ThunderCore（TT鏈）白皮書

2019年10月28日

目錄

第一部分：ThunderCore簡介

ThunderCore（TT鏈） 是區塊鏈公鏈，它是公開、去中心化、與乙太坊虛擬機器（EVM）相容的，並且採用全球領先的權益證明共識機制（PoS）， 其安全性經過嚴格驗證。

ThunderCore 於2018年1月成立於美國矽谷，志在結合頂尖的學術研究及區塊鏈技術專家，以大規模共識機制，打造出最快速、高安全、強擴充性的區塊鏈公鏈。

區塊鏈是一系列帶有時間戳記和具備不可竄改特性的記錄，由分散式且去中心化的伺服器（也稱「節點」）運作。 ThunderCore對所有使用者開放，允許全球參與者參加保護及驗證這些記錄。

ThunderCore不僅是個記錄交易的平臺，還可執行「智能合約」。 智能合約是以客觀和公平的邏輯直接管控各方之間資產轉移及內容分享的電腦程式。 乙太坊是最受歡迎的智能合約執行平臺，而ThunderCore與乙太坊完全相容，部署在乙太坊上的合約或應用，可在數分鐘內轉移到ThunderCore上。

這個簡介的第一部分說明為什麼需要區塊鏈，什麼是區塊鏈，以及ThunderCore創新之處。 第二部分概述ThunderCore協定的技術框架； 第三部分則闡述ThunderCore未來的發展方向。

為什麼需要區塊鏈？

任何兩個或多個實體之間的互動都需要信任，信任是依靠他人承諾並採取行動的基石。 但是，信任和承諾有可能易變，而且今社會和商業的「信任成本」非常昂貴。 然而，信任問題可以通過區塊鏈技術來解決，而不再需要個人或機構背書。 信任可由代碼提供保證，通過運用公私金鑰組加密技術和創新的獎懲機制，新協定可以讓個人和其他實體信任記錄的可靠性，而無需依賴協力廠商監督者。 人為因素有太多不確定性，原本只有通過昂貴且複雜的法律條款，甚至要通過體面的偽裝才能強制執行。 如今有了區塊鏈的智能合約，上述人為因素就可以被排除，對各方而言，區塊鏈的操作變得更高效，更可靠，更可預測，成本也更低。

初始動力

眾多行業正開始認識區塊鏈的功能和優點，其實金融行業早已關注區塊鏈。 想像一下，一個全球性去中心化的金融系統，沒有邊界和仲介機構，而系統中的合約又是不可竄改的，全部由代碼完成，那是多便捷啊！

舉例來說，目前全球約有17億人口沒有機會使用基本的理財產品，這嚴重地限制了他們選擇投資和獲得投資的機會。 然而，由於區塊鏈使用方便、價廉、耗能相當低，隨著智慧手機和數位素養的普及和發展，此前從未使用過理財產品的人，現在可以輕鬆使用區塊鏈理財了。

深度應用

區塊鏈從根本上改變了關於擁有權、可靠性、協作和信任的設想。 區塊鏈的運用極為廣泛，我們現在甚至無法想像它未來影響我們生活的深度和廣度，但區塊鏈已經改變和解決許多現有的問題，它的潛力已顯而易見。

- **反欺詐**：由於區塊鏈記錄不可竄改，且永久存在，因此區塊鏈技術可提高審計效率，降低審計成本，簡單直接地解決欺詐問題。

- **眾籌**：已有無數的成功專案運用區塊鏈技術進行公開和匿名的眾籌。 區塊鏈平臺能處理眾籌的款項，投資者則化資產為代幣。

- **遊戲**：從移動端休閒遊戲到骰子遊戲，從紙牌遊戲到競猜或橋牌拍賣遊戲，都能從區塊鏈上運作透明，成本低廉的智能合約中受益。

- **治理：**無論是私有或公共組織的章程，都可用區塊鏈與智能合約來實現。 用智能合約的代碼規範及約束組織成員的行為舉止。 智能合約直接從利益相關者那裡收集選票並執行通過的議案；智能合約同時自動執行和驗證資金或資產的收支，整個過程無需任何人為的信任操作。 公共機構還可以利用區塊鏈資訊不可竄改的特性，讓投票流程變得更公開、安全、完整、透明。 所有資訊易於驗證審核，無法被竄改。

- **擁有權**：使用區塊鏈解決方案，會使無論是現實世界或數位世界所持有的資產管理變得更簡單，更便宜，更可自己掌控。

- **個人資料擁有權**：使用區塊鏈金鑰共用技術，可以更安全、更完整地管理互聯網瀏覽和其他數位瀏覽的歷史資料。 例如，醫療記錄可以存儲在鏈上，並且可以通過私密金鑰隨時查看。 這些記錄是不可竄改的，從而改善醫生的工作和患者的醫護品質。

事實上，區塊鏈技術具有巨大的潛力，目前開發人員對它的挖掘才剛剛開始。 我們現在可以通過全新的方式來存儲價值，自動化流程並解決信任難題，且成本很低。 區塊鏈仍有大量工作和運用有待開發，前途無限。

網路訪問、電子通訊、個人計算裝置等市場已成熟並飽和；目前，已有不計其數的開發人員、從業人員和使用者投入區塊鏈行業，我們相信， 未來幾年，區塊鏈創新將迎來爆炸式增長，這將是我們這一代人從未見過的情景。 區塊鏈時代已經到來！

區塊鏈是什麼？

區塊鏈是一連串帶有時間戳記的資訊記錄，這些記錄由分散式伺服器（又叫節點）處理並確認，它的每個塊（block）記錄了消費者的交易情形，又儲存了前一塊的稽核代嗎，串成一條無法竄改的鏈。「共識協定」是區塊鏈技術的核心，指參與此網路的每一台電腦一致同意鏈中資料內容的方法，也就是規定了節點網路如何通信以及如何將新塊添加到鏈中。當然，區塊鏈協定種類繁多，每種協定都有各自不同的性能和獎懲機制。無論是哪種類型的協定，存儲在區塊鏈上的資料都具有不可變性，這個特性可作為構建新經濟體系的基礎。

不可變性

經過加密演算法的應用，存儲在區塊鏈的資料具有不可變性，亦即鏈上的資料無法被竄改或刪除。區塊鏈最大的特色是，任何試圖竄改之前交易紀錄的動作，會造成鏈上紀錄的級聯效應，破壞資料的一致性，立即被檢驗出來。

因此，區塊鏈上的資料是不可竄改的，非常適用于透明展現銀行餘額、民意調查、產品溯源認定等資訊。而更先進的區塊鏈協定，例如ThunderCore，還具有「若P則Q」的邏輯性，可以啟動被稱作**智能合約**的程式。如上所述，在特定條件下，這些智能合約可以直接管控各方之間的資產轉移，而無需任何協力廠商。這些管控規則通過代碼實現，且能取代具強制力的法律契約，因此人們常說「**代碼就是法律**」。

代碼開源

有些區塊鏈協定是**無需授權的**，允許任何電腦（又叫節點）加入；有些區塊鏈協定是**需要授權的**，設有審查機制，僅允許「經批准」的電腦加入。但是幾乎所有區塊鏈協定的代碼都是開源的，就像ThunderCore一樣，這些協定正在構建新的經濟體系。從本質上講，魯棒性強的經濟體系應允許價值的自由流入和流出。

此外，區塊鏈允許任何開發者和參與者訪問、審查、使用或改善其代碼，這也將反過來推動區塊鏈的發展。這樣一來，任何消費者，開發者或企業都可以使用區塊鏈協定，在鏈上搭建應用程式，通過部署服務來增加區塊鏈的價值。區塊鏈代碼開源盡可能地降低准入門檻，並鼓勵更多新使用者參與進來，從而提高區塊鏈系統的整體價值。

去中心化

區塊鏈網路需要電腦（又稱節點）網路來支撐，這並不是因為區塊鏈網路需要大量的運算能力；相反地，電腦數量越多，區塊鏈就會更加去中心化，魯棒性更強，性能也更強大，可以抵禦網路中斷、合謀、或腐敗等故障或攻擊行為。

可以說，去中心化是引發區塊鏈革命的核心價值。一些由政府和公司主導的中心化網站，在隱私、管控、效率方面，不可避免地需付出更高成本。而現代的經濟學和密碼學技術使區塊鏈能夠

挑戰這些問題，並提供替代方案。 區塊鏈方案將全部治理權給予使用者，並具備審查腐敗和失誤的能力。

ThunderCore 區塊鏈

區塊鏈協定在使用上遇到了一些重大的挑戰，首要是「不可能三角」的難題。 眾所周知，區塊鏈無法同時實現安全性、去中心化、和可擴充性這三個條件，必須犧牲這三者中的一個。 因此許多區塊鏈犧牲了可擴充性，接受了低輸送量和冗長的確認時間。

ThunderCore解決了上述「不可能三角」難題，並確信我們的共識協定是最好的權益證明共識協定。 （ThunderCore採用的PaLa共識協定將在本文第二部份詳述。） 此協定對任何人開放，無需授權，交易處理速度達到4,000TPS以上，1-2秒內可完成交易確認。 ThunderCore作為一個無需授權的公鏈，ThunderCore共識協定允許任何代幣持有者成為提案人（proposer）或投票者（voter），保障ThunderCore的安全性和去中心化。

無需授權

如上所述，區塊鏈分為需要授權的和不需授權的，其中不需授權是指所有人可參與，也稱公開性。 ThunderCore堅信，無需授權是讓區塊鏈發揮最大價值的最佳方式。

區塊鏈是創新的技術，基於科技的社會經濟系統， 因此ThunderCore堅信無需授權的系統是實現區塊鏈真正價值的唯一方式。 一個人是否能從科技進步帶來的創新服務與金融工具獲益，不該由任何把關者審查。 此外，區塊鏈作為一個價值轉移的平臺，很容易推論出：開放性是確保區塊鏈穩健增長的基本原則。 提高去中心程度，區塊鏈系統將會得到更好的保護。 ThunderCore 借由部署一個無需授權的區塊鏈網路， 提高了去中心化程度，從而強化了整體區塊鏈網路的安全性。

與乙太坊虛擬機器相容

我們在設計ThunderCore時，已有近200,000名開發人員具有利用乙太坊開發應用的經驗，這是一個豐富而無法忽視的人才庫。 因此，為了充分利用這個人才庫，ThunderCore的設計與乙太坊虛擬機器（EVM）完全相容，以便開發人員僅在幾分鐘內，便可將去中心化應用程式（DApp）遷移到ThunderCore上，且性能、 體驗和可負擔性都得以巨量提升。

不出所料，ThunderCore主網上線兩周內，就有多個開發團隊把他們在乙太坊上的遊戲遷移到ThunderCore上。 由於ThunderCore的高效和高輸送量，與乙太坊同類遊戲相比，這些被遷移到ThunderCore上的遊戲迅速吸引到更多交易和玩家加入。

強擴展和高效率的共識

ThunderCore的權益證明共識機制依靠PaLa共識協定來推動。 區塊鏈的每個塊包含了多筆消費者的交易紀錄，又儲存了前一塊的稽核碼，串成一條無法竄改的鏈。 共識是指參與此網路的電腦一致同意鏈中資料內容的過程；此過程是任何區塊鏈協定的核心，與其他同等級共識協定相比，PaLa共識協定是性能最先進、最高效、最簡易的，其安全性經過嚴格驗證。 PaLa共識協定技術水準之高，使得ThunderCore成為強擴展，高效率的公鏈。

本文第二部分將會詳細介紹ThunderCore技術相關內容，適合有技術背景或有興趣的讀者閱讀。

第二部分：ThunderCore技術概覽

比特幣的迅猛發展也引起了人們對古典分散式拜占庭容錯（BFT）共識協定的關注。 這些協定提供了更高的性能、最終確定性，及解決當前工作量證明（PoW）區塊鏈的擴充性問題和耗能問題的可能方向，但這些古典共識協定同時需更複雜的機制 ；如何利用古典協定同時實現無需授權參與網路又是另一挑戰。

ThunderCore共識簡介

ThunderCore最初是以Thunderella共識演算法為基礎設計的，該演算法結合了需要授權的（permissioned）古典共識協定和去中心化的中本聰共識協定的優點。 從那時起，我們的技術已再次有了顯著發展。 我們的研究團隊發現了具有卓越性能的新共識機制。 本文將著重介紹我們現用於ThunderCore公鏈的PaLa共識協定。 我們的共識協定是由密碼學和分散式共識研究領域的前沿研究人員開發的，並有嚴格的數學證明以保證該演算法的一致性（consistency）和活躍性（liveness）。

古典共識演算法一般會依照輪次進行並最多可以容忍⅓的惡意節點。 在每一輪中，一個提案人（proposer）將向由一組投票者（voters）組成的委員會（committee）提出新的區塊。 如果收到了至少⅔的委員會的支援票，則稱之為公證（notarization），這表示有足夠數量的節點已同意了區塊鏈的某個狀態。 在正常運行時，這個過程是快速、高效且安全的。 但是與此同時，我們也需要一種機制來確保可以在提案人宕機或作出惡意行為的情況下進行恢復。 該過程稱為提案人切換（proposer switch）。 提案人宕機時，投票者必須就提案人宕機前最後確認的狀態達成一致，這一任務先前是由提案人負責的。 因此，經典的共識演算法需要在一個區塊上進行兩次公證才能最終確定（finalize），即將該區塊包含在區塊鏈上不可改變的歷史中。 第一次公證用於確認狀態，第二次公證用於確認足夠的委員會成員已經認可了第一次公證。 下面我們將介紹PaLa共識演算法如何極大地簡化切換機制並優化公證過程。

PaLa共識演算法

PaLa是基於部分同步（partially synchronous）網路假設的區塊鏈共識協定，最多可容忍1/3惡意節點。 下面我們描述稱為**Basic Pala**的協定簡化版本來說明其簡單且高效。 Basic Pala是理解完整版PaLa的基礎。 完整版PaLa將在本文後段概述。 對PaLa協定的詳細資訊有興趣的讀者可以查看PaLa研究論文。

設定

假設一個固定的由**投票者**組成的**委員會**（稍後將詳述如何選擇這些節點）。 每個節點都維護一個**本地時期**（local epoch）計數器*e*和區塊鏈的本地視圖（view）。 每個區塊包含一個時期編號、一系列交易以及其父塊的雜湊值。 一條鏈的時期編號定義為其最後一個塊的時期編號。 每個時期都有一個唯一的提案人，網路中的所有節點都知道該提案人。 在此簡化版本中，每個投票者也是某些時期的提案人。

每個區塊進行一次共識。 提案人如果有資格在當前時期做出提案，則可以提出區塊。 如果滿足一系列條件，投票者就對該提案人提出的區塊進行投票。 在一個區塊中獲得委員會投票數的⅔就是對該區塊的**公證**。 如果某個區塊擁有了公證證明，則該區塊已**被公證（notarized）**。 每個塊都有一個單調遞增的時期編號。 如果一個時期e的區塊具有一個時期e-1的父塊，則該區塊稱為**正常塊（normal block）**，否則為**超時塊（timeout block）**。 如果某個區塊是一個經過公證的正常塊的父塊，則該區塊已**被最終**確認**（finalized）**。 一個已被最終確認的區塊成為區塊鏈不可變歷史的一部分並且表明已達成共識。

協定

每個節點都保持其本地的區塊鏈處於**最新（fresh）狀態**。 每當節點發現一條有效區塊鏈比其當前鏈**更新（fresher）**，即更新的鏈的時期編號高於其當前鏈的時期編號時，它們就會切換到該更新的鏈。 一條有效的區塊鏈應滿足以下條件：

1. 所有塊的時期數應嚴格遞增；
2. 區塊鏈中的每個區塊都經過公證。

此外，每個節點還將執行以下操作：

- 如果滿足以下條件則將本地時期計數器增加到*e*
    - 他們當前的本地時期小於*e* 並且
        - 他們看到一條時期e-1的已被公證的鏈 或
        - 他們看到至少⅔委員會成員的有效簽署的clock(e)消息。

- 如果他們在時期e-1停留了足夠久（一個固定數值）的時間
    - •時鐘 （e）*

- 如果他們是時期e的提案人
    - 如果他們當前的鏈以時期e-1結束，則立即為時期e提出一個新的區塊以擴展自己當前的鏈；

    - 如果其當前鏈的時期數為e（由於超時），則等待一段固定的時間（為了收到更新的鏈），並為時期e提出一個新的區塊以擴展自己當前的鏈。

- 從時期e的提案人收到時期e的區塊提案後，如果滿足以下條件，則簽署該提案並廣播簽名：
    - 他們已經看到了提案的父塊的公證；該區塊至少與時期e開始時的當前鏈一樣新；
    - 他們沒有為時期e的任何其他塊簽名。

通過這些簡練的規則，PaLa共識協定可實現活躍性和一致性。 PaLa協定簡潔且經過嚴格證明。 PaLa是基於部分同步網路的假設而設計的，因此從本質上是分區容忍（partition tolerant）和回應積極的（responsive）。 如果存在網路磁碟分割，則活躍性只會暫時中斷。 當分區恢復，它將恢復進度且不會產生任何狀態衝突。

委員會重新配置和雙流水線PaLa

在現實中的權益證明區塊鏈中，我們希望隨著權益在系統中的易手而定期更換委員會成員。 PaLa共識演算法支援高速流暢的委員會切換。 完整的機制在此不詳述。 基本思想是，上一任委員會必須最終確認一個特殊的**重新配置區塊（reconfiguration block）**後，下一任委員會才能開始運作，以確保一致連續性。

ThunderCore將部署研究論文中描述的完整PaLa協定，該協定也稱為雙流水線PaLa（Doubly Pipelined PaLa），它支援**流水線化提案（proposal pipeline）**功能。 此版本允許共識每次前進k個區塊（k是協定設置參數）。 提案流水線可以實現讓較新的塊在較舊的塊仍在進行投票時被緩存。 根據我們的測試發現，當網路延遲相對於區塊時間而言較高時，更高的k值可以提高輸送量。

小結

從性能的角度來看，PaLa是對先前古典共識協定的一項重大改進，古典共識協定要求每個塊進行兩輪投票、傳送 $O(n^2)$ 個消息。 PaLa參考了流水線式BFT（pipelined BFT）演算法中第二輪投票附帶在下一個區塊的第一輪投票中的這一想法。 當期的提案人使用BLS多重簽名來收集投票並分發公證。 PaLa與軸輻式網路拓撲結構（hub and spoke network topology）結合時可以僅傳送 $O(n)$ 個消息便達成共識。

Tendermint，FBFT，Casper FFG和Hotstuff等較新的BFT共識演算法雖與PaLa有些類似的創新，但是都不及PaLa簡練、優雅和最優化。

> PaLa相較BFT共識，就像Kademlia相較分散式雜湊表（DHT）一樣具有開創性意義

ThunderCore還致力於提供最佳的資源以說明大家進一步瞭解PaLa。 PaLa共識協定的參考實現代碼已經發佈，其中包含完整的文檔和更多教程材料。

權益證明（PoS)

有了PaLa，我們有了一種可以進行可靠的委員會重新配置和提案人切換的機制。 完整方案還需要一種激勵相容（incentive compatible）的用於選舉共識節點的權益證明（PoS）設計。 我們選擇了一種簡潔的按照會話（session）進行的前*K*位投票者選舉設計。 每場會話持續3個小時。 在每屆任期中，進行成為下屆任期的共識節點的競標。

一個競標包含以下參數

1. 權益額
2. 簽名公開金鑰
3. 獎勵位址
4. 期望GAS價格
5. 擁有簽名私密金鑰的證明

在會話結束時，所有有效的競標會被收集並按權益額大小排序。 前32名成員構成下屆的新委員會，新一輪會話將在PaLa重新配置區塊最終確定後開始。 為了限制硬碟空間的驟增和網路頻寬的使用，我們將GAS價格設置為全部委員會期望GAS價格的2/3高值以保證有2/3的投票者會對設定的GAS價格或更高的價格感到滿意。

提案人選舉

身為完全無需許可（permissionless）的協定，我們需要一個公平的提案人選舉政策。 我們預期任何提案人也可以充當投票者，因為提案人的硬體要求嚴格高於投票者的硬體要求。 因此選舉中，任何投票者都可以表示是否希望成為提案者。

我們蒐集表達過願意當提案者的委員會當選人的名單，構成提案人清單，再以權益額排序。

要成為提案人，共識節點必須在競標中包含以下附加內容：

1. 公開URI（統一資源標誌符）；
2. 提案公開金鑰；

3. 自選消息。

目前，提案人按權益大小進行排序並輪流提案，在每次會話中，每個提案人僅被允許提議與其權益額成正比的區塊個數。 因此，每個誠實且網路連接良好的提案人每屆任期將至少服務一次。 由於提案人強制切換的設計，即使是一個由惡意節點組成的的占多數聯盟也只能在短時間內暫停活躍性或限制交易。 只要保證至少有一個行為舉止良好的誠實的提案人，就可以確保所有有效交易都將最終被包括在鏈中。

獎懲機制

本節介紹ThunderCore的權益證明獎懲制度。 設計上我們希望有一個能夠實現以下目標的系統：

- 激勵相容性：我們的激勵機制應獎勵誠實和高效的參與。
- 對攻擊具有經濟穩健性（Economically robust）：在均衡狀態下，有足夠的權益保護區塊鏈從而使攻擊成本與貨幣的重要性成比例。

因此我們通過過激勵措施與誘因設計來確保節點遵循規則。 我們的設計為任何試圖破壞一致性的拜占庭式節點帶來了極高的攻擊成本。 對於試圖破壞活躍性的故障節點或拜占庭節點將給予一定的懲罰，並且不會給予任何獎勵。

獎勵

ThunderCore將使用區塊獎勵補貼交易費以激勵參與。 區塊獎勵是從我們現有的委員會獎勵池中分配的。 分配區塊獎勵不會鑄造新的代幣，ThunderCore會將獎勵池交給鏈的協定來控制。

進行分配時，提案人首先獲得一部分獎勵，剩餘的獎勵將按權益比例分配給參與投票的投票者。 提案人的獎勵會依照收集到的票數佔委員會全員的比例調整，以激勵提案人不要只收集滿足公證條件的⅔數量的票。 投票人只有在有確實投票的情況下才能拿到獎勵。 依以上規定不該有人領取的獎勵會返回至獎勵池。

為遵守EVM標準，ThunderCore使用1秒的區塊時間。 我們認為1秒的出塊時間足以負荷廣泛使用情境。 因此，投票者有1秒的時間將投票提交給當期的提案人以獲取獎勵。

懲罰

投票者會話結束後，已抵押的資金將被凍結在智能合約中24小時，在這段時間內，如果記錄到不良行為的證據，則扣除部分抵押資金作為懲罰。

如果某投票者在凍結其權益的期間對兩個相互衝突的提案投票，這一惡意行為的加密證據如果被發現並被舉報提交給區塊鏈，其凍結資金的10%將被返回給獎勵池，其中一小部分將作為報酬提供給舉報者。 剩餘的資金將被凍結一百萬（1000000）個區塊。 已凍結的資金無法再用於該投票者的權益抵押。 為了防止「無成本作惡」（nothing-at-stake attacks）攻擊，線上節點還必須拒絕父塊不在凍結期內的區塊。

鑒於無意掉線的節點不會自動在下一個會話中競標，因此ThunderCore不會因其投票失敗而給予懲罰。 由於ThunderCore僅向參與投票的投票者提供獎勵，不投票的機會成本很高。 如果發現活躍性攻擊的威脅超過了機會成本，ThunderCore將對不投票行為實施懲罰。

第三部分：下一步發展方向

作為一家技術公司，我們有許多令人振奮的想法正在積極研發，包括：

- **Thunderella**仍是個傑出且獨特的共識協定。 它具有同步演算法的容錯邊界和非同步單輪投票的最終確認時間這兩大優勢。 這意味著它比任何其他協定快兩倍。 我們認為，Thunderella如果不是作為第1層區塊鏈的獨立協定，則可能會非常適合用在第2層的側鏈。 提供一個生產就緒的Thunderella參考實現仍在我們的未來規劃圖中。

- **Pili**是一個非常獨特的具有非同步級別性能的同步共識協定。 我們相信，一個生產就緒的參考實現對區塊鏈社區具有巨大的價值。

- **無需信任的亂數產生**使在鏈上易於實現不可預測的隨機行為。 我們將使用與PaLa協定相同的假設，研究基於多方計算（MPC）的實現。

- **無需信任的跨鏈通信**可實現跨越獨立的區塊鏈之間的無信任資訊交換。

- **Paella**將慢鏈回落方案整合到PaLa中，以實現½活躍度的容錯能力和抗審查能力。 這個協定的特性另述如下。

- **亞秒級的出塊時間**可最大程度地提高輸送量，並充分利用雙流水線PaLa的全部潛力。

- 解決長期困擾區塊鏈磁片使用問題的**存儲費**機制。

- 通過EVM優化和樂觀併發處理（optimistic concurrent processing ）以及提案流水線化解決網路瓶頸，實現**100,000+ TPS**。 目前，4,000 TPS足以滿足所有區塊鏈使用。 ThunderCore將持續不斷優化協定，以滿足使用者需求。

- **分片技術**突破了單台機器的輸送量和存儲限制，從而將可擴充性提升至另一個數量級。 PaLa和我們的PoS方案可以輕鬆擴展到分片鏈。 我們可以在單個信標鏈（beacon chain）上選舉出一個大型委員會。 每個分片與委員會池中隨機分配的投票者和提案人一起運行PaLa共識協定。

Paella

PaLa的研究論文概述了選舉提案人的「有利於穩定」和「有利於民主」的選舉方法。 後一種方法要求更頻繁的強制切換，以使得更多節點擔當提案人角色。 ThunderCore將在PaLa中選擇「有利於穩定性」的方法，這意味著較少的提案人切換，從而加速運作。 Paella 結合 Thunderilla和PaLa的優點，避免提案人阻礙特定消息上鏈。

為了增加系統的去中心化程度，我們引入了Thunderella協定中的yell消息。 yell消息是另一個區塊鏈上的交易，在其資料欄位中包含具有有效簽名的ThunderCore交易。 這些交易應被包含在ThunderCore區塊鏈中。 誠實的投票者不會投票給不包含yell資訊的區塊（將造成強迫提案人切換）。 誠實的完整節點應拒絕不包含有效yell消息的區塊。

yell消息還提供了一種新的後備機制，可以從委員會不工作的狀態中實現恢復。 如果沒有提案人能夠收集⅔的票數來公證下一個區塊，交易仍可以通過一定會在未來某時刻被包含在鏈上的yell消息處理；此未來時刻將由協定定義。 特別重要的是, 節點運營者仍可以發送新的競標並選舉一個新的提案人來重新配置參與共識的節點，從而使其可以再次正常運行。

Thunderella需要在慢鏈上定期發佈alive消息以使共識節點協調回退和恢復。 而使用PaLa時，共識節點可以直接協調它們之間的提案人切換，因此不再需要alive消息。 alive消息仍可被用於防止遠端攻擊（long range attacks），如果我們確定遠端攻擊會對區塊鏈安全性構成威脅，則它們可能是ThunderCore協定的一部分。

我們親切地將此修改稱為「**PaLa Paella**」。

第四部分：發展理念

ThunderCore是個具有使命感的技術團隊。 最後，我們想分享推動我們不斷前進的核心理念。

我們堅信：

區塊鏈將從根本上改變人們的生活。
我們正處於人機交互之新時代的初始階段。 區塊鏈技術將從根本上改變人類與技術的互動方式。大量中心化的營利性機構已達到其發展潛力的極限，但區塊鏈的潛力才剛剛開始發揮。

人們將越來越依賴並使用區塊鏈服務。
在日常交互中，人們開始質疑與大型中心化服務提供者的信任問題。 隨著時間推進，人們開始越來越傾向通過代碼，去中心化服務和機構來解決信任問題。 區塊鏈就是建立在這些基本原則上的，我們相信區塊鏈很快會被大規模採用。

不受限制地獲得技術創造的利益和價值是一項全民權利。
區塊鏈有助於實現全球性的平等，意義十分重大。 去中心化和開放性是實現平等公正必需的條件，因為ThunderCore是公開的，無限制的，因此，全世界的人都能使用我們的平臺，享受我們服務的利益，同時，這些參與者也能將他們的價值帶到我們的平臺上。

未來是開放的、去中心化的、和透明的。
未來充滿挑戰。 我們正處於歷史上最奇妙的時刻，未來充滿可能性，我們擁有讓自我書寫未來的機會。 ThunderCore始終不渝地堅信並追求：區塊鏈技術會實現更開放，更去中心化，更透明的未來。