

EN-TAN-MO SCIENCE

繁體中文

AGREED VALUE SHARED BENEFIT

共識傳遞價值

引言

En-Tan-Mo，靈感來源于 Entente（聯盟）、Transaction（交易）和 Mobius（莫比烏斯），是基于納什均衡和價值傳遞理論的新一代區塊鏈項目。2011 年諾貝爾經濟學獎得主、理性預期學派領袖托馬斯·薩金特教授以及來自美國加州理工大學、美國馬裏蘭大學、法國龐加萊研究所的各領域學者們，將博弈論的研究成果革命性融入區塊鏈中，共同創造了具有 SHD 完備性的 En-Tan-Mo。在 En-Tan-Mo 世界中，SCV 矿工和 Pareto 矿池，在 Kantorovich 共識機制下相互支撐、相互激勵，包容各種區塊鏈與非區塊鏈的應用和社區，幫助所有渴望公平、民主、自由的人們，在區塊鏈帶來的去中心化思潮中，均衡的獲得屬於每個個體的最高權益。En-Tan-Mo，不僅僅是一個納什均衡的區塊鏈底層平臺，還包含了最豐富的應用和最廣泛的社區，甚至包含了嚴謹的數學論證和豐富的經濟學內涵，從而形成了完整的哲學思想和系統。因此，“技術白皮書”的形式難以體現出 En-Tan-Mo 的真正優勢，研發團隊以資料匯編的形式從世界、哲學、數學、經濟、計算、生態等多維度向每一個關注 En-Tan-Mo 的人進行闡述。

名詞解釋：

納什均衡：美國數學家，諾貝爾經濟學獎得主約翰·納什提出：在一個多人參加的博弈過程中，所有參與者各自選擇的策略所組成的一個集合，任何人都不能通過單方面改變自己的策略（作弊）獲得更大的利益。En-Tan-Mo 的數學家通過巧妙的設計雙共識機制，讓每個參與者都可以以礦工或投票人的身份平等參與區塊鏈的建設並獲得均衡的獎勵，礦工之間，投票人之間，礦工和投票人之間均通過簡潔有效的共識協議進行調節，從而保證理性的參與者集合達到納什均衡狀態。納什均衡是 En-Tan-Mo 的最核心問題之一，在“En-Tan-Mo 數學”和“En-Tan-Mo 經濟學”部分有更詳細闡述。

SHD 完備性：指區塊鏈的三個最重要指標同時具備：安全性 (Safe)、高性能 (High-performance)、去中心化 (Decentralization)。現有區塊鏈系統均存在三者不可兼得的問題，如何解決 SHD 完備性是區塊鏈 3.0 面臨的主要問題。SHD 完備性在“什麼是 En-Tan-Mo”章節裏有更詳細闡述。

Kantorovich 共識：Kantorovich 共識是一種革命性的 UPOS 權益證明算法，是 En-Tan-Mo 基礎架構的重要組成部分。Kantorovich 共識將工作量和股份授權巧妙的融合並形成歸一化權益，得到全新的統一權益證明協議 (Unified Proof of Stake, UPOS)，從而保證 En-Tan-Mo 的納什均衡。Kantorovich 共識是第一個通過科學驗證均衡性和安全性的 UPOS 權益證明協議，在“En-Tan-Mo 經濟學”部分有更詳細闡述。

SCV 矿工：En-Tan-Mo 中通過基礎算力測試並由選舉制度推選的合作競爭礦工，被稱為 Smart Ledger Scrivener，智能賬本記錄員，簡稱為 Scrivener 或 SCV 矿工。候選礦工根據得票高低當選 SCV 矿工和候補礦工，獲得上傳區塊權利，驗證區塊義務和區塊獎勵。SCV 矿工在“En-Tan-Mo 經濟學”部分有更詳細闡述。

監察官：ETM Token 的持有者在投票選舉 SCV 矿工團隊時的身份，被稱為“監察官”。監察官將手上的 Token 在“En-Tan-Mo”中通過上凸權益映射轉化為可投票數，每投票周期給予相應獎勵。監察官來自拉丁語 tribunus，表示古羅馬時代對行政官員或軍事實行監督的官職或委員會，代表規範化、專業化和職業化。監察官在“En-Tan-Mo 經濟學”部分有更詳細闡述。

Pareto 矿池：在 En-Tan-Mo 中，所有礦機節點組成一個合作競爭型的礦池，每個出塊周期選擇若干 SCV 矿工有序出塊，“En-Tan-Mo”將該周期中未被選中的所有礦機組成 Pareto 矿池，運用特有的側鏈技術和聯盟策略，根據即時收益算法分析，參與外部區塊鏈的生產出塊，按照礦機提供算力分配礦池收入，從而保證所有礦機的正收益。帕累托最優 (Pareto Optimality) 是指資源分配的一種理想狀態，Pareto 矿池最優是公平與效率的“理想王國”。Pareto 矿池在“En-Tan-Mo 經濟學”部分有更詳細闡述。

中心鏈和衍生鏈：En-Tan-Mo 的鏈狀結構為一條中心鏈和多條衍生鏈，衍生鏈可以通過中心鏈的“平行鏈交互層”實現其與中心鏈、其他衍生鏈及外部區塊鏈鏈之間的雙向資產傳遞，這使得用戶能用已有的資產來使用“En-Tan-Mo”系統。中心鏈是主鏈，負責 En-Tan-Mo 網絡安全及價值交換。衍生鏈是一種特殊的區塊鏈，每一個衍生鏈對應一個 DAPP，是一個獨立的、隔離的系統，繼承和復用主鏈強大的區塊鏈技術，每個應用都擁有一套個性化的賬本，擁有個性化的 Token。中心鏈和衍生鏈在“En-Tan-Mo 生態”部分有更詳細闡述。

米爾商城：“En-Tan-Mo”系統通過方便而又高效的米爾商城，幫助企業或開發者更快更經濟的實現區塊鏈應用，使得用戶能够享受到去中心化帶來安全和便利。“鑽石之城”米爾礦是目前世界最昂貴的鑽石礦，米爾商城面向開發者和用戶，是 En-Tan-Mo 的價值所在。米爾商城在“En-Tan-Mo 生態”部分有更詳細闡述。

POW：工作量證明，Proof of Work，簡稱 POW，是一種應對拒絕服務攻擊和其他服務濫用的經濟對策，它要求發起者進行一定量的運算，也就意味着需要消耗計算機一定的時間。比特幣網絡中任何一個節點，如果想生成一個新的區塊並寫入區塊鏈，必須解出比特幣網絡的工作量證明的迷題。這道題關鍵的三個要素是工作量證明函數、區塊及難度值。工作量證明函數是這道題的計算方法，區塊決定了這道題的輸入數據，難度值決定了這道題所需要的計算量。

POS：股權證明，Proof of Stake，簡稱 POS。POS 提出了幣齡的概念，幣齡等於參與者持有 Token 的量和時間的乘積。與 POW 消耗算力解題不同，POS 消耗的是虛擬的幣齡，幣齡作為記錄股權的證明，持有量對應投票權和收益權，即根據幣齡的多少分配相應的權利和利息。

DPOS：委托股權證明，Delegated Proof of Stake，簡稱 DPOS。DPOS 通過不同的策略，不定時的選中一小群節點，這一小群節點做新區塊的創建、驗證、簽名和相互監督，這樣就大幅度的減少了區塊創建和確認所需要消耗的時間和算力成本。常規 POW 和 POS 於任何一個新加入的區塊，都需要被整個網絡所有節點做確認，這是 DPOS 與以上兩種方法的不同點。

UPOS：統一權益證明，Unify Proof of Work，簡稱 UPOS。En-Tan-Mo 的數學家巧妙的將 POW 和 DPOS 融合在一起，顛覆性地提出了雙共識機制，讓每個參與者都可以以礦工或投票人的身份平等參與區塊鏈的建設並獲得均衡的獎勵，礦工之間，投票人之間，礦工和投票人之間均通過簡潔有效的 UPOS 共識進行調節，從而保證理性的參與者策略集合達到一種完美的納什均衡狀態。

0.0 En-Tan-Mo 是什麼

區塊鏈回顧

簡要的回顧區塊鏈歷史，將有助于理解 En-Tan-Mo 的革命性。

2008 年，中本聰發表了著名的論文《比特幣：點對點的電子現金系統》，2009 年 1 月創世區塊被挖掘出來，“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”像魔咒一樣開啟了比特幣區塊鏈的時代。2013 年比特幣發布了其歷史上最重要的版本，該版本完善了比特幣節點本身的內部管理、網絡通訊的優化，比特幣電子現金開始產生全球影響力。比特幣作為第一個加密數字貨幣大獲成功，但是比特幣糟糕的擴展性嚴重制約區塊鏈的後續發展。我們稱比特幣為區塊鏈的 1.0 時代。

為了解決比特幣擴展性的問題，Vitalik Buterin 創立了以太坊。以太坊有着明確清晰的設計思路和框架體系，從 EVM 論文到 ICO、從不同版本的 POC 到 2015 年的 Frontier 階段，從 POW 的 Metropolis 階段到 POS 的 Serenity 階段，以太坊的圖靈完備性，智能合約，抵抗 ASIC 設計和區塊鏈應用構成區塊鏈 2.0 時代的主要標志。以太坊提供了平臺接口和編程語言，使開發人員能够建立和發布下一代分布式應用。

後面的故事開始被人熟知，2018 年 2 月比特幣算力達到 20EH/S，Github 上超過了 9 萬個區塊鏈的開源項目，中國、美國、英國、新加坡、俄羅斯、日本、韓國等 90 多個國家都已加入區塊鏈技術的研究。2008 年到 2018 年，區塊鏈的思想和理念被大眾消化、摸索、實踐，這一切僅僅用了十年時間。對比互聯網的發展，一眼就能看出區塊鏈的成功：1974 是互聯網元年，美國國防部國防高等研究計劃署（ARPA）開發公布了 TCP/IP 協議，20 年後也就是 1994 年中國正式接入國際互聯網。

0.1 為什麼要建設 En-Tan-Mo

En-Tan-Mo 旨在創造一個成熟、均衡、效率的價值傳遞世界。因此，En-Tan-Mo 從創立初始就明確了需要解決的兩條主線問題。

SHD 完備性

在一個分布式系統中，一致性（Consistency）、可用性（Availability）、分區容錯性（Partition tolerance）三者不可兼得，稱之為 CAP 定理。中本聰提出區塊鏈依靠概率強一致性（Probabilistic Strong Consistency）實現一致性共識，並稱為 Nakamoto 共識。

區塊鏈體系中，類似于 CAP 定理，存在安全性（Security，縮寫為“S”）、高性能（High-performance，縮寫為“H”）、去中心化（Decentralization，縮寫為“D”）三者兼容的 SHD 完備性問題。

中本聰在低效 CPU 的前提假設下，保證了安全性 S 和去中心化 D 共存，却幾乎忽略了高性能 H，由於共識算法和區塊容量的設計，比特幣平均十分鐘產生一個區塊，1 秒鐘只能處理 7 筆交易。不僅如此，隨着高性能“ASIC 礦機”的出現，普通的 CPU 算力獲得收益的概率降為 0，礦機輕易的獲得了超線性收益，後期礦場和礦池的出現更是徹底打破了去中心化 D，現在比特幣顯然不是一個平等參與的社區。更糟糕的是，礦場和礦池不斷壟斷算力，必然會有少數參與者超過 51% 的算力（決定權），安全性 S 也會無法保證。因此，我們說比特幣的區塊鏈已經失去了 SHD 的平衡。

以太坊為了避免 ASIC 礦機帶來的破壞性影響，采

取了“反復讀緩存”的 ASIC 抵抗算法，在短時間內維持了安全性 S 和去中心化 D，但其最引以為豪的智能合約的第一個大規模應用“CryptoKitties”，就令以太坊系統完全崩潰，高性能 H 顯得尤為低下。而拋棄了 POW 共識，轉向 POS 或 DPOS 共識的區塊鏈系統，大幅提高了系統性能，卻忽視了去中心化的根本意義，由少數權益擁有者掌握系統的發展方向，本質上和現有的中心化系統並沒有太大區別。

En-Tan-Mo 通過設計基於 UPOS 的 Kantorovich 共識機制，採用礦工團隊選舉制度，保證權證擁有者和區塊礦機的分離和各自權益，在保障安全性的同時提高效率，又保持了去中心化的基本屬性，從而滿足 SHD 完備性。

均衡價值傳遞

互聯網時代改變了信息傳遞的方式和理念，人們通過互聯網技術便捷、低成本的傳遞信息，指數級的提高效率和控制成本，並且獲得了全新的產品或服務。然而，信息傳遞和價值傳遞的概念不同，互聯網不具有點對點的價值傳遞功能，價值傳遞依賴於中心機構承擔記賬功能，因為價值傳遞需要保證權屬的唯一性，這不同於信息傳遞的可複製性。

比特幣通過分布式共享記賬技術，建立去中心化的信任，不再依賴中心化機構，從而支持點對點的價值傳遞，改變了價值傳遞和定價規則。由於礦池的出現，比特幣的價值傳遞發生了傾斜，普通參與者和礦機擁

有者的價值獲取不再對等，價值迅速向礦池集中。

以太坊通過 ASIC 抵抗算法，并消耗“Gas”以抑制鏈上資源，從而在一定程度上減慢了礦機的價值積累速度，我們認為是一種消極和短期的作法，對區塊鏈的長遠發展非常不利。POS 或 DPOS 共識，嘗試通過打破 POW 算力壟斷實現均衡，但是實力雄厚的 Token 擁有者仍然掌握了價值導向，中心化程度比 POW 更加集中。

根據目前區塊鏈及加密貨幣的發展現狀，價值以一種近似 80/20 定律的方式集中在少數人手裏。En-Tan-Mo 希望改變現有價值傳遞的方式，讓價值完成開放式流轉，給用戶提供一個均衡的價值傳遞體系。En-Tan-Mo 認為每個個體同時是服務的提供者和購買者，即是買家也是賣家，去中心化的市場核心是價格調節機制，而價格將以一種動態均衡的方式自組織地形成。En-Tan-Mo 使用平均場博弈論的思想研究價格動態波動，算力或投票權與權益之間應當是正相關，但並非線性的關係，從而抑制權力的過度集中，開創新一代的均衡價值互聯體系 IoV (Internet of Value)，對商業模式和經濟社會產生重大變革。

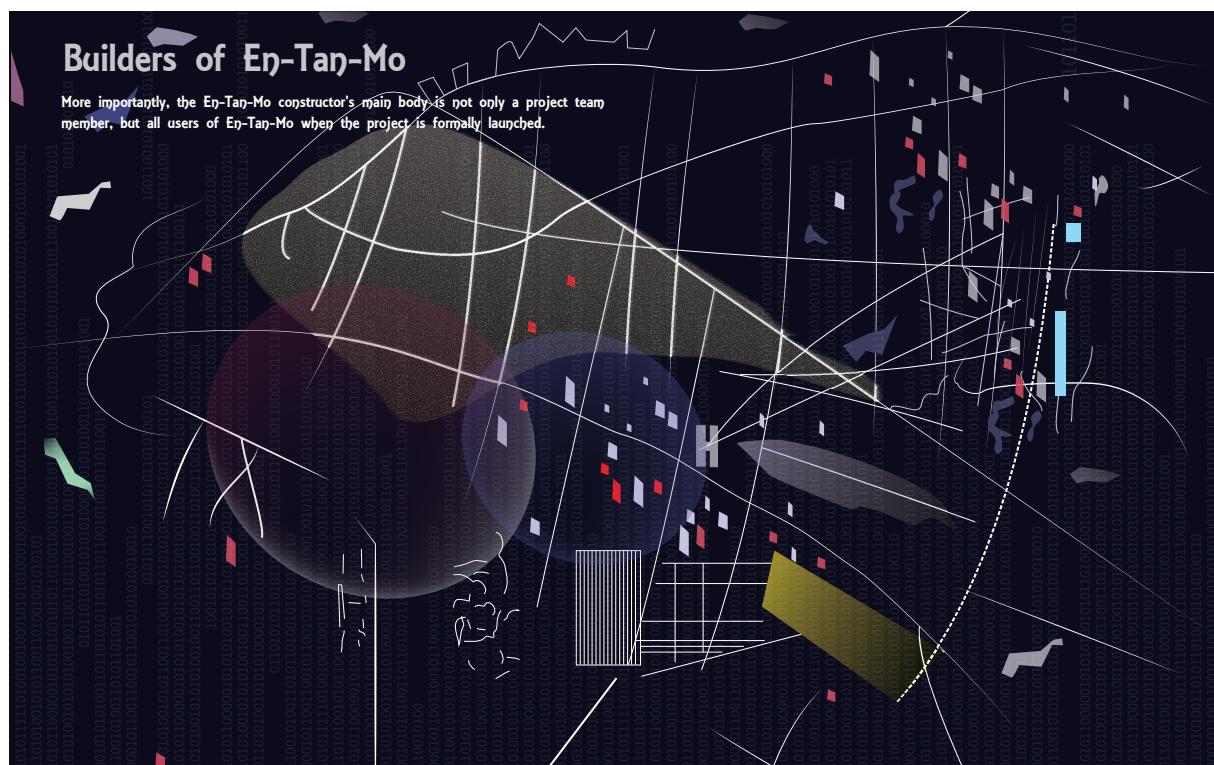
0.2 En-Tan-Mo 的建設者

En-Tan-Mo 的設計師和建設者來自于全球頂尖大學和研究所。最初團隊由法國的數學家們組成，他們將博弈論的成果融入區塊鏈中，并將 Entente 和

Transaction, Mobius 三個單詞的精髓抽提出來，命名為 En-Tan-Mo。隨後通信專家、計算機專家、經濟學專家和哲學家迅速加入了 En-Tan-Mo 的團隊，包括美國加州理工大學、美國馬裏蘭大學、法國龐加萊研究所的各領域學者們。非常榮幸的，2011 年諾貝爾經濟學獎得主、理性預期學派領袖托馬斯·薩金特教授也欣然加入團隊并擔任高級顧問。從此，En-Tan-Mo 的所有理論設計都採取雙重驗證的流程：先由數學家完成共識建模和數值模擬仿真驗證；再由計算機和通信專家以嚴苛的標準對 En-Tan-Mo 項目的理論設計做實際驗證。

En-Tan-Mo 目前的工作成果要歸功于理論與實驗，軟件與硬件，技術與商業各個不同團隊和負責人之間密切的配合和共同勞動。Kantorovich 共識機制由來自數學，通訊，計算機領域的專家共同設計完成；以太坊項目參與者和區塊鏈社區大 V 等一起設計了“En-Tan-Mo 科學”的框架體系和權益分配機制；前谷歌、迅雷、百度等頂尖互聯網公司具有豐富經驗的軟件工程師參與了項目純自主代碼設計。

更重要的是，當項目正式上線後，En-Tan-Mo 的建設者主體就不僅僅是項目團隊成員，而是 En-Tan-Mo 的所有用戶。En-Tan-Mo 倡導自演進和共同參與，歡迎所有用戶按照自己的需要，積極上傳組件和發展衍生鏈。En-Tan-Mo 項目組將把自己的角色定義為奠基人和基礎設施建設維護者，繼續盡最大的努力為這個體系提供安全，穩定，高效的技術服務。同時，項目組也歡迎科學家，工程師和一切認同 En-Tan-Mo 理念的研發者加入我們的團隊或以各種靈活的方式合作。



0.3 En-Tan-Mo 科學

En-Tan-Mo 并非一個簡單的區塊鏈項目，而是有着豐富內涵的科學體系，包含了完整的哲學思想，數學論證，經濟學印證和廣泛的應用生態，研究團隊以資料匯編的形式盡可能詳盡的向每一個關注 En-Tan-Mo 的人進行解釋。

第一章是 En-Tan-Mo 世界。En-Tan-Mo 以服務提升與價值創新增塑區塊鏈 3.0 的世界，En-Tan-Mo 的世界將專注于持續優化、重構、創造市場，也是均衡商業體制本質的回歸和重塑。

第二章是 En-Tan-Mo 哲學。En-Tan-Mo 是一個全新的價值傳遞體系，鏈接一切有價值的事物，因此，復雜系統與多元結構，共識與價值，動態均衡與分權，自演進與開放性泛化為 En-Tan-Mo 的去中心化特徵。

第三章是 En-Tan-Mo 數學。從數學的角度分析去中心化的 En-Tan-Mo，包括已經完成的數學論證和項目的發展規劃，以及研究主要應用的數學工具。

第四章是 En-Tan-Mo 經濟學。SCV 礦工和 Pareto 礦池，在基于 UPOS 機制的 Kantorovich 共識機制下相互支撐、相互激勵，形成統一的 UPOS 算法。En-Tan-Mo 不單是技術的創新，更是商業邏輯的改革。

第五章是 En-Tan-Mo 計算。軟件工程師編寫了 En-Tan-Mo 的數據結構、流程圖、API 接口和全部代碼，用程序的形式體現了 Kantorovich 共識機制的精美和巧妙。

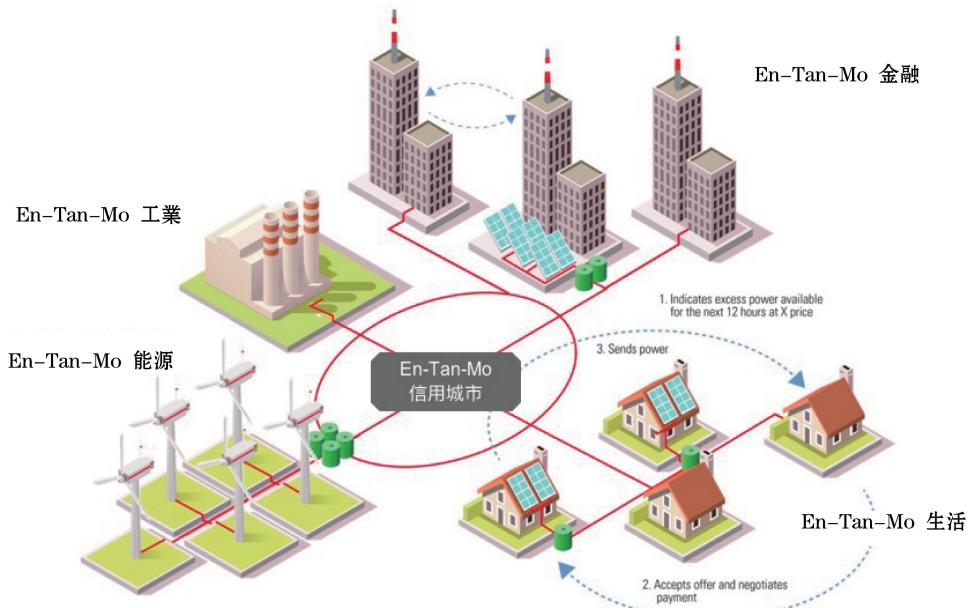
第六章是 En-Tan-Mo 生態。En-Tan-Mo 的跨鏈技術包括中心鏈、衍生鏈，將區塊鏈從分散的孤島中拯救出來，是區塊鏈向外拓展和連接的橋梁，從而構建了一個可以包含千萬級應用的區塊鏈生態系統。

第七章是 En-Tan-Mo 組織結構。En-Tan-Mo 社區由 En-Tan-Mo 基金會，ETM FinTech 和 ETM BD 三個組織構成。基金會對用戶社區提供全方位的支持，保證 En-Tan-Mo 項目的順利運營；ETM FinTech 是隱私安全研究和系統開發的組織實體；ETM BD 是協助商業企業的合作伙伴組織。

參考文獻：

- 【01】 S. Nakamoto. A Peer-to-Peer Electronic Cash System. www.bitcoin.org/bitcoin.pdf, 2009.
- 【02】 M. E. Hellman. A cryptanalytic time-memory trade-off. *IEEE Transactions on Information Theory*, 26(4):401-406, 1980.
- 【03】 V. Buterin. Long-range attacks: The serious problem with adaptive proof of Work. <https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-withadaptive-proof-of-work/>, 2014.
- 【04】 V. Buterin. Proof of stake. <https://github.com/ethereum/wiki/wiki/Proof-of-StakeFAQ>, 2016.
- 【05】 G. Wood. Ethereum: A secure decentralised generalised transaction ledger. <http://gavwood.com/Paper.pdf>.
- 【06】 M. Mainelli, C. von Gunten. Chain of a lifetime: How blockchain technology might transform personal insurance. Dec 2014. Z/Yen Group, Long Finance.
- 【07】 J.-P. Delahaye. Les blockchains. "Les big data à découverte". Editions du CNRS, Chapitre 15, 118, 2017.
- 【08】 J.-P. Delahaye. Le Bitcoin: première cryptomonnaie. "1024" Bulletin de la Société Informatique de France, n° 4, pp. 67-104, octobre 2014.
- 【09】 J.-P. Delahaye. Le Bitcoin: une monnaie révolutionnaire. Laboratoire d'Informatique Fondamentale de Lille, janvier 2014.
- 【10】 M. Perrin. Distributed Systems: Concurrency and Consistency. ISTE Press, Elsevier, 2017.
- 【11】 R. Perez-Marco. Bitcoin and Decentralized Trust Protocols. Newsletter of the European Math. Soc., 100 p.32, 2016.
- 【12】 W. Feller. An introduction of probability theory and its applications. Vol.1, 3rd ed. John Wiley & Sons, 1957.
- 【13】 Л.В. Канторович, Математические методы организации планирования производства. Издание Ленинградского государственного университета, 1939.
- 【14】 С. М. Меньшиков. Актуальность экономической модели Л. В. Канторовича в наше время. Зап. научн. сем. ПОМИ, 2004, том 312, 30–46.
- 【15】 M. Doob, Kantorovich. On Optimal Planning and Prices. *Science & Society*, Vol. 31, No. 2 (Spring, 1967), pp. 186-202.
- 【16】 C. Grunspan, R. Pérez-Marco. Double spend races. arXiv:1702.02867v2 [cs.CR].
- 【17】 R. Perez-Marco. A simple dynamical model leading to Pareto wealth distribution and stability. arXiv:1409.4857, 2014.
- 【18】 J. P. Aubin, I. Ekeland. Applied Nonlinear Analysis. Wiley-Interscience, 1984.
- 【19】 J. P. Aubin. Optima and Equilibria. Springer-Verlag, 1998.
- 【20】 Notes on Mean Field Games, from Pierre-Louis Lions' lectures at Collège de France.
- 【21】 J.-M. Lasry, P.-L.Lions. Mean field games. *Jpn. J. Math.*, 2 (2007), No. 1, 229-260.
- 【22】 M. Kamgarpour, H. Tembine. A Bayesian Mean Field Game Approach to Supply Demand Analysis of the Smart Grid. 2013 First International Black Sea Conference on Communications and Networking.
- 【23】 T. J. Sargent, Lars Ljungqvist. Recursive Macroeconomic Theory. MIT Press, 2000.

1.0 En-Tan-Mo 世界



1.1 En-Tan-Mo 世界藍圖

“En-Tan-Mo”是一次打破國界的科學革新，其內涵涉及哲學、數學、經濟學、計算科學，相互交織、相互印證。“En-Tan-Mo”同時也在詮釋一個顛覆性的全新世界。

“En-Tan-Mo”的世界藍圖：一根根緯線代表一條條供求，每個參與個體就是一根自由的經綫，他可以與任意緯線發生關係，還可以自己增加緯線。而這一經緯交織的網絡通過混沌排序機制，不斷自主學習和自主完善。在“En-Tan-Mo”世界裏，每個個體的行為都在塑造世界。這種職業自由使人們更理性、更積極、更自主、更長遠。

金字塔的崩解，真正的去中心化意味着不再有集權和壟斷，En-Tan-Mo 創造的是一個自由平等，富有創造性，同時高效均衡的世界。這是一個非自上而下的，完全由供需市場驅動的世界，讓價值完成開放式流轉，給大眾提供一個均衡的價值傳遞體系。在En-Tan-Mo世界裏，每個人不再被動的每月領取固定薪水，而是自發參與不同項目得到直接獎勵，同時，自己也可以創造項目發放獎勵。每個人同時站在價值傳遞的兩端，而交易價格將以動態均衡的方式自發調節以保證公平。

更為重要的一點：下一代區塊鏈技術消除了職業的地緣限制，人類將成為全新的游牧民族，根據需要，在En-Tan-Mo世界中自由的行動。

1.2 數字貨幣世界史

仰望互聯網的星空，“區塊鏈”更像是一顆特別的新星在這片天空中閃耀，在它的面前，任何中心化的應

用都將成為歷史。區塊鏈中的“數字權證”就像人類文明長河中的貨幣，將會極大地提升網絡交易的速度和容量，使網絡不再僅僅是信息共享的通道，更是價值傳遞的橋梁。2009年，比特幣率先帶來了一個“數字黃金”系統，淘金的熱潮一次又一次地席卷着整個互聯網絡。到2018年伊始，大約30000PH/s算力每小時產生僅僅6個區塊75枚比特幣。根據Digiconomist的比特幣能源消費指數顯示，當前比特幣“挖礦”所產生的年用電量估計為39.45TWh，等價于20億美元。如此龐大在算力進入到“數字黃金”的淘金熱潮中，正如1848–1851年美國淘金熱期間，人口急劇增長，衣食住行變得陡然緊張，尤其是服務業的發展無法滿足社會的需要，美國批發商品的價格指數847提高到1025，這些情況與2017年的比特世界非常接近。但難以想象的是，歷史長河中幾百年形成的“金本位”貨幣體系，在比特世界中僅僅用了9年。

2013年，Vitalik Buterin首次提出以太坊的概念，“下一代加密貨幣與去中心化應用平臺”，這一次的革新制造出具有圖靈完備性的智能合約體系，也把以太幣推向了“數字汽油”的寶座。以太坊提供各種模塊讓用戶來搭建應用，使建立應用的成本和速度都大大改善。具體來說，以太坊通過一套圖靈完備的腳本語言(Ethereum Virtual Machine code，簡稱EVM語言)來建立應用，所建立的應用被稱為智能合約(簡稱合約)，這是以太坊的核心。智能合約相當於一個以太坊系統裏的自動代理人，當用戶向合約的地址裏發送一筆交易後，該合約就被激活，然後根據交易中的額外信息，合約會運行自身的代碼，最後返回一個結果，這個結果可能是從合約的地址發出另外一筆交易。需要指出的是，以太坊中的交易可以是一次交易也可以執行一段指令，這樣

的優勢是使以太幣被大量使用起來，但是，這又會過于消耗以太坊的資源，導致了以太坊隨時可能被合約拖垮。這些特點使以太坊就像一條無法拓展的高速公路，所有的應用就像公路上的汽車，以太幣成為汽車消耗的汽油。目前，以太坊上雖然已經有超過 9 萬種合約，但是，這些合約幾乎全部是同質化的 Token 應用，這就像一條狹窄擁堵而又收費過高的公路上難以承載大型汽車一樣。

簡而言之，比特幣代表的是金本位經濟，以太坊代表的是能源經濟，在這兩種經濟生態中，可以理性地預測出未來的發展走向。

金字塔化的世界：“黃金和石油”能夠成為世界經濟的柱石，第一因素是稀缺性。而能源經濟能夠取代金本位經濟是因為能源具有核心使用價值，成為人類生存最重要的不可再生的消耗品。這種資源型的屬性使得世界變成一個超級金字塔，某些國家成為金字塔的頂端，更多的國家成為以提供廉價勞力的第三世界國家。國家中形成社會，社會又是一個金字塔，強有力的公司成為金字塔的頂端，大量的微小企業或組織在為這些頂端的企業提供廉價的服務。企業和組織的內部又形成一個個小的金字塔，絕大多數的普通勞動者為企業提供勞力服務，獲得微不足道的工資報酬。企業和組織之間也形成金字塔的結構，頂端企業和組織獲得資源的成本越來越低，底端却承受了越來越大的壓力。整個世界就像層層嵌套的金字塔，金字塔的頂端對底端施加的壓力越來越大。隨着時間的推移，終有一天，金字塔會坍塌下來，經濟危機被引發了。然而，這不是結束，金字塔又會逐漸自發的建立起來，最後坍塌，一次又一次的往復。

1.3En-Tan-Mo 大遷徙

1) POW 和 DPOS 雙穩態結構打破壟斷和中心化趨勢

POW 創世說：在現實世界中，人類最大的共識是“勞力”，通過凝結最等量的勞力而形成的商品演變成一般等價物，即是貨幣。在區塊鏈的世界中，最廣泛的共識是“算力”，通過凝結最等量最公平的算力而形成的數字權證必然會演變成一般等價權證。因此，引入公平等量的算力構建起一個初始穩定的平衡，是未來權證價值穩定的基礎。比特幣、以太坊的創立伊始，也正是基于公平穩定的算力而逐步形成的普遍共識。

POW 和 DPOS 雙穩態：POW 帶來的公平會被超性能算力打破，就像每一次的技術革命帶來的高性能必然會打破原有的公平。農業的世界如此，工業的世界亦如此、互聯網的世界、區塊鏈的世界中，金字塔也在周而復始的形成和坍塌。而 DPOS 帶來的高效使得公平被更快的打破，因為沒有了算力的公平支撐，金字塔會更快的形成，這就像現實中的各種權證，“超發”和“集中”會更快的形成。POW 和 DPOS 交織的雙穩態 UPOS 結構，使 POW 和 DPOS 的集中化和中心化被最大程度的限制，這種去中心的機制在保證高效的同時又保證了安全性，持幣人與礦工均可以參與到 En-Tan-Mo 中，共同參與社區的重大決定，決定未來的更新和發展，這是 En-Tan-Mo 世界的一項創舉。

2) 礦工合作競爭關係是一種完美的公平聯盟法則

POW 機制下需要礦工經過大量嘗試計算，計算時間取決于機器的哈希運算速度，礦工之間是單純的競爭關係，導致收益過低和資源極大浪費。因此，礦工們組成礦池的方式結盟，但又導致了中心化趨勢加劇。合作競爭理論認為礦工活動是一種特殊的博弈，是一種可以實現雙贏的非零和博弈，En-Tan-Mo 世界通過博弈思想分析礦工的互動關係，為所有參與者建立起公平合理的合作競爭關係。

只有合作競爭關係才能創造參與者價值鏈的新觀念，利用價值鏈來描述所有參與者合作競爭的互動關係。價值鏈的思想強調了 En-Tan-Mo 世界中同時競爭與合作兩種行為，兩者的結合意味着一種動態的關係，而不是“競爭”和“合作”所表達出的單獨的意思。礦工之間全新的關係可以用三個詞定義：貢獻 (Impact)、親密 (Intimacy) 和遠景 (Vision)。這涵蓋了礦工建立合作競爭關係後能够創造的具體有效的成果，即能够增加的實際生產力和價值，成果主要來源于三個方面：一是減少重複與浪費，最高程度節約算力和電能；二是借助彼此的核心能力，加快整個 En-Tan-Mo 的出塊速度；三是創造新機會，參與外部區塊鏈的建設。

3) 動態供需和理性選擇帶來納什均衡

加入 En-Tan-Mo 即是選擇了數字化世界中的最佳聯盟。而在以往的礦池聯盟中，往往採取的是最優控制理論，在某一時刻所選擇的最優，隨着時間的推移，所有參與者的收益會銳減，這是因為最優的選擇必然是會引起最大的外部競爭，從而最終使所有競爭者的收益下降。在托馬斯·薩金特教授的指導下，En-Tan-Mo 的科學家運用理性經濟預測理論，為合作者選擇處于上升通道的動態供需選擇，這是因為只有動態供需才能滿足參與者的理性選擇要求，實時形成納什均衡。選擇性合作即是供需關係的體現，價值正是成本與需求的有機結合。En-Tan-Mo 世界中的 POW 體現的成本因素，與 DPOS 體現的供需關係，相互糾纏，才能形成最大價值體現的統一權益法則 UPOS，並得到相對穩定的價值曲線。

4) 上凸函數機制保證參與人均衡權益

在以往的世界中，聯盟內部更趨向于更強有力的合作者，越強的合作者所獲得的收益比例會超越更弱小的合作者，這種超線性的收益模型最終會傷害到相對弱小的合作者，正是這個過程促使了金字塔的形成與坍塌，到最後，即使是強大的合作者也會因為金字塔的坍塌而受損。只有注重長尾效應的 En-Tan-Mo，使更廣泛的合作者亦得到相對可觀的收益，成為一種具有永續特性聯盟機制，那麼即使是強大的合作者在初始讓出了部分的利益，也會隨着時間的推移獲得比以往更大的收益。

En-Tan-Mo 世界的基礎正是一種摒除了“獨角獸礦池”的貢獻等量算法，甚至將這種“完全等量”（線性化算力函數）轉變為一種“上凸函數”，這使得公正的天平還稍微向更廣大的參與者去傾斜，通過理性的經濟學預測，這會促使更大的受眾產生更廣泛的共識，從而使 En-Tan-Mo 成為一種最為公平公正的區塊鏈網絡。

5) 混沌排序抵抗女巫攻擊和聯合作弊

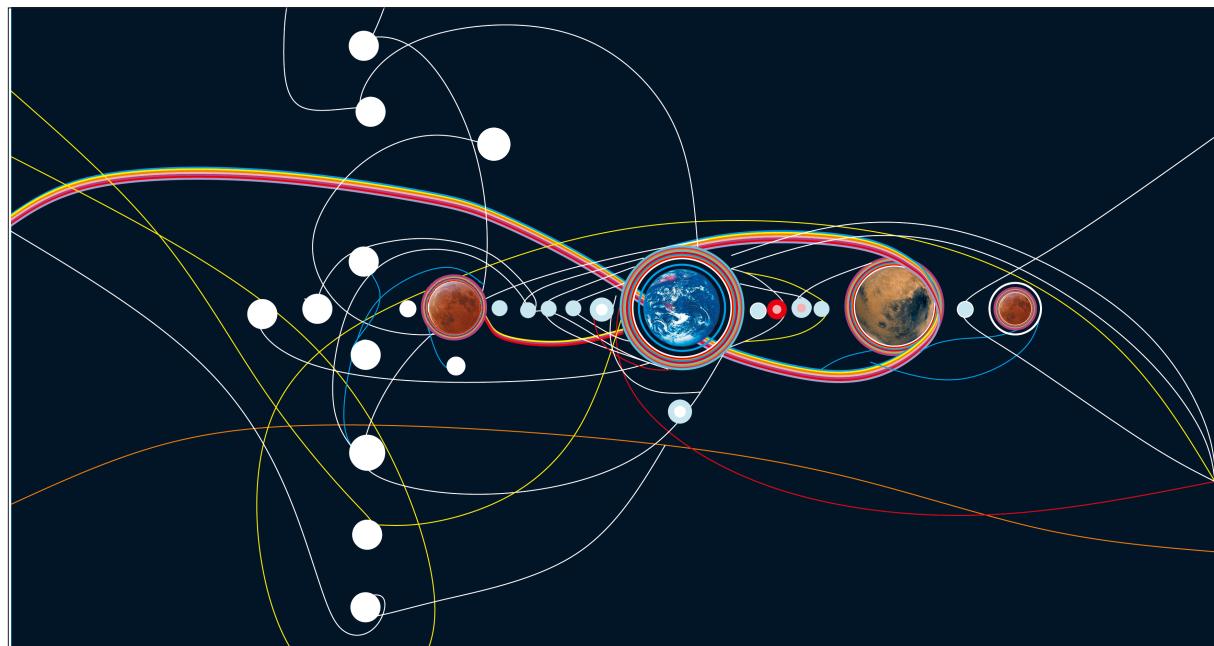
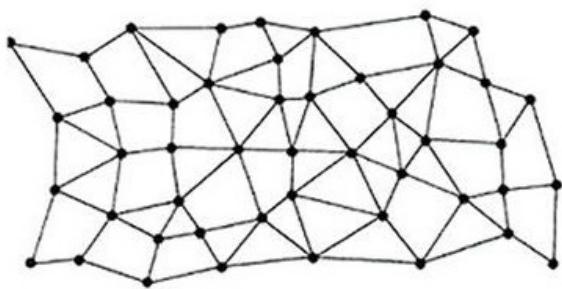
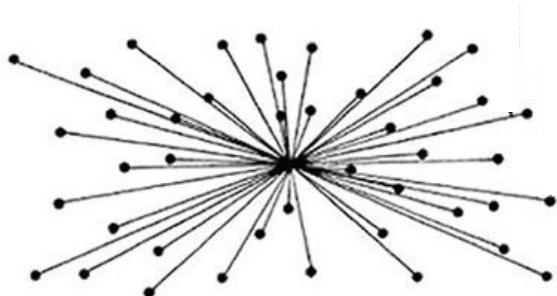
區塊鏈的 SHD 理論中，去中心化和安全性之間存在一個無法回避的問題：女巫攻擊（Sybil Attack）。女巫攻擊是指利用社交網絡中的少數節點控制多個虛假身份，從而利用這些身份控制或影響網絡的大量正常節點的攻擊方式。由於區塊鏈節點的對等性，單一節點具有多個身份標識，可以通過控制系統的大部分節點來削弱冗餘備份的作用。聯合作弊也會出現相同的問題。

En-Tan-Mo 的數學家運用現代動力系統、拓撲幾何理論，研究復雜不變集的結構與分岔，得出系統穩定性與復雜行為控制方法，從而基於混沌理論的遍歷性和對初始條件的敏感依賴性提出了強大的混沌排序方法，為區塊上傳順序打造了高度的偽隨機性機制，同時又具有可以抵抗量子攻擊的最高級的安全性。

6) 開放的組件庫和友好的開發者大廳定義了自演進和共同參與的發展方向。

En-Tan-Mo 以 BaaS (Blockchain as a Service, 區塊鏈即服務) 為理念，以微服務為基準，以自演進組件庫為核心，以開發者社區為生態原動力，為其他區塊鏈提供適配平臺完成資產和應用的自由轉移，為非區塊鏈的應用和數據提供軟通道完成雙向調用，為開發者提供共享大廳完成組件上傳、評價和獎勵的功能，為普通用戶提供 BaaS 網關實現無障礙服務調用。倡導自演進和共同參與的 En-Tan-Mo，歡迎所有用戶按照自己的需要，積極上傳組件和發展衍生鏈。

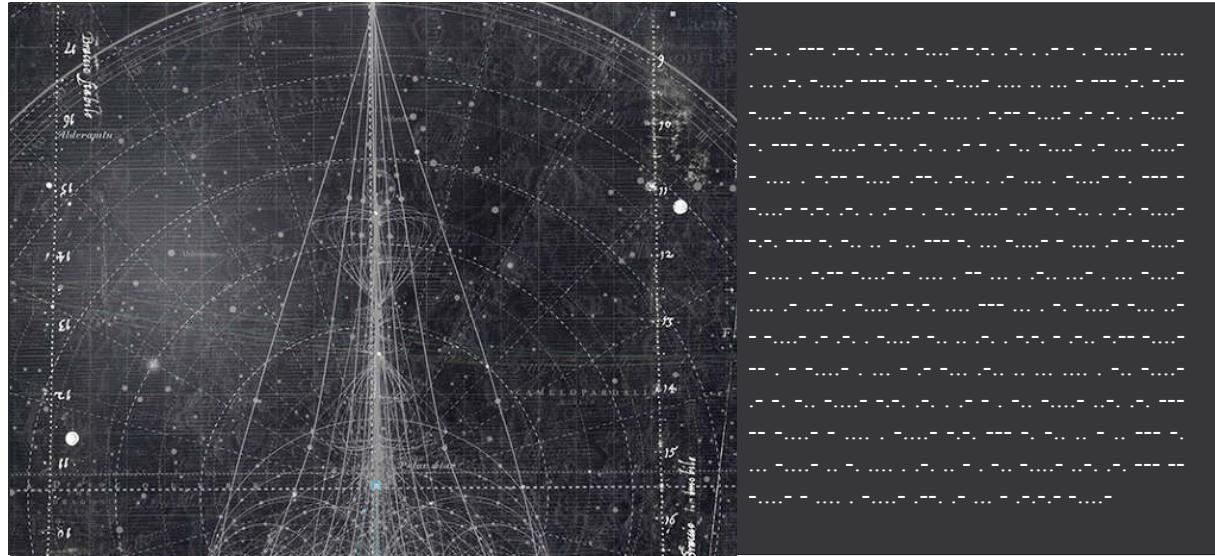
En-Tan-Mo 世界打通鏈與鏈之間，區塊鏈和非區塊鏈之間的信息孤島，應用側鏈獨立於主鏈，甚至每個供需關係都成為一條獨立鏈存在於網絡當中，這是一個無限延展的平行網絡，供需雙方立於價值傳遞的兩端。每個人在供需兩端隨意切換，在不同服務鏈間自由切換，提供服務和接受服務，高效且沒有附加費用的消耗，價值在鏈與鏈之間任意流轉。



“Hello! En-Tan-Mo World!”所有加入的礦工會進入到一個資源網格聯盟，是一種具有長期最佳收益的算力、存儲、帶寬承載分布式雲；所有的節點根據供需關係，自由平等的選擇交易，獲得均衡的受益。En-Tan-Mo 本身就是一個能够承載高頻次、高流量的大型去中心化數字權證交易所、聯盟礦池，混沌排序機制還天然形成一個博弈場。En-Tan-Mo 還是一個最好的開發者社區、區塊鏈DAPP 應用平臺。你好！歡迎來到一個處處體現均衡、平等的全新世界。
t

2.0 En-Tan-Mo 哲學

En-Tan-Mo 是在一種抽象空間中對現實物理世界中的價值生產及交換關係通過拓撲同構映射實現的重建，蘊含着深厚的哲學思想。在其龐大架構之下，滲透的是去中心化之精髓，將 En-Tan-Mo 層層剝離，可抽出“泛我”的概念。溯源於古希臘時期普羅泰格拉的“人是萬物的尺度”，去中心化自此由“梵我”至“同我”至“泛我”之進化。復雜系統與多元結構，共識與價值，動態均衡與分權，自演進與開放性泛化為 En-Tan-Mo 的去中心化特徵。



2.1 復雜系統與多元結構：“符號價值與象徵交換”

多元結構是受符號代碼支配的描述，再度被釋放于 En-Tan-Mo 復雜系統之中，多元結構將運作于不同領域之間的通路，轉化為一張復雜的系統網絡。符號逐步脫離所涉對象的過程，以及這種符號對人的控制。多元結構所取用的，En-Tan-Mo 復雜系統會將其還回，但却多了一重差异，將周流的象徵解放出來以營造一種差异，遵循 En-Tan-Mo 自身的相互包含律。

En-Tan-Mo 的多元結構，有力地溢出了自身的界定，以潛在的方式居間、聚焦，外在于復雜系統的限制條件，界定抽離于 En-Tan-Mo 的過程之外。除了通過界定而擁有的結構之外，還帶有一種意義的過剩，復雜系統與 En-Tan-Mo 的述行力融為一體，從而產生關聯的共變。衆多韻律，衆多主體，共變着的滑移，形成了空間形式化的符號價值與象徵交換。

2.2 共識與價值：“千座高原”

“千座高原”盤踞于傳統思想模式中的種種層、編碼、超越性平面、紋理化空間等，一座座流播強度的“高原”，En-Tan-Mo “高原”平等與對等的形態從中抽提。多元性、異質性的連接則成為鏈節點之間彼此溝通的橫貫線，共識在連接中凸顯，而價值傳遞成為了可能。“千

座高原”是影響一個鏈段走向的元素，它不限于時間上，還意味着重現思想與人生開端的溯源能力。這也就是說，它能讓我們重回起頭處，體驗到最初的、邊緣上的取向如何發生，并由此而生出某種邊際處的敏感。

節點的平等被分布于一條 En-Tan-Mo 演變曲面之上，被分配于一個輪回語段結構之中。目的就是描繪一種對等事實狀態，維持 En-Tan-Mo 主體間關聯的平衡，或探索一種已經存在的無意識。鏈段抽提的平等旨在模仿某種完全完美之均衡，作為既成之物而被給予的事物，而此種對均衡的模仿是基于 En-Tan-Mo 化結構或支撐性的對等軸面。

2.3 動態均衡與分權：“波斯人信札”

通過 En-Tan-Mo 世界同時性發展所形成的均衡，這些具有相似的速度，共有階段的序列。主體不再關涉部分性的客體，而是關涉差異性的速度，En-Tan-Mo 的動態均衡將脫離預先存在或被導向存在的主體。不具有客體，也不具有主體，一種自然實在和一種客體之中，統一性不斷遭到阻礙，但在泛主體化的 En-Tan-Mo 之中，新的統一性却獲得分權與開放之間的互補，而主體也不再能够形成二元分化。

中心化的權力，自由結構體制的問題，永遠糾纏於最有權力的因素。而 En-Tan-Mo 的分權，換取的是去中心化的自治，自治並不等同于非完全的自由，僅是一種較中心化更自由的形態。“人生而自由却無往不在枷鎖之中”，這種二律背反已經證明了形而上學的不可能。

2.4 自演進與開放性：“作者之死”

在主體的解構和漸進缺席下，結構本身成為了總體，個體在和總體的相互關係中定義自身的意義和存在方式。因此，結構本身作為獨立於個體的存在和對現實進行的同構映射將作為歷史記錄和真實性的依據。顯然，一種靜態的結構將與歷史結構的演進和現實世界結構的複雜性將不斷產生矛盾。Levi-Strauss 在其名著“原始社會”的後記中已經提出了結構和演進之間

關係的複雜性問題及其在人類社會政治經濟學分析中的重要性。En-Tan-Mo 中解決這一問題的方式是在設計中內嵌入自演進的邏輯，使得這一體系能够在去中心化和結構保持穩定的前提下保障與現實之間的共時性和映射的合理性。

作者之死指作者作為創作的主體對作品不再具有壟斷的地位，在現代寫作中主體的身份已經被消解。因此，時間，空間和起源的概念都必須重新被理解。En-Tan-Mo 的建設過程本身就是一種寫作，這種寫作的目的是在一個新的空間維度內實現自由意志和秩序結構的統一。這種創作在制定一種自身體系內的元歷史或書寫歷史的規則，而真實性將通過對歷史結構的共識得到定義。對任何一個主體而言，任意地制定規則乃至於改變歷史將帶來一種難以克制的權力誘惑。因此，En-Tan-Mo 不僅意識到創作主體被解構的可能性，而且主動地實現這一解構過程，以創造一個真正去中心化的，公平的體系。

En-Tan-Mo 系統要創造的是一種新的歷史結構和在歷史結構中精神性的展開過程。這種創造絕非隨意的，而是基於嚴格的數學論證和對現實世界經濟結構的研究。En-Tan-Mo 將在以集中的形式和速度對人類社會經濟結構的發展史進行重現，正如同單個胚胎的發育能夠在某種程度上重演生物的進化階段。因此 En-Tan-Mo 不僅僅是一種新的交易方式，而是一場宏大的人類學實驗，它將重新構建我們對包括財產的本質，所有制的起源和權力的分配方式等基本問題的認識。

“人們自己創造自己的歷史，但是他們並不是隨心所欲地創造，並不是在他們自己選定的條件下創造，而是在直接碰到的，既定的，從過去繼承下來的條件下創造。”

每一個 En-Tan-Mo 的參與者都會是一種新的歷史結構的建設者和見證者。

LA MORT DE L'AUTEUR

L'énonciation même qui le définit, suffit à faire « tenir » le langage, c'est-à-dire à l'épuiser.

*
L'éloignement de l'Auteur (avec Brecht, on pourrait parler ici d'un véritable « distancement », l'Auteur diminuant comme une figurine tout au bout de la scène littéraire) n'est pas seulement un fait historique ou un acte d'écriture : il transforme de fond en comble le texte moderne (ou — ce qui est la même chose — le texte est désormais fait et lu de telle sorte qu'en lui, à tous ses niveaux, l'auteur s'absente). Le temps, d'abord, n'est plus le même. L'Auteur, lorsqu'on y croit, est toujours conçu comme le passé de son propre livre : le livre et l'auteur se placent d'eux-mêmes sur une même ligne, distribuée comme un *avant* et un *après* : l'Auteur est censé *nourrir* le livre, c'est-à-dire qu'il existe avant lui, pense, souffre, vit pour lui ; il est avec son œuvre dans le même rapport d'antécédence qu'un père entretient avec son enfant. Tout au contraire, le scripteur moderne naît en même temps que son texte ; il n'est d'aucune façon pourvu d'un être qui précéderait ou excéderait son écriture, il n'est en rien le sujet dont son livre serait le prédictat ; il n'y a d'autre temps que celui de l'énonciation, et tout texte est écrit éternellement *ici et maintenant*. C'est que (ou il s'ensuit que) écrire ne peut plus désigner une opération d'enregistrement, de constatation, de représentation, de « peinture » (comme disaient les Classiques) mais bien ce que les linguistes, à la suite de la philosophie oxfordienne, appellent un *performatif*, forme verbale rare (exclusivement donnée à la première personne et au présent), dans laquelle l'énonciation n'a d'autre contenu (d'autre énoncé) que l'acte par lequel elle se profère : quelque chose comme le *je déclare* des rois ou le *je chante* des très anciens poètes ; le scripteur moderne, ayant enterré l'Auteur, ne peut donc plus croire, selon la vue pathétique de ses prédécesseurs, que sa main est trop lente pour sa pensée ou sa passion, et qu'en conséquence, faisant une loi de la nécessité, il doit accentuer ce retard et « travailler » indéfiniment sa forme ; pour lui, au contraire, sa main, détachée de toute voix, portée par un pur geste d'inscription (et non d'expression), trace un champ sans origine — ou qui, du moins, n'a d'autre origine que le langage lui-même,

LA MORT DE L'AUTEUR

c'est-à-dire cela même qui sans cesse remet en cause toute origine.

*
Nous savons maintenant qu'un texte n'est pas fait d'une ligne de mots, dégageant un sens unique, en quelque sorte théologique (qui serait le « message » de l'Auteur-Dieu), mais un espace à dimensions multiples, où se marient et se contestent des écritures variées, dont aucune n'est originelle : le texte est un tissu de citations, issues des mille foyers de la culture. Pareil à Bouvard et Pécuchet, ces éternels copistes, à la fois sublimes et comiques, et dont le profond ridicule désigne précisément la vérité de l'écriture, l'écrivain ne peut qu'imiter un geste toujours antérieur, jamais originel ; son seul pouvoir est de mêler les écritures, de les contrarier les unes par les autres, de façon à ne jamais prendre appui sur l'une d'elles ; voudrait-il s'exprimer, du moins devrait-il savoir que la « chose » intérieure qu'il a la prétention de « traduire », n'est elle-même qu'un dictionnaire tout composé, dont les mots ne peuvent s'expliquer qu'à travers d'autres mots, et ceci indéfiniment : aventure qui advint exemplairement au jeune Thomas de Quincey, si fort en grec que pour traduire dans cette langue morte des idées et des images absolument modernes, nous dit Baudelaire, « il avait créé pour lui un dictionnaire toujours prêt, bien autrement complexe et étendu que celui qui résulte de la vulgaire patience des thèmes purement littéraires » (*les Paradis artificiels*) ; succédant à l'Auteur, le scripteur n'a plus en lui passions, humeurs, sentiments, impressions, mais cet immense dictionnaire où il puise une écriture qui ne peut connaître aucun arrêt : la vie ne fait jamais qu'imiter le livre, et ce livre lui-même n'est qu'un tissu de signes, imitation perdue, infiniment reculée.

*
L'Auteur une fois éloigné, la prétention de « déchiffrer » un texte devient tout à fait inutile. Donner un Auteur à un texte, c'est imposer à ce texte un cran d'arrêt, c'est le pourvoir d'un signifié dernier, c'est fermer l'écriture. Cette conception convient très bien à la critique, qui veut alors se donner pour tâche importante de découvrir l'Auteur (ou ses hypothèses : la société, l'histoire, la

3.0 En-Tan-Mo 數學

本節將從數學角度研究去中心化的區塊鏈系統，包括我們完成的工作和項目的發展規劃和方向，以及通俗地介紹項目開發應用到的數學工具。同時從這一角度給出我們發展 En-Tan-Mo 項目的理由。

3.1 去中心化的安全性問題

2009 年，中本聰發表了題為“*A Peer-to-Peer Electronic Cash system*”的論文，給出了比特幣區塊鏈思想的核心數學模型和理論證明，利用泊鬆分布證明該區塊鏈的作弊（我們稱之為對系統安全性的攻擊）可能性很低，從而解決了分布式記賬體系的信任困難問題，即拜占庭將軍問題。時至今日，中本聰理論中的一些重要假設發生了變化，導致比特幣區塊鏈相關結論不再正確。

中本聰關於在區塊鏈中作弊可能性的概率定量估計的基本思想：

當一個交易完成後，一組可具有合作性的攻擊者立即開始上傳包含虛假信息的區塊并以此為基礎建造假鏈。如果在誠實的礦工已經延伸了 z 個區塊的時刻，攻擊者所挖的區塊數量滿足泊鬆分布。則在此前提下，中本聰利用全概率公式計算出了假鏈能够在某一時刻取代真鏈的定量估計，但隨着 ASIC 矿機和礦池的出現，上述前提假設不再成立。依靠算力得到新的區塊，本質上是 Binomial 隨機游走問題，其中：

p = probability an honest node finds the next block; p 表示某一個誠實者找到下一個區塊的概率

q = probability the attacker finds the next block; q 表示作弊者找到下一個區塊的概率， $p+q=1$

當交易後誠實礦工已經挖出了 n 個區塊時，我們將攻擊者所挖的區塊數量記為隨機變量 X_n 。該問題可以轉化為賭博積分問題 (Problem of points)，即把作弊者每次建造一個區塊記為成功，概率為 q ；將誠實者建造一個區塊記為失敗，概率為 $p=1-q$ 。則 $P\{X_n=k\}$ 表示這個隨機試驗在 n 次失敗前恰有 k 次成功的概率，滿足負二項分布 (Negative Binomial distribution)：

$$P\{X_n=k\} = C_{k+n-1}^k p^n q^k$$

如果滿足以下條件：

1. 誠實礦工所挖的區塊數量 n 較大；

2. 存在一個有限的常數 λ ， $n \frac{q}{p} \rightarrow \lambda$ 記， $I_n = n \frac{q}{p}$ 則根據以下計算

$$P\{X_n=k\} = \frac{n^n}{(n+I_n)^n} \frac{I_n^k}{(n+I_n)^k} \frac{(k+n-1)!}{(n-1)! k!} = \frac{I_n^k}{k!} \frac{1}{(1+\frac{I_n}{n})^n} \frac{n(n+1)...(n+k-1)}{(n+I_n)^k}$$

$$(1+\frac{I_n}{n})^n \rightarrow e^\lambda$$

可得隨機變量 X_n 的分布律趨近于參數為 λ 的泊鬆

分布 (Poisson distribution):

$$P\{X_n=k\} \rightarrow \frac{\lambda^k}{k!} e^{-\lambda}$$

在礦機和礦池存在的條件下，上述假設條件 (2) 難以滿足，因此中本聰的定量估計是不正確的，該數學模型已經不能對比特幣金融風險進行精確控制。不僅如此，當作弊者擁有一定強度的算力資源，並且通過非光滑控制的方法調節自己的算力（例如在作弊開始時突然增大算力），則作弊成功的概率遠非如中本聰所估計的那樣小。

因此，通過不依賴於算力的權益計算方法，控制 q 的大小，同時加快區塊產生的速度，可以更有效地控制作弊者成功的概率，并得到關於這一概率的更準確的定量估計。

當誠實礦工已經挖出 z 個區塊時，誠實礦工與攻擊礦工所挖的區塊數量差距可以用隨機變量 $z - X_n$ 來表達。利用賭徒破產問題 (Gambler's Ruin problem) 的方法可以得到，當真鏈和假鏈之間的差距為 $z - k$ 個區塊時，假鏈長度最終在某一時刻能超過真鏈的概率是：

$$\begin{cases} (q/p)^{z-k}, & \text{if } z > k \\ 1, & \text{if } z \leq k \end{cases}$$

此時，作弊者成功的概率估計 $P(z)$ 可用全概率公式計算如下：

$$P(z) = P\{X_z \geq z\} + \sum_{k=0}^{z-1} P\{X_z = k\} \left(\frac{q}{p}\right)^{z-k} = 1 - \sum_{k=0}^{z-1} C_{k+z-1}^k (p^z q^k - q^z p^k)$$

根據 C. Grunspan 和 R.-P. Marco 的工作，作弊者在掌握遠小於 51% 的算力時，就有很大成功的可能性。這說明單純的算力證明法 (POW) 的安全性並不如預計的強，我們提出 POW 加 DPOS 相結合的對偶共識，用礦工的選舉制度來進行監督和制約，可以有效地加強安全性。

3.2 Nash 均衡與共識算法

“En-Tan-Mo” 在設計共識算法時，利用了 Nash 均衡的思想，我們先介紹 Nash 均衡的基本定義，然後簡要說明如何利用在我們的共識設計中。

設 S_1, S_2, \dots, S_N 為緊致的距離空間， J_1, \dots, J_N 為定義在 $\prod_{i=1}^N S_i$ 上的連續函數。我們記 $P(S_i)$ 為定義 S_i 的所有 Borel 概率測度所構成的緊致距離空間

定義：在混合策略博弈中的 Nash 均衡表示這樣的策略組合 $(\pi_1, \dots, \pi_N) \in \prod_{i=1}^N P(S_i)$ ，使得對於任意的 $i = 1, 2, \dots, n$,

$$J_i(\bar{\pi}_1, \dots, \bar{\pi}_N) \leq J_i((\bar{\pi}_j)_{j \neq i}, \pi_i) \quad \forall \pi_i \in P(S_i)$$

$$\text{其中 } J_i(\pi_1, \dots, \pi_N) = \int_{S_1 \times \dots \times S_N} J_i(s_1, \dots, s_N) d\pi_1(s_1) \dots d\pi_N(s_N).$$

定理：((J. Nash, 1950), (Glicksberg, 1952)) 在以上假設條件下，對於混合策略存在至少一個不動點。

目前已有大量文獻討論例如比特幣等區塊鏈系統的

博弈論分析且文獻數量在不斷增加。Nash 均衡指一種策略狀態的集合，任何人不能通過單方面地改變策略來獲得更大利益。這對於去中心化系統是至關重要的，因為在這類系統中沒有一個中心化的控制者可以通過“懲罰”偏離行爲來維持秩序。

問題在於：Nash 均衡的策略並非一定是高效的。在比特幣系統中甚至可以說 Nash 均衡對應的策略是非常低效浪費的。這是因為對於比特幣而言唯一的安全機制來源是算力證明，礦工可以隨意加入或離開系統。這種挖礦一個純粹非合作遊戲，獲勝的唯一決定因素是算力。這種算力證明機制在令參與者服從共識方面是非常成功的，例如誠實挖礦和服從“最長鏈法則”。但同時，每個礦工都有驅動依靠升級挖礦裝備來獲得更大利潤。這種“軍備競賽”導致了巨大的資源浪費和實質性的壟斷者出現。這種浪費和損耗現象在經濟學中被稱為“公地悲劇”，在算法博弈論中則被稱為“無秩序的代價”。

這一問題的唯一解決方式是通過機制設計，“經濟學的工程層面”。機制設計又被稱為經濟學中的逆問題：不是在已有機制設計下研究結果，而是尋找能夠實現所需要結果的機制。區塊鏈系統是應用機制設計理論的完美領域，因為在這裏設計者在制定規則方面有極大的自由。在這裏，機制可以被視為將策略和結果相連接的過程。Nash 均衡的重要性在於，如果博弈參與者都是理性的且能很好地預測結果，則他們一定會預測到 Nash 均衡策略。否則，一定會有參與者有驅動采用其他策略。在區塊鏈體系下這一問題更為迫切：因為沒有中心化權力的限制，一旦參與者感受到更大利益的驅動就會實施新的策略而不再服從共識。在 ETM 系統中使用了 POW 與 DPOS 雙共識機制設計以實現去中心化前提下 Nash 均衡狀態的高效性。在未來計劃的工作中將在機制設計中引入康托洛維奇價格機制和 Vickery 拍賣模型。

3.3 投票制度中的權益調節模型

目前在許多區塊鏈系統中採用了代表權益證明(DPOS)，相對於單純的算力證明(POW)有節省資源和區塊產生速度較快的優勢。這一理論的預設是在一個區塊鏈體系中占有較多權益(Token)的人更可以被信賴。“En-Tan-Mo”認為，根據目前區塊鏈及加密貨幣的發展現狀，權益以一種近似 Pareto 分布的方式集中在少數人手裏。為了避免選舉權力的過度集中，所以我們需要對他們的投票權與權益之間應當是正相關，但並非線性的關係。在這裏對我們的方案作出一些簡要說明。

設系統中有 N 個節點，某個節點 i 在投票開始時占有的權益占總權益的比例為 α_i ， $\sum_{i=1}^N \alpha_i = 1$ 。我們定義一個嚴格上凸函數映射 f ， $\frac{\partial f(\alpha_i)}{\partial \alpha_i} > 0$ ， $\frac{\partial^2 f(\alpha_i)}{\partial \alpha_i^2} < 0$ ，我們規定這一節點所擁有的選票數量在總選票中的比例為

$$B_i = \frac{f(\alpha_i)}{\sum_{i=1}^N f(\alpha_i)} \quad , \text{顯然} \quad \sum_{i=1}^N B_i = 1$$

根據嚴格上凸函數的簡單性質 $f(\sum_i \alpha_i) < \sum_i f(\alpha_i)$ ，可得對於兩個相對權益分別為 α_i ， α_j 的節點（不失一般性，設 $\alpha_i > \alpha_j$ ）：

$$\frac{B_i}{B_j} = \frac{f(\alpha_i)}{f(\alpha_j)} = \frac{f\left(\frac{\alpha_i}{\alpha_j}\alpha_j\right)}{f(\alpha_j)} < \frac{\frac{\alpha_i}{\alpha_j} f(\alpha_j)}{f(\alpha_j)} = \frac{\alpha_i}{\alpha_j}$$

問題在於，在這一機制下，大股東有可能嘗試通過將自己的股權分散到多個不同賬戶以在投票中獲得優勢。這一類行爲在網絡安全中被稱為女巫攻擊。

從博弈論的角度，我們認為這將不是一種理性策略。論證如下：

大股東在已有的 stake 基礎上分散化到多個節點確實可以增加自己的投票權；

參與者行爲的最終動機是獲得更大的利益，在 En-Tan-Mo 中即是獲得更多的 Token 獎勵。投票權只是手段而不是目的；

在 ETM 的交易機制中，每次投票是伴隨着一段交易發生的。而交易會產生交易費用。這樣對於攻擊者（女巫攻擊）而言，分散化投票是有成本的。因為攻擊者必須產生大量的毫無意義的交易以獲得更多投票機會，隨之帶來交易費用的損耗。

En-Tan-Mo 建立在博弈論和 Thomas Sargent 的理性預期(rational expectation)經濟理論之上。我們的數學理論認為，大股東 stake 分散化的理性預期收益將無法覆蓋其所付出的交易費用損耗。因此，這種分散化將不是參與者的合理選擇。

3.4 混沌排序

En-Tan-Mo 項目的共識設計將安全性作為核心目標之一，並設定了極高的標準。針對 DPOS 體系中可能出現的多位 SCV 矿工協調進行作弊的問題，共識層將採用混沌排序的方式加以解決。

混沌：動力系統中動力學行爲對初值的極度敏感性。

通俗地說，混沌就是指對初值極小的擾動可以導致映射結果極大的變化，因此在預測過程中會導致一種不確定性。這種不確定性正是我們需要的。在上傳區塊的過程中，如果某幾個礦工希望聯合起來作弊，則他們需要連續地確認一個包含虛假信息的區塊。為此目的，他們需要盡早地知道不同礦工上傳區塊的排列次序並有足夠的時間加以協調。混沌重排指礦工上傳的順序並非一開始就確定，而是共識層的設計規定一種算法，提取每一次成功上傳區塊中的某些信息作映射 Ψ 并進行多次迭代計算出下一名礦工的編號。因此直到礦工祇有在最後一刻才知道應該上傳區塊的礦工身份。

1. 一個類 Hénon 多維映射，其動力學方程如下：

$$\begin{aligned} x(n+1) &= ax(n) + by(n)^2 \\ y(n+1) &= cx(n) + dy(n) + dx(n)z(n) \\ z(n+1) &= x(n)^2 + ey(n)x(n) \end{aligned}$$

2. 令 256bit 的二進制和其對應的十進制數分別為 I 和 D，其映射關係可描述如下：

(1) 利用 Matlab 中均匀分布生成函數 randi 生成一個隨機迭代數 $N_1 (3 \leq N_1 \leq 13)$ 。

(2) 利用時刻的系統輸出，隨機產生初值的選取維度
 $(idxo) \quad s = x(N_1) + y(N_1) + z(N_1)$
 $idxo = \text{mod}(s, 3) + 1$

(3) 利用其它 2 個維度的信號產生 2 個隨機數
 $(seg1, seg2)$

例如：

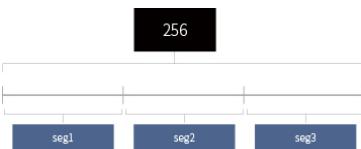
$idxo = 2$, (即從 x 維選取 i 作為初值)，那麼

$seg1 = \text{mod}(x(N_1), 12)$
 $seg2 = \text{mod}(z(N_1), 12)$

(4) 將 I 看作 32 個 8bit 塊構成，利用 seg1 和 seg2 將 I 切分為 3 個區塊

$I1 = \text{slit}(I, seg1), I2 = \text{slit}(I, seg2), I3 = \text{slit}(I, seg3)$

其中， $seg3 = 256 - seg1 - seg2$, slit 函數所對應的切分規則如下圖：



(5) 利用 $I1, I2, I3$ 分別生成“系統參數縮放值”(var-par), “系統迭代次數”(val-N), “系統初值縮放值”(val-init)

(6) 利用 val-par, val-N, val-init 初始化超混沌系統，并進行計算，選取第 $idxo$ 維的信號作為輸出，并通過換取運算產生 1-101 之間的一個整數，即 D。

混沌映射是確定性的，因此所有礦工都通過自己的計算得到完全一致的排序結果。系統的穩定性和安全性在去中心化的前提下得到了實現。

3.5 Kantorovich 對偶，最優輸運與去中心化

“En-Tan-Mo”區塊鏈的共識稱為康托洛維奇共識，來自于蘇聯數學家康托洛維奇在最優輸運領域的工作，尤其是其在 1939 年的著作中提出的康托洛維奇對偶定理。這一定理是線性規劃和最優輸運中早期的開創性結果之一。我們簡要介紹這一理論及其在去中心化的區塊鏈系統中應用的可能性。

設 X, Y 為兩個集合（或對應現實中的區域），我們要將 X 處的物質運送到 Y 處。設 $c(x, y)$ 為將每個對應的點 x 到 y 的輸運成本（或密度函數）。設 γ 表示在區域 $X \times Y$ 上物質的概率分布， μ 和 ν 分別表示其在 X 和 Y 上的邊緣分布。可用 $\int_{X \times Y} c(x, y) d\gamma(x, y)$

表示從 X 到 Y 的整體輸運成本。康托洛維奇對偶定理指出：

$$\inf_{\gamma \in \Pi(\mu, \nu)} \int_{X \times Y} c(x, y) d\gamma(x, y) = \sup \left\{ \int_Y \psi(y) d\nu(y) - \int_X \varphi(x) d\mu(x) : \psi(y) - \varphi(x) \leq c(x, y) \right\}$$

其中 \inf 和 \sup 分別表示下確界和上確界。在此略去嚴格的數學細節，僅給出一個通俗的解釋：如果“En-Tan-Mo”有一個去中心化的交易體系， $\psi(y)$ 表示在 y 處

賣出的價格； $\varphi(x)$ 表示在 x 處買入的價格，那麼

$$\int_Y \psi(y) d\nu(y) - \int_X \varphi(x) d\mu(x)$$

表示這個交易體系的最終利潤。對偶定理的結果表示，在限制條件 $\psi(y) - \varphi(x) \leq c(x, y)$ 下，整體輸運成本最小化的策略恰好對應利潤最大化的策略。

這一定理指出了建立一個合理價格體系對於優化資源輸運和配置的重要性。由於這一理論在經濟學層面的可能解釋，康托洛維奇的這一理論在蘇聯學術界曾長期遭到批判，他本人也被逮捕入獄。

在區塊鏈的技術層面，最優輸運對應的就是價值傳遞的最佳策略和組合方式。“En-Tan-Mo”認為合理的方式應當是採用去中心化的體系建立完善的信任機制，讓每一個節點根據自身掌握的交易信息作出決策，形成一個透明的、信息公開化的市場，利用市場自身的調節機制形成一個動態均衡的價格體系。這也就是“En-Tan-Mo”希望實現價值傳遞的方式。

3.6 去中心化體系中的動態價格形成

在“En-Tan-Mo”系統中，每一個個體同時是服務的提供者和購買者，即是買家也是賣家。去中心化的市場核心是價格調節機制，而價格將以一種動態均衡的方式自組織地形成。“En-Tan-Mo”使用平均場博弈論的思想研究去中心化交易體系中的價格動態形成問題。這一模型又被稱為 Lasry-Lions 價格形成模型。假設價格偏好具有一定的隨機性。用密度函數 f_B, f_V 分別描述買家和賣家的數量。 t 表示時間， x 表示價格。例如 $f_B(x, t)$ 表示時刻 t 而價格為 x 時的買家數量。用 $p(t)$ 表述動態均衡過程所產生的價格。 a 表示交易費用。得到如下平均場方程組：

$$\begin{aligned} \frac{\partial f_B}{\partial t} - \frac{\sigma^2}{2} \frac{\partial^2 f_B}{\partial x^2} &= \lambda \delta(x - p(t) + a), & \text{if } x < p(t), \quad t > 0 \\ f_B &\geq 0, \quad f_B(x, t) = 0 \quad \text{if } x \geq p(t), \quad t \geq 0 \\ \frac{\partial f_V}{\partial t} - \frac{\sigma^2}{2} \frac{\partial^2 f_V}{\partial x^2} &= -\lambda \delta(x - p(t) - a), & \text{if } x > p(t), \quad t > 0 \\ f_V &\geq 0, \quad f_V(x, t) = 0 \quad \text{if } x \leq p(t), \quad t \geq 0 \\ \lambda &= -\frac{\sigma^2}{2} \frac{\partial f_B}{\partial x}(p(t), t) = +\frac{\sigma^2}{2} \frac{\partial f_V}{\partial x}(p(t), t) \end{aligned}$$

其中乘子 λ 用于刻畫時刻 t 的交易數量。 σ 用于描述隨機性， δ 表示一個 delta 函數。給定初始條件：

$$f_B(x, 0) = f_B^0, \quad f_V(x, 0) = f_V^0$$

這一方程組類似於一維熱傳導方程，但它的難度在於其中出現的自由邊值問題。自由邊值問題是現代偏微分方程理論中的核心問題，起源于物理學中的相變問題，在目前在許多領域中有廣泛的應用。

在去中心化的區塊鏈體系中，由於採取了分布式記賬，每個節點可以通過它所掌握交易信息動態地調節自身的行為，因此這實質上是一種貝葉斯型反饋控制問題，即參與者可以通過後驗概率實時地調整策略以盡可能增加自己的收益。“En-Tan-Mo”將在後續工作中引入帶貝葉斯控制系統的動態價格方程模型，將區塊鏈技術與人工智能，深度學習技術緊密結合。

4.0 En-Tan-Mo 經濟學

區塊鏈與其相關技術的變化將會對當代經濟狀況產生巨大的顛覆作用。工業革命出現在一個商業模式以等級制度和金融資本主義為根據的世界裏。區塊鏈革命將會見證一個由人力資本主義和高度自治為主導的經濟體制。

這一切最終將如何呈現，目前尚不清晰。企業家和創新者將會一如既往地通過不斷試錯去解決這個不確定性。毋庸置疑的是，在我們確切知道這種顛覆將如何呈現之前，大量的財富將被創造和毀滅。

而 En-Tan-Mo 的貢獻在於，當這場顛覆出現時，En-Tan-Mo 提供一個均衡的價值傳遞模型，讓人們清晰地認識到這場顛覆的含義。

4.1 En-Tan-Mo 加密貨幣經濟學

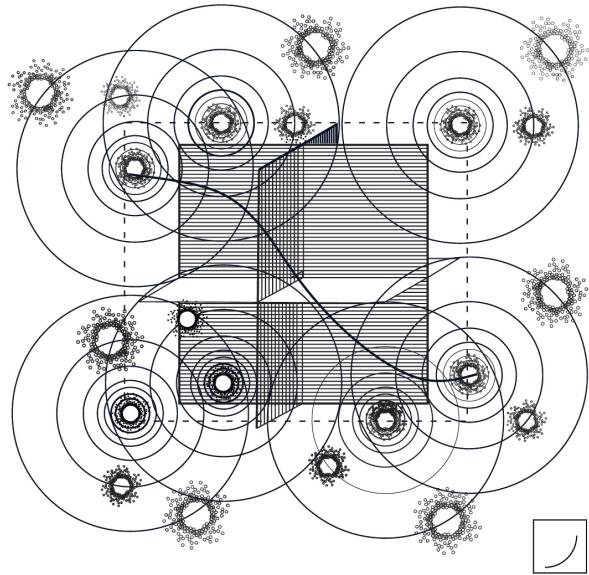
信任關係廣泛存在于商業活動尤其是金融系統中，交易中每一組信任關係背後，都代表著相應不確定性的存在，與相應交易費用的節省。En-Tan-Mo 讓可絕對信任的交易信息流成為現實，這使許多交易環節中人與人的信任關係能夠轉為人與技術的信任，將不確定性將至 0，以及整個交易過程中的信任關係重新組織，讓交易費用整體下降成為可能。

現有的區塊鏈技術除了整體效率較低，還帶來了顯著的負面影響。目前區塊鏈的應用在交易速度（比特幣 7 筆 / 秒）、隱私性、資產可追回性（Mt.Gox 被黑）等存在一些不够理想的地方。En-Tan-Mo 不僅需要提高整體效率，還將在商業組織中提供一種業務穩定運作，其相關業態將隨之配套，利益分配機制也相應確定，En-Tan-Mo 在應用時採用技術保證決策者利益沒有明顯的負面影響。

En-Tan-Mo 加密經濟學的研究對象是：在密碼安全且無需信任的賬本中，制度的重要性。古典主義和新古典主義經濟學家將稀有資源的生產和分配，以及支撐生產和分配的要素作為研究對象。這是一門把規則作為研究對象的經濟學。規則（如法律、語言、產權、規定、社會準則和意識形態）使得分散的和投機的人們之間的活動得以相互協作。規則可以促進交換——不僅是經濟交換，還有社會和政治交換。

En-Tan-Mo 加密經濟學正是聚焦在支撐區塊鏈及其衍生應用上的經濟學原理和理論。它着眼于區塊鏈機制設計中主要使用到的博弈論和激勵設計。經濟和作為其分支的制度經濟學一樣，都是一個協調交換的系統。但制度經濟學並非着眼于規則，而是聚焦在賬本上：由規則構成的數據。

En-Tan-Mo 經濟學對如下內容感興趣：傳遞價值的治理規則；服務於這些價值的社會、政治和經濟機構的發展；以及 En-Tan-Mo 是如何在全世界範圍內改變價值傳遞模式的。



4.2 納什均衡

En-Tan-Mo 系統的一個重要優勢是在設計的過程中積極與深刻地應用博弈論作為機制設計的工具。在已有區塊鏈系統如比特幣系統中效率低下的問題可被稱為“無秩序的代價”。在 En-Tan-Mo 中，En-Tan-Mo 的數學家通過巧妙的設計雙共識機制，讓每個參與者都可以以礦工或投票人的身份平等參與區塊鏈的建設並獲得均衡的獎勵，礦工之間、投票人之間、礦工和投票人之間均通過簡潔有效的共識協議進行調節，從而保證理性的參與者策略集合達到一種完美的納什均衡狀態。共識機制及其算法是 En-Tan-Mo 實現去中心化的核心和基礎，其本質是要實現“沒有統治者的統治”或者說“去中心化的自適應控制”。En-Tan-Mo 共識機制算法的最重要基礎是納什均衡。這一概念由美國數學家，諾貝爾經濟學家得主 John F. Nash 提出，其定義是：

在一個多人參加的博弈過程中，所有參與者各自選擇的策略所組成的一個集合，任何人都不能通過單方面改變自己的策略（作弊）獲得更大的利益。

En-Tan-Mo 研究中的另一個重要創新是將理性預期理論和博弈論相結合。ETM 項目的資深顧問托馬斯·薩金特教授是理性預期理論領域的領軍人物。在區塊鏈系統的博弈論分析中需要注意到如下事實：參與者會受到驅動進行預測，而他們對未來的預測將直接影響到他們當下的決定。這對於 ETM 的機制設計是至關重要的。因為設計者本身需要“預測”參與者在不同處境下所可能採取的決定和策略。這一類設計對應於現代控制理論中的預測控制問題。系統的安全性依賴於對納什均衡的正確預測，而這一預測本身又依賴於機制設計者對於參與者信念和決策的預測。ETM 科學顧問委員會將在這一方進行更具有數學嚴格性的研究。

En-Tan-Mo 認為，單純的 POW 和 DPOS 共識無法保證所有區塊鏈參與者的納什均衡狀態。以比特幣為例，礦工在最先算出哈希值之後，如果上傳虛假的區塊最終不會被系統採用，這樣會導致損失算力挖礦所消耗的成本，從而保證所有參與者的均衡收益。具體地說：1. 如果所有區塊鏈參與者都可以參加挖礦，那麼計算的難度要足夠大才可以使得作弊成功（即包含虛假信息的分叉在某一時刻超過主鏈長度）的概率足夠小；2. 每個礦工付出的成本要足夠大才能阻止他冒險採用作弊的策略。隨著 ASIC 礦機的出現，普通參與者在比特幣區塊鏈中幾乎不可能得到任何收益，算力的大幅提升同時會導致挖礦難度的增加，從而增加了作弊者相互協調採取合作策略的可能性，納什均衡狀態被完全打破。以太坊的完全節點也都是經過加強的專用 GPU 礦機，普通大眾根本承受不起，幾乎所有的輕客戶端根本不需要操心挖礦的問題。與 POW 同理，POS 或 DPOS 共識機制，以 Token 擁有數量作為唯一標準，大股東在投票權上是處於壟斷地位的，這必然將導致決策是由少數人制定的，沒有大眾參與，財富迅速向少數人手中集中，均衡同樣被打破。

En-Tan-Mo 的納什均衡是讓所有的參與者都能成為 En-Tan-Mo 世界的直接受益者，利益不能被大礦池或大股東壟斷，必須在底層共識機制提出基礎性變革。En-Tan-Mo 中的博弈參與者即所有用戶，參與者在 En-Tan-Mo 中有三種身份狀態：SCV 礦工、監察官和 Pareto 礦池，獲得的利益指其通過投票選舉或上傳區塊的方式得到 ETM Token 及非 ETM Token 獎勵。通過選舉制度遴選 SCV 礦工，每個出塊周期由若干 SCV 礦工合作有序出塊，每個礦工作弊損失的挖礦成本雖然變小了，但是隨之增加的是作弊被開除出礦工團隊的預期損失；為了提高 En-Tan-Mo 出塊效率，監察官有義務選擇出最佳 SCV 礦工，並根據選擇成功率獲得相應 ETM Token 獎勵，票數和 Token 數量的關係被上凸函數抑制，保證了全體股東的利益。SCV 礦工和監察官之間獨立性和關聯性並存，權利和利益分配清晰平衡。Pareto 礦池中的礦機雖然在本周期內不能獲得 ETM Token 獎勵，但是以聯盟的形式參與外部區塊鏈的生產出塊，獲得其他區塊鏈的 Token

獎勵，從而保證所有礦機的正收益。因此，通過 DPOS 和 POW 統一權益證明共識，En-Tan-Mo 中 SCV 礦工、監察官和 Pareto 礦池三者內部和三者之間達到了納什均衡。

為了說明共識機制的經濟學設計如何影響參與者的決策（策略選擇包括兩種：誠實挖礦或作弊），我們重複強調如下假設和規則：

假設：至少一半的參與者是誠實的；

規則：1. 只有最長的鏈會被最終認可；2. 選舉制度中，上傳包含虛假信息的區塊或效率低的參與者將被排除 SCV 礦工。

4.3 Kantorovich 共識

採用 POW 算力證明的第一代和第二代區塊鏈被人批評的地方包括：1. 交易處理的速度過慢，如比特幣目前的交易速度完全不能與傳統的金融體系如銀行信用卡相比；2. 區塊上傳的速度過慢導致拖累交易最終確認的速度；3. 容量問題，目前的效率使得這些區塊鏈難以擴大規模；4. 算力挖礦導致的資源浪費和環境污染。

為此，En-Tan-Mo 提出基於納什均衡的 Kantorovich 共識機制。監察官作為 En-Tan-Mo 股東，不直接參與 En-Tan-Mo 出塊，而是根據擁有 Token 獲得投票選舉權利從而獲取投票 ETM Token 獎勵，監察官將礦工算力和過往表現作為投票的主要依據選擇出最佳 SCV 礦工，使得 En-Tan-Mo 保持高效率和安全性；SCV 礦工作為 En-Tan-Mo 出塊節點，被監察官選出合作競爭的挖礦，從而獲得出塊的 ETM Token 獎勵，SCV 礦工在每個出塊周期有序出塊，在不降低安全性的前提下減小哈希值的計算難度，從而增加每個區塊的產生速度，提高效率；未被選中的礦機進入 Pareto 礦池組成聯盟，運用特有的衍生鏈技術參與外部區塊鏈的生產出塊，按照礦機提供算力分配非 ETM Token 獎勵，從而保證所有礦機的正收益。所以，Kantorovich 機制可以在保障安全性的同時提高效率，增加系統的可擴展性。

目前中心化的體系在效率方面仍具有較強的優勢。但是如果採用更加巧妙的數學結構設計，通過去中心化和適當的合作競爭制（比如 En-Tan-Mo 的 Kantorovich 共識）之間的平衡，完全可以得到安全性，穩定性和效率兼備的區塊鏈系統，這也是我們的主要工作目標。

Kantorovich 共識是一種革命性權益證明算法，它決定了各個礦工節點如何達成網絡的一致性，該算法是 En-Tan-Mo 基礎架構的重要組成部分，是區塊鏈技術的重大創新。Kantorovich 共識重新設計了需要能量消耗的工作量證明（POW）協議，該問題是區塊鏈長久以來無法擴大應用的障礙。算法由科學顧問委員會領導的博弈論團隊設計而成，並通過同行評審，這是第一個具有科學憑證其安全性的 UPOS 統一權益證明共識。

Kantorovich 共識的思想受到了蘇聯數學家，1975 年諾貝爾經濟學獎得主 Leonid Kantorovich (列昂尼德·康托洛維奇) 工作的啟發。他在 1930 年代提出嚴格的最優輸運數學模型和 Kantorovich 對偶定理，這一理論證明了可以利用價格非集中化的方法達到資源配置的最優。康托洛維奇由於去中心化經濟學觀點長期受到蘇聯主流學術界批評和抨擊，慶幸的是，他本人因為參與蘇聯原子彈計劃免于更嚴厲的迫害。同時，康托洛維奇的經濟理論在西方學術界得到了認可並被廣泛應用。Kantorovich 最優輸運理論是近 20 年數學最重要研究方向之一，菲爾茲獎得主 Cedric Villani 和 Pierre Louis Lions 的工作都建立在這一基礎上。因此 En-Tan-Mo 將共識機制命名為 Kantorovich 共識以致敬他的數學成就和特殊時代表現出的超凡勇氣。

4.4 SCV 矿工和監察官

En-Tan-Mo 中經過礦工團隊選舉制度被選中並通過基礎算力測試的礦工被稱為 SCV；Token 的持有者在投票選舉 SCV 矿工團隊時的身份，被稱為“監察官”。監察官將手上的 Token 在 En-Tan-Mo 中通過上凸權益映射轉化為可投票數，每投票周期給予相應獎勵；候選礦機根據得票高低當選 SCV 矿機和候補礦機，獲得上傳區塊權利，驗證區塊義務和區塊獎勵。

假設一個 SCV 矿工作弊，試圖上傳包含虛假信息的區塊，Double Spend 等，面對的結果是：1. 由於大多數 SCV 矿工是誠實的，可以利用概率論方法證明，作弊礦工上傳的虛假區塊將會最終成為分叉并消失，因此將損失掉算力挖礦過程中所耗費的成本；2. 由於 Kantorovich 共識機制中的輪換選舉制度，作弊礦工將確定地在下一次選舉中被開除出礦工團隊，從此失去挖礦獲取 Token 的機會和之前投入的保證金。因此，任何一個 SCV 矿工一旦被投票選入礦工團隊中，理性選擇必然是高效地完成任務並上傳真實的區塊信息。

由此可見，雖然整個 En-Tan-Mo 體系中並沒有一個中心化的監督者強制規範 SCV 矿工和監察官的行為，但是其中包含的經濟學設計將作為“看不見的手”利用 SCV 矿工和監察官對自身最大利益的追求引導所有參與者服從共識，這樣就解決了 En-Tan-Mo 參與人相互之間的信任問題和效率問題。

4.5 Pareto 矿池

En-Tan-Mo 系統的獎勵方式採用經濟學理論作為設計基礎，其優點體現在三個方面：

1. 公平性：在外部 POW 區塊鏈體系中，個體之間分配不均，例如比特幣和以太幣的權益嚴重向若幹中心礦池或礦場集中；在 En-Tan-Mo 體系中，所有個體在共識機制面前是平等的。
2. 去中心化：在外部 DPOS 區塊鏈體系中，實力雄

厚的 Token 持有者掌握系統的決定權，重新回到中心化軌道或出現多個寡頭壟斷；在 En-Tan-Mo 體系中，Token 持有者和區塊生產者職、權、利分離，所有個體均享有去中心化帶來的資源和優勢。

3. 最優性：在外部區塊鏈體系中，個人收益單一，鏈與鏈之間像一座座孤島，未能打通；在 En-Tan-Mo 體系中，Token 持有者獲得投票激勵，礦機節點在 SCV 矿工和 Pareto 矿池間的切換從而獲得最佳收益。

在 Kantorovich 共識機制中，所有礦機節點組成一個合作競爭型的礦池，每個出塊周期選擇若干 SCV 矿工有序出塊，En-Tan-Mo 將該周期中未被選中的所有礦機組成 Pareto 矿池，運用特有的側鏈技術和聯盟策略，根據即時收益算法分析，參與外部區塊鏈的生產出塊，按照礦機提供算力分配礦池收入，從而保證所有礦機的正收益。

Pareto 矿池的經濟學原理核心在於：訂立聯盟策略；選擇合適區塊鏈；建立聯盟結構與管理制度；礦機在 SCV 矿工和 Pareto 矿池間的切換。

Pareto 矿池具有如下特點：

1. 組織的去中心化：Pareto 矿池以共同分享市場、合作挖礦為基本目標，礦池間的成員關係由外部區塊鏈收益策略決定，並非一成不變。Pareto 矿池本身是一個動態的、開放的系統。

2. 行為的戰略性：Pareto 矿池的方式與結果是對外部區塊鏈競爭環境的長期謀劃。聯合行為也注重從戰略的高度改善礦池聯盟共有的經營環境和經營條件，其最大的着眼點是在經營活動中積極地獲取外部經濟資源。

3. 合作的平等性：Pareto 矿池不同於以往的戰術性合作，它是聯盟各方在資源共享、優勢互補、相互信任、相互獨立的基礎上，通過事先達成共識結成的一種平等關係，按照算力分配收益，從根本上改變了礦機之間不平等關係的局面。

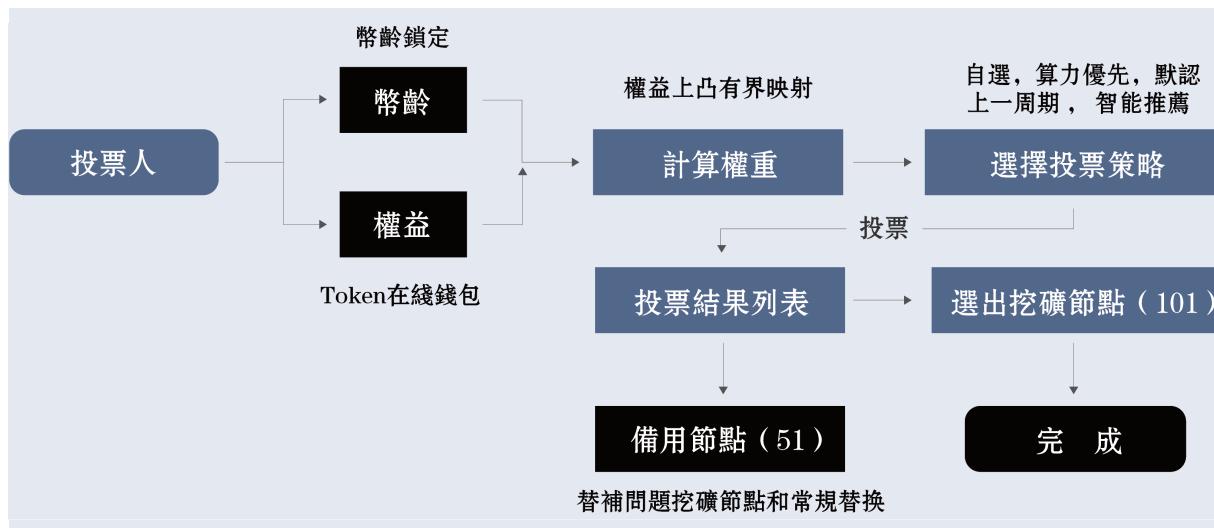
4. 管理的複雜性：在 Kantorovich 共識機制中，第一次出現了真正意義的“雙挖”，礦機需要在 SCV 矿工策略和 Pareto 矿池策略間切換，最大的收益建立在嚴謹的共識機制和巧妙的管理制度上。

帕累托最優（Pareto Optimality），也稱為帕累托效率（Pareto efficiency），是指資源分配的一種理想狀態，假定固有的一群人和可分配的資源，從一種分配狀態到另一種狀態的變化中，在沒有使任何人境況變壞的前提下，因此，帕累托礦池最優是公平與效率的“理想王國”。

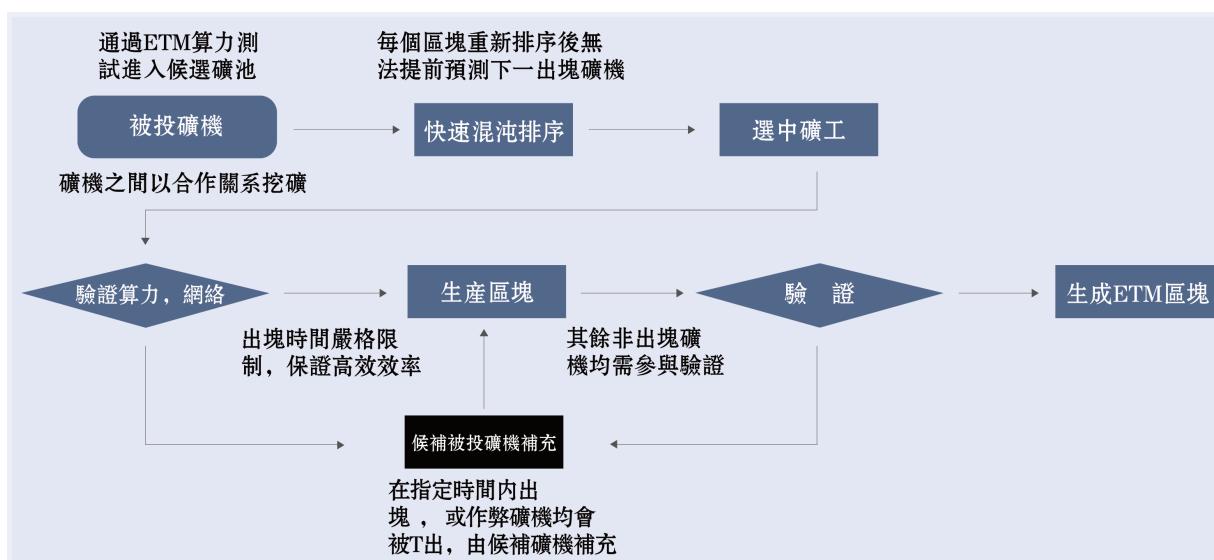
5.0 En-Tan-Mo 計算

5.1 En-Tan-Mo 算法與流程

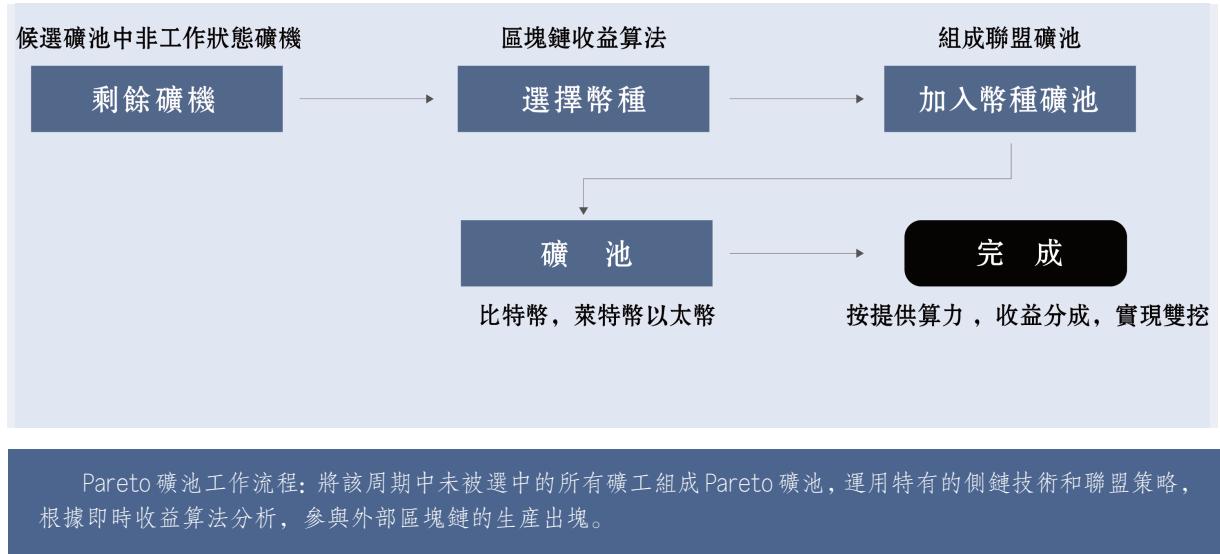
Kantorovich 共識流程圖：基于 Nash 均衡思想的 Kantorovich 共識機制采取了礦工團隊選舉制度，每個出塊周期選擇若干 SCV 級別有序出塊，在不降低安全性的前提下減小哈希值的計算難度，從而增加每個區塊的產生速度，提高效率。



監察官投票流程：監察官將手上的 Token 在 En-Tan-Mo 中通過上凸權益映射轉化為可投票數，每投票周期給予相應獎勵。



SCV 級別工作流程：候選礦工根據得票高低當選 SCV 級別和候補礦工，獲得上傳區塊權利，驗證區塊義務和區塊獎勵。



核心代码

1. 监察官 Token 权益均衡算法

SCV 矿工通过监察官由投票选举产生，获得上传区块的权利。监察官的票数与其拥有的 Token 数量呈上凸函数关系，从而保证了 En-Tan-Mo 生态的均衡性。“权利”是表明 SCV 矿工上传区块的顺利性和合法性。“上凸”表示监察官的 Token 兑换率，为了权益均衡，Token 越多者兑换率越低，反之 Token 越少者兑换率越高。

$$F(balance) = weights$$

// 阈值映射关系 注：为了权益均衡 Token 越多者兑换率越低，反之 Token 越少者兑换率越高
 $thresholdMap = Map(range,rate)$
// 根据阈值区间得到计算率
 $rate = thresholdMap.get(range)$
// 根据兑换率得到委托人 Token 权重
 $weights = balance * rate$

2. 监察官 投票激励机制

En-Tan-Mo 的 UPOS 机制通过对监察官的 Token 奖励提高其投票的积极性，增强平台参与度，遴选出最佳 SCV 矿工，保证 En-Tan-Mo 高效安全运行。En-Tan-Mo 的投票激励机制包含投票奖励和出块奖励两种，监察官可以自由选择百分比获取这两种奖励。投票奖励根据监察官拥有票数固定获得，参与投票即获得奖励，该奖励为恒定值；出块奖励必须当监察官正确选择了 SCV 矿工才可以获得，该奖励为浮动对冲值。

$$F1(tickets) = token$$

// 投放比例
 $tickets1 = fixed\ assignment$ // 分配给固定 tickets
 $tickets2 = dynamic\ assignment$ // 分配给动态 tickets
// 固定收益 + 动态收益 (根据投票选中节点占总节

点数比例)

$$token = fixed(tickets1) + dynamic(tickets2)$$

3. SCV 矿工 出块顺序算法

为了确保 En-Tan-Mo 的安全性，选择 SCV 矿工来生成区块的排序方法必须是确定性系统，同时又具有伪随机。由此，En-Tan-Mo 运用了绝对安全的、具有混沌性的非线性动力学理论来达成这点。

```

// 锁定委托人投票权益
lock(balance)
// 计算可用投票的权重
tickets = F(balance) * F(time)
// 投票得到受托人列表
delegations = votes(tickets)
// 打乱改变顺序
shuffle(delegations)

```

4. SCV 矿工 出块哈希算法

En-Tan-Mo 不仅需要安全性和去中心化，还需要达到高效率，SCV 矿工之间不是竞争关系，而是采用合作竞争的方式出块，通过快速混沌排序为每一个区块指定一个 SCV 矿工，该矿工需要尽快完成 Sha256 计算，上传区块。

```

// 双 hash 计算
blockhash = sha256(sha256(block))
// 检查计算时间，如果没在指定时间内计算出结果表示矿机不达标
checkNodePerformance(useTime)
// 检查计算量是否达到指定要求
checkResult(blockhash,difficulty)
// 如果不符合则改变 nonce
block.nonce = block.nonce + 1

```

5.2 En-Tan-Mo 數據

塊頭數據結構

塊頭包含有關該塊的所有信息。由下列字段組成塊

- 一個標識塊的版本的 32 位整數
 - 塊創建時的 32 位時間戳
 - 前一個塊的 64 位 ID
 - 與事務數相對應的 32 位整數
 - 一個 64 位整數，對應于傳送的總量
 - 一個 64 位整數，對應與該塊關聯的總費用
 - 與代表的獎勵相對應的 64 位整數
 - 一個 32 位整數，對應于有效負載的長度
 - 有效載荷的 256 位散列
 - 生成該塊的代理的 256 位公鑰

Version	Timestamp
	Previous block Id
Number of transactions	Length of payload
	Amount of ETM transferred
	Amount of fee
	Reward of the delegate
	Payload hash
	Delegate's public key

(摩爾斯電碼)-----

快頭數據樣例

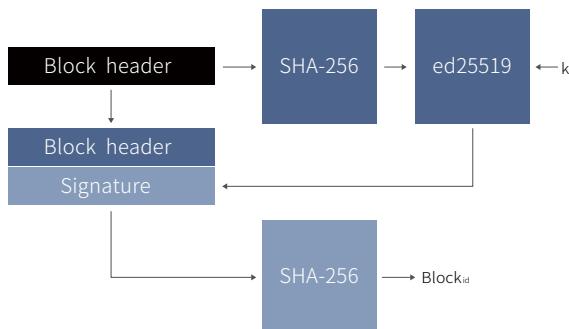
```
"id": "15787022670460703397",
"version": 0,
"timestamp": 23039010,
"height": 1574052,
"previousBlock": "4576781903037947065",
"numberOfTransactions": 0,
"totalAmount": 0,
"totalFee": 0,
"reward": 500000000,
"payloadLength": 0,
"payloadHash":
>e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855",
"generatorPublicKey":
"c0ab189f5a4746725415b17f8092edd3c266d1e758e840f02a3c99547b3a527f",
"blockSignature":
"c6b2bcc960066be078efbffffed625f61553a7bc18ebde3892636c2f36850de234a9c
70ba3e33b606db2eff724398026984e4d391c1fbe70c94dd9d07ff0060b",
"totalForged": "500000000"
}
```

區塊 ID 生成流程

生成塊頭的 SHA-256 哈希，並使用委託的密鑰進行(ed25519 算法)簽名。

一旦塊頭已經被簽名，系統就會使用 SHA-256 對完成的塊頭進行散列生成 Block Id。

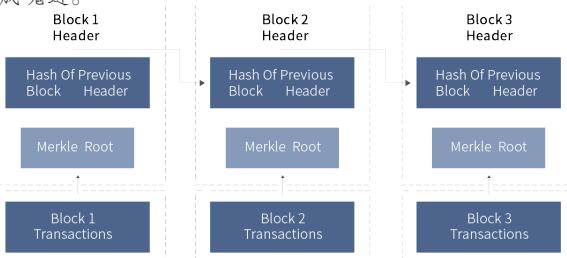
A signed block generates its block using the following flow:



區塊鏈結構

可以看出區塊主要由區塊頭和區塊體兩部分組成。區塊頭包含版本號、前一區塊地址、時間戳、Merkle樹的根植等信息。區塊體主要包含交易的計數和交易賬單詳情。

區塊鏈是由一串使用密碼學方法產生的數據塊組成的，每一個區塊都包含了上一個區塊的哈希值(Hash)，從創始區塊(Genesis Block)開始連接到當前區塊，形成塊鏈。



數據存儲默克爾樹結構

Merkle Tree，通常也被稱作 Hash Tree 運用樹狀數據結構存儲哈希值。

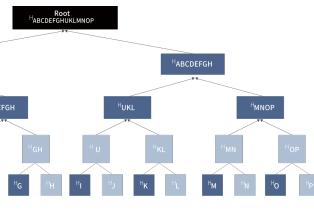
Merkle 樹的葉子是數據塊(例如，文件或者數據)

參考文獻：

- [24] D. Fudenberg, J. Tirole. Game Theory. Boston: MIT Press, 1991.
- [25] N. Nisan, A. Ronen. Algorithmic mechanism design. Proceedings of the 31st ACM Symposium on Theory of Computing (STOC '99), pp. 129–140, 1999.
- [26] C. Papadimitriou. Algorithms, games, and the Internet. Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC '01), 749–753, 2001.
- [27] N. Houy. The Bitcoin mining games. Ledger, vol, 2016.
- [28] A. Kiayias, E. Koutsoupias, M. Kyropoulou, Y. Tselekounis. Blockchain Mining Games. arXiv:1607.02420v1 [cs.GT] 8 Jul 2016.
- [29] A. Sapirshtein, Y. Sompolinsky, A. Zohar. Optimal selfish mining strategies in bitcoin. CoRR, abs/1507.06183, 2015.
- [30] J. P. Aubin, A. Desilles. Traffic Networks as Information Systems: A Viability Approach. Mathematical Engineering 8445, Springer, 2017.
- [31] J. F. Nash. Equilibrium points in n-person games. Proceedings of the National Academy of Sciences, 36(1):48–49, 1950.
- [32] I. Bentov, A. Gabizon, A. Mizrahi. Cryptocurrencies without proof of work. In 3rd Workshop on Bitcoin and Blockchain Research - Financial Cryptography, 2016.
- [33] S. Micali. Computationally sound proofs. SIAM J. Comput., 30(4):1253–1298, 2000.
- [34] I. Bentov, C. Lee, A. Mizrahi, M. Rosenfeld. Proof of activity: Extending bitcoin’s proof of work via proof of stake. SIGMETRICS Performance Evaluation Review, 42(3):34–37, 2014.
- [35] C. Dwork, N. A. Lynch, L. J. Stockmeyer. Consensus in the presence of partial synchrony. J. ACM, 35(2):288–323, 1988.
- [36] S. Dziembowski, S. Faust, V. Kolmogorov, K. Pietrzak. Proofs of space. In CRYPTO 2015.

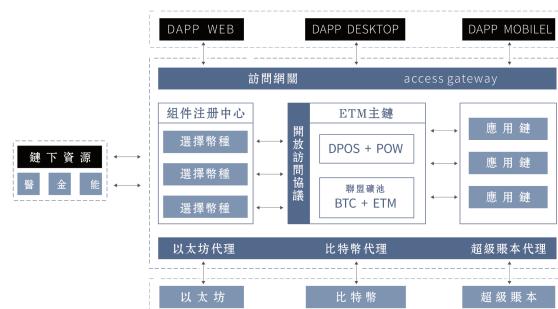
的哈希值。

非葉節點是其對應子節點串聯字符串的哈希值。



5.3 En-Tan-Mo 接口

En-Tan-Mo 以 BaaS (Blockchain as a Service, 區塊鏈即服務) 為理念，以微服務為基準，以自演進組件庫為核心，以開發者社區為生態原動力，為其他區塊鏈提供適配平臺完成資產和應用的自由轉移，為非區塊鏈的應用和數據提供軟通道完成雙向調用，為開發者提供共享大廳完成組件上傳、評價和獎勵的功能，為普通用戶提供 BaaS 網關實現無障礙服務調用。從而打通鏈與鏈之間，區塊鏈和非區塊鏈之間的信息孤島，幫助技術開發者和普通用戶從互聯網轉向區塊鏈。系統架構圖如下：



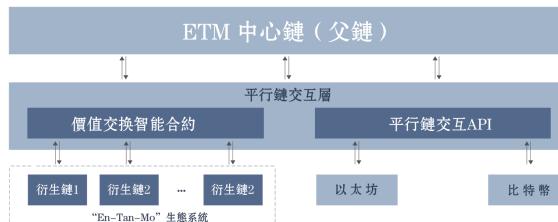
系統架構圖描述：

- . 應用層 (Web, 桌面, 移動) 通過統一訪問網關進行數據訪問
- . 通過應用組件與鏈下資源 (現有系統) 進行數據交互
- . 應用組件通過開放訪問協議進行鏈上數據交互
- . 應用組件內部對鏈上鏈下數據進行整合
- . 主鏈與應用鏈通過內部協議數據交互和價值傳遞
- . 通過代理層與第三方進行跨鏈交互

6.0 En-Tan-Mo 生態

6.1 中心鏈和衍生鏈

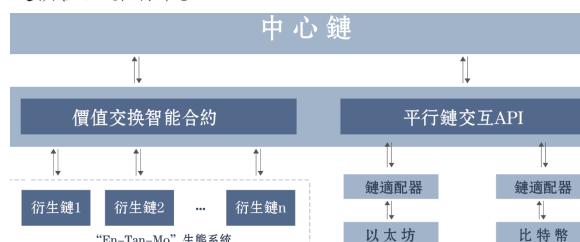
在區塊鏈所面臨的諸多問題中，區塊鏈之間互通性極大程度的限制了區塊鏈的應用空間。不論對於公有鏈還是私有鏈來看，跨鏈技術就是實現價值傳遞的關鍵，將區塊鏈從分散的孤島中拯救出來，是區塊鏈向外拓展和連接的橋梁。現有的跨鏈技術主要以側鏈為主，但其實際上實現的僅僅只是價值鎖定，而不是價值傳遞。為此，En-Tan-Mo 經過對現有跨鏈技術的研究，提出了一種平行鏈交互協議，很好地實現了鏈與鏈之間的價值傳遞，從而構建了一個可以包含千萬級應用的區塊鏈生態系統。



為了解決區塊鏈快速膨脹和區塊鏈即服務 (BaaS) 的問題，En-Tan-Mo 采用了一條中心鏈加多條衍生鏈的設計，中心鏈負責網絡安全及價值交換。衍生鏈是一種特殊的區塊鏈，每一個衍生鏈對應一個 DApp，是一個獨立的、隔離的系統，繼承和復用主鏈強大的區塊鏈技術，每個應用都擁有一套個性化的賬本和 Token，其共識機制、區塊參數、交易類型都是可以被定制的。各衍生鏈之間具有平行關係，即衍生鏈與衍生鏈之間互為平行鏈。它們可以通過中心鏈的“平行鏈交互層”實現其與中心鏈、其他衍生鏈及外部區塊鏈之間的雙向資產傳遞，這使得用戶能用已有的資產來使用 En-Tan-Mo 系統。

6.2 平行鏈交互協議

En-Tan-Mo 的平行鏈交互協議使得支持多種不同的區塊鏈的價值交換成為可能，主要包含鏈一適配模塊和價值交換智能合約兩部分。設計鏈適配器主要目的是為價值交換智能合約提供 En-Tan-Mo 與不同鏈的交互接口，以便驗證不同鏈上的交易。同時，鏈適配器也可以由社區建設者自己開發和不斷改進並獲得 Token 獎勵，以適用於更多的功能，例如應用可以借助於鏈適配器在不同協議的底層區塊鏈之間切換。價值交換智能合約是平行交互協議的核心，它可以讓用戶在 En-Tan-Mo 中心鏈與衍生鏈、衍生鏈與衍生鏈、及 En-Tan-Mo 與外部區塊鏈（包括但不限於比特幣、以太坊等）系統等實現資產交換，從而構建成一個鏈一鏈價值互聯網絡。



鏈適配器

鏈適配器就如同計算機的設備驅動程序，它把下層區塊鏈協議轉換為 En-Tan-Mo 中心鏈更容易使用調用的程序，從而運行 En-Tan-Mo 中心鏈上的價值交換智能合約。其涉及的技術包含不僅限于 Hash Time Lock Contracts (HTLC)、SPV 證明、API 開發等。

En-Tan-Mo 首先會提供比特幣區塊鏈、以太坊 (Ethereum) 等幾種最常用的區塊鏈系統的適配器實現，并在運行穩定後進行開源。任何人都可以貢獻、改進開放鏈訪問協議，或實現新的適配器。En-Tan-Mo 計劃支持更多的區塊鏈協議，並給予相應的 Token 獎勵。

價值交換智能合約

雖然區塊鏈這一創新技術早已成為全球焦點，但始終存在着一個問題：不同區塊鏈系統之間的價值交易仍然需要像交易所等這樣的第三方中間商，而這正是這些去中心化技術所想要取代的東西。En-Tan-Mo 用最小化信任的智能合約與鏈適配器取代了這種第三方，來承擔起不同鏈之間的橋梁。這種方式加深了區塊鏈領域中最主要的兩個元素之間的互連，使 En-Tan-Mo 離統一的全球性價值傳遞網絡更近一步。

價值交換智能合約依賴於 En-Tan-Mo 的圖靈完備虛擬機而運行，給用戶提供了足夠的安全性保障。一個衍生鏈與中心鏈的價值交換智能合約就像一個去中心化的交易所一樣，它擁有一個 ETM 錢包地址和對應鏈錢包地址的控制權。當用戶在衍生鏈上發起轉賬，並且被中心鏈通過適配器確認後，價值交換智能合約就會自動在中心鏈上發起對用戶的 ETM 錢包地址等額的轉賬，以此來完成價值的交換。同時，為了防備用戶交換價值時面臨的風險，En-Tan-Mo 融入了比特幣系統的 Hash Time Lock Contracts 技術。

對於具體交換過程，以比特幣與 ETM 的互換為例，步驟如下：

比特幣區塊鏈用戶 A 首先必須在 En-Tan-Mo 註冊，以便綁定用戶 A 的 ETM 錢包地址與 BTC 錢包地址的映射關係；

用戶 A 生成一個隨機秘密數 a，求得其哈希值 H(a)。然後，在比特幣區塊鏈上向價值交換智能合約的比特幣地址發起一筆特殊交易，該交易基於 Hash Time Lock Contracts 技術鎖定 12 小時。En-Tan-Mo 價值交換智能合約為了獲得該筆 Token 必須出示一個哈希值 H(a) 的原像，否則 12 小時後，該交易的 BTC 自動返回到用戶 A 的比特幣錢包地址中。

En-Tan-Mo 智能合約通過比特幣鏈適配器監控着比特幣區塊鏈中這些特殊交易的確認情況，並對其進行 SPV 驗證。一旦 SPV 驗證通過，En-Tan-Mo 價值交換智能合約會在中心鏈中向用戶 A 的 ETM 錢包地址發起一筆特殊交易，該交易鎖定 6 小時。若用戶 A 想要獲取該交易中的 ETM Token，必須出示哈希值 H(a) 的原像 a，否則 6 小時後，該筆交易中的 ETM Token 自動退回智能合約的 ETM 錢包地址中。一旦用戶 A 出示秘密數 a 領取了該筆交易中的 ETM Token，智能合約就會知曉秘密數 a，因此智能合約就可以通過適配器訪問比特幣區塊鏈網絡，並作為一個用戶領取用戶 A 在比特幣區塊鏈中所發起的那筆交易中的比特幣。

至此，交易完成。

需要強調的是，中心鏈僅僅只是作為一個去中心化的價值交換場所，并不是依靠鎖定用戶 A 的比特幣來實現的價值轉移。用戶 A 轉賬給智能合約比特幣錢包地址的比特幣，智能合約服務于需要將 ETM Token 交換成比特幣的用戶。同時，用戶 A 將比特幣交換成 ETM Token 之後，中心鏈并不限制其僅能轉移回比特幣區塊鏈，也可以選擇通過同樣的過程轉換成其他外部區塊鏈的 Token。因此，En-Tan-Mo 實現的是價值交換，而不是資產鎖定。另外，初始的價值交換智能合約的所有錢包地址 Token 數量都為零，它需要相應區塊鏈用戶的投資。作為回報，智能合約將價值交換過程中用戶所花費的交易費按投資比例分紅給相應的投資者。在投資過程中，用戶可以隨時向智能合約取回投資款。

總之，基于價值交換智能合約，En-Tan-Mo 所構建的是一個鏈 - 鏈價值互聯網絡。同時，En-Tan-Mo 不憑空創造價值，僅作為價值互聯中一個價值傳遞者。

應用生態系統

En-Tan-Mo 是新一代的區塊鏈平臺，它把不同應用加到獨立運行的不同衍生鏈上，有效地解決了外部區塊鏈系統的區塊快速膨脹，區塊體積龐大，同步時間超長等關鍵問題。En-Tan-Mo 的多衍生鏈模式為處理高交易量下如何解決網絡擁堵的問題提供了一種理想的解決方法，用戶祇有用到相關的應用時才需要下載對應的衍生鏈，大大減小了無效的同步數據，保持了整個 En-Tan-Mo 網絡的高效運行。而且，得益于價值交換智能合約實現的鏈 - 鏈價值互聯網絡與網絡編碼技術、閃電支付網絡等技術有效結合，En-Tan-Mo 將可以支持千萬級應用和打通整個區塊鏈生態系統。

6.3 米爾商城

En-Tan-Mo 系統通過方便而又高效的米爾商城，幫助企業或開發者更快更經濟的實現區塊鏈應用，使得用戶能够享受到去中心化帶來安全和便利。類似于現在中心化的 App 應用，我們將衍生鏈上去中心化的應用稱為 DApp 應用。

米爾商城有如下優勢：

- (1) 提供容納千萬級應用的區塊鏈生態系統。
- (2) 衍生鏈上的資產也可以通過 En-Tan-Mo 的平行鏈交換協議完成和其他幣種(ETM/BTC/ETH 等)的兌換，使得基于“En-Tan-Mo”開發的應用將具有更大的用戶群體。
- (3) 基于“En-Tan-Mo”的平行鏈交換協議，DApp 可以訪問多個底層區塊鏈的數據，從而使得 DApp 可以基于多個底層區塊鏈而運行。

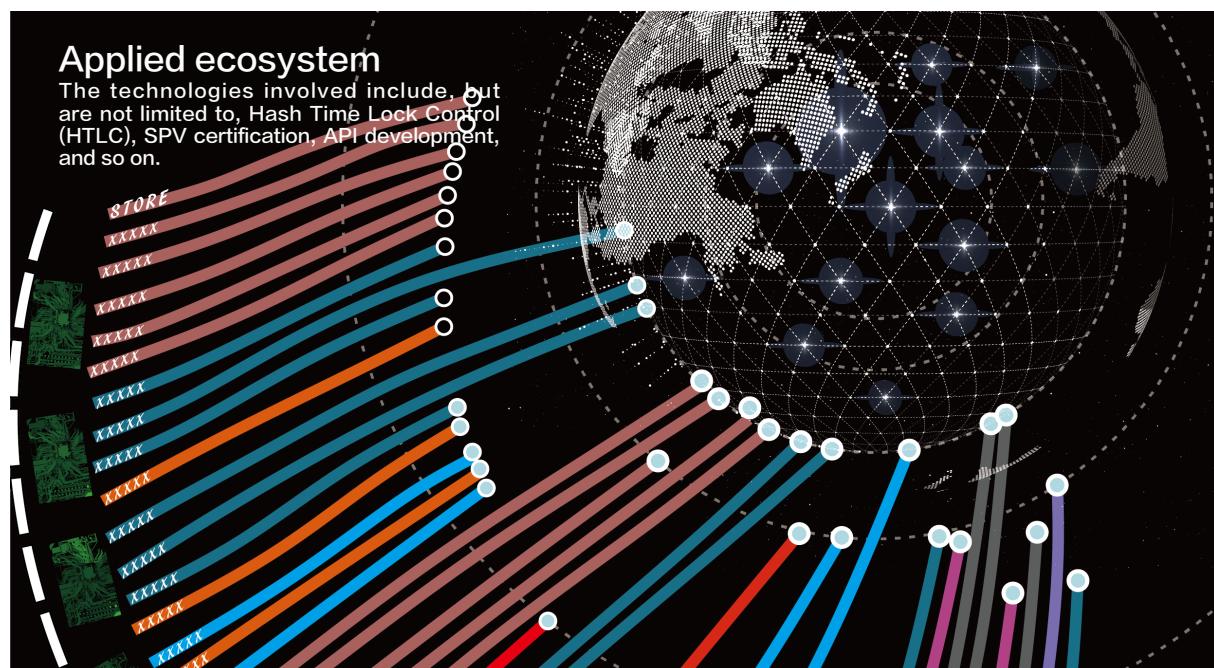
(4) 利用“En-Tan-Mo”的衍生鏈技術及其提供的一系列 SDK、API 和模板，開發者祇需要關心業務邏輯，就能夠很容易的構建、測試和發布自己的個性化 DApp，這將極大的降低了新型應用的落地的研發成本，有助于開發者更好更快速的擁有米爾商城的 DApp。並且，這些 DApp 可以被所有 En-Tan-Mo 的節點下載並執行，並對所有的區塊鏈用戶提供服務。

(5) 基于“En-Tan-Mo”的衍生鏈技術，熟練的開發者可以自行定制米爾商城 DApp 個性化的數據庫、共識機制、交易類型以及賬戶體系。

(6) “En-Tan-Mo”將內建一套完善的獎勵制度，對於優秀的DApp，米爾商城將給與Token獎勵。

西伯利亞東部發現了一處全球最大鑽石礦——“鑽石之城”米爾礦，這處礦藏的估值過 1000 億人民幣，是目前世界最昂貴的鑽石礦。這裏用米爾商城表達 En-Tan-Mo 的 DApp Store 資源豐富，潛力巨大。

----- (摩爾斯電碼)



7.0 En-Tan-Mo 組織結構

En-Tan-Mo 社區由 En-Tan-Mo 基金會，ETM FinTech 和 ETM BD 三個組織所構成。En-Tan-Mo 基金會是三個組織的核心，該基金會是在新加坡成立的非營利性機構，保證 En-Tan-Mo 項目的順利運營，為 En-Tan-Mo 用戶社區提供全方位的支持。此外，En-Tan-Mo 還有一家領導區塊鏈技術研究和開發的組織實體 ETM FinTech 技術開發公司、一家協助商業企業投資和應用開發的 ETM BD 商務拓展公司。

7.1 En-Tan-Mo 基金會

En-Tan-Mo 基金會是在新加坡成立的非營利性機構，其核心任務是規範，保護和推廣自主研發的 En-Tan-Mo 底層架構和區塊鏈協議。同時，還起到研究和提議區塊鏈與加密貨幣的法規的作用；保護、加強和進化 En-Tan-Mo 生態系統；聚集、教育和培養 En-Tan-Mo 社區。

與此同時，在整個 En-Tan-Mo 社區的有效監督下，以獨立的第三方身份，為社區的長期發展提出總體規劃。除此之外，En-Tan-Mo 基金會還將作為公益機構，關注世界範圍內的公共事業與慈善事業，促進全球公信體系的發展。

En-Tan-Mo 基金理事會，通過民主決策來確定基金會的大政方針，理事會領導下的秘書長負責，執行決策制。監事會，監督理事會的運作，監事會中一般都包括一些知名公眾人物和專業的財務人員。

En-Tan-Mo 基金會理事會

En-Tan-Mo 基金會理事會直接管理慈善項目部。基金會分為產品研發、財務管理、市場推廣，人力資源、及法務事項等部門，共同維護基金會的日常維護與管理。

En-Tan-Mo 基金會慈善項目部

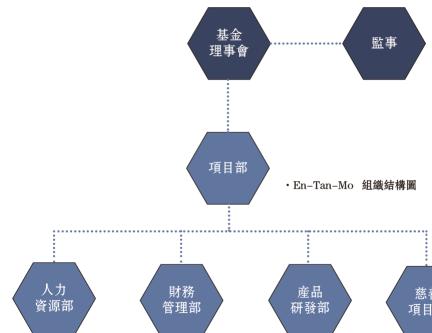
En-Tan-Mo 基金會慈善項目部，是基金會的核心業務部門，負責運作和管理基金會的公益項目，實現基金會的公益目標，用以執行理事會的整體決策。En-Tan-Mo 基金理事會將通過規劃和籌資，幫助基金會實現預期目標。在基金會的早期發展過程，負責起草 En-Tan-Mo 基金會章程，由理事會通過作為理事會的運營規則。

En-Tan-Mo 基金會項目部，還負責緊急事件的應急機制，需要由 En-Tan-Mo 理事會商討公關處理，共同討論并一致決策後，方可對外披露。基金發展的整體方向，由理事會對新增推廣渠道進行調研，包括渠道的方向、可延伸性和推廣力度。

En-Tan-Mo 財務管理部

En-Tan-Mo 擁有一套獨立、公開、透明的財務管

En-Tan-Mo



理機制。

(a) En-Tan-Mo 基金會所有的交易將為專業財務人員核準，并記錄在區塊鏈的區塊中，實現公開、透明、不可回溯的財務監管。此外，基金會的所有支出，亦會通過專業財務人員審核，并在區塊中進行財務的相關登記。

(b) En-Tan-Mo 基金會將每月發布月財務報告，對資金進行對帳，財務報告將由基金委派的專家財務人員，和 En-Tan-Mo 社區人事管理委員授權人員進行審核。

(c) En-Tan-Mo 基金會通過財務報告制度對資金進行對帳，財務報告將由基金委派的專家財務人員，和 En-Tan-Mo 社區人事管理委員授權人員進行審核。

En-Tan-Mo 人力資源部

En-Tan-Mo 擁有向全社區公開的人力資源體系，有別于傳統的公司結構，En-Tan-Mo 的人事從招聘到錄用，都是公平公正公開，并全程區塊鏈記錄的。

(a) 對於任何新增人員的招聘，都由專業的人員對其進行兩輪以上面試，形成獨立評價報告並寫入招聘記錄。所有的記錄將具有不可篡改，永久回溯的特性。

(b) 對於滿足招聘要求的人員，需要最終向相關委員會進行審批。核心開發人員，以及核心管理人員需要經過盡職調查流程。最終由 En-Tan-Mo 的基金會核心團隊審核。

(c) 對於可能外包的業務，將擬定外包協議，確定工資薪酬，并簽訂相關的外包協議，對全社區進行公開，外包的合同將寫入智能合約中。

En-Tan-Mo 基金監事會

En-Tan-Mo 基金會監事會對所有 En-Tan-Mo 參與者負責。對基金會理事、項目人員履行職責的合法性進行監督，維護公司及股東的合法權益。監事需要對基金會的財務狀況和經營管理情況進行有效的監督、檢查和評價。基金理事會應當根據監事會的要求，向監事會報告基金項目的簽訂、執行情況、資金運用情況和盈虧情況。

7.2 ETM FinTech 技術開發公司

ETM FinTech 技術開發公司的角色主要是開發，維護這一全新生態系統，En-Tan-Mo 的開發主要分為四個階段：“彼特拉克”：實現完全由網絡基礎協議和嚴格的加密技術保護和支持的、全新的、均衡的、高效的、去中心化的 En-Tan-Mo 區塊鏈，形成了一套全新的 Token 規則和體系，同時開放技術社區和開發者大廳，培育和形成 En-Tan-Mo 的文化。

“馬薩喬”：開發零知識證明技術以更好的保護用戶隱私，結合閃電網絡及網絡編碼技術以提升交易速度、降低區塊鏈的負擔，提高可擴展性。通過智能合約、平行鏈交互協議和鏈配適器形成 En-Tan-Mo 的生態系統，各類資產在中心鏈和衍生鏈上進行數字登記，得到資產安全和數據完整性保證。

“達·芬奇”：共識機制完全實現動態納什均衡：算力單元會進入到一個混幣計算聯盟，是一種具有長期最佳收益的算力承載組件；所有的節點根據供需關係，自由平等的選擇交易，獲得均衡的受益。En-Tan-Mo 成為一個能夠承載高頻次、高流量的大型數字權證交易所、聯盟礦池、DApp 應用平臺，混沌排序機制還天然形成一個博弈場。En-Tan-Mo 還是一個最好的開發者社區、區塊鏈應用組件承載平臺。

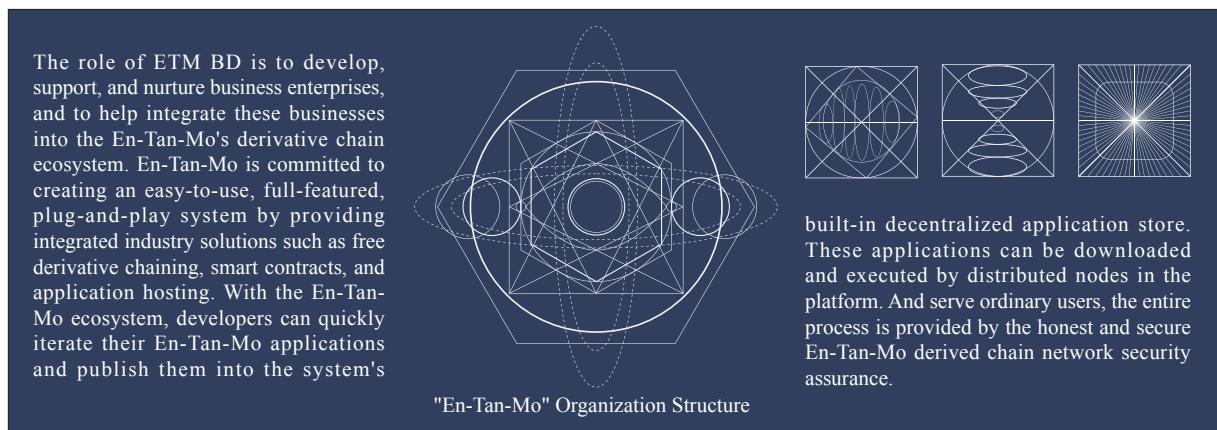
“喬爾喬內”：在這一時期中，En-Tan-Mo 將進一步超越經濟領域，迎來區塊鏈 3.0 時代的輝煌和盛況。En-Tan-Mo 可用于實現全球範圍內日趨自動化的物理資源和人力資產的分配，促進科學、健康、教育等領域的大規模協作，主要在自動化采購，智能化物聯網應用，供應鏈自動化管理，虛擬資產兌換、轉移，產權登記等場景中都將得以實現。

系統一旦發布，ETM FinTech 將不再掌控系統的走向，祇有系統的權益人、Token 的擁有者和有興趣的研究人員一起決定系統將來的發展。

7.3 ETM BD 商業拓展公司

ETM BD 商業拓展公司的角色是開發、支援和孕育商業企業，並且協助將這些業務整合至 En-Tan-Mo 的衍生鏈生態系統中。En-Tan-Mo 通過提供自由衍生鏈、智能合約、應用托管等一體化的行業解決方案，致力於打造一個易于使用、功能完備、即插即用的系統。利用 En-Tan-Mo 生態系統，開發者可以快速迭代他們的 En-Tan-Mo 應用，並發布到系統內置的去中心化應用商店中，這些應用可以被平臺中的分布式節點下載並執行，並服務於普通用戶，整個過程都由誠實安全的 En-Tan-Mo 衍生鏈網絡提供安全保證。

任何對 En-Tan-Mo 區塊鏈技術感興趣，希望通過該技術改革產業的個人或企業，ETM BD 都將通過直接投資、協助開發、提供解決方案等多種靈活的方法，幫助他們實現 En-Tan-Mo 的鏈上應用。



後注：

1、政策性風險

目前各國家對於區塊鏈項目以及互換方式融資的監管政策尚不明確，存在一定的因政策原因而造成參與者損失的可能性；市場風險中，若數字資產市場整體價值被高估，那麼投資風險將加大，參與者可能會期望互換項目的增長過高，但這些高期望可能無法實現。

2、監管風險

包括En-Tan-Mo在內的數字資產交易具有極高不確定性，由於數字資產交易領域目前尚缺乏強有力的監管，故而電子Token存在暴漲暴跌、受到莊家操控等情況的風險，個人參與者入市後若缺乏經驗，可能難以抵禦市場不穩定所帶來的資產衝擊與心理壓力。雖然學界專家、官方媒體等均給出謹慎參與的建議，但尚無成文的監管方法與條文出臺，故而目前此種風險難以有效規避。

不可否認，可預見的未來，會有監管條例出臺以約束規範區塊鏈與電子Token領域。如果監管主體對該領域進行規範管理，互換時期所購買的Token可能會受到影響，包括但不限于價格與易售性方面的波動或受限。

3、團隊風險

當前區塊鏈技術領域團隊、項目衆多，競爭十分激烈，存在較強的市場競爭和項目運營壓力。En-Tan-Mo項目是否能在諸多優秀項目中突圍，受到廣泛認可，既與自身團隊能力、願景規劃等方面挂鈎，也受到市場上諸多競爭者乃至寡頭的影響，其間存在面臨惡性競爭的可能。En-Tan-Mo基於創始人多年行業積累的人脈，匯聚了一支活力與實力兼備的人才隊伍，吸引到了區塊鏈領域的資深從業者、具有豐富經驗的技術開發人員等。團隊內部的穩定性、凝聚力對於En-Tan-Mo的整體發展至關重要。在今後的發展中，不排除有核心人員離開、團隊內部發生衝突而導致En-Tan-Mo整體受到負面影響的可能性。

免責聲明

本文檔僅作為傳達信息之用，文檔內容僅供參考，不構成在En-Tan-Mo及其相關公司中出售股票或證券的任何投資買賣建議、教唆或邀約。此類邀約必須通過機密備忘錄的形式進行，且須符合相關的證券法律和其他法律。

本文檔內容不得被解釋為強迫參與互換。任何與本文檔相關的行為均不得視為參與互換，包括要求獲取本文檔的副本或向他人分享本文檔。參與互換則代表參與者已達到年齡標準，具備完整的民事行為能力，與En-Tan-Mo簽訂的合同是真實有效的。所有參與者均為自願簽訂合同，並在簽訂合同之前對En-Tan-Mo進行了清晰必要的了解。

En-Tan-Mo團隊將不斷進行合理嘗試，確保本文檔中的信息真實準確。開發過程中，平臺可能會進行更新，包括但不限於平臺機制、Token及其機制、Token分配情況。文檔的部分內容可能隨着項目的進展在新版中進行相應調整，團隊將通過在網站上發布公告或新版文檔等方式，將更新內容公布于眾。請參與者務必及時獲取最新版文檔，並根據更新內容及時調整自己的決策。

En-Tan-Mo明確表示，概不承擔參與者因：依賴本文檔內容本文信息不準確之處，以及本文導致的任何行為而造成的損失。團隊將不遺餘力實現文檔中所提及的目標，然而基於不可抗力的存在，團隊不能完全做出完成承諾。

En-Tan-Mo是平臺發生效能的重要工具，並不是一種投資品。擁有En-Tan-Mo不代表授予其擁有者對En-Tan-Mo平臺的所有權、控制權、決策權。En-Tan-Mo作為一種數字加密貨幣不屬於以下類別：

- (a) 任何種類的貨幣；
- (b) 證券；
- (c) 法律實體的股權；
- (d) 股票、債券、票據、認股權證、證書或其他授與任何權利的文書。

En-Tan-Mo的增值與否取決於市場規律以及應用落地後的需求，其可能不具備任何價值，團隊不對其增值做出承諾，並對其因價值增減所造成的後果概不負責。在適用法律允許的最大範圍內，對因參與互換所產生的損害及風險，包括但不限於直接或間接的個人損害、商業盈利的喪失、商業信息的丟失或任何其它經濟損失，本團隊不承擔責任。

En-Tan-Mo平臺遵守任何有利于互換行業健康發展的監管條例以及行業自律申明等。參與者參與即代表將完全接受並遵守此類檢查。同時，參與者披露用以完成此類檢查的所有信息必須完整準確。

En-Tan-Mo平臺明確向參與者傳達了可能的風險，參與者一旦參與互換，代表其已確認理解並認可細則中的各項條款說明，接受本平臺的潛在風險，後果自擔。

“ “ AGREED VALUE SHARED BENEFIT

共識傳遞價值 ” ”

備註：

本文檔是對英文版技術白皮書的中文翻譯，盡管我們盡量保證精確性但仍可能與英文版本存在微小偏差，如果本文內容和解釋出現和英文版的區別則以英文版本為基準。