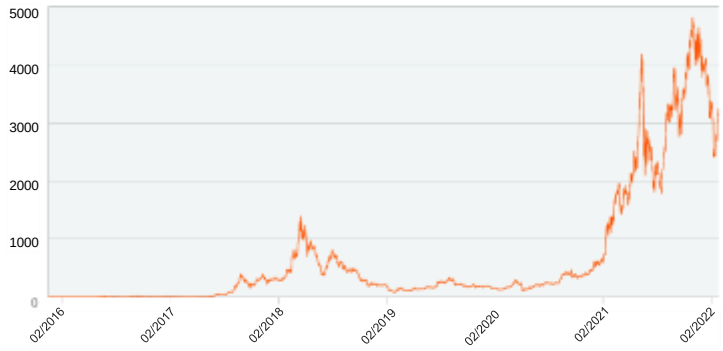
以太幣 (ETH) 可用於發送簡單的支付，類似比特幣，但相比貨幣它更類似於商品，因為它主要用於在以太坊上支付去中心化計算。以太坊上的所有交易和智能合約配置都需花費以 ETH 支付的不固定費用。簡單的支付通常比智能合約互動便宜。這種支付方案創造了對 ETH 的自然需求，因為以太坊 DApp 終端用戶必須購買 ETH 才能與平台互動。

ETH 沒有實體代表；它是擁有相應私鑰的人所擁有的數碼不記名資產。與比特幣類似，以太坊使用公鑰密碼學和數碼簽名來防止不良行為者花費他人的 ETH。如需更深入地了解公鑰密碼學和數碼簽名，請參閱比特幣：基礎資訊。

ETH 於 2014 年 9 月 2 日首次發售，價格為每比特幣 (BTC) 2,000 ETH。目前，ETH 是第二大加密貨幣，總市值為 3,560 億美元。[1]

**今日以太幣 (ETH) 價格**

資料來源：Etherscan.io 截至 2022 年 3 月 1 日




## 節點：驗證交易和保護網絡的電腦

節點是在以太坊網絡運行以太坊客戶端的電腦。以太坊客戶端是執行以太坊協議或其網絡規則的軟件。以太坊網絡是由連接的節點所聚合，每個節點在添加到區塊鏈之前皆會驗證其所接收到的交易和區塊在協議規則下是有效的。

**節點互連網絡**

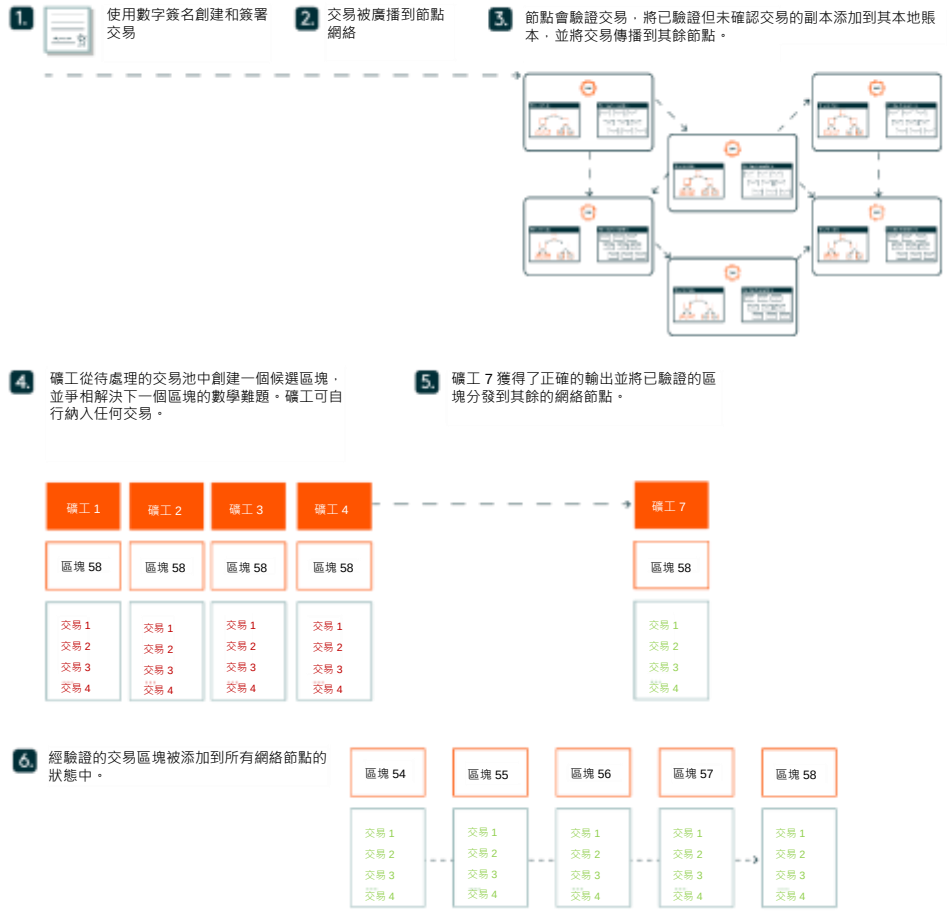
資料來源：Global X ETFs

交易會改變網絡內數據的狀態，它們通常涉及數碼資產的轉移或智能合約的執行。所有交易都必須包含以 ETH 計價的交易費用，稱為礦工費 (Gas fee)，它代表在區塊鏈上發佈、驗證、執行和存儲交易的成本。

每當一筆交易以用戶的私鑰進行數碼簽署時，它就會被廣播到連接節點的網絡。當節點接收新交易時，以太坊客戶端會根據一套在協議規則概述的綜合準則獨立驗證該交易的有效性，包括評估數碼簽名。如果交易為有效，則節點將保存交易在其本地待處理交易池中，並進一步將其傳播到其所有比鄰節點。這種相互連接的節點網絡使所有參與者在幾秒鐘內就可以分發、驗證和記錄交易。

## 以太坊交易詳細解說

資料來源：Global X ETFs



## 挖礦節點：解決數學難題以創建下一個區塊的特殊節點

所有以太坊節點均獨立驗證交易，但挖礦節點（礦工）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，挖礦節點因為在鏈上創建交易區塊而與別不同。

每個節點都保持一個經驗證但待處理的交易池，稱為內存池。一旦礦工將交易包含在已開採的區塊中，交易就會從內存池中刪除。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，這是一種確保網絡完整性的共識機制。

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值。以太坊依賴於與比特幣不同的加密哈希函數，而礦工之間並不直接競爭。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。只有具備有效數碼簽名的交易才被視為有效交易，同理，候選區塊需要工作量證明才能成為有效區塊。在所有其他參與者之前通過工作量證明達到特定輸出，可讓礦工驗證、記錄和傳播候選區塊。

一旦礦工成為第一個解決下一個區塊的數學難題的參與者，他們就會通過網絡廣播已驗證的區塊。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。所有礦工都會創建一個新的候選交易區塊，並嘗試成為第一個解決將包含在區塊鏈中下一個區塊的難題。區塊時間通常在 12 到 14 秒之間，決定了新區塊的持續流動。此外，區塊大小是有限的，並非所有待處理交易都包含在一個區塊中。

第一個解決這個難題的礦工可獲經濟獎勵。首先發送具有有效工作量證明新區塊的礦工可獲 2 ETH 的區塊獎勵和該區塊內的一部分礦工費。此外，通過設置其區塊中的交易順序並由於搶先交易策略，礦工可以產生稱為礦工可提取價值 (MEV) 的增量收入流。

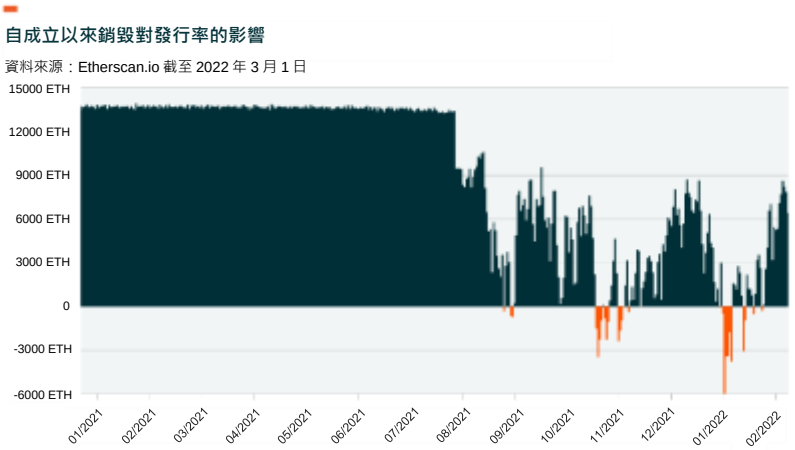
區塊中的礦工費可以分拆為基本費用和小費，兩者的價格都會隨著區塊空間需求而波動。小費會作為優先將交易包含在區塊中的激勵而直接支付給礦工。基本費用類似股票回購，它會被銷毀並且相應的 ETH 將從循環供應中移除。

以太坊改進方案 (EIP) 旨在激勵網絡參與者和建設者不斷改進以太坊網絡。其中一個方案有關礦工費結構。它於 2021 年 8 月隨以太坊改進方案 1559 (EIP-1559) 實施，在網絡使用與 ETH 發行之間建立了直接關聯。

EIP-1559 為 ETH 持有者創造價值，因為銷毀機制降低了淨供應發行率。隨著更多的交易在鏈上進行，會消耗更多的 Gas，這有可能減少或消除區塊獎勵產生新 ETH 供應的影響。如果網絡需求高並

且銷毀機制超過了由區塊獎勵產生的新發行，ETH 可以成為一種通縮資產。迄今為止，自 EIP-1559 推出以來已銷毀超過 190 萬 ETH，使 ETH 的淨發行量減少了 68%以上。[2]

NFT 日漸流行，其產生的交易量形成對區塊空間的更多需求，從而增加了被銷毀的 ETH 數量。自 EIP-1559 推出以來，NFT 市場 OpenSea 一直是消耗礦工費的最大貢獻者，總計 230,041 ETH。[3]




## 真正結算：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結算。

在獲得足夠數量的確認後實現真正結算，即在包含特定交易區塊之上在鏈中添加區塊。由於區塊以引用前一個區塊哈希的每個新挖礦區塊而相互連接，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。順帶一提，流行的中心化交易所通常認為交易在記錄 20 到 50 次確認後才有效，而以太坊區塊時間應該只需要幾分鐘。

若一個惡意分子想撤銷一個交易，他們需要返回包含他們欲操縱交易的區塊。因此，如果一筆交易有 50 次確認，他們將需要返回 50 個區塊。他們需要對該區塊以及分叉鏈上其他後續區塊重新挖礦，並分別找到每個區塊的有效工作量證明。同時，所有遵循協議規則的良好分子都在進行挖掘和擴展主鏈，它就是其上累積挖掘工作最多的鏈。

惡意分子需要控制整個網絡超過 50% 的計算能力，並持續一段足夠時間，才可克服與主鏈相比的區塊不足。此外，惡意分子將面臨重大風險，因為若行動失敗他們將浪費電力而沒有獲得任何 ETH 獎勵。

## 智能合約：DApp 的可編程基礎架構

智能合約提供了通過遵循 EVM 標準的特定編程語言將自動執行程序和協議編寫入以太坊的能力。開發人員可以使用專有的編程語言 Solidity，該語言的創建是為了方便不太高階的參與者接觸編程工具。開發人員還可以使用更高階的語言，例如 Vyper 和 Yul。

換句話說，智能合約是基於代碼以編程方式執行的合約。嵌入在合約中的數據饋送、條件、規則和協議會自動觸發預定義的結果，而無需一個受信任的中介來執行合約。任何去中心化應用程式都可以配置智能合約並組合功能，例如支持資產交換或借貸原語。

通過將合約作為交易提交來啟動和配置以太坊智能合約。它們還有 ETH 餘額，一旦滿足合約條件，就可以通過網絡觸發交易。由於網絡是開源的，因此提供了一個已執行的智能合約庫供開發人員參考，從而增強了應用程式開發的可組合性。

智能合約通常包含現實世界的數據饋送作為輸入變數來決定合約的輸出。Oracle 是促進區塊鍊和外部系統之間的連接和互操作性的媒體。Oracle 允許根據非區塊鏈原生的輸入數據來執行智能合約。常見例子包括價格數據、天氣數據、選舉結果、物聯網 (IoT) 感應器讀數、了解您的客戶 (KYC) 標準的身份驗證以及可驗證的隨機函數。

由於 Oracle 提供的數據可以決定許多智能合約的輸出，因此允許中心化實體提供這些信息將違背使用無需信任的區塊鏈這一目的。Chainlink 是旨在解決這個問題的去中心化 Oracle 網絡的優秀案例。它依賴於一個獨立的 Oracle 節點網絡，這些節點在經濟激勵下以一種無需信任的方式在鏈上提供準確的真實世界數據。

## DApp：使用智能合約構建的應用程式

智能合約允許去中心化應用程式創建具有不同用例和規則的協議。DApp 使用以太坊區塊鏈作數據儲存及保安，並使用智能合約技術作應用程式邏輯。實質上，DApp 就像一個在網絡上寄存具有用戶界面的應用程式，但是在去中心化電腦網絡上運行的智能合約促進了 DApp 的後端計算。

此特性為 DApp 提供了韌性，因為代碼的執行不依賴一個中心化的雲供應商。以太坊網絡包括一系列 DApp，包括金融應用程式、管治架構、供應鏈管理項目、文件儲存和非同質化代幣化計劃。

去中心化金融服務應用程式在以太坊 DApp 生態系統中非常突出。其中一些 DeFi 協議具有原生代幣，許多頂級 DeFi 應用程式均符合 ERC-20 標準。USDT、USDC 和 DAI 等流行的穩定幣也使用

ERC-20 代幣標準。ERC-20 標準允許開發人員在相同的準則和兼容性框架下構建可互操作和同質化代幣，這為應用程式和智能合約的可組合性創造了最佳條件。

DeFi 應用程式對許多傳統的金融交易進行去中心化，例如借貸、資產交換、衍生品、保險和資產管理。當今最流行的兩個應用程式是 Uniswap 和 Aave。Uniswap 是一家非託管、開源、去中心化的自動化莊家，為希望交換資產的買賣雙方提供流動性池。Uniswap 允許個人通過將流動性存入交易池中來充當莊家，藉提供流動性從用戶的交易中賺取交易費用。2022 年 1 月，Uniswap 流動性池的交易額約為 580 億美元。[4]Aave 是一個去中心化、非託管流動性和貨幣市場，用於借貸數碼資產。例如，市場參與者可以使用 Aave 以其數碼資產獲得即時資產抵押貸款。

另一個流行的智能合約應用程式包括另一種以太坊代幣標準。ERC-721 實現了非同質化代幣創建的標準化。NFT 是無法複製、不可互換的代幣，這意味著沒有兩個代幣是相同的。迄今為止，數碼藝術是 NFT 的主要用例。但鑑於其潛在應用範圍廣泛，我們預計在如游戲產業的邊玩邊賺概念、房地產代幣化、票務、體驗、身份標籤、獨家存取、會籍和供應鍊時間戳等領域，將出現更多有創意的 NFT 應用。

鏈上去中心化自治組織 (DAO) 也將以太坊的區塊鏈基礎架構和智能合約技術用於投票權和決策。流行的用例包括 DeFi DAO，參與者可以數碼資產換取治理型代幣。代幣持有者可為累積資產庫的資產分配、投資決策進行投票，這些分配獎勵可支付給代幣持有者。

## 以太坊網絡前景如何？促進可擴展性的更新

考慮到以太坊網絡的發展，開發人員已就一個包含數個升級的路線圖達成一致。這些更新包括共識機制的變動，試圖讓網絡更具可擴展性和環保性。

### *從工作量證明到權益證明的轉變*

以太坊共識層（前稱為以太坊 2.0）是以太坊的升級路線圖，其中包括在網絡轉變到新狀態時所需的改變。此升級令到可擴展性提高，且對硬件和能源需求更爲適度。

工作量證明提供了強大的安全保證，但它需要大量的硬件和能源。相比之下，權益證明需要最少的能源。權益證明共識中的驗證者類似工作量證明共識中的礦工。驗證者負責對交易進行排序、創建新區塊並認證其他驗證者創建的區塊。

權益證明並非使用電力來防止網絡操縱，而是要求驗證者擺放 ETH 作為抵押品以保護網絡。當驗證者擺放他們的資產時，他們知道如果他們惡意行事或未能履行職責，他們的資產將被沒收，這個過程被稱為罰沒。罰沒的風險刺激驗證者遵循協議規則並為網絡的最佳利益行事。要成為驗證者，市

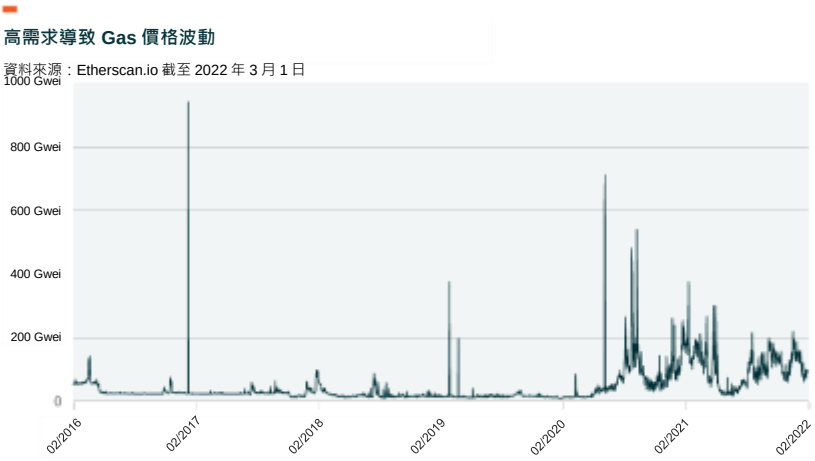
場參與者必須質押 32 ETH。較小的市場參與者可以通過 Lido 等平台參與流動質押池，將少量的 ETH 聚合成 32-ETH 的增量，並相應地分配獎勵。

驗證者可以分為兩類：提議者和認證者。提議者是從一組驗證者中隨機選擇出來以便提議鏈中的下一個區塊。未被選為提議者的驗證者必須認證該提議。認證者審查提議的區塊並認證它在協議規則下是有效的。提議者和認證者的參與將獲得 ETH 獎勵。但是，如果他們惡意行事或未能履行職責，他們的質押資產將面臨風險。明顯的惡意行為或蓄意勾結將導致驗證者失去全部質押品。惡意較少的行為，例如由於服務器中斷而未能驗證，可能導致只有一小部分質押品被罰沒。

*擴展以太坊的解決方案*

隨著越來越多的 DApp 而日益增長的用戶群互動，以太坊網絡的容量已達限制。近年來，對以太坊有限區塊空間的更大需求加劇了 Gas 價格的波動性，使該網絡對所有人來說（除最大的市場參與者以外）都過於昂貴。

以太坊礦工費以 Gwei 計算，每 Gwei 等如十億分之一 ETH。高昂的礦工費導致用戶尋求容量替代的方法和降低成本。




EIP-1559 提供了更好的定價結構，具有更高的 Gas 價格可預測性，但它不保證 Gas 價格會下降。目前，以高成本效益方法擴展以太坊的解決方案包括鏈上擴展和鏈下擴展。鏈上擴展涉及在以太坊基礎層尋找方法改善成本和吞吐量。例如，作為以太坊共識層推出的一部分，以太坊網絡計劃引入分片鏈。分片鏈是指將一個數據庫水平拆分為多個切面以減少網絡擠塞並增加每秒交易量的過程。

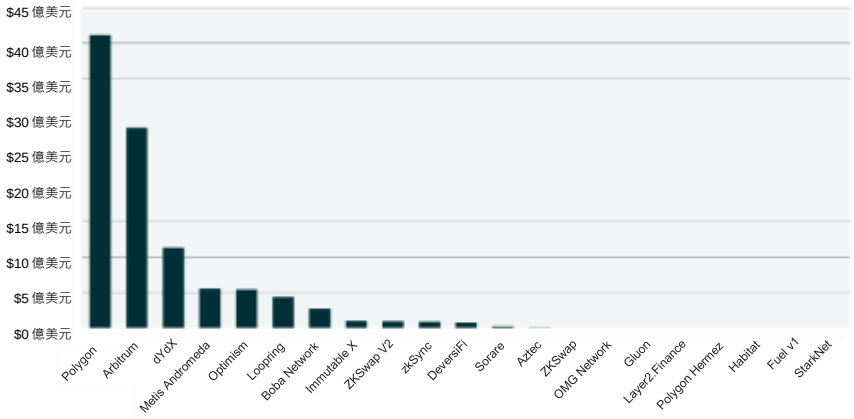
向權益證明的轉變是分片的先決條件。在工作量證明系統中，分片會削弱安全特性，讓惡意礦工更容易破壞個別分片。

鏈下擴展旨在在以太坊之上構建替代擴展協議，稱為第一層 (L1)。在以太坊以外實施的解決方案稱為第二層 (L2)。第二層最終從主網（主要的以太坊網絡）獲得安全性。這些應用程式一般以單獨的狀態處理個別交易，並根據解決方案的類型以各種方式與以太坊主網通信以進行結算。

L2 解決方案由於可幫助更快、更便宜地處理小額交易，同時使用以太坊主網實現安全性和透明度而越來越受歡迎。Polygon 是主要的 L2 解決方案之一，它可幫助開發人員以最低的交易費用構建可擴展的 DApp。像 Solana 這樣的競爭型智能合約平台，已經成功以一定程度的去中心化來提高交易吞吐量，但是，L2 解決方案提供了一種廉價的交易方式，同時保留在以太坊生態系統中。L2 在其平台上擁有相當數量的總鎖定價值 (TVL) 或加密資產的總價值。

**第二層解決方案生態系統擁有 100 億美元的總鎖定價值**

資料來源：DeFillama.com 與 L2beat.com 截至 2022 年 3 月 1 日




## ETH 的價值：它為網絡培育了一種增長導向型的經濟

ETH 作為結算貨幣，其價值來自於對以太坊網絡的需求。ETH 通常用於：

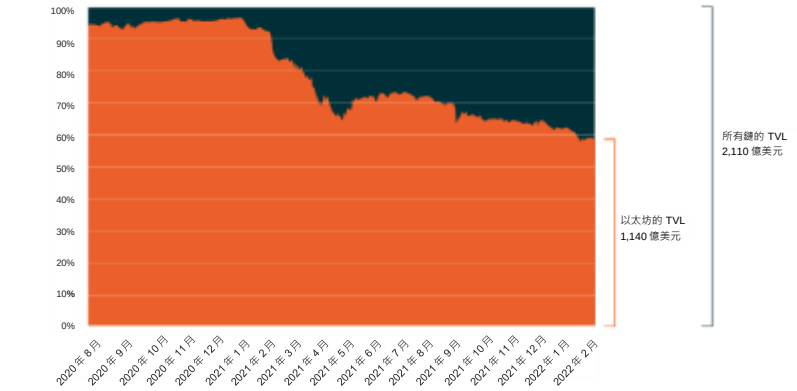
- 支付交易費或礦工費。
- 與 DeFi DApp 互動。
- 支付作將智能合約配置到區塊鏈中的費用。

- NFT 市場和交易的基本記賬單位。

以太坊在 DApp 鎖定約 1,140 億美元總價值，領先於加密貨幣領域。[5] 在 DeFi 中，總鎖定價值是一個重要指標，因為它可以洞識應用程式中存放的貨幣價值，並作為衡量情緒和增長的可靠指標。在協議中鎖定資產顯示生態系統中的增長、效用和用戶信念。此外，約 970 萬 ETH，相當於約 280 億美元，被鎖定在權益證明驗證者合約下以保障網絡的將來狀態：進一步減少流通中的 ETH 數量。[6]

**以太坊在 DeFi 鎖定 2,110 億美元總價值處領先地位**

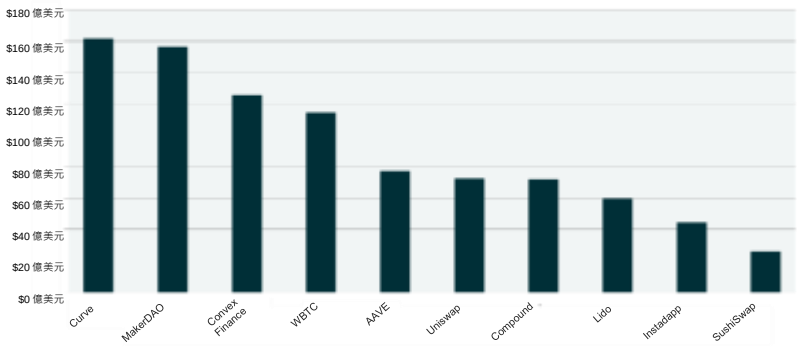
資料來源：DeFillama.com 截至 2022 年 3 月 1 日




以太坊的優點在於總鎖定價值分佈在許多 DeFi DApp 中。

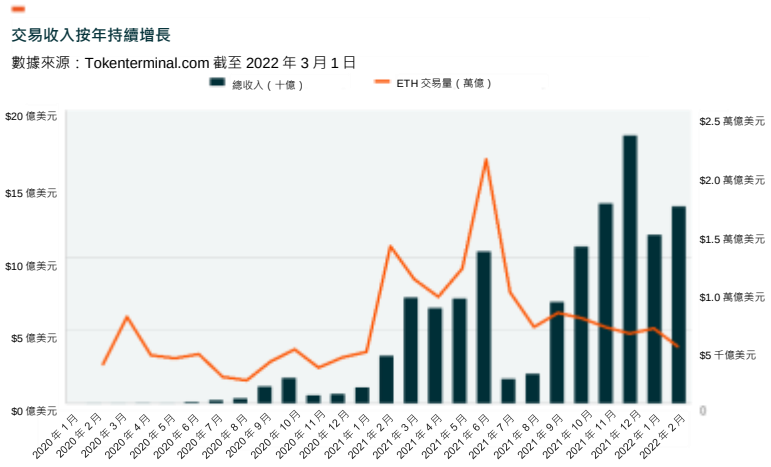
**讓我們看看頭十大貢獻者在以太坊智能合約 DApp 中鎖定的 1,140 億美元總價值的分佈**

數據來源：DeFillama.com 截至 2022 年 3 月 1 日




此外，錢包數量和每日交易數量等鏈上指標隨時間日益增加，顯示對以太坊生態系統的需求。交易數量與已支付的交易費用直接相關。


在 2021 年，以太坊通過已支付的用戶交易費用產生了 99 億美元收入，而 ETH 的交易量總計為 11.5 萬億美元。[7]




理論上，ETH 是無限供應的，因為以區塊獎勵形式進入流通的代幣沒有限制。EIP-1559 因爲允許可變的區塊獎勵發行比率，從而改變了 ETH 的貨幣政策。由於交易量影響從流通中移除 ETH 的數量，因此可變比率可能實現。

通過銷毀機制，可變發行率會隨著網絡需求增加而下降，並且隨著交易需求持續上升，它會導致代幣的浮動減少。礦工費銷毀機制和年度發行帶來的影響加劇了受需求的 ETH 的稀缺性。

目前，以太坊的年度網絡發行率約為 4.5%，而每個區塊獎勵 2 ETH。[8] 隨著時間流逝，區塊獎勵曲線可能會在向一個改進的、更可擴展的以太坊版本過渡的過程中繼續下降。

## 為什麼現在是發展以太坊的好時機：具有創造價值和可擴展性機制的智能合約區塊鏈

為了解以太坊日益增長的吸引力和價值，需認識 Buterin 在他的白皮書中闡述的內容：以編程方式擴展區塊鏈去中心化特性的潛力。對於有興趣接觸以太坊（可編程區塊鏈的首個成功應用）的投資者，我們預計：

- 在其生態系統中的鎖定價值、代幣和智能合約的效用和互操作性，以及不斷增長的交易數量及其對銷毀 ETH 的影響，可以繼續推動價值。
- 諸如過渡到權益證明以及鏈上和鏈下擴展提升（包括以太坊共識層的推出和第二層應用程式的改進）等升級，賦予以太坊可擴展性。由於其網絡效應，這些升級還將吸引更多開發人員加入這個不斷發展的生態系統，進一步拉高對 ETH 效用的需求。

以太坊的適應特性，使其處於有利地位在諸如互聯網演進至 Web 3.0 等顛覆性運動中扮演重要角色，該運動的核心是用戶擁有的區塊鏈生態系統。考慮到以上發展動態以及它們可能為 ETH 創造的需求，我們認為這種數碼資產和它所推動的區塊鏈網絡具富有意義的增長潛力。

**註：**

1. CoinMarketCap。(2022 年 3 月 1 日)。*歷史快照 – 2022 年 3 月 1 日*。
2. Watch the Burn。(2022 年 3 月 1 日)。*區塊*。
3. Ultrasound.money。(2022 年 3 月 1 日)。*超聲波喚醒：追蹤 ETH 成為超聲波*。
4. Uniswap。(2022 年 3 月 1 日)。*以太坊：概述*。
5. DeFi Llama。(2022 年 3 月 1 日)。*DeFi TVL 排名：以太坊*。
6. Etherscan。(2022 年 3 月 1 日)。*合約。0x00000000219ab540356cBB839Cbe05303d7705Fa*。
7. Token Terminal。(2022 年 3 月 1 日)。*項目：以太坊*。
8. EthHub。(n.d.) *以太坊基礎資訊：貨幣政策*。
9. Hotchkiss, G. I. (2019 年 12 月 19 日)。1.x 檔案：無狀態的以太坊狀態。*以太坊基礎網誌*。
10. Agarwal, A., Smith, C., Wackerow, P., Samani, Q., Joshua, Leung, N. H., Singh, H., & Richard, S. (2022 年 2 月 4 日)。礦工可提取價值 (MEV)。以太坊。

## 詞彙表

術語按出現次序列出。

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

區塊鏈：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，而無需可信的中介介入。

圖靈完備編程語言：可以執行任何計算操作的編程語言。

智能合約：基於代碼以編程方式執行的合約。

去中心化應用程式 (DApp)：使用區塊鏈技術在智能合約上構建的去中心化應用程式。

去中心化金融服務應用程式 (DeFi)：無需中介即可提供金融工具的 DApp。DeFi DApp 由智能合約驅動。DeFi 允許用戶通過去中心化途徑參與貨幣市場活動，例如借貸。

非同質化代幣 (NFT)：不可互換及獨一無二的可識別資產。

去中心化自治組織 (DAO)：去中心化組織的規則和權限存在於智能合約中。

交易：一個儲存著準備從外部擁有帳戶發送的訊息的已簽署數據包。交易代表以加密方式已簽署的指令。一筆交易可被視為將可用的數碼資產轉移到另一個地址，和發佈或執行智能合約。

狀態：描述所有賬戶和餘額的當前狀態，以及所有智能合約的數據。

區塊：以太坊網絡中包含交易細節的數據結構。每一個新創建的區塊都包含對其父區塊或上一個區塊的索引。

以太坊虛擬機 (EVM)：開發人員用於創建 DApp 及寄存賬戶和智能合約的底層平台。EVM 儲存網絡數據並保持網絡狀態更新。

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。

公鑰密碼學：亦稱為非對稱密碼學，它使用兩個相互不同但在數學上關聯的密鑰，一個用於加密，一個用於解密，其中公鑰用於接收 ETH，私鑰用於簽署交易以花費 ETH。

節點：分佈式電腦網絡，運行以太坊網絡軟件用於在交易和訊息進入區塊鏈之前對其進行驗證。節點有不同類型。

以太坊客戶端：運行完整節點需要的應用程式。節點本質上運行客戶端軟件，該軟件在多種開源編碼語言上可得到。客戶端的目的是用作根據網絡標準驗證交易的軟件。

礦工費 (Gas fee)：以太坊網絡中的交易是有代價的。礦工費代表為驗證、包含和保障區塊鏈中的交易而支付的以太幣數量。礦工費以 Gwei 計價，處理交易所需的 Gas 通常基於網絡需求。

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。

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。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。

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。

區塊時間：挖掘新區塊所需的時間。

區塊大小：每個區塊的數據容量。

區塊獎勵：一種特殊交易，允許礦工向自己發送固定數量的新創造 ETH，作為解決該區塊的經濟獎勵。

搶先交易：在內存池中探測有利可圖的套利機會。該構思是識別這些機會並提交具有更高 Gas 限制的交易，以便從任意機會中受益，因而搶先原始交易。

礦工或最大可提取價值 (MEV)：指通過包含、排除和更改區塊中的交易順序，可以從區塊生產中抽取超過標準區塊獎勵和礦工費的最大價值。[10]

鏈上：指出現在實際區塊鏈上的交易。

以太坊改進方案 (EIP)：描述以太坊網絡的當前標準和所有商定的更新。網絡建設者可以對現有網絡提出新的想法和改變。

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，都會添加額外確認。

分叉鏈：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。

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。

ERC-20：基於智能合約的 EVM 代幣標準。ERC-20 代幣提供了一套通用規則，以激勵代幣之間的可組合性。

穩定幣：加密貨幣代幣被設計為以 1：1 的比例與美元掛鉤，旨在通過增加流動性和交易渠道來穩定市場。

可組合性：操作其他同類資產並與它們互動的能力。

ERC-721：基於智能合約的 EVM 代幣標準。ERC-20s 和 ERC-721s 之間的主要分別在於編程非同質化代幣的能力及其背後的規則。

權益證明：一種共識機制，在該機制中驗證者必須「質押」他們的資產來確認和記錄交易。

驗證者：在權益證明共識機制中驗證和確認交易的網絡參與者。

罰沒：工作量證明共識機制下的驗證者處罰，其中全部或部分質押資產被沒收。

提議者：通過演算法選擇出的、提議一個新區塊的驗證者。

認證者：未被選中提議區塊的驗證者必須認證被選中的驗證者所提議的區塊，並確認信息符合標準。

Gwei：Giga-wei 或 Gwei 通常用於描述以太坊網絡上的 Gas 成本，表示以太幣的十億分之一。

主網：用於描述主要區塊鏈的術語。

## 免責聲明

數碼資產投資是涉及高度風險的投機性投資，包括部分或全部投資資金的損失。這些投資不適合任何無法承受全部投資損失的投資者。以太幣 (ETH) 是一種相對較新的資產類別。它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。

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。

以太幣 (ETH) 在很大程度上不受監管，投資以太幣可能比受監管的投資更易遭遇欺詐和操縱。以太幣 (ETH) 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。