2023 Fall DeFi 期末報告

ZK decentralized sequencer- Espresso system

Group 75 陳彥倫 陳昕

## I.TDLR

### What is a sequencer?

* 排序器從區塊鏈用戶接收交易訊息，交易會被記錄在排序器的platform
* 接著排序個筆交易，並週期性地將它們傳送至CanonicalTransactionChain合約中
* 如此一來將可以確保交易資料的順序及數據可用性以達成類似「快車道」的效果，並降低了gas成本。

### What if it’s unavailable?

* 若排序器無法使用或是中毒，layer 2的使用者將可以直接上傳交易至CanonicalTransactionChain合約。為了避免有惡意用戶的交易紀錄包含了可能使batch無效化的內容，設定適當的延遲是必要的。

### Espresso 排序器

* 為一去中心化共享排序層
* 作為針對Rollup 的去中心化排序和資料可用性的層，它可以充當L1 和L2 之間的中間層
* 其核心是共識協議 HotShot。HotShot 以 HotStuff 共識協議為基礎，結合了多個不同領域的最新發展成果（起搏器、可驗證資訊釋出（「VID」）等）。

HotShot 是開放的、無許可權的，它將參與排序器網路的權力下放，在提供高吞吐量和快速最終結果的同時，還保證了安全性和有效性。HotShot 採用的是權益證明（「PoS」）安全模型，Espresso 團隊對其提出的關鍵要求之一是在不影響驗證器集規模的情況下實現強大的效能。具體來說，HotShot 至少應能擴充套件到包括所有以太坊驗證者（目前超過 70 萬）的參與。

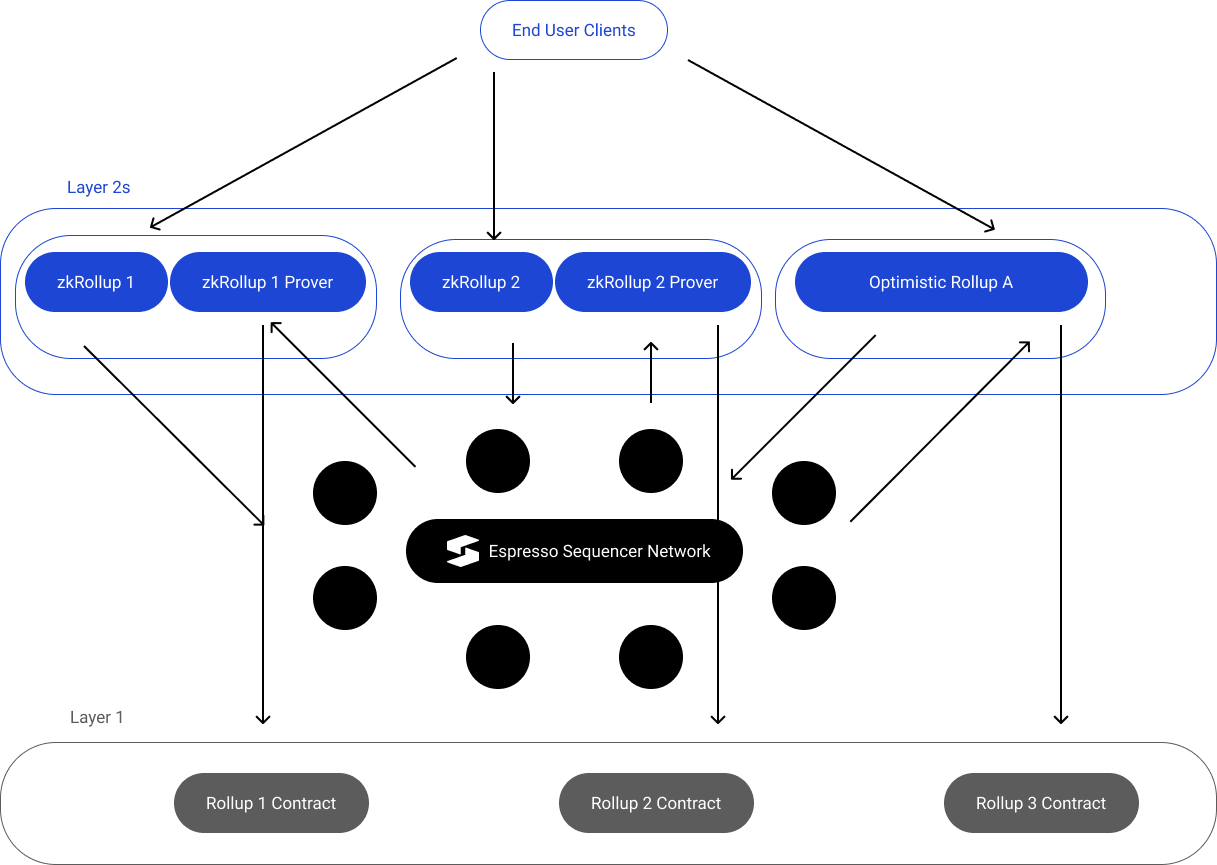


Fig.1 Espresso System Overview

## II.中心化 vs 去中心化排序器

目前以太坊上的 Rollup 大多使用中心化排序器。儘管中心化排序器性能出色，能為信任服務的用戶提供高吞吐量、低延遲和即時確定性，但它卻削弱了許多原本在以太坊上運行應用程式的優勢。

在中心化排序器和完全去中心化共識之間，存在折衷方案：用去中心化共識協議替代中心化排序器。在理想情況下，這種協議能提供比以太坊原生系統更高的吞吐量和更快的交易確認。該協議只需要負責交易的排序和可用性，而不需要執行。如果與適當設計的共識協議結合，將執行與排序和可用性分開可以為吞吐量帶來巨大的益處。這種方法可以將交易數據傳播從共識的關鍵路徑中移除，意味著可以交換多輪共識消息，這些消息只引用區塊的哈希值，而區塊的數據內容尚未被所有節點接收，但保證最終會到達或可用。還可以讓 layer 1 的驗證者參與操作此共識協議，以增加序列器的去中心化程度和與 layer 1 的共享安全性。

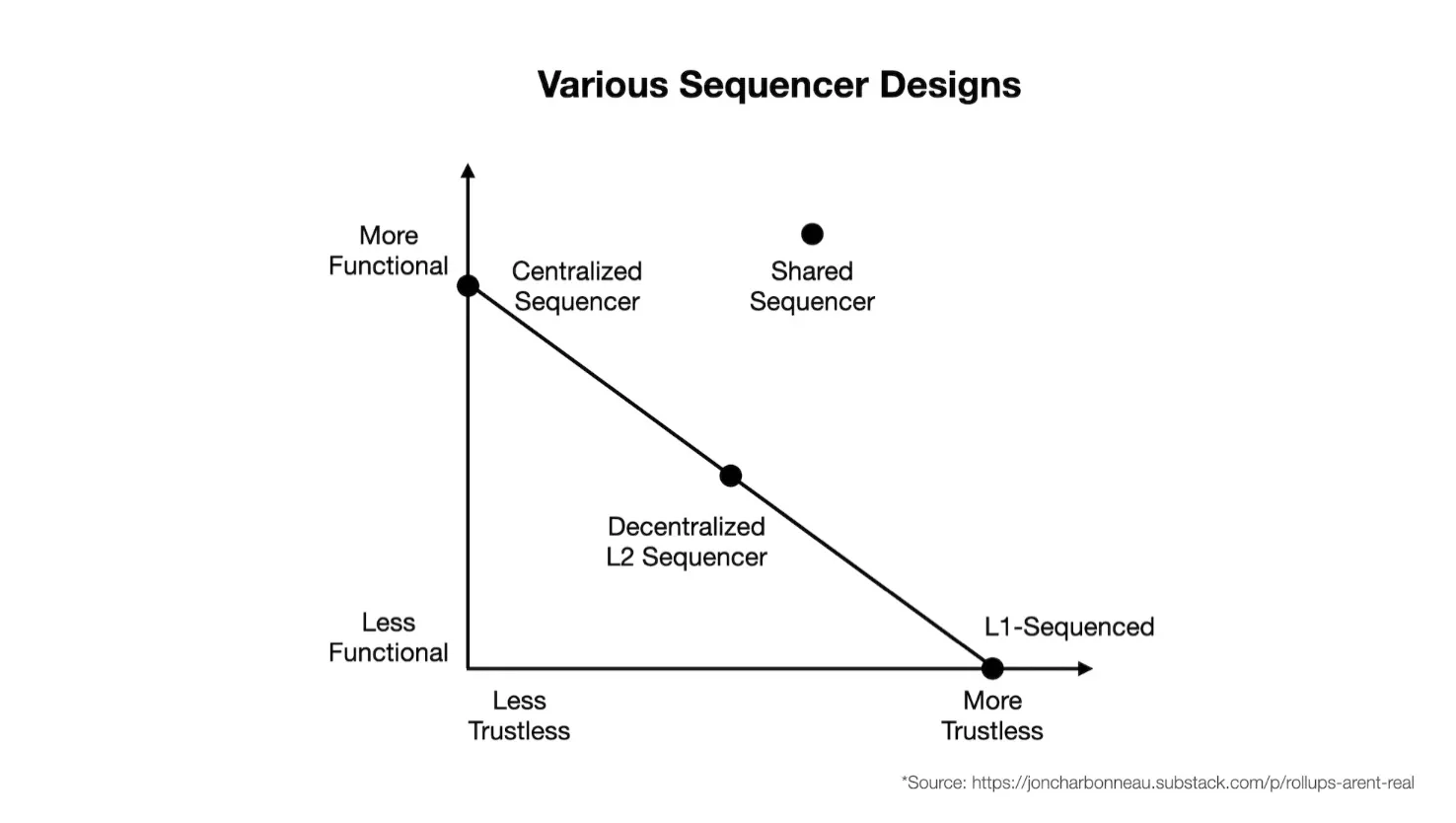


Fig.2 Trade-offs between centralized and decentralized sequencer

## III.安全性

安全性對於 Espresso sequencer 來說是一項十分重要的議題，因為它的核心目標即是移除信任在中心化排序器中的必要性。

在數據可用性方面，其是指節點對區塊鍊網絡中交易數據進行查看和下載的需求。它要求在一定時間段內產生的所有交易數據都能被整個網絡獲取並見證。

在達成共識之前，所有參與共識的節點之間必須傳播所有交易數據，這一標準要求是排序（即共識）協議吞吐量的基本瓶頸。因此，透過一些設計將數據可用性外包給一組較小的受信任節點來進行性能/安全性權衡。這組節點，稱為 DA commitee，也可能從較大的權益質押集合中隨機抽樣，並在每個時期甚至每個區塊進行輪換。Commitee 可以繼續傳遞數據，以便所有節點最終都能趕上，但不會影響共識進展的關鍵路徑。這通過利用數據在較長的延遲窗口內以更高吞吐量傳遞的事實來提高共識吞吐量，但如果需要在必須做出決策的短延遲窗口內到達每個節點，則可能會迅速成為共識瓶頸。

另一種解決方案是 VID，它在所有參與共識的節點之間可驗證地分配數據的糾刪碼(erasure codes)份額，以便擁有足夠高權益份額的任何節點子集都能夠協同恢復數據。VID 大大降低了使一個數據塊可用所需的廣播通信複雜性（漸近地消除了對節點數量的依賴），但大大增加了數據恢復的複雜性。

## IV.與區塊鏈生態的互動

* + Americano 是 Espresso Sequencer 和 HotShot 的第一個測試網路。而這次發布代表了僅限內部使用的測試網，以及對optimistic network path的初始基準測試集。
  + Doppio 是 HotShot 和 Espresso Sequencer 的第二個重要里程碑和測試網。與此同時，Espresso Systems 釋出了整個專案的白皮書。Doppio 為 HotShot 帶來了許多效率上的改進，包括可驗證資訊去中心化（「VID」）、新的檢視同步子協議和法定人數證書的簽名聚合。Doppio 還實施了 Tiramisu 的前兩層，預計未來的測試網將包括第三層和最後一層。Espresso Systems 還發布了其排序器與全功能 zk-rollup 的首次端到端整合，特別是 Polygon zkEVM 的分叉。

## V.未來展望

第三層（「L3」）即服務公司 Spire 宣佈將與 Espresso Sequencer 和 Tiramisu 整合。Spire 的基礎設施允許開發人員在 zkEVM L2 之上輕鬆部署自己的 L3 應用鏈。Spire 將與 Espresso 團隊合作，將他們的解決方案整合到 Spire L3 框架中。測試網路預計將於 2024 年建成。

## VI.資料來源

https://www.espressosys.com/

https://hackmd.io/@EspressoSystems/EspressoSequencer#The-Espresso-Sequencer

https://medium.com/@richardchen\_81235/intro-to-shared-sequencing-1622d1fd51c9

https://group.hashkey.com/zh/insights/layer-2-explained-optimistic-rollup