

## alpha network是一個與 EVM 兼容的區塊鏈

旨在補充原始無evm虛擬機的move語言的公鏈(如: aptos)。作為權益證明區塊鏈, 尋求帶來可擴展性、安全性、魯棒性和對 evm虛擬機的實用性。簡而言之, alpha network不與move語言的公鏈。相反, 它旨在與原始 move語言的公鏈相協調並通過智能合約增強它能力。

值得注意的是, alpha network 項目是一個nft 交易所優先的應用型區塊鏈, 旨在授權move語言使用者和愛好者。alpha network最終將為move語言用戶提供可以訪問區塊鏈遊戲、NFT 和不斷增長的 DeFi 生態系統, 其中之一是他們可以展示他們最喜歡的 nft, 用於廣泛的應用。

## alpha network帶來的解決方案

alpha network 的主要目標是通過為其提供急需的實用程序。aptos用戶只需包裝他們的 \$APT 即可實現這一目標。進入 alpha network 智能合約並獲得 \$APT PoS 代幣作為回報。\$wAPT 代幣生活在 alpha network 區塊鏈上, 將允許用戶訪問 DeFi 產品的生態系統, NFT 和 GameFi, 都間接由其原始的 \$APT 代幣提供支持。潛力的例子用例包括:

- 通過支付gas費來鑄造和交換NFTs, 參與NFT市場與 \$APT。
- 參與利潤豐厚的 GameFi 機會並參與不斷發展的區塊鏈遊戲社區。
- 加入去中心化交易所交換代幣並推測其價值。
- 訪問先進的金融工具, 如抵押、借貸、借貸和流動性挖礦。
- 通過基於alpha network的 NFT 參與即將到來的元界革命。
- 參與 DAO 並資助整個社區。
- 還有更多.....

總而言之, alpha network 承諾將一次性使用的 alpha network 加密貨幣轉變為 DeFi 強國。運氣好的話, alpha network 將能夠輕鬆與許多頂級智能平台競爭當前區塊鏈環境中的合約平台。

## **alpha network 的特點**

alpha network 依賴於 Polygon Edge 框架來構建其獨立的、與 EVM 兼容的區塊鏈。EVM 代表 Ethereum Virtual Machine, 意思是這個智能具有合約功能的平台將與部署在以太坊上的 dApp 兼容。

EVM 是以太坊區塊鏈的核心, 在創建去中心化的應用程序。特別是, 它允許開發人員構建和部署解決方案, 並協議更快(而不是從頭開始構建它們)。的確, 與 EVM 兼容的協議採用了穩健且經過驗證的架構, 因此是一種 DeFi 產品開發人員的遊戲規則改變者。除了現有協議之外, alpha network 還將提出自己的智能合約, 從而建立在廣泛的 DeFi 生態系統之上。比特幣和其他以支付為中心/價值存儲的區塊鏈無法調用與支持智能合約的平台的需求相同。相比之下, alpha network 的提升能力 Web3 生態系統生產力有望增加區塊空間需求。本次活動同樣在增加對 alpha network 的原生加密貨幣 \$AN 代幣的需求方面發揮了作用。鑑於 alpha network 的高吞吐量和去中心化能力, 代幣用戶將不需要遭受與許多 PoW 代幣相關的相同用戶擔憂(包括低交易每秒、公鏈擁堵、中心化挖礦和高額交易費用)。而且, 由於其 PoS 架構, alpha network 將保持高度的去中心化。alpha network 依賴預定義數量的驗證器來促進其權益證明 (PoS) 共識機制, 一種可以縮短出塊時間並降低費用的設置。在 PoS 中, 擁有最多質押代幣的驗證人候選人被允許成為驗證人並產生積木。該代幣還採用了削減方案, 因此具有安全性, 去中心化、可靠性、透明度、穩定性和區塊確定性。

## **alpha network 的主要特點**

alpha network 依賴於以下關鍵原則:

- IBFT Proof-of-Stake (PoS) 共識: 社區用戶可以參與

網絡，確保無許可和去中心化的區塊鏈。

- EVM 兼容:現有的以太坊智能合約可以輕鬆遷移到狗鏈無需任何進一步修改。
- 去中心化治理:社區成員(代幣持有者)可以提出提案,委託,對區塊鏈參數和事件進行投票,並影響治理決定。
- 跨鏈兼容性:alpha network可以在alpha network網絡上輕鬆使用通過alpha network鏈橋包裹apt, 並發送回apt網絡根據需要。



## 以太坊虛擬機(EVM)

虛擬機是可執行代碼和執行代碼之間的抽象層機器。該層對於提高軟件的可移植性並確保應用程序彼此分開並與它們的主機分開。

以太坊虛擬機 (EVM) 是一個軟件平台，開發人員可以使用它來構建以太坊上的去中心化應用程序(dApps)。所有以太坊賬戶和智能合約住在這個虛擬機裡。

以太坊虛擬機和 EVM 代碼是使用內存、字節以及區塊鏈概念，例如工作量證明 (PoW) 或權益證明 (PoS)、默克爾樹和哈希函數。EVM 的目的是確定以太坊的總狀態是什麼區塊鏈中的每個區塊。

## 共識協議

### 工作量證明(PoW)——中本聰共識

工作量證明 (PoW) 是一種去中心化的共識協議，可以在對等網絡，無需任何受信任的第三方。它解決了拜占庭的困難礦工可以生成任意身份的開放網絡中的一般問題（也稱為 Sybil 攻擊）通過解決隨機散列難題來競爭下一個生成的塊。為了避免 Sybil 攻擊，PoW 用於強制礦工擁有並運行預定義的計算資源。此外，PoW 保護區塊鏈的安全性不受最長的連鎖攻擊。不幸的是，PoW 需要大量的能量來保持隨著越來越多的礦工加入網絡而增加。

### 伊斯坦布爾拜占庭容錯 (IBFT)

IBFT 是另一種基於實用拜占庭容錯的拜占庭容錯協議 (PBFT)。在高層次上，拜占庭共識是確定性地實現的，如下所示：選擇領導者或投標人/提議人。

每個提議的區塊都經過節點之間的幾個通信階段

在被添加並在區塊鏈上確認之前。

節點之間交換的消息有四種類型：

- Pre-Prepare、Ready、Commit: 通過普通的共識算法操作使用。
- Round robin: 用於在當前生產者是時選擇新的塊生產者懷疑失敗或在特定時間範圍內未創建塊時。

此外，Polygon Edge 框架中有兩種選擇塊的方法

生產商：

- Round-robin: 這是一種區塊生產者選擇策略，其中不同的投標人為每個區塊生產階段選擇。
- 附加投標人: 只有在惡意行為發生時才會選擇新的投標人。被當前投標人檢測到。

在這兩種方法中，每個驗證者都事先知道其中哪一個將成為下一個區塊生產者。這是因為決定是通過確定性計算做出的基於節點 ID。與 PBFT 類似，IBFT 也保證只有一個

每一輪的投標人。此外，投標人需要得到其他節點的響應才能繼續執行其進一步的任務。這意味著在網絡分區超過  $n$  的情況下節點（至少超過  $3n+1$  個節點），協議不做任何不中斷的決定

直到分區被修復並且他們的通信被及時同步之前的共識。這也是允許立即確定，不允許發生分叉。

### IBFT 權威證明(PoA)

在 PoA 中，驗證者負責創建塊並將它們按順序添加到區塊鏈。所有驗證器都會創建一組動態驗證器，可以在其中添加驗證器或使用分散投票機制從集群中刪除。

這意味著驗證者可以被包含或排除在驗證者組中，如果大多數 (51%) 的驗證者節點投票決定從集合中添加/刪除特定的驗證者。因此，可以在任何時間點檢測到惡意驗證者並將其從網絡中刪除，並且可以將新的受信任驗證者添加到網絡中。

所有驗證者依次提議下一個區塊(通過循環領導者選擇)。為了要驗證/添加到區塊鏈的塊，絕大多數驗證者 (即，超過 2/3) 必須批准該塊。除了驗證器，還有不直接參與出塊但參與出塊的非驗證者驗證過程。IBFT PoA 是 Polygon Edge 的默認共識機制框架

### IBFT 權益證明(PoS)

Polygon Edge Proof-of-Stake (PoS) 實施旨在替代現有的 IBFT PoA 實施，讓節點運營商能夠輕鬆地在啟動鏈時的兩個。時期被認為是特定的時間範圍 (以塊為單位) 在此期間，一組給定的驗證器可以生成塊。

epoch 長度可以改變，這意味著節點操作者可以設置實例創建期間的紀元。在每個 epoch 結束時，創建一個 epoch 塊，之後這一事件，一個新的紀元開始了。驗證器集在每個 epoch 週期結束時更新。節點在創建一個質押智能合約期間請求一組驗證器 epoch 塊並將結果數據存儲在本地存儲中。

這個查詢和保存週期在每個紀元結束時重複出現。從根本上說，這允許質押智能合約完全控制驗證者中的地址組，只留下一個任務給節點。每個合約查詢每個週期只執行一次獲取有關驗證器集的最新信息。這消除了交易的責任來自各個節點的驗證器集。

## Raft

Raft 是一種基於 Paxos 的分佈式共識機制。Raft 協議與節點故障模型，其中每個錯誤（例如，丟失消息、網絡分區或僅硬件故障）被視為節點故障。

因此，它應該運行  $n \geq 2f+1$ ，其中  $f$  是可能失敗的最大節點數， $n$  是節點總數。Raft 協議首先在一組節點中選擇一個領導者，然後讓 leader 全權負責接收事務請求和處理複製其他節點上的日誌（即塊）。

每個節點可以是候選人、追隨者或領導者。領導者選擇程序是確定性的，所以協議不能運行，直到領導者被超過一半的人選擇節點。

## 比較與選擇

IBFT 保護區塊鏈免受各種惡意攻擊，而 Raft 僅保護節點故障。如果我們假設所有節點都不會被破壞，那麼 Raft 可以不用有任何顧慮。

但是，如果假設僅對驗證者有部分信任，那麼它將是更好地利用 IBFT。由於狗狗鍊是去中心化且無需許可的，因此它將運行 IBFT 作為其底層共識協議。

## alpha network (AN) 架構

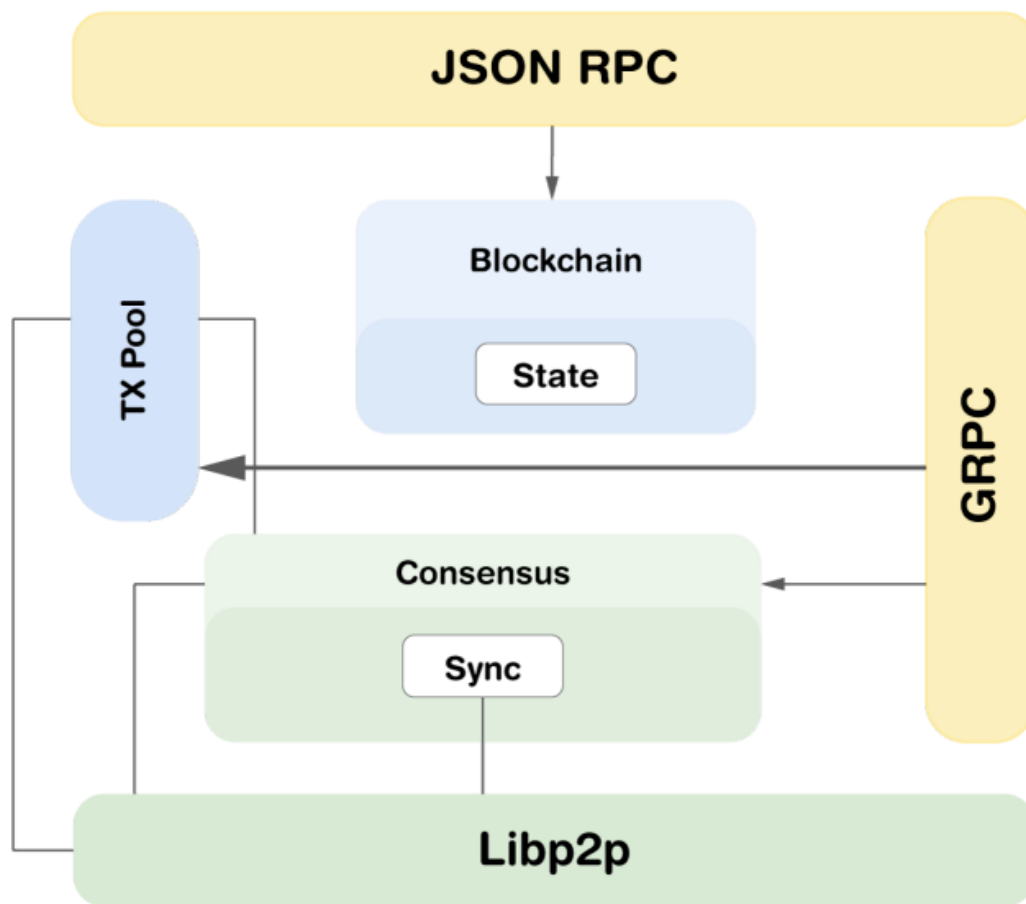
alpha network 使用 Polygon Edge 框架構建獨立的區塊鏈。最後，它不使用 Polygon 的“安全即服務”功能，而是依賴於自己的一套驗證器。值得注意的是，alpha network 禁用了兩個 Polygon Edge 功能——它的檢查點機制及其主鏈合約。

有了這個框架，我們的開發者社區可以構建一個更好的區塊鏈網絡適合他們的需要和要求。他們可以做到這一點，因為 Polygon Edge 採用了用於創建與 EVM 兼容的區塊鏈網絡的模塊化和可擴展框架，側鍊和全球擴展解決方案。畢竟，Polygon Edge 主要用於推出新的與以太坊智能合約和交易完全兼容的區塊鏈網絡。最後，Polygon Edge 使用 IBFT 共識機制，因為它提供了 PoA 和 PoS。同樣，alpha network EVM 區塊鏈使用內置系統合約調用 IBFT

PoS。和在 Polygon Edge 的幫助下, Dogechain 可以使用以下功能:

- 重用現有的以太坊智能合約技術及其API。
    - 用戶可以通過 JSON-RPC 與標準錢包進行交互。
    - 開發人員享受 Solidity/Vyper 編程和完整的 EVM 支持。
    - 訪問流行的以太坊工具、開發工具和庫。
    - 優化跨網絡交易時的用戶體驗。
  - 網絡之間的通信。
    - 完全去信任和去中心化的嵌入式以太坊橋解決方案。
    - 從任何 EVM 兼容網絡轉移資產, 尤其是 Polygon 和以太坊主網。
    - 在 shell 中轉移 ERC20 代幣、NFT 或本地代幣。
    - 使用現有插件自定義橋接功能的能力。
  - 特殊功能。
    - 通過插件開發構建網絡可用性
    - 用共識插件替換核心功能的能力。
    - 通過整合 Runtime 超越以太坊智能合約
- 得益於底層的 Polygon Edge 架構, Dogechain 可以實現完全兼容使用以太坊智能合約技術。也可以使用IBFT PoS保證高網絡去中心化、安全性和可擴展性

alpha network Layering Architecture



- Libp2p: 該模塊始終從底層網絡層開始。Libp2p 是模塊化的, 可擴展, 快速。特別是, 它為更高級的特徵。
- Synchronization & Consensus: 同步和共識的分離協議支持模塊化和可定制同步的實現  
共識機制(取決於客戶端的操作方式)。多邊形邊也提供開箱即用的可插拔共識算法。
- 區塊鏈: 區塊鏈層是管理內部任務的核心層  
多邊形邊緣系統。
- 狀態: 狀態層提供狀態之間轉換的邏輯。它處理添加新塊時狀態如何變化。
- JSON RPC: dApp 開發者將此層用作 API 層, 以便與區塊鏈。
- TxPool: TxPool 層是一個交易池, 與其他模塊緊密耦合。



系統(因為可以從多個入口點添加交易)。

- GRPC: GRPC 層對於實現與運營商的交互至關重要。這一層確保節點運營商可以輕鬆地與客戶端交互，提供可用且高效的用戶體驗。