



BTCC “**新手專享**”

註冊並入金 BTCC，領取最高價值**17,500USDT**獎勵。  
推薦好友還有更多返佣獎勵。

立即註冊/查看詳情

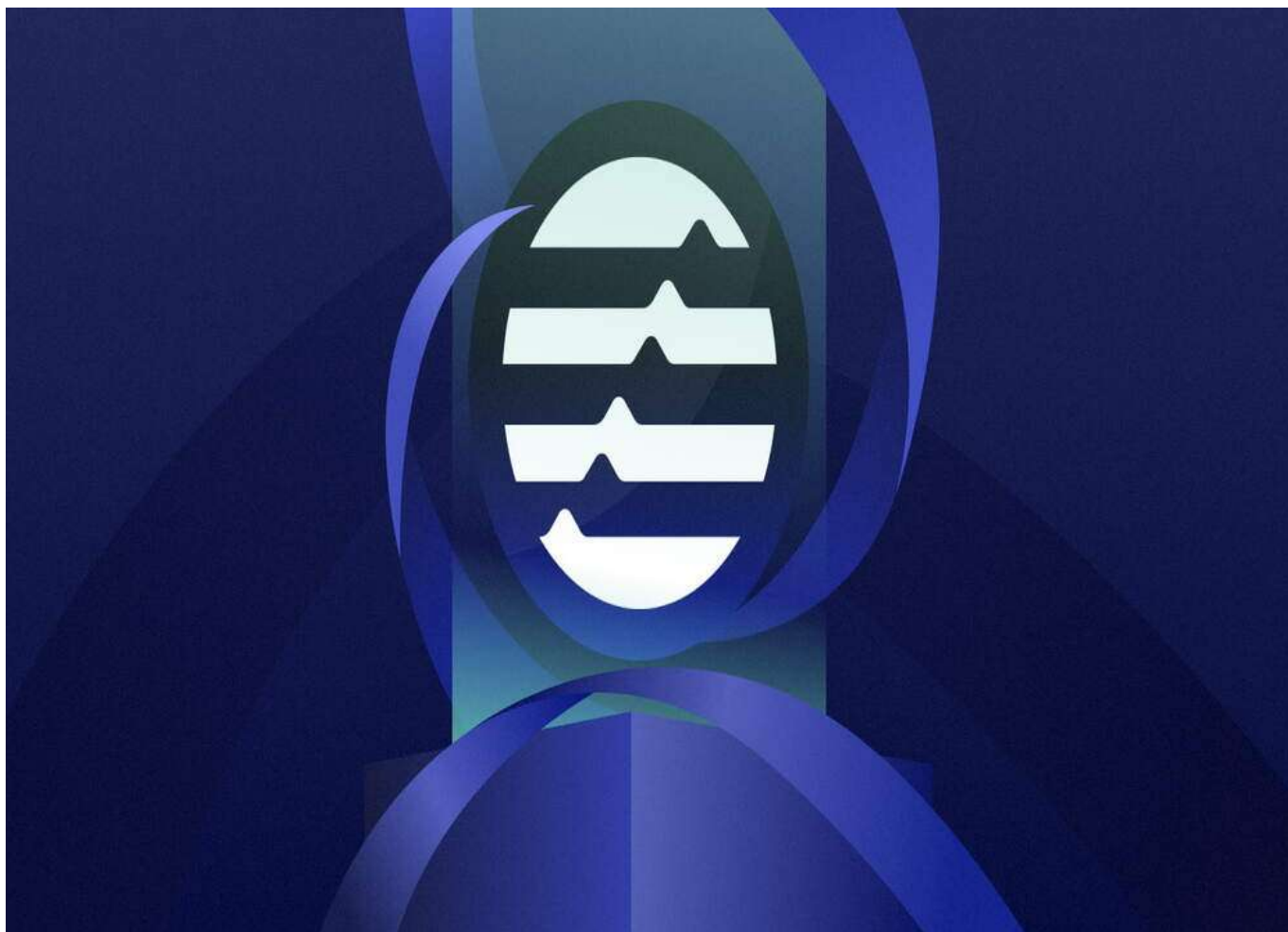
## Aptos公鏈如何一夜成為「網紅」？其潛力與局限是什麼？

原文：

<https://www.btcc.com/zh-TW/academy/research-analysis/how-aptos-public-chain-became-popular-over-night>

Aptos是一個具擴展性的Layer 1區塊鏈，其採用了權益證明的共識，並結合了新的智能合約程式語言「Move」。隨著 Aptos 主網的發布以及空投APT，該項目最新在幣圈討論區突然聲名大噪。

那麼，這個項目特別在哪裡？Aptos 是如何實現一夜爆紅的呢？其潛力和局限是什麼？本篇文章將為你一一進行分析。



# Aptos 的爆紅

---

Aptos是一個具擴展性的Layer 1區塊鏈，採用權益證明（Proof-of-Stake）共識機制，結合新的智能合約程式語言「Move」、平行運算處理交易，目標達到理論上10萬每秒交易量（TPS）。順帶一提，比特幣的TPS大約為7到15，以太坊1.0大約為15到17。

作為Meta（原Facebook）嘗試創建加密貨幣項目Libra的「遺孤」，Aptos繼承了Libra的願景，即成為未來數百萬加密用戶使用的區塊鏈。

Aptos的首要重點是提供可擴展、安全和可靠的區塊鏈。為此，Aptos依賴於一種新的智能合約語言Move，它表面上是一種比當前以太坊的「黃金標準」Solidity更「安全」的語言。當然，Aptos並不是第一個將自己標榜為「可擴展、安全和可靠」的L1區塊鏈。其他L1，尤其是Solana，過去也曾嘗試將其作為他們的口號，也取得了不同程度的成功。

Aptos今年三月首次在幣圈掀起波瀾，當時在美國創投公司Andreessen Horowitz（a16z）領投的種子輪募資，Aptos募集了2億美元。今年七月，Aptos又在FTX Ventures和Jump Crypto領投的A輪募資，募到了1.5億美元，交易前估值達19億美元。

再兩個月後，在幣安旗下風險投資與創新孵化機構Binance Labs領投下的創投募資，使Aptos估值達到40億美元。

值得強調的是，Aptos在10月17日主網上線前就做到這一切。為回報測試網的早期使用者、公平分發第一批代幣，Aptos空投了150APT幣（發行時價值約1237美元）到11萬235個合格地址。從CoinGecko數據來看，Aptos目前完全稀釋後的市值大約92億美元。

最近在該項目在幣圈討論區突然聲名大噪，則是因為Aptos空投APT給早期測試網參與者，創造了熊市難得一見的暴富傳奇。完成Aptos激勵測試網申請或鑄造測試網NFT的用戶，符合資格申領代幣，網路上許多羊毛黨、科學家用幾百個帳戶去申請測試網，據傳每個測試網帳戶可以拿300個代幣，鑄造NFT有150個代幣，拿到一百、一千個帳戶代幣直接「幣圈畢業」，財富自由。



[下載Android版](#)

[下載iOS版](#)

[台灣用戶專享優惠活動（10,055 USDT 交易大禮包）<<<<](#)

## Aptos 特別在哪裡

---

從技術角度來看，Aptos的特色可以歸為以Rust為基礎、由Meta獨立研發的程式語言Move，以及Aptos平

行運算處理交易的能力。

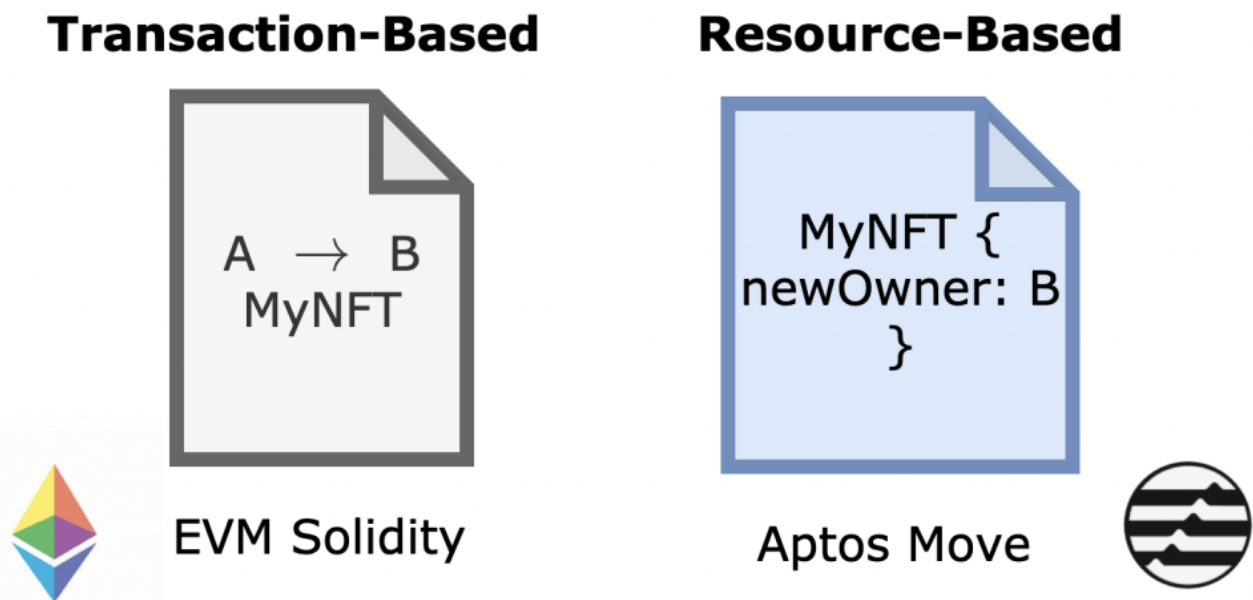
## 1. Move 語言

Move 語言可以說是Aptos 大部分潛力的來源。因此，在了解 Aptos 的技術原理前我們需要對 Move 語言有一定的了解。

Move 最初由Meta 的Libra 團隊（現名為Diem）開發，旨在提供與其他智能合約語言相比在範式上不同的智能合約編程模型；Move 沒有採用基於交易的方法，而是採用基於資源的方法來定義智能合約模型。

那麼這一切意味著什麼呢？從比特幣開始，絕大多數的區塊鏈都採用了「交易優先」的方法，區塊中的每個條目都是一筆交易（比如Alice 和Bob 之間的交易）。交易是相對的對象。要進行交易，需要存在Alice 和Bob 地址。為了確保Alice 不會「雙重花費」代幣，我們需要檢查這筆交易與所有其他交易沒有衝突，這不可避免地會減慢交易速度。

然而，Move 「基於資源」的方法卻截然不同。Move 不記錄A 到B 的交易，而是記錄對象（或資源）的易手情況，並相應地更新屬性。重要的是，資源是原子實體——資源X 的存在不依賴於任何其他現有的資源。因此，使用基於資源的方法支援針對並行執行的更加獨立的結構。



Move 中的「資源」本質上是具有某些屬性的對象。用技術術語來說，它們是容器數據結構。此時，有以太坊編程背景的人可能會提出一個問題：Solidity 也有結構體，還有其他數據結構體。是什麼讓Move 的結構特別？我認為最重要的區別在於，雖然Solidity 中的結構在語言中具有相對外圍的部分（主要用於清晰起見），但結構是Move 中一切的基礎。此外，Move 的結構具有不同的「功能」，包括「複製」、「刪除」、「儲存」，它們定義了對象是否可複製、可儲存、可刪除等。這種結構與Solidity 或絕大多數常見編程語言（例如C/C++）完全不同。然而，這些不同的「能力」是非常直觀的。有些東西你可以「複製」，比如代幣。有些東西你可以「丟掉」。

現在思考一下Move 上「資源」的官方定義：「如果結構值無法複製且無法刪除，我們通常將其稱為資源。」

因此，「資源」本質上是獨一無二的「結構」，將永遠存在於你身邊。

Move 對「結構」的完全重新定義允許它使用一種數據結構簡潔地定義代幣、NFT、智能合約和其他數位資產。這是以太坊的EVM 根本無法比擬的；任何有EVM 開發經驗的人都知道Solidity 中的處理結構（和嵌套結構）是多麼令人沮喪。

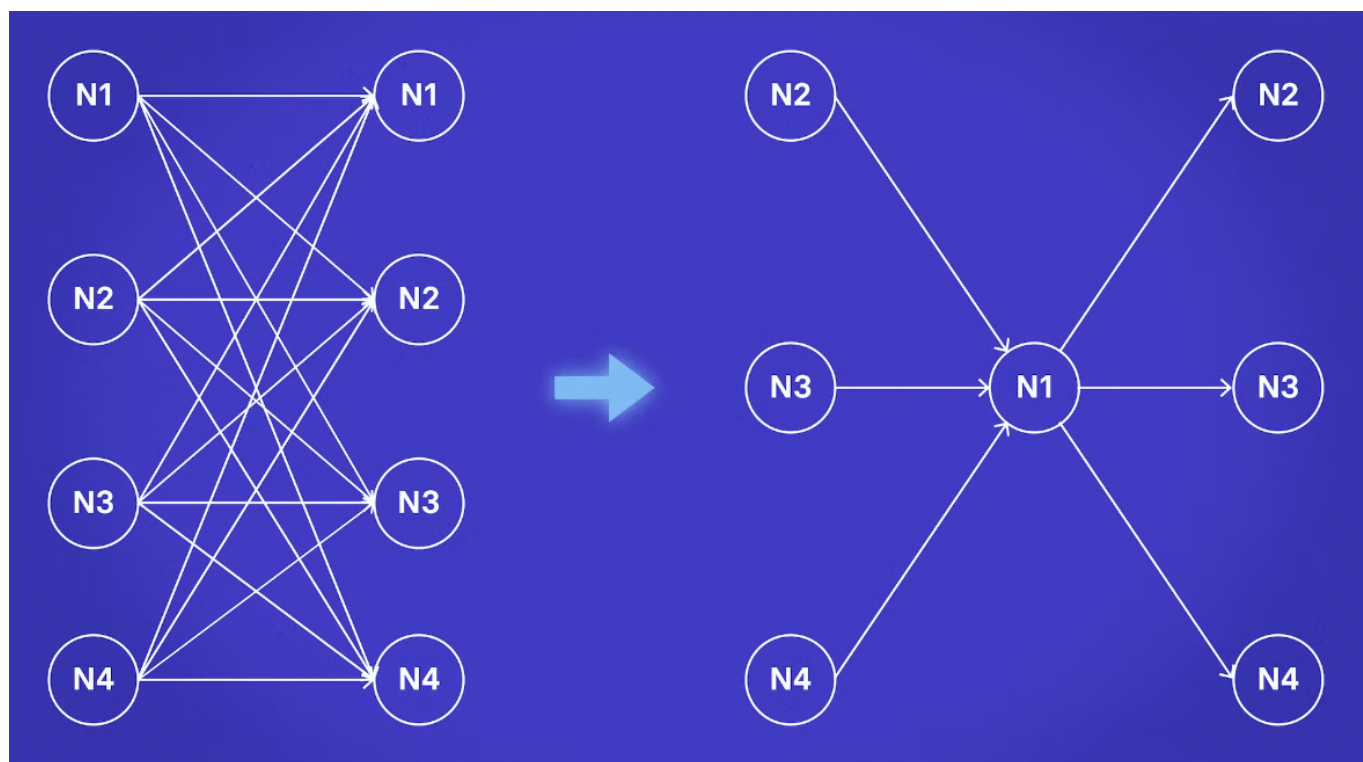


至關重要的是，Move 的基於資源的方法為其安全性提供了保障。正如Move 的白皮書所提到的，在許多程式中存在資產的間接表示，這意味著稀缺性和訪問、控制是不可擴展的。例如，雖然ETH 代幣的稀缺性被EVM 硬編碼和保護，但其他ERC-20 代幣「不繼承這些保護，它們必須小心不要引入允許複製、重用或資產丟失的錯誤」，例如經典的重入攻擊。這是長期困擾EVM 項目的問題，經常導致它們損失數百萬美元。由於Move 的基於資源的方法，重入攻擊是不可行的。因此，Move 編碼的入門門檻可以說比EVM 更容易獲得——這是大規模採用的一個關鍵因素。

## 2.Aptos 的技術原理

可以說，Aptos 最大的成就是將Move 作為一種語言推向市場。事實上，Aptos 的大部分設計都直接取自Meta 開發的Diem (Libra) 區塊鏈。回想一下，Aptos 是一個強調可擴展性和安全性的區塊鏈。有兩種主要的技術用於實現這一點。首先是在它的共識層，即AptosBFT 共識機制。第二個是它的執行層，即Block-STM 執行引擎。

首先，AptosBFT 是一種拜占庭容錯共識機制，這本質上意味著只要網路上不超過1/3 的節點是惡意行為者，它就可以繼續保證安全性。這是一種標準做法：比特幣的工作量證明、以太坊的權益證明等都是拜占庭容錯的。那麼 AptosBFT 究竟是如何實現其共識機制的呢？與所有其他權益證明鏈一樣，Aptos 依賴於「質押」節點。它實現了HotStuff 共識算法的變體，HotStuff 是一種PoS 算法，與早期模型（例如pBFT）相比，它通過讓節點與「輪換領導者」通信，而不是與所有其他節點進行通信，從而在節點之間提供更簡潔的通信協議。雖然AptosBFT 在HotStuff 之上引入了多項優化，最顯著的優化是「密鑰輪換機制」（以增強安全性）和減少開銷（以增強可擴展性），但HotStuff 的PoS 設計[10]沒有重大的結構變化。



另一方面，Block-STM 並行執行引擎是一個更具原創性的設計，可以說是該項目的主要技術突破點。回想一下，資源是原子的——某個資源 X 的易手不依賴於任何其他資源。通過將交易分組（就像樂高積木），我們可以在執行資源交易時利用大規模並行性，與以太坊相比，計算速度提高了20 倍。

## Aptos 會是下一個Solana 殺手嗎？

上線約一週的Aptos已經被捧為潛在的「Solana殺手」，主因號稱有10萬TPS，相較之下曾經號稱「以太坊殺手」的Solana只有約6萬TPS，而且有事沒事就會掛掉一陣子。

除了高擴展性，Aptos跟Solana還有其他共同點，包括創投富爸爸的強力支持、由上而下打造生態系。若Aptos能培養出繁榮的生態系，就很可能搶走Solana的光環，而Solana前行銷長維茲（Austin Virts）目前也負責打造Aptos生態系。

目前以生態系健康程度和採用程度來說，Solana還是領先一些。Aptos一開始代幣經濟學不透明引發社區不滿，可能帶來傷害，但若其技術目標可達成一半就好，那麼就有機會從其他Layer 1區塊鏈搶到一大塊市占。

**延伸閱讀：** [在下一輪新公鏈週期中，Aptos 能否接棒Solana？](#)



[下載Android版](#)

[下載iOS版](#)

[台灣用戶專享優惠活動（10,055 USDT 交易大禮包）<<<<](#)

## Aptos 的潛力和局限

Aptos 是目前第一個也是唯一一個推出主網的基於Move的L1鏈。因此，Aptos的主網發布是一個非常具有像徵意義的事件。Aptos所吸引的資金和媒體關注不一定與其內在的技術創新相匹配。

如上所述，Aptos自身的主要技術創新在於其Block-STM並行執行引擎。大多數其他技術方面，包括其共識機制和Move語言的使用，都是從Meta繼承的略微改進的遺留產品。關於Block-STM並行執行引擎，目前尚不清楚這是否會導致Aptos上的用戶體驗與Solana上的用戶體驗之間存在本質上的差異，但如果用戶體驗是相同的，那麼用戶不會關心它在技術層面是如何實現的。

與任何L1一樣，Aptos的長期成功將取決於在其之上構建的項目。目前，其生態系統中的項目，如Liquidswap DEX、Topaz NFT市場和Aptos域名服務，雖然是任何區塊鏈生態系統中的必要產品，但對於Aptos的設計來說還不夠獨特。這些項目就像一個小村莊的雜貨店、學校和醫院，雖然對村莊的運作是必要的，但它們並沒有賦予村莊任何其他村莊所沒有的獨特特徵。

回顧過去，Solana的部分成功可能要歸功於StepN等項目，這些項目實際上利用了Solana的並行優勢。這些GameFi和SocialFi項目往往涉及大量相對孤立的並行數據。因此，這些應用程式特別適合併行執行引擎，例如Aptos和Solana，同時還能夠帶來龐大的用戶、消費者基礎和高交易量。事實上，在某一時刻，僅StepN就佔Solana付費用戶的約20%。

因此，要讓Aptos作為L1取得成功，需要有一系列獨特的項目來充分利用Aptos的並行執行引擎，而這些項目無法在以太坊甚至Solana上完成。借助Aptos新穎的Block-STM設計，這些項目可能會以一種新

的SocialFi 的形式形成，用戶在這些項目中以小圈子的形式進行交互（如群聊），因為這些群組可以是流動的和動態的，同時也有點相互獨立，所以相比Solana 或以太坊，Aptos 的並行執行引擎更適合它們。但當然，這只是一個推測。

儘管如此，Aptos 的主網發布仍然是加密世界中非常重要和具有象徵意義的事件。它代表了Meta 工程師多年來為解決以太坊的可擴展性瓶頸而努力的結晶。Move 獨特的語言特性意味著一定會有許多dApp 轉而在Move 上實現，而不是繼續在Solidity 或其他智能合約語言上實現。但是這些項目一定會在Aptos 生態系統中實施嗎？沒人知道。Aptos 可能會享有一些先發優勢，即能夠將Move 投入使用，並將其與Move 語言聯繫起來。但與此同時，它很可能會遭遇類似MySpace 先發製人卻逐漸隕落的命運。

---

## 相關閱讀：

[什麼是 Aptos 公鏈？它值得投資嗎？](#)

[剛上主網的Aptos被高估了嗎？承諾達到10萬TPS實則僅有4](#)

[Aptos空投2千萬枚\\$APT；AptoScan上線，交易數破230萬](#)

[APT上架幣安後暴漲至100美高點，驚現「巨額砸盤」跌近 50%](#)

[ANS註冊域名過萬；Aptos域名項目apt ID宣布停止服務](#)

如果你想要知道更多關於加密貨幣的資訊，可以進入 [BTCC 學院](#) 及 [資訊](#) 頁面進行了解。