High Performance L1 - Solana

資工碩一 張語棠 R13922116

大綱：

- Solana 介紹
- Solana 的團隊背景
- 融資情況
- 技術機制
- Solana TVL 數據
- 近期發展更新
- 總結：爲什麼 Solana 能夠改變未來？

Solana 介紹：

Solana 是由 Anatoly Yakovenko 所創立，Anatoly Yakovenko 在 2017 年提出 Solana 的白皮書，並隨後在 2018 年與在高通的前同事完成測試網的開發工作，2019 年開始陸續創投機構獲得數千萬到數億美元的投資。

Solana 順利在 2020 年三月上線，號稱是「世界上最快的高性能公鏈」，也由於 Solana 交易速度快速、手續費低廉，故很大程度上彌補了以太坊的缺陷，這也是為何加密貨幣社群將 Solana 稱為「以太坊殺手」的主要原因。

由於功能的不斷完善，以太坊早已成為僅次於比特幣的主流區塊鏈平台，擁有大量的用戶和交易量，但隨著以太坊的廣泛使用，許多問題也開始顯現，例如最主要的就是網路擁塞、手續費高昂、交易速度緩慢等三大問題。

由於進入以太坊的使用者越來越多，這導致了以太坊網路的擁塞十分影響使用者的體驗，儘管以太坊正向更高級的 ETH 2.0 邁進，但開發進展卻十分緩慢，故這使得大量的以太坊使用者開始尋找新的公鏈來替代以太坊。

而 Solana 就是為了解決以太坊網路擁塞、手續費高昂、交易速度緩慢三大痛點而生的新區塊鏈。

Solana 之所以能夠那麼快地崛起，很大一部分的原因是 Solana 實現了被稱為區塊鏈不可能的三角，即「安全性、去中心化、效率」，由於 Solana 在每秒可以處理的交易量、平均交易手續費、交易延遲時間都勝過以以太坊為頭的其他智能合約區塊鏈，在驗證者數量上也有顧及到去中心化程度。

Solana 四大特色

1.去中心化程度

比特幣使用傳統的 PoW (Proof-of-Work) 工作量證明機制，以太坊則轉型 PoS (Proof of Stake) 權益證明機制，而兩者皆擁有著大量的使用者，並在全球各地擁有超過 50,000 個節點來保護區塊鏈上的安全，而這樣的共識機制是目前最去中心化的，並且安全性高，但也由於使用者數量龐大，故傳輸速度低落一直是嚴重問題。

而 Solana 同樣是使用以太坊 PoS 機制為基礎的 DPoS 機制，雖然目前 Solana 在全球擁有著近 2,000 個節點，雖然沒有達到比特幣、以太坊的去中心化程度，但也遠遠超過了其他同樣使用 PoS 的公鏈。

2.代理權益證明機制 (DPoS)

所謂的代理權益證明機制 DPoS (Delegated Proof of Stake)，是以 PoS 權益證明機制為基礎衍生，與其不同的地方在於多了 Delegated (委託)。

而 Delegated 的意思是 DPoS 與 PoS 相同都是以質押代幣的方式去獲得驗證交易的資格，而 PoS 是質押越多代幣則獲得驗證與記帳的機會越高，DPoS 則是表現越好越穩定，那麼就越能夠獲得機會。

DPoS 的概念可以理解為一場選舉，用戶所質押的 SOL 幣是選票，投票 (Vote) 選出驗證者 (Witness) 來負責驗證與記帳區塊，並且有著負責監督的代表人 (Delegates) 負責維護 Solana 鏈的穩定性與性能。

能夠當選的驗證者 (超級節點) 的數量較少，且如果驗證者的表現不好，選民們可以再投票罷免該驗證者，換上更好的驗證者來維持 Solana 的性能。

因此汰弱留強的 DPoS 機制交易速度通常會比 PoS 來得更快更有效率。

3.歷史證明機制 (PoH)

在歷史證明機制 (Proof-of-History,PoH) 出現之前，區塊鏈上要完整紀錄交易的話，是由一個節點將交易資訊打包成區塊，再分發給其他的節點，等到所有的節點都接受且更新區塊鏈，交易才算是完成，雖然安全性高但速度慢，因此容易有交易「塞車」的狀況發生。

然而，另一個讓 Solana 可以在交易處理速度上大勝其他區塊鏈的，就是推出創新的歷史證明機制 (PoH)。

歷史證明機制 (PoH) 是透過創建歷史記錄，證明交易在一個特定時間發生，PoH 會先記錄交易發生的順序，再由各個節點來更新與同步狀態。

以餐廳來比喻的話，歷史證明機制就像發放號碼牌，先記錄了客人先來後到的順序，就不會需要一大群人在門口大排長龍。

Solana 透過歷史證明機制 (PoH)，就不需要等待所有節點驗證就能夠通過該筆交易，既節省資源也節省時間，如此一來 Solana 得以實現高交易速度的目標。

4.傳輸效能高

Solana 身為第三代的區塊鏈，可以說是一條性能相當出眾的公鏈之一，而作為以太坊的眾多對手之一的區塊鏈，因為透過結合不同的共識演算法，讓 Solana 可以減少交易所需的確認時間。

Solana 在每秒交易吞吐量 (TPS) 上可以處理多達 6 萬多筆的交易資訊，相當於以太坊的四千多倍，如此快速的交易處理速度，使得 Solana 成為加密世界當中最快的區塊鏈之一。

而且在平均所需的交易費用中，Solana 每筆交易也只需要 0.0015 美元，因此和其他區塊鏈相比，Solana 在高效性能和低成本等優勢的展現之下，進而增加了許多加密貨幣的莫大興趣。

Solana 之所以能夠那麼快地崛起，很大一部分的原因是 Solana 實現了被稱為區塊鏈不可能的三角，即「安全性、去中心化、效率」，由於 Solana 在每秒可

以處理的交易量、平均交易手續費、交易延遲時間都勝過以以太坊為頭的其他智能合約區塊鏈，在驗證者數量上也有顧及到去中心化程度。

Solana 的團隊背景：

Solana 團隊由一群在高性能計算、分散式系統和密碼學領域擁有豐富經驗的工程師和企業家組成。他們的專業背景涵蓋了科技、金融和軟體工程，特別是在 Qualcomm 等大型科技公司的工作經驗，為 Solana 提供了高性能區塊鏈設計的基礎。

Solana 重點人員：

Anatoly Yakovenko（Founder and CEO at Solana）：

背景：

在創辦 solana 以前，主要在 Qualcomm 工作超過 12 年，專注於分散式系統設計和高效運算。有十年以上建構高效能作業系統的經驗。

在 solana 的貢獻：

提出了 Solana 的核心創新概念 Proof of History (PoH)，PoH 是 Solana 大幅提高交易的技術。帶領團隊設計了高性能、高擴展性的區塊鏈架構。

Raj Gokal(Co-Founder of Solana)

Solana Labs 的聯合創始人 Raj Gokal 是一位來自加州舊金山的企業家和經濟學專家。作為 Web3 世界中最大的平台之一的領導者，Gokal 擔任 Solana Labs 的 COO，負責協調日常運營。

Gokal 擁有出色的商業頭腦，幫助新興的 Solana ecosystem projects 在快速變化的環境中站穩腳跟。

Greg Fitzgerald（CTO of Solana）

背景：

Greg 是 Solana 的首席架構師和 CTO。他深入探索了嵌入式系統（embedded systems）的完整領域。他為 BREW operating system 創建了一個雙向的 RPC bridge，連接 C 和 Lua，協助啟動了 LLVM compiler toolchain 的 ARM backend，並發布了多種開源項目，包括用 Haskell 編寫的 streaming LLVM optimizer、用 Python 開發的 license analysis 工具，以及用 TypeScript 開發的 reactive web framework。

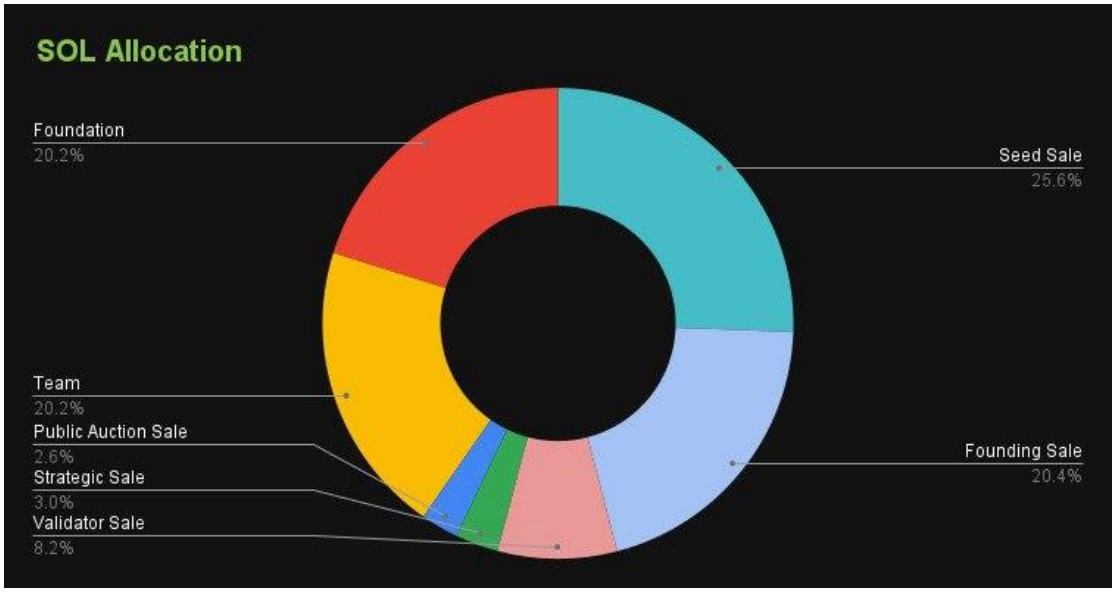
融資情況：

Solana 總共通過 13 輪融資籌集了 319.5M 美元（約 3.195 億美元）。他們最新

的一輪融資是在 2024 年 8 月 14 日，通過 Secondary Market round 完成的

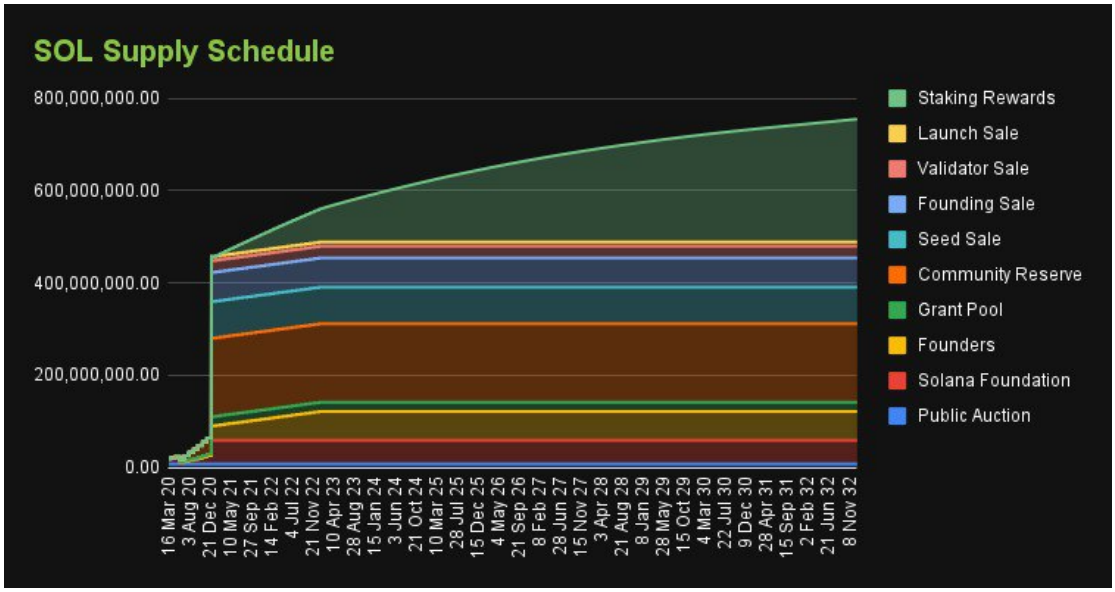
Solana Funding History

Announced Date	Transaction Name	Number of Investors	Money Raised	Lead Investors
Aug 14, 2024	Secondary Market - Solana	1	—	—
Dec 5, 2023	Funding Round - Solana	1	—	—
Feb 3, 2022	Seed Round - Solana	7	$3.8M	Lemniscap
Aug 19, 2021	Corporate Round - Solana	—	$13.8K	—
Jun 7, 2021	Initial Coin Offering - Solana	23	$314M	Andreessen Horowitz, Polychain
Mar 25, 2021	Seed Round - Solana	1	—	—
Oct 5, 2020	Initial Coin Offering - Solana	—	—	—
Mar 26, 2020	Initial Coin Offering - Solana	—	$1.8M	—
Jan 15, 2020	Seed Round - Solana	2	—	—
Jul 30, 2019	Seed Round - Solana	11	—	Multicoin Capital



上圖為 SOL 幣的代幣分配，初始分配如下：

- 15.86% SOL 幣分配給種子銷售
- 12.63% SOL 幣分配給創始銷售
- 5.07% SOL 幣分配給驗證者銷售
- 1.84% SOL 幣分配給策略性銷售
- 1.60% SOL 幣分配給公開拍賣
- 12.50% SOL 幣分配給團隊
- 12.50% SOL 幣分配給基金會
- 38.00% SOL 幣分配給社區儲備金



上圖為 SOL 幣供應時間表，首個區塊於 2020 年 3 月 16 創建，於 Coinlist 進行拍賣後，根據通膨型排放率，預計到 2030 年，SOL 幣的總供應量將達到 7 億枚。

技術機制：

Solana 是一個第三世代的權益證明 (PoS) 區塊鏈，採用多種獨特創新技術，達成高流通量、快速交易與低費用等目標：

有以下三個主要的技術：

1. **Proof of History (PoH)**

   A clock before consensus

2. **Tower BFT**

   A PoH-optimized version of PBFT

3. **Turbine**

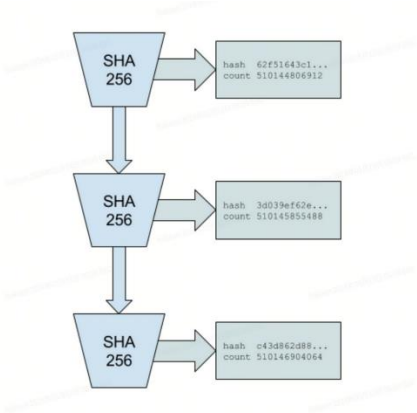
   A block propagation protocol

POH 演算法

POH（歷史證明，Proof of History）是一種用來確定交易順序的演算法。它並非一種共識機制。。POH 技術源自最基礎的密碼學 SHA256 技術。SHA256 通常用於計算資料的完整性，給定一個輸入 X，則會產生且僅產生唯一的輸出 Y，因此對該 X 的任何改變都會導致 Y 的完全不同。

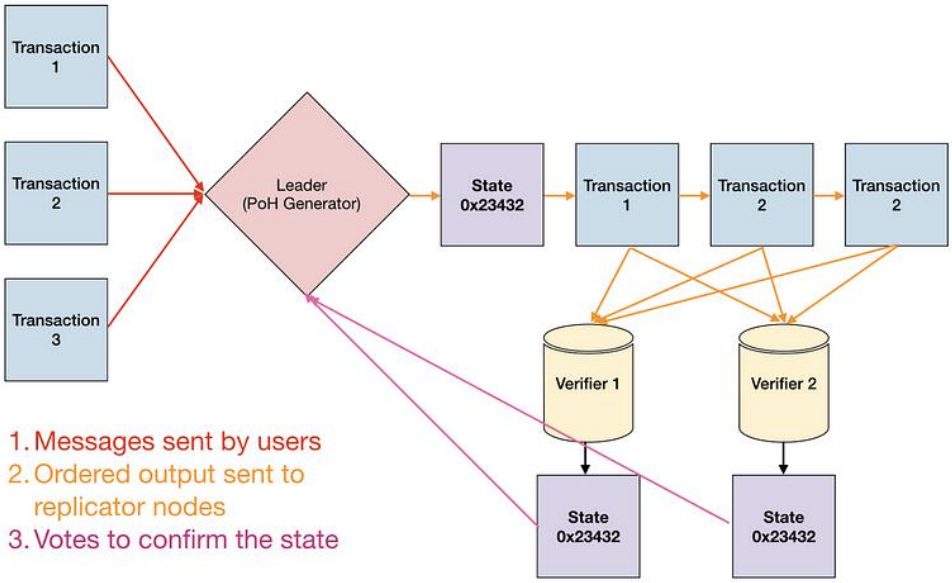
PoH Sequence

Index	Operation	Output Hash
1	sha256(”any random starting value”)	hash1
2	sha256(hash1)	hash2
3	sha256(hash2)	hash3

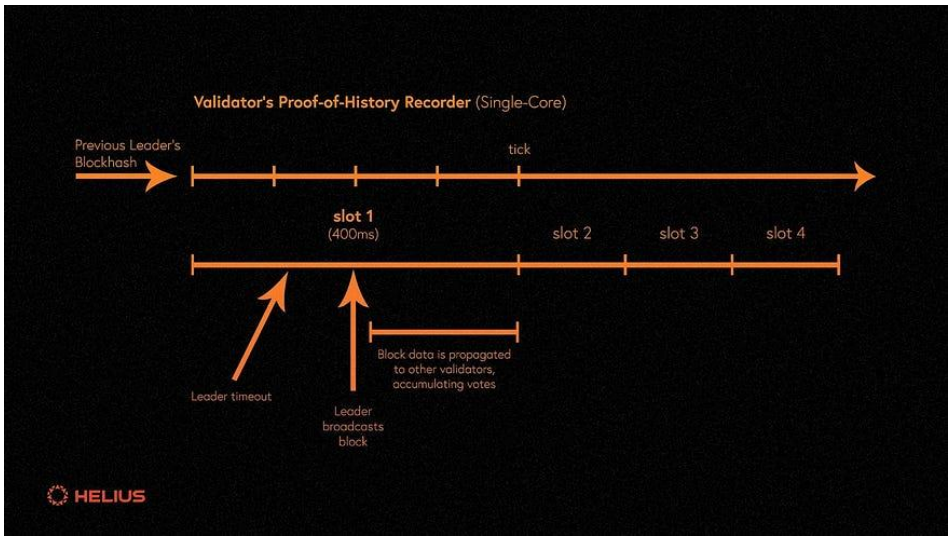


在 Solana 的 POH 序列中，透過應用 SHA256 演算法即可確保整個序列的完整性，也就確定了其中交易的完整性。舉個例子，如果我們將交易打包成一個區塊，生成對應的 SHA256 雜湊值，那麼這個區塊內的交易就被確定，任何變動都會導致雜湊值的改變。之後這個區塊的雜湊值將作為下一個 SHA256 函數的 X 的一部分，並再加入下一個區塊的雜湊值，這樣上一個區塊以及下一個區塊就都被確定下來，任何變動都會導致新的 Y 不同。

這就是其 Proof of History 技術的核心意義：上一個區塊的雜湊值將作為下一個 SHA256 函數的一部分，類似於一個鏈條，最新的 Y 總是包含了歷史的證明。



在 Solana 的交易流架構圖中，描述了 POH 機制下的交易流程。在一個稱為 Leader Rotation Schedule 的輪替機制下，所有鏈上的驗證者（Validator）中會產生一個 Leader 節點。該 Leader 節點負責收集交易、進行排序與執行，生成 POH 序列，之後會生成一個區塊並傳播給其他節點。

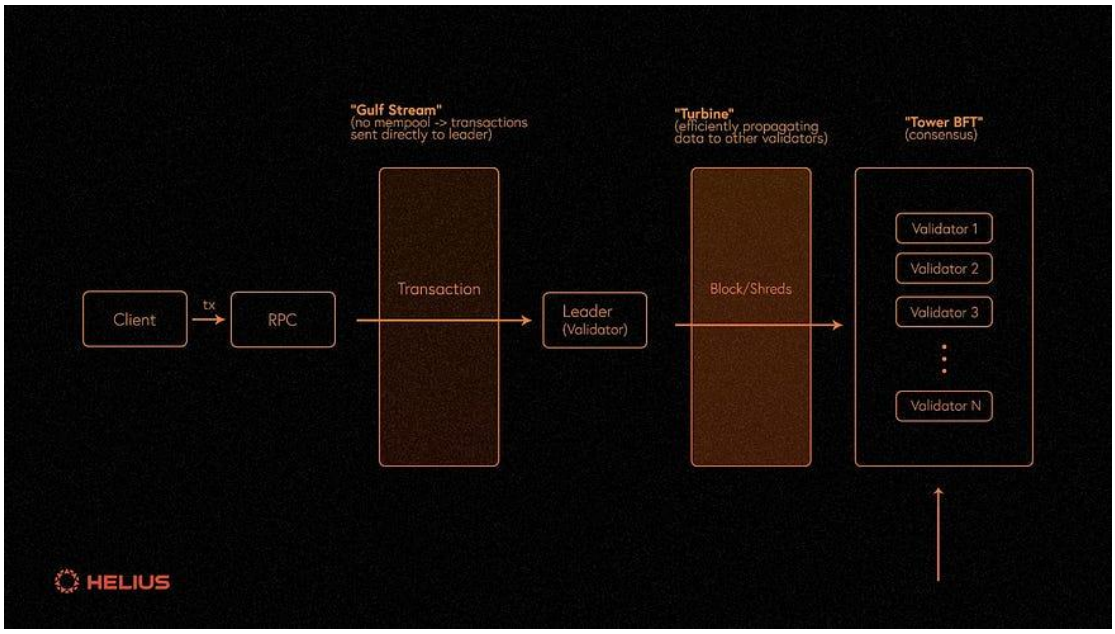


為了避免 Leader 節點出現單點故障，Solana 引入了時間限制。Solana 中的時間單位以 epoch 進行劃分，每個 epoch 包含 432,000 個 slot（時隙），每個 slot 持續 400 毫秒。在每個 slot 中，輪替系統會為該 slot 分配一個 Leader 節點，Leader 節點必須在給定的 slot 時間內發布區塊（400 毫秒），否則將跳過該 slot，並重新選舉下一個 slot 的 Leader 節點。

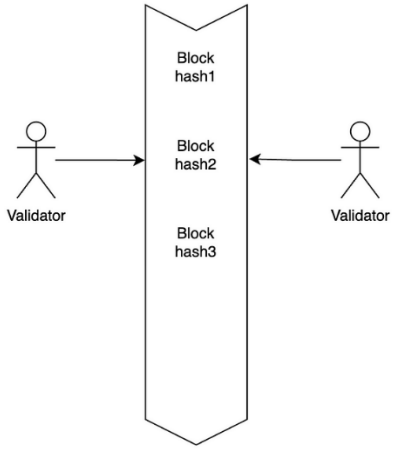
總體來說，Leader 節點通過 POH 機制能將歷史交易全部確定下來。Solana 的

基本時間單位是 slot，Leader 節點需要在一個 slot 內廣播區塊。用戶通過 RPC 節點將交易發送給 Leader 節點，Leader 節點將交易打包、排序，然後執行生成區塊，並將區塊傳播給其他驗證者。驗證者需要通過一種機制達成共識，對區塊內的交易以及順序進行確認，該共識機制採用的是 Tower BFT 共識機制。

Tower BFT 共識機制



Tower BFT 共識協議源自於 BFT 共識演算法，是其一種具體的實作，該演算法與 POH 演算法仍然密切相關。在對區塊進行投票時，如果驗證者的投票本身被視為一種交易，那麼用戶交易以及驗證者交易所形成的區塊雜湊也能作為歷史證明。無論是用戶的交易細節還是驗證者的投票細節，都能被唯一地確認。

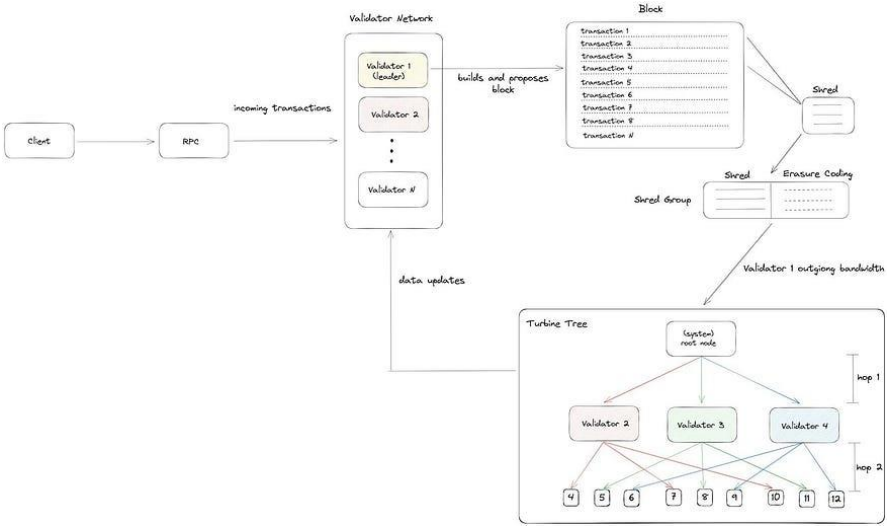


在 **Tower BFT** 演算法中規定，若所有驗證者對某個區塊進行投票，且超過 2/3

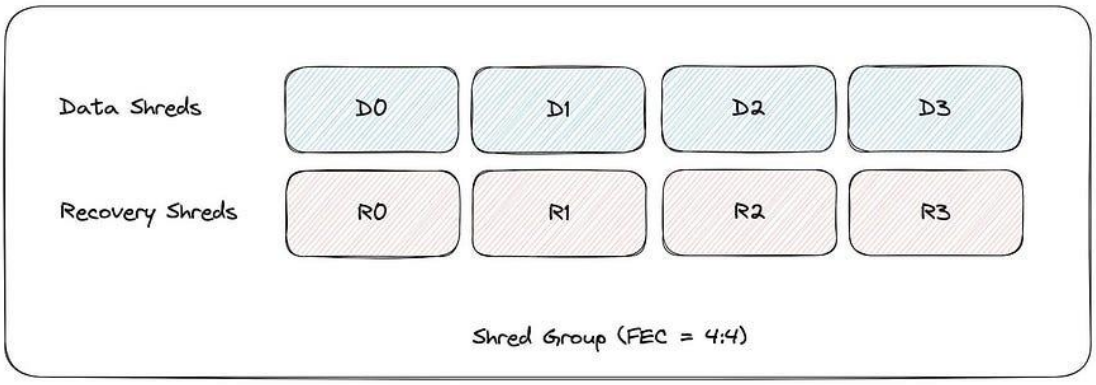
的驗證者投了「批准」（approve）票，則該區塊即可被確定下來。該機制的優點是節省大量記憶體，因為僅需要對雜湊序列進行投票即可確認區塊。然而，在傳統的共識機制中，通常採用的是區塊泛洪（Block Flooding）的方式，即驗證者接收到區塊後會將其傳送給周圍的其他驗證者，這會導致網路中的大量冗餘，因為驗證者可能接收到多次相同的區塊。

在 **Solana** 中，由於存在大量驗證者的投票交易，並且因為 Leader 節點的中心化帶來的高效性以及 400 毫秒的 Slot 時間，導致整體區塊大小以及出塊頻率都特別高。大區塊在傳播過程中，會對網路造成很大的壓力。Solana 採用了 **Turbine 機制** 來解決大區塊的傳播問題。

Turbine 機制:

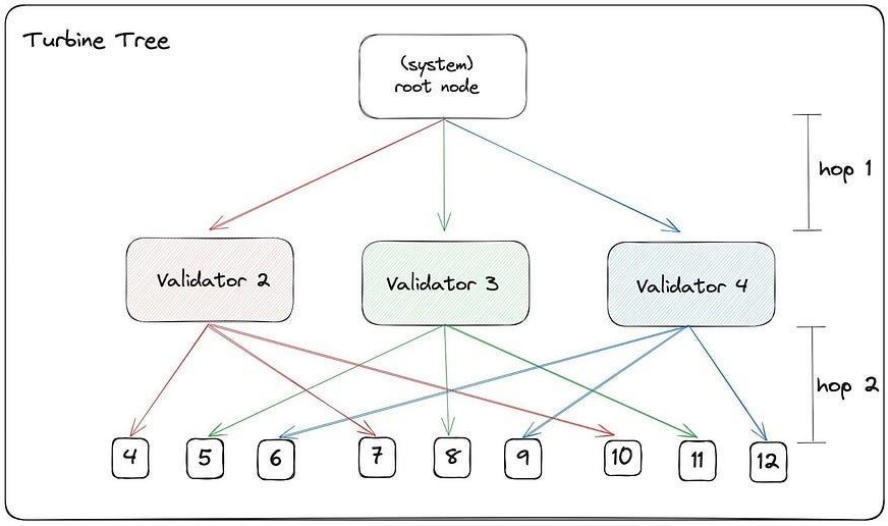


Leader 節點透過一個稱為 **Sharding** 的過程，將區塊拆分為 **shred**（子區塊）。這些子區塊的大小以 **MTU**（最大傳輸單元，指無需進一步分割即可從一個節點傳輸到下一個節點的最大數據量）為單位進行規範。隨後，通過使用 **Reed-Solomon 擦除碼方案**，確保數據的完整性與可用性。



通過將區塊分成四個 **Data Shreds**，為了防止數據在傳輸過程中丟包和損壞，Solana 使用 **Reed-Solomon 編碼** 將這四個包編碼成八個包。這套方案能容忍最多 50% 的丟包率。在實際測試中，Solana 的丟包率大約為 15%，因此這套方案能很好地兼容目前的 Solana 架構。

在底層數據傳輸中，通常會考慮使用 **UDP/TCP 協議**。由於 Solana 對丟包率的容忍度較高，因此選擇了 **UDP 協議** 進行傳輸。UDP 的缺點在於丟包時不會重新傳輸，但優點是傳輸速率更快。相對而言，**TCP 協議** 在丟包時會進行多次重新傳輸，這會大幅降低傳輸速率和吞吐量。而引入 **Reed-Solomon 編碼** 後，這套方案能顯著提升 Solana 的吞吐量。在實際環境中，吞吐量可提高 9 倍。



Turbine 將數據分片後，採用多層傳播機制進行數據傳播。Leader 節點會在每個 **Slot** 結束之前，將區塊交給任意一個區塊驗證者，該驗證者會將區塊分片成 **Shreds**，並生成糾刪碼（Reed-Solomon 編碼），然後啟動 **Turbine 傳播**。傳播過程如下：

1. **傳播到根節點**：
   根節點確定哪些驗證者位於哪一層，整個過程分為以下步驟：
   - **創建節點列表**：根節點將所有活躍驗證者彙總到一個列表中，並根據每個驗證者在網絡中的權益（即質押的 SOL 數量）進行排序，權重較高的驗證者位於第一層，以此類推。
   - **節點分組**：每個位於第一層的驗證者也會創建屬於自己的節點列表，以構建其自己的第一層。
   - **層級形成**：從節點列表頂部開始劃分層級，通過確定深度和廣度

兩個值，就可以確定整棵樹的形狀。這些參數會影響 **Shreds** 的傳播速率。

2. **節點層級優勢**：
   權益佔比較高的驗證者在層級劃分中會位於更高層級，因此能夠更早獲取完整的 **Shreds**，並恢復完整區塊。而後面層級的節點，由於傳輸損耗，其獲得完整 **Shreds** 的概率會降低。如果這些 **Shreds** 不足以構建完整的碎片，這些節點會要求 Leader 節點重新傳輸數據。此時，數據傳輸將從樹內部傳播，而第一層的節點已經提前完成完整區塊的確認。後面層級的節點完成區塊構建的時間會更久。

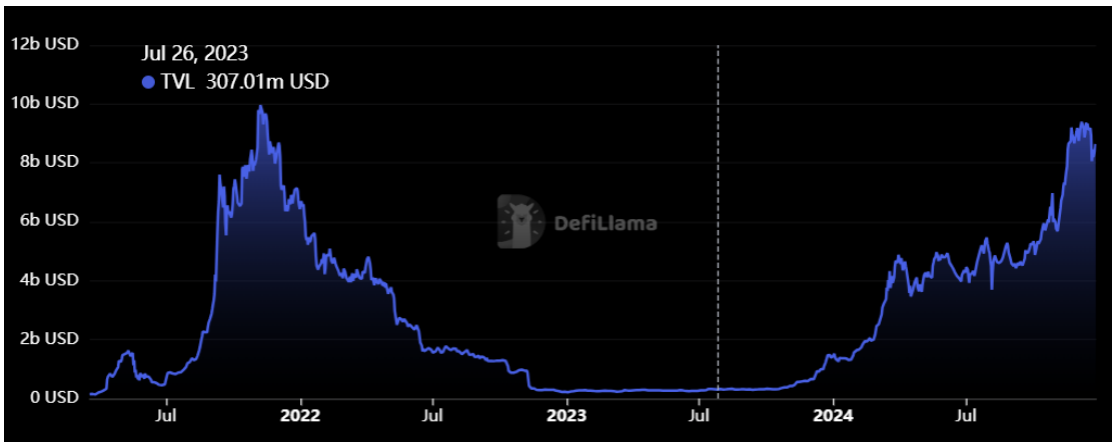
這套機制的核心思想類似於 Leader 節點的單節點機制。在區塊傳播過程中，一些優先節點（通常是權益較高的節點）會首先獲得 **Shreds** 並組建完整區塊以達成投票共識。將冗餘數據推向更深層級，能顯著加快 **Finality** 的進程，並最大化網絡的吞吐量與效率。實際上，前幾層的節點可能已經覆蓋了 2/3 的網絡節點，因此後續節點的投票對最終共識影響不大。

Solana TVL 數據：

總鎖倉價值（TVL），全名為 Total Value Locked，指的是 DeFi 協議（平台）的流動性資產總量，是常被用來衡量在資金池裡鎖定的代幣資產總量的指標，通常以美元為單位。

有些投資者會透過此指標來快速地判斷 DeFi 項目的市場整體狀況與市佔率，亦或者直接與其他不同 DeFi 協議的 TVL 指標做比較，評估該協議是否有價值或潛力。

Solana TVL: $8.587b (2024/12/26)



分析：

Solana 的 TLV 基本上跟著大盤走，之前 2021-2022 和這次 2024~的牛市 Solana 的 TLV 也跟著漲與跌。

近期發展更新：

主要挑戰：

1. Solana 有時候會停機

Solana 網絡有時會崩潰。每一次網絡故障都是對社區信任的打擊，必須儘快解決這個問題。

2. 競爭對手也在進步

更新 2.0 的以太坊、Avalanche 和 Polkadot 是強有力的競爭者。爲了生存，Solana 不僅要保持發展勢頭，還要提供獨特的東西。

3、加密貨幣市場受到監管機構密切關注。 Solana 必須迅速適應新規則，以避免失去優勢。

2025 年預測

• SOL 價格：如果生態系統繼續發展，SOL 可能會達到 150-300 美元。如果大規模實施 - 甚至更高。

• 生態系統增長：平臺上的 dApp 和項目數量將增加一倍甚至三倍。 Solana 將成爲 Web3 開發人員的中心。

• Metaverses 和 GameFi：Solana 可能成爲遊戲和虛擬世界的關鍵區塊鏈。

總結：爲什麼 Solana 能夠改變未來？

Solana 不僅僅是一個平臺。這是對既定標準的挑戰。它的速度和創新爲創造一個讓區塊鏈成爲日常生活一部分的世界帶來了希望。如果能夠克服其弱點，Solana 可能會在 2025 年成爲下一次加密貨幣革命的領導者。

參考資料：

https://www.linkedin.com/in/anatoly-yakovenko/

https://dailycoin.com/anatoly-yakovenko-founder-of-solana/

https://www.ccn.com/news/solana-ethereum-killer-anatoly-yakovenko/

https://www.oanda.com/bvi-ft/lab-education/cryptocurrency/sol/

https://medium.com/@miixcapital/solana-%E8%B0%83%E7%A0%94%E5%88%86%E6%9E%90%E6%8A%A5%E5%91%8A-59248789aaee

https://dailycoin.com/raj-gokal-solanas-right-hand-man/#h-who-is-raj-gokal

https://www.crunchbase.com/organization/solana-io/investor_financials

https://www.blockchain-council.org/blockchain/what-is-proof-of-history-and-how-does-it-work/

https://www.youtube.com/watch?v=7nFsvTaMi1M

https://www.rayskyinvest.com/58954/defi-tvl#TVL-%E6%98%AF%E4%BB%80%E9%BA%BC%EF%BC%9F

https://www.binance.com/zh-TC/square/post/18005181641170

https://medium.com/@gate_ventures/%E8%AF%A6%E8%A7%A3solana-%E7%9A%84%E6%8A%80%E6%9C%AF%E6%9E%B6%E6%9E%84-

%E5%B0%86%E8%A6%81%E8%BF%8E%E6%9D%A5%E7%AC%AC%E4%BA%8C%E6%98%A5%E5%90%97-47a7d7bb64fd