



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

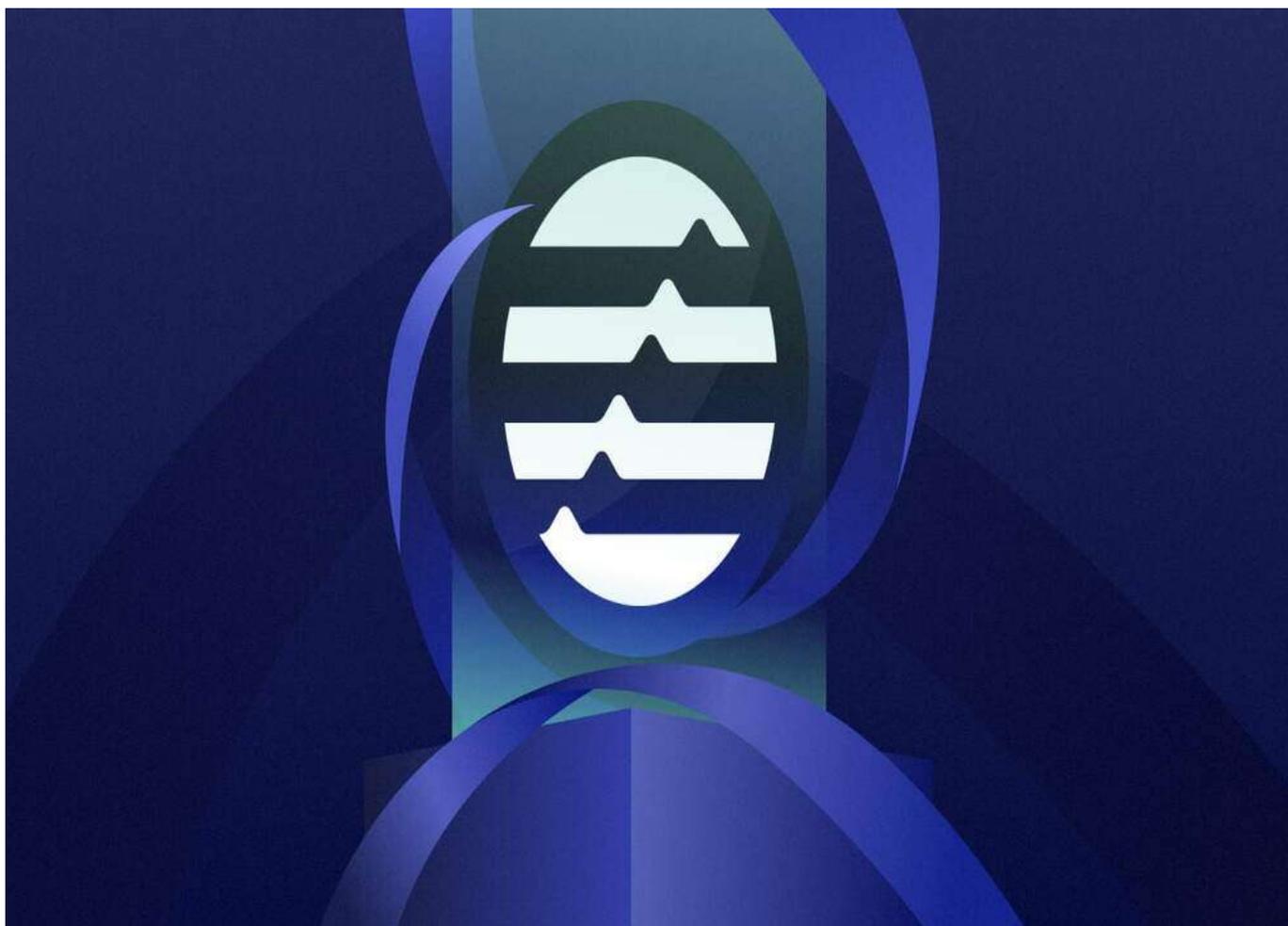
## 在下一輪新公鏈週期中，Aptos 能否接棒Solana？

原文：

<https://www.btcc.com/zh-TW/academy/research-analysis/in-the-next-round-of-new-public-chain-cycle-can-aptos-take-over-solana>

新公鏈總是呈現週期性發展，上個週期以Solana 為首的新公鏈憑藉著激進的低費高速模式快速崛起，也因為一些內在的缺陷而有可能被Aptos 等新公鏈逐漸趕超。而老牌公鏈以太坊，已經在多鏈未來中擁有了強大的護城河。

那麼，在下一輪新公鏈週期，Aptos 是否有望接棒Solana呢？



## 公鏈賽道的初步劃分

---

2015 年，以太坊的上線，開創了[智能合約](#)公鏈時代，也讓公鏈成為了整個[Web3](#) 不可或缺的基礎設施。

2017 年，[ICO](#) 與加密貓（Crypto Kitties）的爆火，幾乎使[以太坊](#)網路陷入癱瘓。從此所有從業者都意識到，此時的區塊鏈完全不足以承擔更大面積的現實社會交易需求，擴容必然是[Web3](#)長期剛需的黃金賽道。

為了方便進行對新公鏈的討論，我們暫且擱置已擁有大量應用、大量開發者、超強影響力，但受制於已有的眾多利益相關者、不得不緩慢轉型的以太坊，而優先觀察沒有早期影響力與用戶積累，但是歷史包袱更輕、可以輕鬆採用全新高性能方案的新公鏈。Solana 一度是新公鏈賽道絕對的王者，但如今，Aptos 被眾多投資人視為「Solana Killer」。



[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）<<<<](#)

## 高性能新公鏈賽道的規律

---

首先，我認為Aptos 有較大概率能衝擊Solana 的位置。

在以太坊正式落地分片、實現足夠高性能前，高性能新公鏈賽道將表現出一定的周期律。

具體來說，一條新公鏈受益於激進的高速與低費而快速生長，同時因為激進的高速低費選擇帶來的漏洞而走入負向飛輪。本輪的 Solana 的高性能敘事開始失去光彩，「宕機鏈」的綽號逐漸取代「以太坊殺手」的稱號，資本開始尋找周期律下新的接棒人。

## Solana 的崛起與衰落

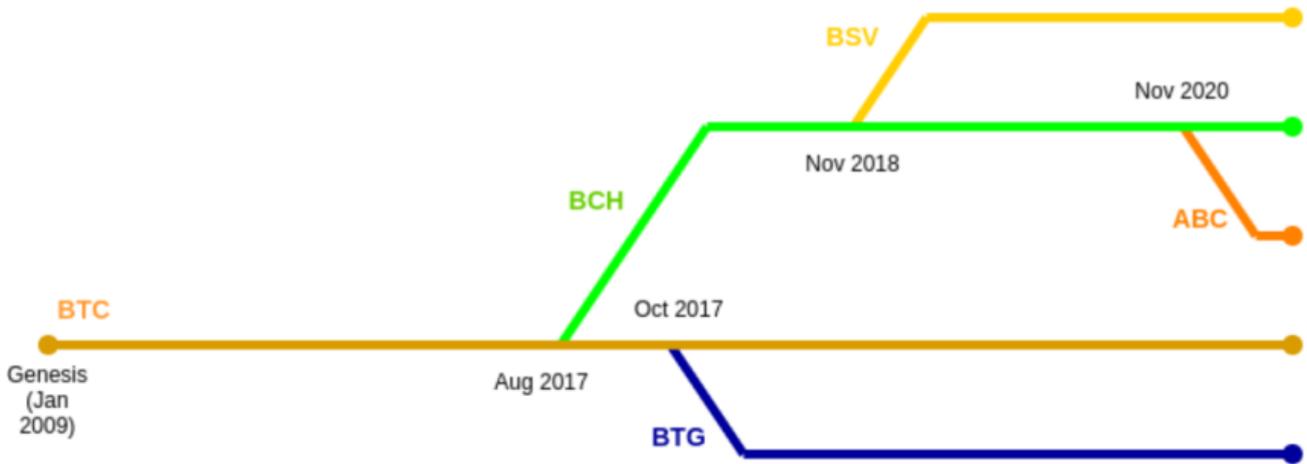
---

### 一、超高的 TPS

Solana 高TPS 是建立在10 倍的區塊大小、低冗餘度及1/30 的出塊時間，還有並行計算後約10 倍的速度之上的，這使其實現了ETH 約3000 倍的理論TPS。

## 1. 區塊大小

其中，Solana 將區塊體積從約1MB 增加至10MB，由此帶來10 倍的性能提升。但是增加區塊體積並不是非常值得採用的方案，因為區塊體積過大，在增加系統處理能力的同時，會造成兩個明顯弊端：能存儲區塊鏈完整交易的全節點大幅減少、大區塊在系統中傳輸時間過長甚至易受攻擊（比特幣的幾個著名分叉BCH、BSV 等都來源於區塊大小的激烈爭論，最終比特幣堅持了小區塊）。



雖然Solana 在通信過程中做了較多改進而規避了一些風險，但是Solana 的大區塊依然增加了全節點的門檻，減少了全節點的數量，對於去中心化程度和網路安全性造成了一定的負面影響。

## 2. 共識層面的改進

### (1) 中心化的交易處理流程

在web2.0 的中心化系統中，以支付寶為例，由於後台只有支付寶官方的服務器，交易的處理是非常簡單的：

- I. 交易信息被發送至支付寶
- II. 支付寶直接確認並執行交易
- III. 沒有人負責驗證，因為大多數人默認相信支付寶不願意作惡。

總計1 次發送，1 次執行，0 次檢驗，總時長幾乎可以忽略。

### (2) 去中心化的交易處理流程

但是在公鏈領域，成為驗證者是幾乎無門檻的事，我們無法直接相信一個驗證者做出了正確的交易處理。因此，我們需要大量驗證者，且驗證過程也會非常複雜：

#### • 以太坊

我們不妨來觀察以太坊是如何確認交易的：

- A. 交易完成後，相關交易信息經過6 秒傳輸至以太坊全網n 個節點
- B. 由一個隨機節點處理，將處理好的交易打包，生成區塊
- C. 區塊被發送到全網n 個節點進行檢驗。

總體增加了大量傳輸與檢驗次數，一個出塊流程為12 秒。

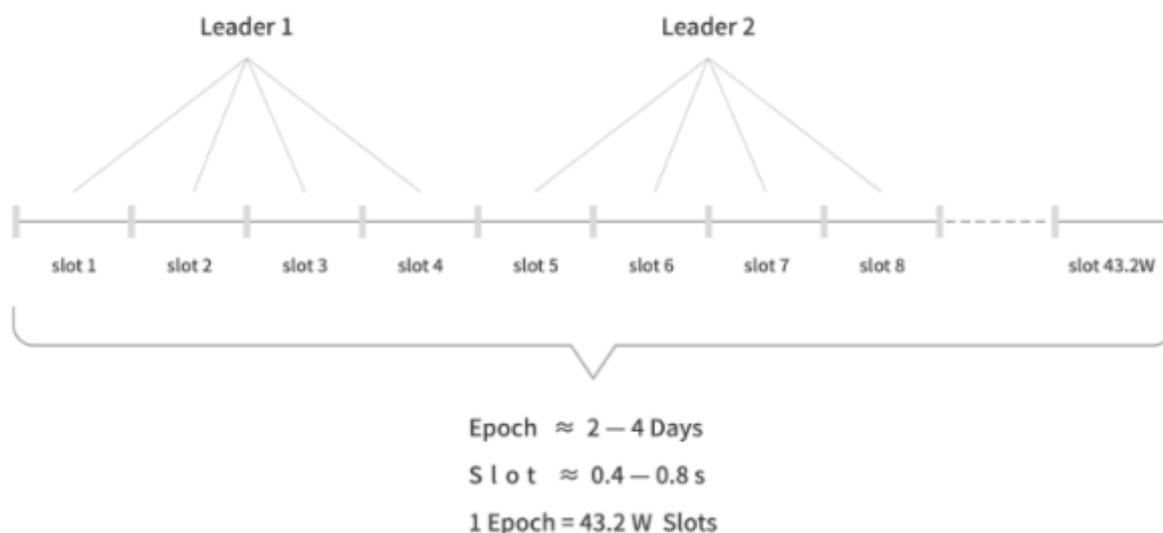
由於單個節點的不可信，區塊鏈時代一定會有輪博奕機制，讓所有節點相互驗證，從而維護區塊鏈最終結果的準確性，這增加了時間消耗和冗餘計算，也是區塊鏈不可能三角存在的重要原因。

Solana 在傳輸層面和區塊驗證層面均大幅提升了速度。Solana 將出塊時間從以太坊的12 秒降低下降至0.4 秒（最多0.8 秒），從而實現了約30 倍的擴容。

## • Solana

我們來看看Solana 是如何記賬的：

- A. 交易傳輸層面： Solana 會在每個運轉週期（Epoch）提前公佈每次出塊（Slot）的負責人（Leader），也就意味著，所有的交易只需要被傳輸到Leader，而無需傳遍全網，這降低了傳播環節的冗餘。
- B. 交易的驗證層面： Solana 出塊負責人將區塊分割，其他驗證者只需檢驗分到自己的部分，而不是整個區塊。



Solana 的出塊機制下，計算的冗餘程度從 $n^2$ 下降至 $\log n$ ，從而實現了更高效的運轉（以下進行簡單的科普）。

我們不妨來回憶一些經典數學題：

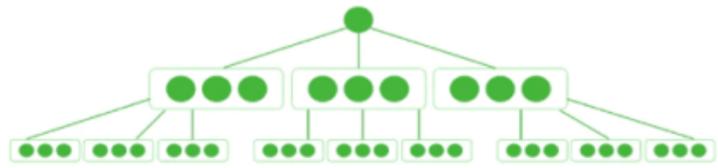
- ①如果 $n$  個人中，任意2 人都需要互換賬本，一共出現了多少次賬本互換呢？答案是 $n(n-1)$  次，或者說 $n^2$  級別。
- ②相應的，假設 $n$  個人中，任意一人都需要和一個已知的「領導」互換賬本，賬本一共被交換了多少次呢？答案是 $2(n-1)$  次，或者說 $n$  級別。
- ③再次假設，如果 $n$  個人中，已知的「領導」和每個人互換賬本的一部分，那麼賬本總計被交換了多少次呢？顯然比 $n$  級別還要低，我們可以簡單理解為 $\log n$  級別。

其中①對應以太坊，③對應Solana。

我們可以得到如下圖示，Solana的共識機制下，系統出塊所需的冗餘計算大大減少，出塊速度也明顯提升。



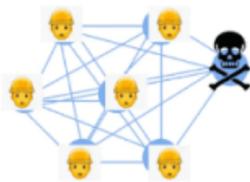
**Ethereum:**  
Every node checks every other node  
Redundancy is quadric to n  
 $O(n^2)$



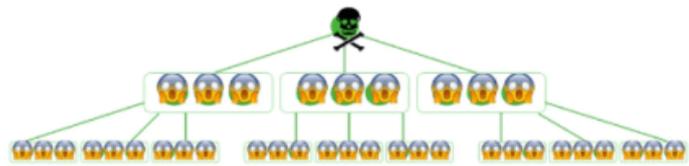
**Solana:**  
A leader-based division-of-work protocol  
Redundancy is logarithmic to n  
 $O(\log n)$

在Solana 誕生之初，這樣的設計確實可以讓Solana 實現飛速的運轉。但是大家很容易發現這種模式的弊端：接受各種交易、識別有效交易、打包交易、分割區塊、要求其他驗證者各自驗證並回收驗證結果等工作，都是領導節點完成的。

領導節點面臨著極大的壓力，在交易量很大/ 無效交易很多等情況出現時，很容易出現崩潰。而從下圖我們很容易看出，領導節點一旦崩潰，整個系統是非常難正常運轉的，這就引發了整個區塊鏈的頻頻宕機。



**Ethereum:**  
A lost node is fine, business as usual  
 $O(n^2)$



**Solana:**  
Failed leader disrupts entire network  
 $O(n^4)$

此外，提前公佈的領導節點被賄賂作惡、被針對性攻擊等中心化問題也無法規避，這對整個區塊鏈也有一定負面影響。

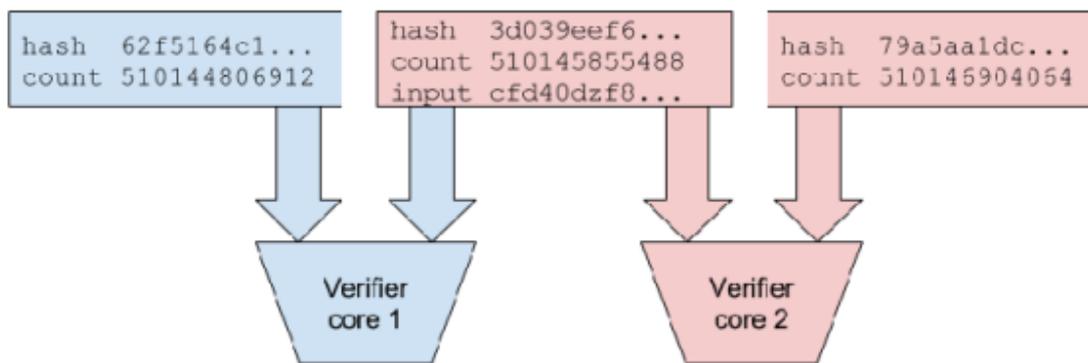
2021 年9 月Solana 生態爆發後，至今已經發生了多次宕機事故。頻繁的宕機事故，限制了Solana 的發展空間。在下輪牛市，用戶需要一條不會頻繁宕機（至少暫時沒有表現出極高宕機風險）的新公鏈。

### 3. 並行計算

在基本的共識機制之外，Solana 也做了智能合約並行處理的改進。

早期以太坊採用了EVM 作為智能合約運行環境，這種選擇的重要特性是串行計算（依次處理交易事務），是相對低效的處理模式。雖然以太坊社區也有將EVM升級（為EWASM）的規劃，但是距離落地還很遙遠。

而Solana 採用了Sealevel 支持智能合約的並行處理，支持了使用英偉達4096 核GPU 進行超強的並行計算。這讓Solana 在大多數情況下，都可以表現出超強的運轉能力。



但是Solana 也會面對以下一些特殊情況：

1. Solana 需要正確的判斷交易是可以並行的，而判斷錯誤可能引起故障。
2. 如果Solana 判斷後發現交易是必須串行的，則它串行運轉的速度，比以太坊還要慢。

總結下來，4096 核並行計算的特性，讓它在可並行處理的程序中擁有超高的效率，但是一旦遇到無法並行處理的交易，他的效率會低於以太坊，甚至可能出現故障而宕機。此外，Solana 低冗餘度的特性，也就是通過「領導節點分配任務」的模式，讓Solana 可以輕鬆獲得更高的正常運轉效率。但是一旦出現故障，以太坊的高冗餘度使它可以迅速恢復，而Solana 的低冗餘度極容易使網路崩潰。總體上，Solana 項目做出了非常多高價值的創新，早期Solana 可以迅速通過高TPS 崛起，但後期，它不得不為容易宕機的特性埋單。

這就是區塊鏈版本的「用冗餘對抗不確定性」吧。

## 二、超低的費用

### 1. 公鏈的收支與「印鈔」

Solana 崛起的另一大依靠是低費用。概括的說，低費用一方面來源於超高的處理能力，另一個方面來源於系統的發幣補貼。我們可以詳解這種發幣補貼模式下的收支。

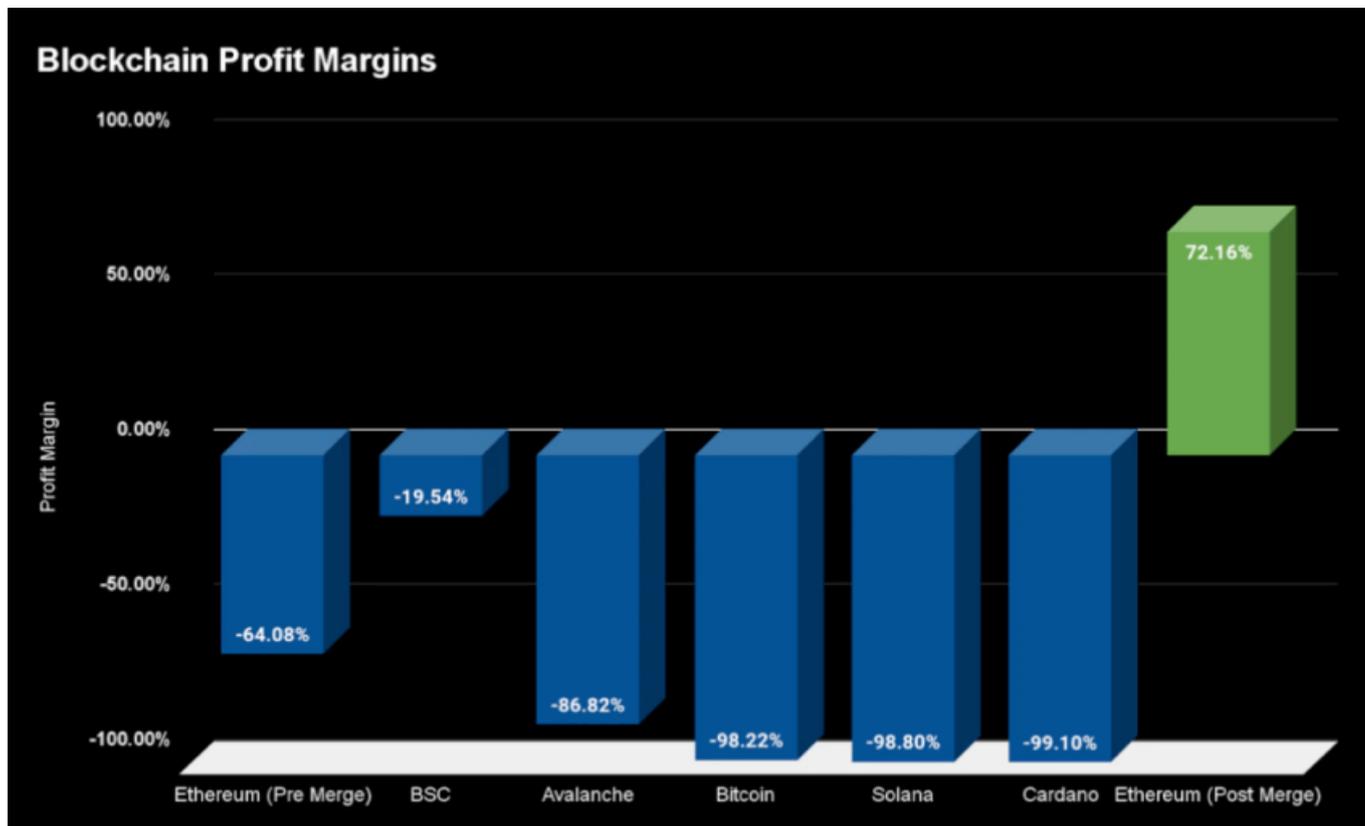
如果我們思考公鏈的商業邏輯，它為各種商業項目提供營商環境，同時對所有的用戶收稅，那麼公鏈會很像一個國家，而公鏈代幣更像是用於交稅的法幣。

進一步分析，我們按照大多數公鏈的共同特徵，對這個收入與支出進行簡化。這些「國家」的稅收，是所有用戶的手續費，而這些「國家」的財政支出，則是為驗證者發放的激勵。如果大家去翻閱政府財政報告，大概率會看到這個詞：「收支平衡」。

正如國家需要收支平衡一樣，公鏈也需要收支平衡。但如果我們查閱每條公鏈的收與支，就會發現，絕大多數公鏈的支出，是超過其收入的：

- 給驗證者的獎勵- 手續費收入=公鏈的虧損

Bankless 曾經對公鏈的虧損率做出過如下的統計：



在一條公鏈的收入少於需要給驗證者的支出時，這些虧損的額度，往往只能通過「開啟印鈔機」，發幣進行補貼，也就是：

- 公鏈的虧損=增發獎勵

那麼，驗證的獎勵往往來源於兩部分：正常收入與「印鈔補貼」：

- 手續費收入+ 增發獎勵=給驗證者的獎勵

對Solana 來說，區塊鏈驗證者應收100 元「工資」時，Solana「印鈔補貼」給驗證者的金額往往高達98.8 元，實際從用戶收費大約只有1.2 元。當然，這個數據會隨時間變化，但是Solana 距離收支平衡與可持續運轉，還有很長的路要走。

## 2. 「印鈔」帶來公鏈的通貨膨脹

我們選擇了將公鏈類比為國家，將公鏈代幣類比為法幣，則對於一條公鏈來說，貨幣的總價值與商品的總價值應當是完全對應的。

我們可以簡單地進行如下思考：一個國家的商品只有蘋果，第一年，國家總計生產了100 千克蘋果，而總計發行了100 元貨幣，則蘋果的市場價格將為1 元/ 千克。如果第二年，這個國家發展迅速，有了200 千克蘋果，也增發了100 元貨幣，則蘋果的價格也可以穩定在1 元/ 千克。而如果第三年國家發展陷入停滯，仍然只生產了200 千克蘋果，但再次增發了100 元貨幣，則蘋果的價格，將變成1.5 元/ 千克，也就是出現了較為嚴重的通貨膨脹。

相應的，對於以較高速度增發「貨幣」的Solana「國家」來說，早期由於鏈上商品總價值的快速增長，增發貨幣的負面影響將被幾乎抵消。

但是，當Solana 已經遇到了明顯發展瓶頸之後，當總貨幣量與總商品價值開始失調之後，Solana 繼續印鈔來彌補虧空，或者減少印鈔而增加「收稅」，本質上都是不利於區塊鏈發展的。這也被一些人稱為「新公鏈的周期律」。

至少在下一輪，市場期待一條重新找到收支平衡，或至少通過早期生態的快速發展，不讓用戶感覺到收支

不平衡的公鏈。目前看來，Solana 可能被接棒，Aptos 也有望成為那個接棒人。

我們也不妨在此也探討一下以太坊的商業模式：對於以太坊來說，在2021 年實現EIP1559 銷毀機制和2022 年正式合併而降低運營成本後，對應的公式已經變成了：

- 手續費收入+ 增發- 銷毀=給驗證者的支出
- 如果按照收入- 支出=利潤，那麼對於以太坊來說：
- 利潤=銷毀- 增發

其中，合併後增發量由每年450 萬個下降到18-209 萬個，而銷毀量則與區塊鏈使用情況決定。不難算出，在以太坊gas 價格超過15 時，以太坊大概率是一條超越了盈虧平衡線區塊鏈，若能長期保持，則能實現長期的發展和生存。

### 3. 收支視角下的一些分析案例

收支或許是大家常常忽略的話題，但是即使在全新web3 世界中，商業的最基本邏輯也依然離不開收入與支出。

2022 年6 月，Starkware 上Immutable X (IMX) 項目增加收費，dydx 出走自建鍊等，其實也暗示了收支對公鍊格局的一些影響。我們可以在這裡按照收支的視角，對兩個項目進行一定的分析。

#### (1) 中小企業

對於Immutable X 來說，我們不妨將其收入與支出進行基本的拆解：

作為一個zkrollup，2022 年6 月前， Immutable X 宣稱完全0 gas，因此主要的業務收入基本為0。

而作為基於starkware 開發的zkrollup，它需要將交易記錄打包至以太坊主鏈進行驗證和存儲以保證安全性，並向以太坊支付相應費用，主要支出為以太坊的gas fee。此外，IMX 也需要向starkware 交使用費等。

這樣的收支顯然不平衡，於是2022 年6 月，IMX 開始加收2% 的交易費，以維持系統收支的平衡。

#### (2) DYDX 與短期應用鏈風潮

接下來，我們可以站在DYDX 的視角觀察它的收支與選擇：

對於Starkware 上的DYDX 來說，其如果選擇以太坊layer2，則其收入=交易手續費，支出=給Starkex 的付費+ 給以太坊系統的gas fee+ 做鏈上應用的成本。

對於去Cosmos 自建鏈的DYDX 來說，其收入=交易手續費+ 自建鏈gas fee，支出=做鏈成本。

也就是說，DYDX 如果選擇去Cosmos 自建鏈，則其將省下給以太坊的付費，增加做鏈成本和gas fee 捕獲，當然也會損失一定以太坊生態的流量。在當前以太坊的比較高的區塊租金和Cosmos 低建鏈成本的前提下，DYDX 切換到Cosmos 自建鍊是一種順理成章的選擇。

當然，在以太坊分片落地，變得更低費高效時，應用（鏈）視角下，自建鏈將不再是足夠經濟學理性的選擇，原先DYDX 等項目的應用鏈敘事，也就會到達一定的轉折點。

那麼按照高TPS 和低費用的邏輯與週期律，新公鏈賽道中Solana 的發展明顯遇到了瓶頸，新公鏈龍頭的接棒人將會出現。這個接棒人，從資本追捧、技術的重新取捨和Move 語言敘事可以初步看出，有可能是Aptos。



[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 有望接棒新公鏈

目前看來，Aptos 與Solana 的投資方高度重合，Solana 的部分高管以及鏈上項目方也都有轉投Aptos 的趨勢，這對於Aptos 接棒Solana 是較大的機遇。此外，高性能的重新取捨、Move 語言的新故事，也都讓Aptos 有了較為強大的競爭力。當然Aptos 是否可以接棒以及接棒後的實際發展情況，可能要考驗項目團隊的能力了。

上線首日，Aptos 團隊在Token 分配、社區管理等方面均引發一定爭議，也讓筆者對項目團隊的能力不敢過於樂觀。

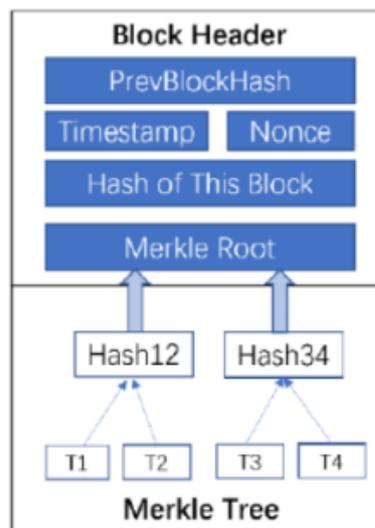
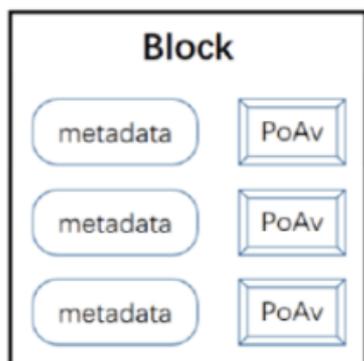
### 一、高性能

#### 1. Diem-BFT V4 共識機制

這種共識機制的核心創新之處大致如下：

- I. 首先，系統每次把一大批交易記錄壓縮成一個「摘要」（圖中的「PoAv」）。
- II. 其次，區塊中只包含「摘要」而不是全部交易記錄。

這樣一來，同樣大小的區塊，包含了更多交易記錄，也就實現了較高的擴容水平。當然，這種壓縮也會存在若干潛在風險，例如不同批次的交易記錄需要分割得不重不漏，否則會出現交易處理故障。



(1) Block structure of Aptos (2) Traditional block structure

由於Aptos 當前公佈的Tokenomics 較為模糊，我們暫時不深入研究其經濟模型的持續性問題。

## 2. 並行計算

Aptos 採用了樂觀假設，即默認交易沒有關聯性後將其並行處理。如果交易之間的相關度很低、可以並行處理，Aptos 將因為並行計算大幅加速。但如果交易關聯度很高，則Aptos 將獲得略低於ETH 的處理速度，但後果相對沒有特別嚴重。

當然，Aptos 最終選擇了16 線程並行處理，對於節點硬件的要求也是較高的，符合要求的節點數量也會有所減少（從Aptos 當前的節點篩選中也可以看出一些信號），這也會犧牲去中心化程度與安全性。

應該說，從純技術角度看並行計算，Aptos 更多是又一次的權衡取捨而非完全的創新，筆者對於樂觀假設等方案持保留態度。

## 二、Move 語言

Move 語言是Aptos 的主要敘事之一，也確實擁有較強的影響力。

Move 是一種靜態的編程語言，強調了安全性。例如，Move 不支持動態調用（Dynamic Dispatch），也就是所有的代碼必須在正式運轉前，具備讓人完全一眼看懂各種運轉關係的能力，這是更注重安全性的方案，在金融領域中具有獨特價值。Solidity 則支持了動態調用，更強調靈活性。

總體來說，Move 語言在很多區塊鏈場景中都值得採用。但Solidity 具備的靈活性等自身優勢與過往積累，也足以維持相當數量的用戶。

Aa	☰ Solidity	☰ Move
图灵完备	是	是
安全性	差	极好
开发者友好	是	是
分散存储	否	是
工程能力	差	良好
灵活性	动态调用	泛型编程
金融场景增强	否	 Buidler DAO

## 新公鏈與以太坊的對決

筆者對Aptos 衝擊以太坊持悲觀態度，雖然Aptos 與以太坊在區塊鏈性能層面各有取捨，但在多鏈未來的角度中，當下以太坊與Aptos 很難稱為同一維度的競爭對手：

以太坊已經構建起了安全且規模宏大的多鏈體系（包括Optimism、Arbitrum、Starkware、Zksync 等若干Rollup），且部分Rollup 已經有了接近新公鏈龍頭的發展水平，而Aptos 暫時仍屬於流動性割裂的單鏈。安全的多鏈體系將是以太坊隱形的護城河。

### 一、多鏈未來

首先，由於區塊鏈天生存在不可能三角，而區塊鏈上的賽道逐漸增多（Defi、Gamefi、NFT...）等，一條區塊鏈很難滿足多種用戶需求，所以未來一定會是多鏈的。

### 二、跨鏈的風險性

2021 年，高性能新公鏈、各賽道專用鏈飛速發展，但與此同時，用戶也注意到了極為明顯的問題，就是跨鏈風險與流動性割裂。如果一個用戶在Aptos 上購買和使用域名，在Solana 鏈上玩Stepn，在Flow 鏈買最新的NFT...用戶可能需要經常在不同區塊鏈之間劃轉資產，但目前為止，暫時沒有出現安全的跨鏈交互手段。「跨鏈橋」這種應用，因為多次出現被盜新聞，已經被業界稱為「黑客的提款機」。

眾所周知，單個區塊鏈受到共識機制的約束，是安全的。但兩條區塊鏈交互時，沒有一個共識機制來約束，因此跨鏈橋類項目存在無法消除的安全風險。

因而筆者對於多鏈時代的預測，是安全的多鏈體系，而不是流動性割裂的若干單鏈。

### 三、多鏈體系的安全性

在多鏈時代，以太坊做為共享安全層，各具特色的Rollup 滿足不同的用戶需求，其實是非常安全的多鏈體系。

設想一下，用戶可以存入資產去IMX 玩Illuvium 遊戲，也可以通過以太坊主鏈，將資產轉移至Arbitrum 參加奧德賽做任務，這些資產轉移過程（Cross-Rollup），都是由以太坊主鏈保證安全性，規避了絕大多數跨鏈中存在的問題。

## 四、以太坊的強大多鏈體系

以太坊的多鏈生態已經有了強大的競爭力，以太坊上的兩大OP Rollup: Optimism 和Arbitrum 的TVL 都衝進了前8。而在明年的以太坊上海昇級中，預計以太坊上各種Rollup 項目與以太坊交互的成本將大幅降低，這將促使各種Rollup 發展再次出現飛躍，進而使以太坊為共享安全層的多鏈體系擁有極為穩固的行業地位。

此外，以太坊Rollup 中的ZK Rollup 也在快速發展，且ZK Rollup 長期來看，在安全性、交易速度、交易費用等多個維度均相比OP Rollup 有更高的上限。隨著Zksync 本月上線主網，Polygon zkvm 與Scroll 的發展，在不遠的將來，ZK Rollup 的生態也將有望達到新公鏈龍頭的水平，Aptos 等流動性割裂的單鏈，即便有多鏈發展規劃，衝擊強大的以太坊多鏈體系，也是有極大難度的。



[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）<<<<](#)

## 結語

---

從目前來看，在新的公鏈競爭賽道裡，剛剛上主網的 Aptos 是有望接棒的 Solana 的，但想要與以太坊競爭仍然是比較困難，甚至可以說目前兩者很難稱為同一維度的競爭對手。

當然，Aptos 實際上是否可以接棒以及接棒後的實際發展情況，就要考驗項目團隊的能力了。

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。