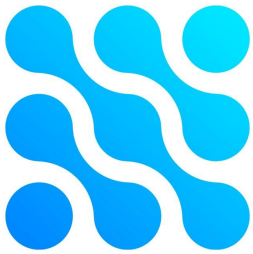


AUTHERIUM

標準跨金融鏈

下一代跨鏈金融互動高性能公鏈標準

V2.1.5

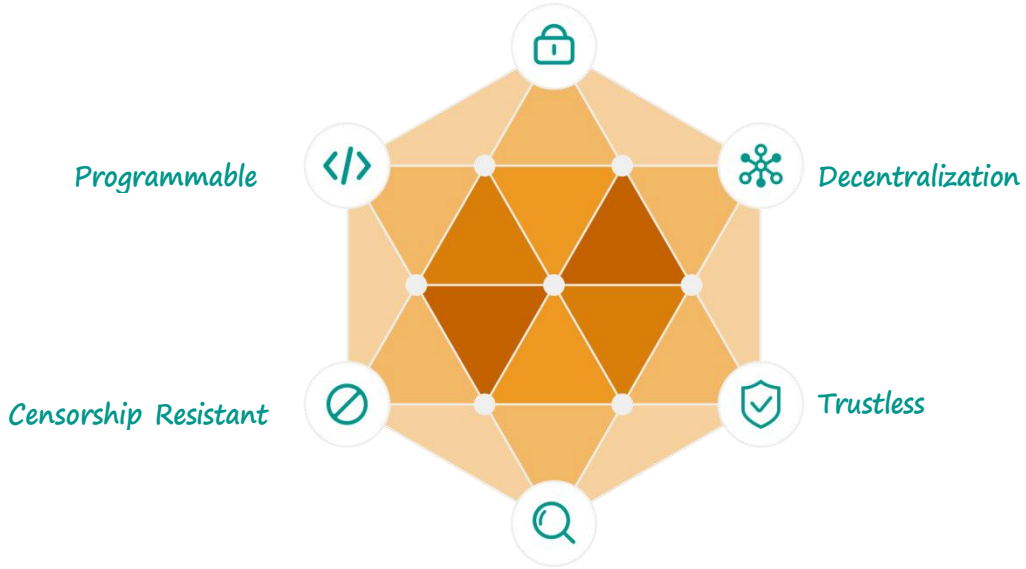
Table of Contents

背景

近百年來，金融業為社會提供了快速獲取原始資本的管道，大大推動了人類文化的發展與進步。然而隨著資本的膨脹，主流金融機構與監管機構佔據了主導地位，逐漸佔據了金融體系的主導地位，不可動搖。然而，它們也因權力過於集中和操作漏洞而受到批評。這些金融機構和所謂的監管機構因一己私利而屢屢被質疑操縱市場，導致投資者的資產風險增加。傳統的金融模式與監理手段未能從根本解決投資人對資金安全的擔憂，導致投資環境不斷惡化。因此，金融市場亟需改變來改變這種狀況。

DeFi

終於，從2019年開始，以區塊鏈技術為基礎的去中心化金融（DeFi）讓人們探索了一種全新的市場範式，程式碼就是法律，投資者可以完全在不需要信任的區塊鏈上開展金融活動。



分散式帳本技術（DLT）讓金融交易和資產存管更加透明、安全。

智能合約和不可篡改的特性，消除了風險重重的人工操作流程和中介作惡的潛在隱患，進一步提升了金融數據的安全性和撮合效率。

閃電貸、演算法穩定幣等一群傳統金融難以想像的創新模式如雨後春筍般湧現，充分發揮了共識的底層特性。毋庸置疑，區塊鏈金融讓世界變得更精彩、更美好。但我們也清醒地意識到，創新之路上仍存在著許多亟待解決的挑戰。

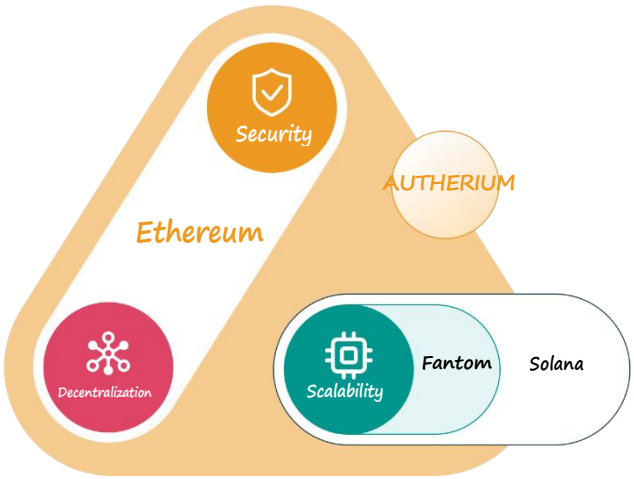
現有公鏈的吞吐量難以滿足大規模金融服務的中心化和並發響應，多鏈競爭造成的數據/資訊孤島問題日益嚴重，跨鏈金融交互問題尚未得到充分解決。此外，加密產業的高開發門檻也讓許多致力於DeFi的優秀團隊和傳統機構望而卻步。Web 3.0世界呼喚一條超高效能的公鏈，能夠打通傳統金融、加密金融、多鏈互動之間的技術鴻溝，成為DeFi蓬勃發展和普及的基石。

1. 項目介紹

為了打造更好的DeFi基礎設施，史丹佛大學畢業生Bob Lambert和William Thompson組成了一支由區塊鏈資深技術專家和金融科技學者組成的團隊，打造了一條雙鏈架構的金融公鏈AUT。歸根結底，所有公鏈都基於各自的目標，尋求優化區塊鏈不可能三角，即高效能（即可擴展性）、安全性和去中心化。

去中心化就是利用大量網路節點打包區塊進行資料驗證。通常，節點越多、越分散，去中心化程度就越高（更接近理想的區塊鏈概念）。安全性是取得網路控制權的成本，通常在共識機制設計時與現實世界的資產掛鉤。例如，工作量證明（PoW）機制與雜湊率掛鉤。效能可以簡單理解為每秒處理的交易數量。區塊鏈效率低下的主要原因是每筆交易在更多節點上就資料達成一致所需的時間。
傳統的單鏈結構無法調和三者的平衡，這是由邏輯定律決定的。

AUT並發性能優於以太坊，同時擁有Solana等去中心化程度不夠的鏈難以忽視的海量計算和驗證節點，擴展了性能，完善了生態。



Ethereum	Security + Decentralization
Fantom/Solana	Scalability
AUTHERIUM	Security + Decentralization +

Main-Chain	Security + Decentralization
Fin-Chain	Scalability

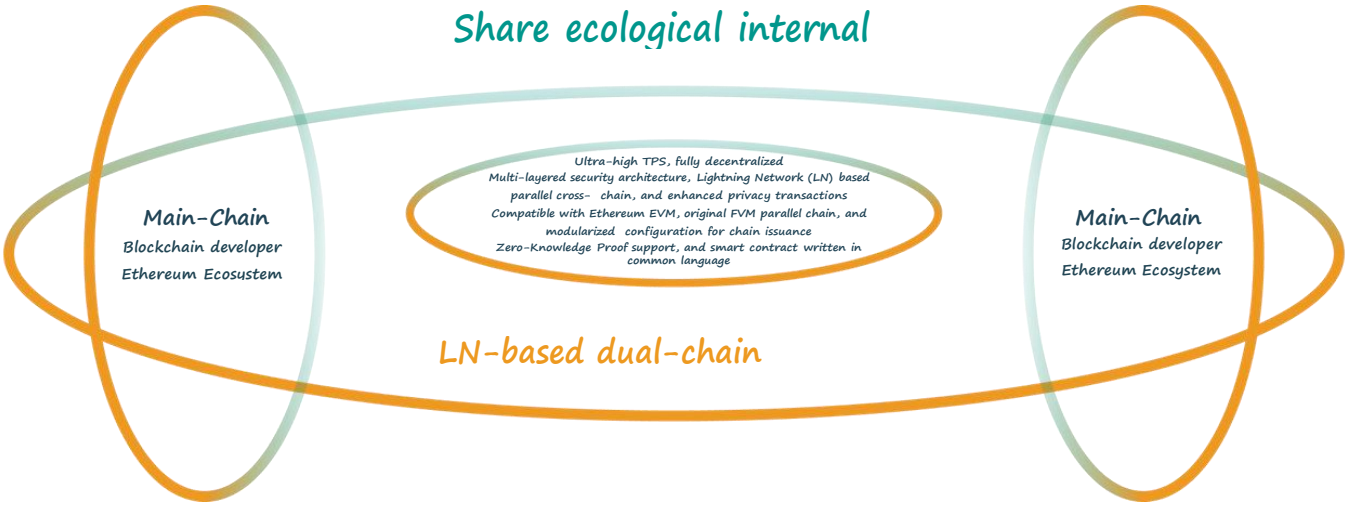
我們相信金融創新是伴隨社會發展的終極命題，未來的Web3.0網路必將創新百花齊放，只有具備足夠前瞻性和包容性的全能型公鏈才能成為DeFi的基礎設施矩陣。

在AUT的設計上，我們透過雙股架構建構網路層，透過原子交換和標準程式介面建構跨鏈生態，結合下一個跨鏈DEX，展現應用層的創新實踐，為產業提供系統的方法論，最終建立下一代跨鏈金融互動的標準模型。

2. 雙股架構

2.1 架構介紹

AUT 代表標準交叉金融(Standard Cross Finance)，開創了雙鏈結構，分別服務於區塊鏈產業和傳統金融機構。每條鏈都發揮各自的功能並有效地相互交互，解決了金融業在性能、安全性、去中心化、跨鏈交易和生態可擴展性方面的挑戰。AUTHERIUM 的網路層包括主鍊和Fin-Chain。



2.2 主鏈特點

主鏈是AUTHERIUM存在的基石，面向區塊鏈開發者和用戶，處理原生治理代幣與以太坊EVM專案之間的合約互動。主鏈的功能和特性包括：

·執行智能合約

高效執行智能合約，執行代幣創建和原生交易，支援使用Solidity語言進行智能合約開發。

·相容以太坊EVM

幫助開發者快速將以太坊DApp移植到AUT生態系統。

·為區塊生成APoS共識

處理公鏈主區塊的APoS共識以進行交易驗證和確認。

·資產跨鏈原子交換鏈

幫助用戶快速將資產從各個鏈轉移到AUTHERIUM。

2.3 金融鏈特徵

Fin-Chain起源於金融，代表金融，旨在幫助大量傳統金融機構快速移植應用上鍊。Fin-Chain的功能和特點是：

·基於LN的平行跨鏈

不同於主鏈原子交換鏈外的資產跨鏈，Fin-Chain透過閃電狗底層合約，實現雙鍊和不同共識的Fin-Chain並行鏈之間數據和資產的高效互動。在確保節點穩定性的同時，Fin-Chain提供更多的鏈間連接，形成閃電網絡，具有極佳的秒級跨鏈響應效率，從而將公鏈之間的項目連接起來，形成更穩健的內環共生。（隱私鏈資料只能由構成隱私通道的節點和認可地址存取）

·基於零知識證明的隱私交易

·兩款AUTHERIUM均支援「零知識證明」技術，該技術可實現鏈下擴容、交易隱私保護、反共謀、鏈上壓縮等多項前沿關鍵應用，後續章節將詳細討論該技術。

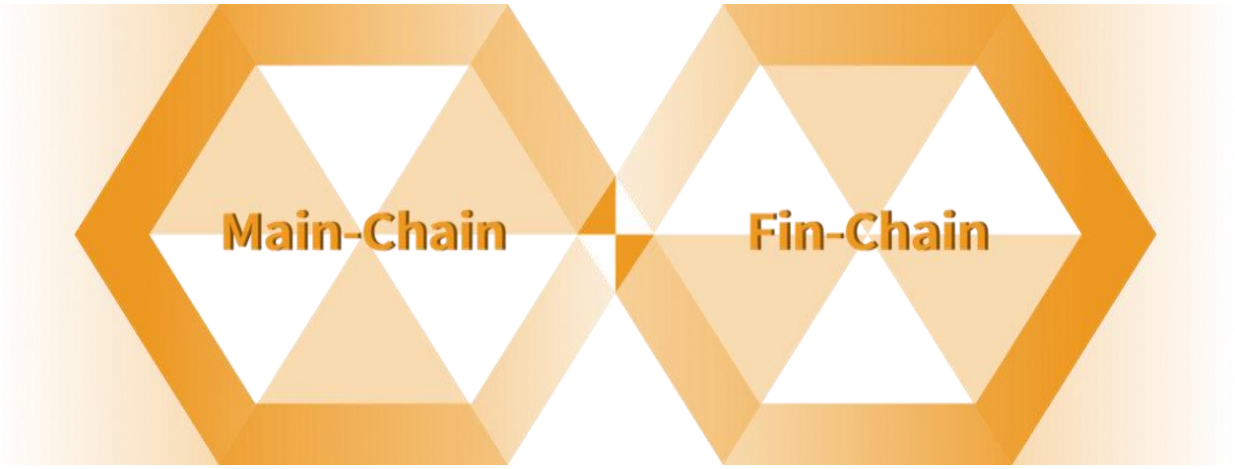
·模組化部署，一鍵發鏈

第三方開發者可以建立自己的平行鏈（PBFT、PoW、PoS、APoS），選擇不同的共識機制和配套設施，包括區塊瀏覽器、錢包等。模組化部署技術大大降低了企業建置複雜DApp服務及其公鏈的開發成本。

·常用語言的複雜智能合約開發

支援Java、GO等主流語言的智慧合約開發，是金融、網路領域非區塊鏈開發者最友善的入口。

AUTHERIUM的APoS即Asset Proof of Stake，APoS共識機制繼承並發展了現有的PoS，走的是PoW共識的去中心化路線，更加環保節能。同時，其融合PoS和DPoS的經濟模型也避免了其過度中心化的弊端。



AUT的雙鏈架構為金融中的不可能三角提供了最優解，簡單合約和複雜合約用不同鏈處理，降低了整個鏈的計算負荷，有利於資源隔離，Fin-Chain上的生態項目可以基於自身硬體叢集無限制提升TPS，進而讓效能暴漲。

3. 績效與需求評估

公鏈性能通常以TPS（Transactions Per Second）來衡量，主鏈硬體性能平均TPS超過7500+，金融鏈超過80000+，相比其他公鏈更能滿足超大規模金融應用的極限並發需求。

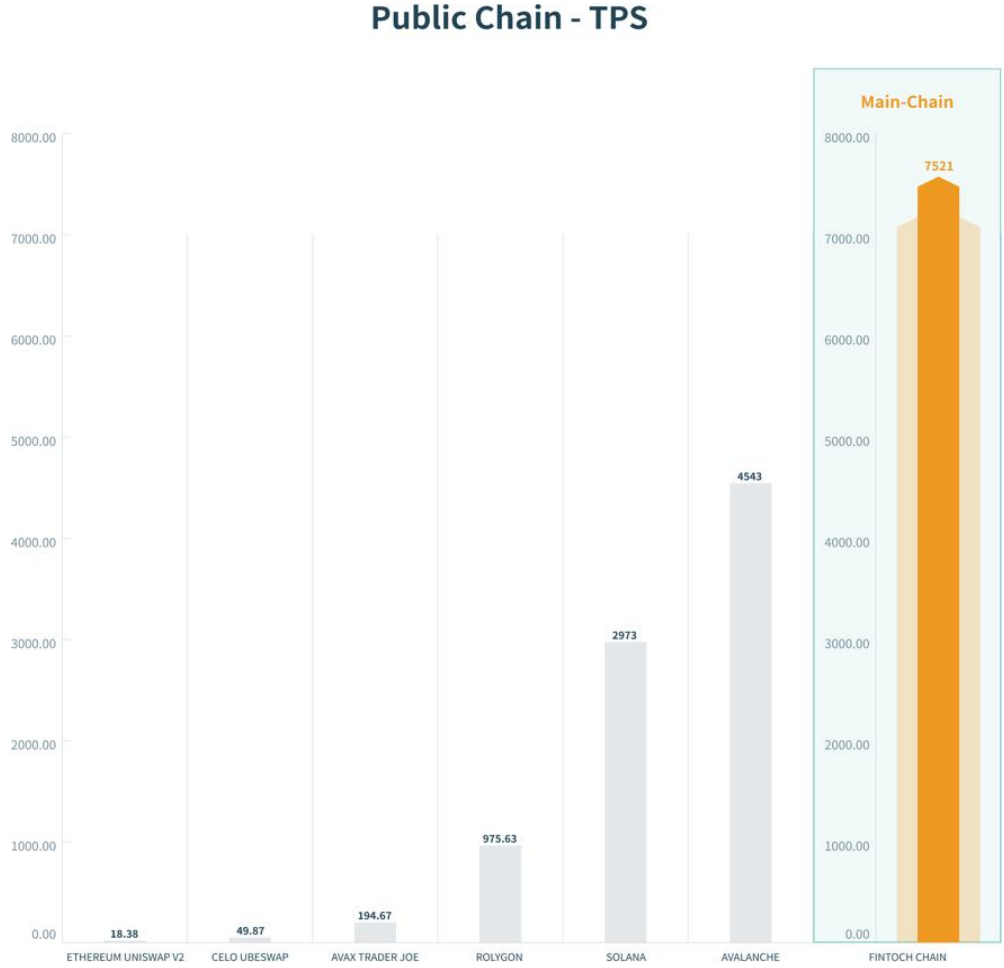
目前市面上各公鏈提供的TPS值（以千為單位）都是理想情況下的理論峰值，為了與ETH進行差異化競爭，一旦大規模部署節點，由於多節點網路差異、程式碼最佳化、跨境防火牆、複雜應用等因素，真實平均TPS會衰減數十倍甚至數百倍。

公鏈效能評估最科學的方法是計算Swap合約交互消耗的Gas，公式為：

$$TPS = \frac{\text{GasLimit}}{\text{GasUsedPerTx}} \div AverageBlockTime$$

Solana 比較獨特，沒有Gas Limit，超過TPS 限制會帶來區塊阻塞、同步延遲、交易失敗等問題。不過，我們可以透過瀏覽器查看歷史數據來觀察它可能達到的上限。

這個公式是公眾認可的相對公平的計算方式，因為每條鏈的交易成分都不一樣，如果只計算常見的交易，差異就會很大。



從上圖我們可以看到，在各條公鏈的主鏈中，TPS上限最高的是AUT，為7521，其次是Avalanche的4543和SOL的2973。在相容EVM的鏈中，最高的是Coin BSC的194和ETH的18。AUT的主鏈TPS是以太坊的417倍。

各條鏈都曾遭遇過效能問題，AUT雙鏈從根本上解決了以下問題：

以太坊：自誕生以來，以太坊每年都會經歷幾輪持續的大規模區塊擁塞事件。2021年4月，以太坊在Uniswap的單筆交易費用高達100美元，同步延遲成長了數十倍，無法承載要求嚴苛的金融服務。

Solana：在高峰期限制了請求流量，並經歷了幾次宕機災難，導致整個Sol區塊鏈癱瘓。雖然後來引入了資料流控技術，並改進了Gas模型，但專家評估其效果有限。
Avalanche：DEX Pangolin負載過高引發跨鏈功能錯誤，導致社群出現短暫恐慌。

BSC/Polygon：2021年第二季度，由於鏈上活動激增，導致擁堵，隨後Gas費用飆升。

從使用量上衡量：假設X為每日交易筆數，所需TPS為T。

根據帕累托原則（80/20法則）：X筆交易的80%需要在20%的時間內完成，T1需要滿足尖峰需求。則得出：
T1 !X * 80%/（24h * 20%）* 3600）!X / 21600

在網路穩定、用戶需求成長的前提下，我們可以進一步考慮平均用戶分佈，得出平均TPS需求。
T2 !X /（24h * 3600）!X / 86400

某公鏈每日平均交易實際所需TPS：見下表

Development	Total average daily transaction	T1 demand(TPS)	T2 demand(TPS)
Startin	10,000	0.46	0.12
Developmen	1,000,000	46.3	11.6
Surging	10,000,000	463.0	115.7
Maturit	30,000,000	1388.9	347.2
y	150,000,000	6944.4	1736.1

上表顯示，約7000的TPS可以實現1.5億筆/天的交易處理。

主鏈對於原生治理代幣的應用及其合約交互，平均每天可以處理1.5億筆交易。

根據硬體部署情況，Fin-Chain生態專案可以處理超過VISA信用卡的資料量，平均每天有15-20億筆交易。

AUT將成為市場上唯一能夠滿足傳統金融巨頭融入生態需求的超級金融公鏈。

4. 共識機制

4.1 主鏈共識

在全球碳中和的大背景下，PoW的高能耗問題日益凸顯，在一定程度上限制了區塊鏈網路在全球的廣泛應用。在評估了安全性、效能、能源效率、使用者友善性等各方面因素後，主鏈決定採用APoS共識。

我們先來簡單了解一下PoS共識。與需要大量功耗來解決數學難題的PoW不同，PoS是一種以質押為關鍵字的演算法。為了模擬基於權益的驗證者（在PoS中，我們更喜歡用驗證者這個詞，而不是礦工）的選擇過程，我們採用了許多基於PoS的區塊鏈網路（例如Cardano、Dash等）中遵循中本聰（FTS）的演算法。
在有N 個參與者的網路中，選擇節點i 作為驗證者的機率Pi 為：

$$P_i = \frac{S_i}{\sum_{j=1}^{N} S_j}$$

Si代表參與者i的份額（Token持有份額），這意味著節點持有的份額越多，被選為驗證者的幾率就越高，驗證者將獲得Token作為獎勵。
現在我們來談談改進後的APoS，即資產權益證明。APoS共識機制繼承並發展了現有的PoS，它遵循了PoW共識的去中心化路徑，但更環保和節能。同時，其融合了PoS和DPoS的經濟模式也避免了其過度中心化的弊端。

APoS可以更好地優化和呈現基於跨鏈網關的點對點電子現金系統，在支付方面優於所有其他公鏈。由於主鏈為共識層引入了跨鏈中繼，您可以在主鏈上使用多種加密貨幣結算交易。通訊和共識透過Hot Stuff協定進行，在安全的基礎上大大加快了通訊和共識的速度。

理論上，主鏈可以讓任何數位資產的節點參與主鏈共識，任何公鏈Token都可以參與質押，獲得主網生成區塊的AUT激勵，包括主網的治理代幣AUT，是目前最人性化的共識參與機制。

4.2 APoS共識運作機制

每位參與者可以訂閱支持自己喜歡的超級節點候選人，然後該候選人將被選為驗證者，全網選舉產生第100位驗證者。

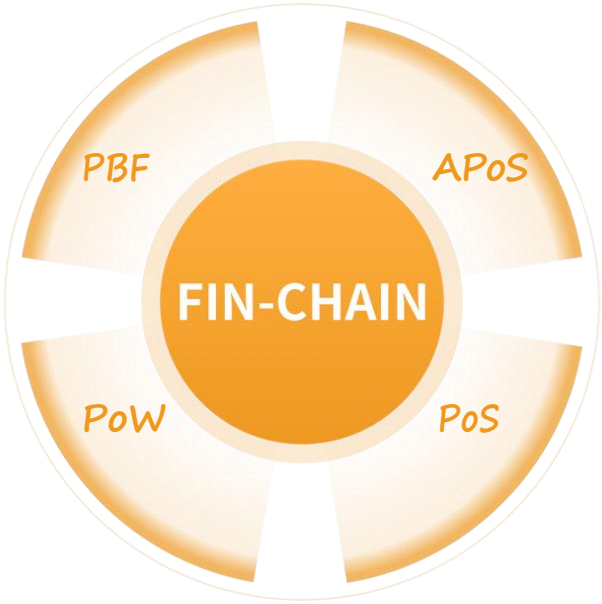
任何擁有合適區塊鏈資源（硬體、伺服器、頻寬）和足夠加密資產的人都可以透過競選申請成為超級節點候選人。全網共設置100個超級節點。APoS共識機制選擇100個超級節點作為區塊驗證者，然後透過零知識證明隨機演算法選出一個超級節點作為驗證者。之後，如果被選中的驗證者作惡或硬體下線，則會觸發相應的懲罰。當懲罰達到閾值時，將選出一個新的超級節點作為續任驗證者。作惡嚴重的超級節點將被取消節點資格。驗證者採用離散循環機制的演算法，依序產生區塊並獲得

AUT獎勵，然後透過內建智慧合約將獎勵分發給每個超級節點。

4.3 金融鏈共識

Fin-Chain 以可擴展性和相容性為設計理念，革命性地允許專案方根據業務需求客製化公鏈，自由選擇不同的共識機制。

目前支援和正在開發的四種共識機制分別是PBFT、APoS、PoS 和PoW。



本節主要介紹實用拜占庭容錯（PBFT）共識。Fin-Chain的PBFT以IBM的Hyperledger Fabric為藍本開發，採用「背書->排序->驗證」的方式達成共識。

傳統的分散式一致性演算法一般透過協商的方式解決共識問題，在確保活躍度和安全性的同時，為n個節點的網路提供（n-1）/3的容錯性。拜占庭節點可以看作是攻擊者攻擊的節點，減少拜占庭節點的生成意味著增加攻擊者的攻擊難度。為此，我們可以增加節點數量，也可以隨機化出區塊節點。

Fin-Chain是一個允許多方參與、開發、部署和營運區塊鏈應用的平行鏈平台。Fin-Chain採用Hyperledger Fabric打造了模組化、可擴展的區塊鏈開發框架，為企業級區塊鏈應用開發提供解決方案。Hyperledger Fabric區塊鏈系統主要包括以下幾個元件：

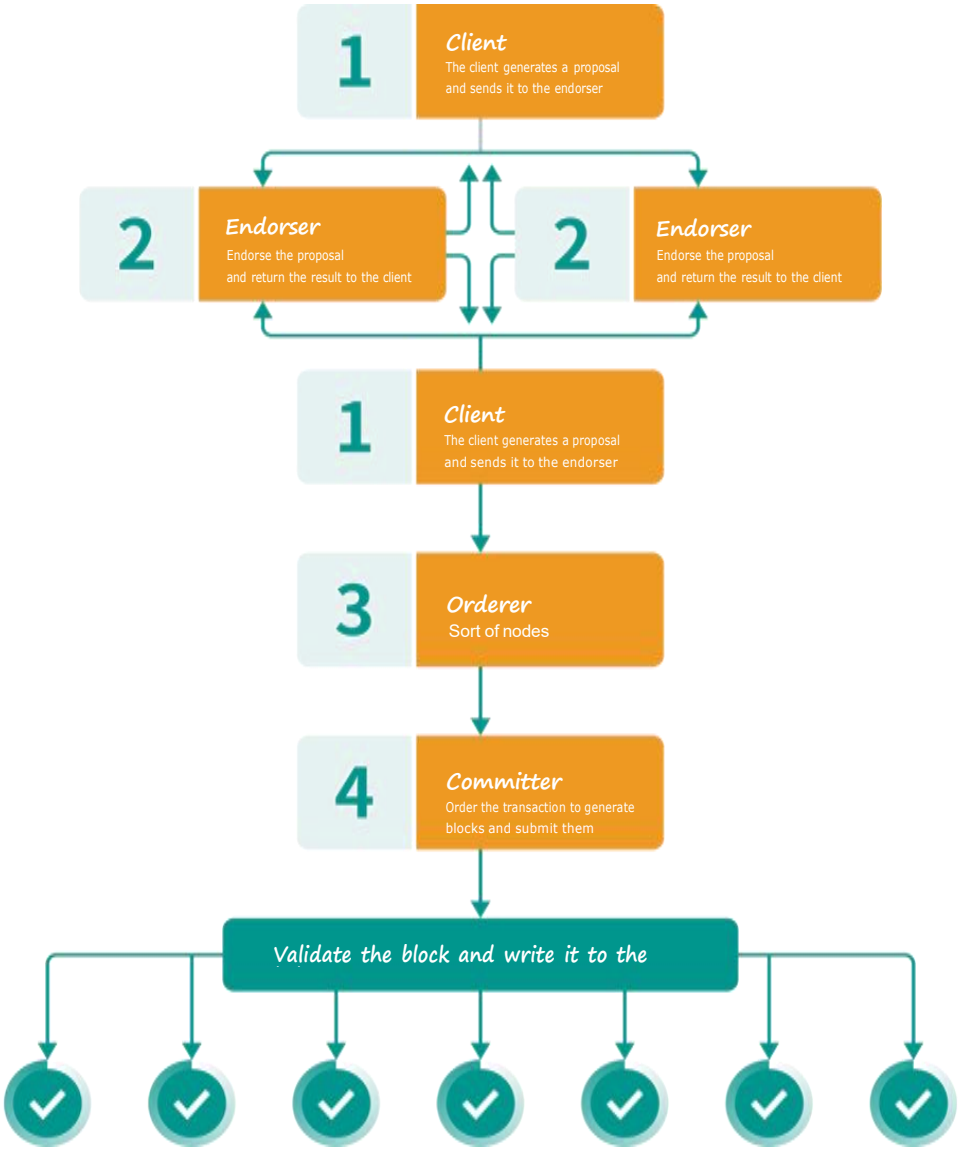
Chaincode：Hyperledger Fabric 中的智慧合約，以程式碼形式將複雜的業務邏輯錨定在Fabric 系統中，當滿足某些條件時，鏈碼就會被執行。

Client：使用者與Hyperledger Fabric 網路之間的存取點，在其上部署了專有的SDK，使用者可以透過客戶端發起交易請求，即ProPoSal。

Endorser：在Hyperledger Fabric 中，當客戶端想要發起交易時，首先需要獲得一定數量的對該交易的背書，這些背書來自背書者，背書者通過運行鏈碼來執行模擬交易，生成讀寫集，然後對交易進行背書（對讀寫集進行簽名並附加其身份），以證明背書者已經處理了該交易。

Orderer：Hyperledger Fabric 透過多個排序者提供排序服務，排序服務從全網接收所有交易，並按時間順序打包成區塊。排序服務不參與交易的執行和驗證，因此不關注交易的具體細節。排序服務的目標是就交易的產生順序達成一致，並廣播結果。

Committer：Hyperledger Fabric 網路中維護帳本的主體。提交者接收排序服務打包的區塊，驗證區塊中交易的有效性，並相應地將有效交易提交到帳本。此外，背書者也屬於提交者，背書是背書者在維護帳本之外的附加功能。



Fin-Chain也支援經典的PoW（Proof of Work）工作量證明機制，即隨機選擇出塊人。「挖礦」就是每個節點不斷嘗試解決一個難以解決但易於驗證的數學難題，最快解決難題的節點獲得下一個區塊的發布權（記帳權）和系統獎勵。PoW的隨機性依賴於雜湊函數值的均勻分佈，但大量的雜湊計算伴隨著大量的能源消耗，而這種消耗所要解決的問題毫無意義。同時，隨著「礦機」的出現與發展，計算量逐漸被一些大型礦池壟斷，對系統安全構成威脅。此外，PoW共識效率較低，出塊和交易確認時間較長，難以滿足現實需求。

雖然權益證明（PoS）也是透過「挖礦」選擇出塊人，但「挖礦」成功的機率與節點的權益有關，節點的權益越大，「挖礦」成功的機率就越大。這些都加快了區塊的生成速度，提高了共識效率，同時由於繁重計算的減少，計算量不再是影響PoS「挖礦」的主要因素，減少了資源浪費。

值得注意的是，在PoS基礎上，委託權益證明（DPoS）透過犧牲一定的「去中心化」特性，實現了更高的共識效率。每個節點可以用自己的權益投票選出代表，得票最多的前N個用戶將組成共識參與“委員會”，各成員輪流打包交易、生成區塊。DPoS由於參與共識節點數量減少，交易速度快。但DPoS在去中心化過程中產生的代理節點，使得攻擊者的攻擊目標更加明確，降低了攻擊者的攻擊成本，因此Fin-Chain暫時沒有支援DPoS的計畫。

5. 零知識證明

零知識證明是AUTHERIUM支援的Layer2擴容方案之一，是透過Fin-Chain建構平行鏈時的選用模組。

零知識證明被定義為證明者在不向驗證者提供任何有用資訊的情況下說服驗證者斷言正確的能力。作為密碼學的迭代成果，零知識證明的應用場景包括但不限於：

- · 串謀與防作惡
- · 去中心化存儲
- · 鏈下擴容－提高交易吞吐量
- · 鏈上壓縮－大幅減少鏈上資料和區塊大小，提高驗證效率
- · 全面保護使用者資料隱私（例如，混合貨幣應用，實際交易地址不可知）

通过深化上述应用，AUT的系统将更加安全和稳健，并适当隔离用户隐私。持续发展甚至可以彻底改变数据共享和区块链的工作方式。现代零知识证明体系起源于 Goldwasser、Micali 和 Rackoff 合著的论文《交互式证明系统的知识复杂性》，该论文由密码学先驱和 AUT 进行了修改。在此基础上诞生的非交互式系统具有完备性，是零知识证明体系的完美选择。

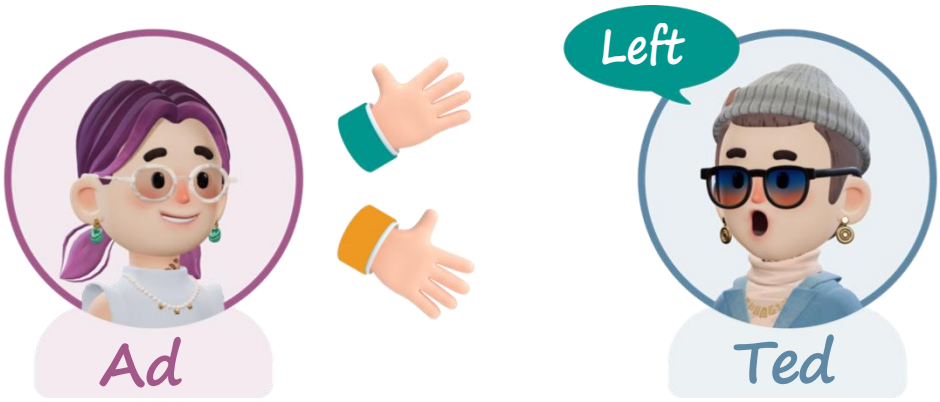
为了便于理解这一重要技术，我们举一个零知识证明的经典例子：

5.1 交互式零知识证明（色盲人士的游戏）

假設Ada是色盲，Ted是色盲。Ted手中有兩個大小和形狀完全相同的球，但一個是綠色，一個是黃色。他需要向Ada證明這兩個球的顏色不同。在這個經典案例中，Ada是驗證者，需要驗證Ted的說法是否正確；而Ted是證明者，如果Ada無法辨識顏色，則需要向Ada證明這兩個球的顏色不同。這是對零知識證明的常見解釋。

過程如下：

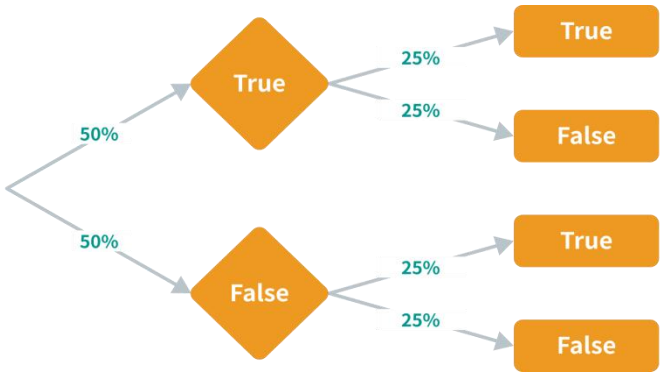
Ada拿起Ted面前的兩個球，左手拿著綠色的，右手拿著黃色的，然後將雙手放在身後，讓Ted看不到球。Ada在身後隨機交換左右手中的球。交換後，Ada伸出手問Ted兩球是否交換了位置。如果泰德能夠辨識球的顏色，那麼每次艾達改變球的位置時，他就能正確回答艾達的問題。



第一次，艾達偷偷地交換了手中球的位置，然後問泰德是否交換了球的位置。如果泰德的回答是肯定的，那麼艾達有50% 的機率相信泰德能區分兩個球的顏色，因為泰德有1/2 的機率猜對。因此，艾達可以第二次測試泰德。如果泰德的回答是否定的，那麼艾達確信泰德不能區分兩個球的顏色。

第二次，艾達不交換手中球的位置，然後問泰德是否交換了球的位置。如果泰德的回答是否定的，那麼艾達有75% 的機率相信泰德能區分兩個球的顏色。

以下是上述情況的機率樹：



第一次迭代後，Ada 斷言Ted 的陳述為真的機率為50%。如果Ted 第二次給出了正確答案，那麼機率將上升到75%，第三次迭代後，機率將達到87.5%。如果Ted 連續n 次通過測試，那麼Ada 有1 - (1/2)^n 的機率相信Ted 的陳述為真。

零知識證明是一種基於機率的驗證方法，驗證者以一定的隨機性向證明者提問。如果證明者能夠提供正確的答案，則證明者擁有其聲稱的「知識」的機率很高。零知識證明不是數學意義上的證明，因為它涉及很小的錯誤機率，即作惡的證明者可能會透過提出虛假聲明來欺騙驗證者。換句話說，零知識證明是機率證明，而不是確定性證明。然而，技術可以將誤差降低到可以忽略的程度。

根據零知識證明的定義，我們可以得知它有以下三個重要性質：

1）完備性：如果證明者擁有相關知識，那麼他就可以通過驗證者的驗證，即證明者有足夠大的機率說服驗證者。
2）可靠性：如果證明者不擁有相關知識，那麼他就無法通過驗證者的驗證，即證明者欺騙驗證者的機率可以忽略不計。
3）零知識：證明者在互動過程中只向驗證者透露自己是否擁有相關知識，而不透露任何有關該知識的額外資訊。

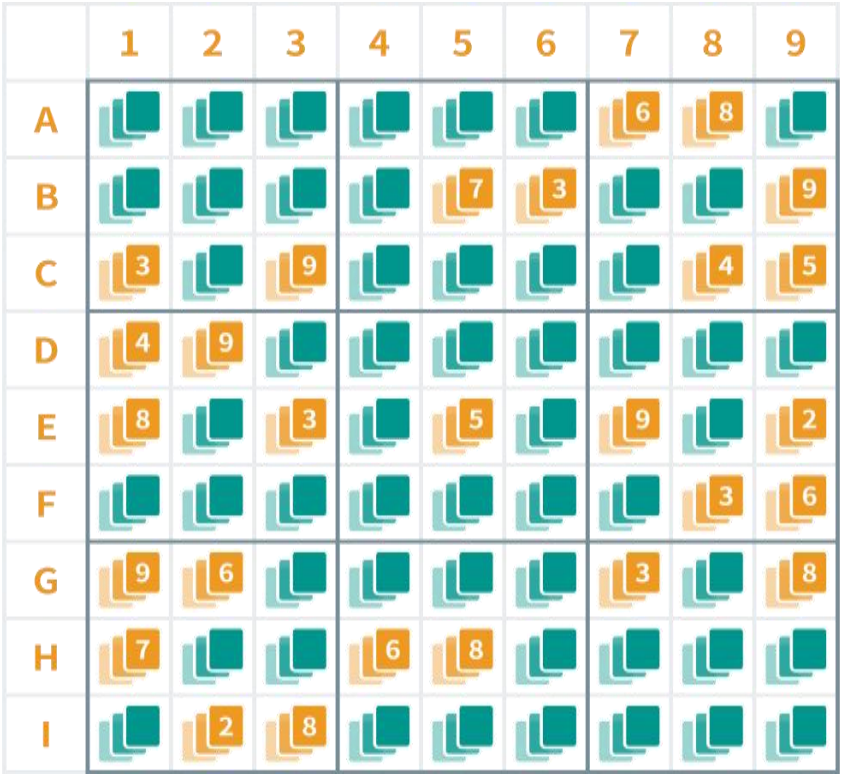
在這個例子中，如果Ted擁有區分球顏色的知識，那麼他每次都會回答正確，這被認為是完備性的。如果Ted不擁有區分球顏色的相關知識，那麼他就無法判斷Ada是否交換過球，這稱為可靠性。在這個協議中，Ada無法看到球的顏色，這就是零知識。

非互動式零知識證明－數獨
互動式零知識證明協議依賴驗證者的隨機嘗試，需要證明者和驗證者進行多次互動才能完成。非互動式零知識（NIZK）證明將互動次數減少到一次，從而實現離線證明和公開驗證。在AUT的零知識證明應用場景中，非互動特性是必要的，因為在區塊鏈系統中，不能假設雙方始終在線並互動。在AUTHERIUM上，證明者只需向整個網路廣播一個證明交易，網路上的礦工在將此交易打包到區塊時幫助證明者驗證零知識證明。

我們可以透過數獨案例來理解AUT的超高效非互動式證明：數獨是一種數值邏輯推理遊戲，起源於18世紀的瑞士，其中計算使用鉛筆和紙進行。玩家需要根據9×9盤上已知的數字，推斷所有剩餘空格的數字，並滿足每行、每列、每個粗線宮（3*3）的數字包含1-9且不重複的要求。

為了向Ada證明自己已經解答了一道數獨題，Ted製作了一台防篡改的機器，把生成的數獨答案放入其中，機器可以將證明發送給Ada。

該機器遵循以下可公開驗證的協議：
首先，將尚未解決的原始數獨謎題以三張面朝上的謎題卡輸入機器。例如，單元格C3 有三張面朝上的數字9 的卡片。
接下來，Ted 將他的答案面朝下放在對應的單元格上，每個單元格同樣有三張卡片。

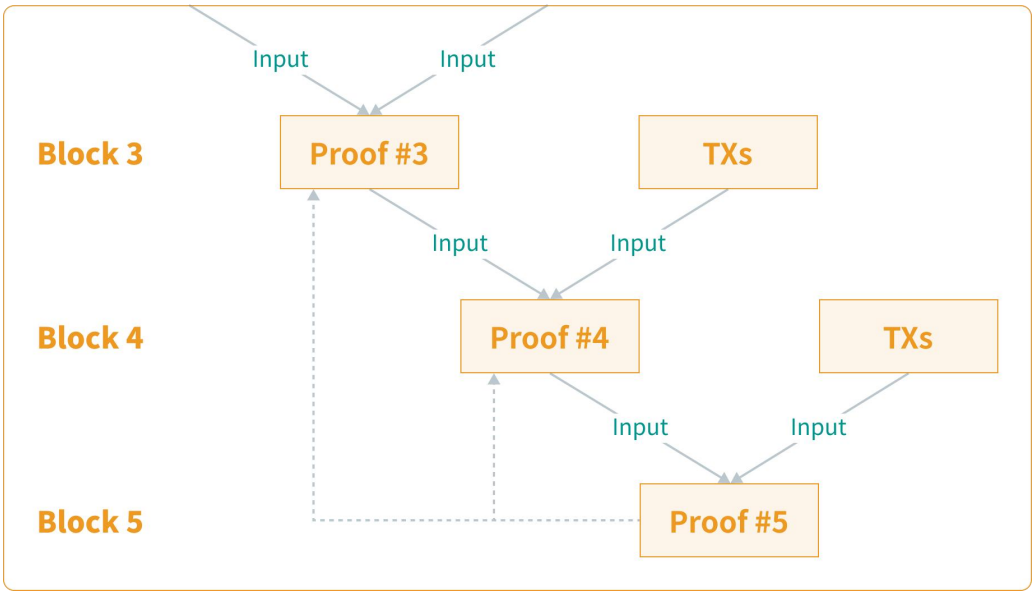


最後，艾達從機器那裡得到了一個證明，機器返回了三類各27個袋子給艾達：
·第一類機器從數獨的每一行中取出9張牌，分別混在一起後放入一個袋子裡，一共有9行9個袋子。
·第二類機器從數獨的每一列中取出9張牌，分別混在一起後放入一個袋子裡，一共有9列9個袋子。
·第三類機器從數獨的每個粗線宮殿（3*3）中取出9張牌，分別混在一起後放入一個袋子裡，一共有9個粗線宮殿和9個袋子。

艾達隨後對這27個袋子逐一進行檢查，如果每個袋子裡的卡片都包含1到9的數字，且沒有缺失或重複的數字，那麼艾達就可以確認泰德確實解答了數獨。此外，Ada 並沒有從機器返回的證明中獲得任何有關數獨解決方案的知識，因為機器返回的袋子中的數字是隨機打亂的。

5.2 遞歸零知識證明

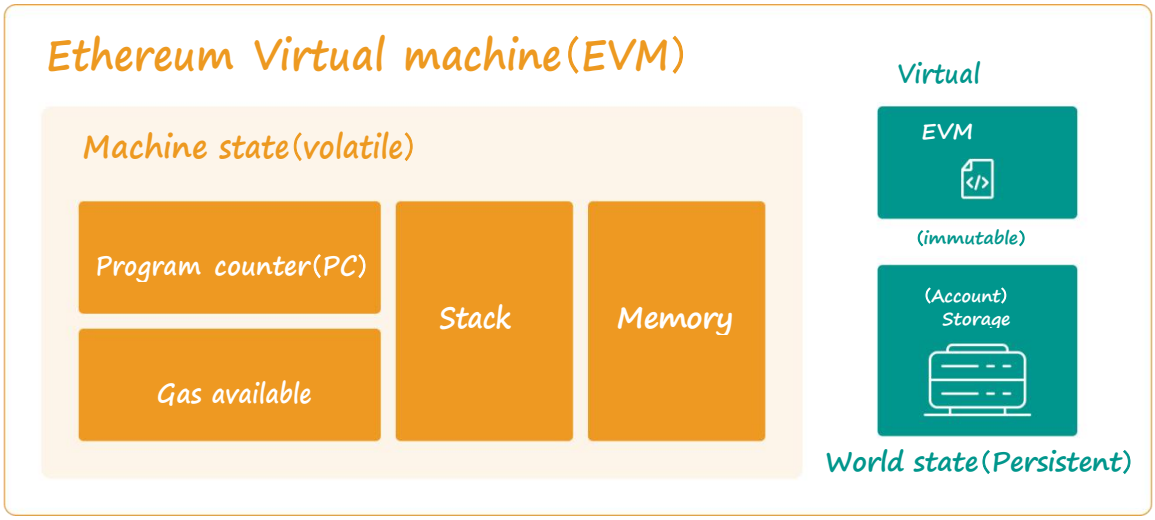
AUT 支援更有效率的遞歸零知識證明產生：它將上一個狀態的證明和當前交易作為輸入，然後驗證上一個狀態的證明和當前交易是否有效。如果所有證明都通過驗證，程式將輸出一個新的狀態和一個證明，如下圖所示：



整個鏈的狀態可以透過簡單地驗證前一個狀態的證明來驗證，即遞歸零知識證明驗證。例如，當證明#5被驗證正確時，相當於遞歸驗證了證明#4和證明#3。

6. 與以太坊EVM的兼容性

.AUT透過eBridge相容於以太坊虛擬機（EVM），每月可支援超過4000名活躍的以太坊開發者快速將DApp移植到AUT公鏈上。EVM是智慧合約執行的主導標準，相容於EVM將極大促進跨鏈流動性和金融專案遷移優化。



EVM 的運作方式類似於堆疊機，它將瞬時資料推送到下推堆疊並從中推送出來，深度為1024 項，每個項都是一個256 位元字。它還以位元組數組的形式維護臨時內存，該內存在以太坊區塊鏈上的兩個交易之間發生變化。編譯後的智能合約程式碼由EVM 作為140 個標準操作碼的集合執行，其他特定於區塊鏈的堆疊操作也由EVM 實現。

7. 原子交換資產跨鏈

AUT透過「原子交換」的方式支援與其他公鏈進行數位資產交互，這是一種利用不同區塊鏈的點對點（P2P）交易系統，可以充分釋放資產流動性，進一步提升用戶體驗。

7.1 原子交換的工作原理

原子交換協議旨在防止交易對手之間的欺詐行為。為了更好地理解它們的工作原理，我們假設Ada想要用她的AUT 交換Ted 的比特幣(BTC)。

首先，Ada 將她的AUT 存入合約地址，該地址類似於保險箱。透過這種方式創建的安全性，Ada 產生一個金鑰來存取它。然後，她與Ted 分享此金鑰的加密雜湊值。請注意，此時Ted 無法存取Ada 的AUT，因為他只有金鑰的雜湊值，而不是金鑰本身。

接下來，Ted 使用Ada 提供的雜湊值建立另一個安全合約位址來存放他的BTC。如果Ada 想要交換BTC，她需要使用與該位址相同的金鑰，同時，她需要向Ted 出示AUT 金鑰（借助hashlock 的特殊功能）。這意味著，一旦Ada 發出交換BTC 的請求，Ted 同時就可以存取Ada 的AUT，而該原子交換的交易過程就完成了。

「原子」一詞代表交易的一致性，即交易要麼完全成功，要麼完全失敗。如果任何一方放棄或未能如預期執行交易，則合約將被取消，資金將自動退還給原所有者。

原子交換可以在鏈上或鏈下進行。鏈上原子交換發生在區塊鏈的線上網路中，適用於任何加密貨幣。

另一方面，鏈下原子交換發生在鏈下。這種類型的原子交換通常基於雙向支付管道，類似於閃電網路中使用的渠道支付。

從技術上講，大多數去中心化交易系統都是基於多重簽章和哈希時間鎖定合約(HTLC) 完成的。

7.2 哈希時間鎖定合約（HTLC）

哈希時間鎖定合約(HTLC) 是原子交換的關鍵組件之一。顧名思義，它基於哈希鎖和時間鎖這兩個關鍵功能。

如果未提供相關金鑰資料（上述情況下為Ada 的金鑰），則雜湊鎖會凍結資金，而時間鎖則確保智慧合約僅在預先定義的時間範圍內執行。因此，使用HTLC 可以建立特定規則，從而消除對集中化的需要，從而防止原子交換被部分執行。

原子交換的最大優點在於去中心化。原子交換消除了對集中交換和任何其他類型中介的需求，因為跨鏈交換可以在兩方或多方之間執行，而無需他們相互信任。由於用戶無需向集中交易所或第三方提供資金，因此安全等級也得到了顯著提高。交易可以直接透過用戶的個人錢包發起。

此外，點對點交易允許非常低的交易費用和更快的交易。從而實現了更高水準的互通性。

8. 模組化平行鏈

Fin-Chain將在業界率先實現一鍵發鏈的模組化配置功能，廣大傳統金融企業可以輕鬆配置符合自身業務集群特徵的平行鏈，實現比傳統DApp更複雜、更大規模的金融服務，同時可以發展自己的平行鏈生態，降低開發成本數十倍甚至數百倍。

<table>
<tr><th>Comparison items</th><th>針對性 開發商</th><th>迅速的 應用 發展</th><th>L2 子鏈 發展</th><th>新的 民眾 鏈 發展</th></tr>
<tr><td>其他 民眾 連鎖生態開發商</td><td>硬幣 圈子</td><td>DApp</td><td rowspan="2">更高的技術和 時間 成本 必需的
在 A 1-3年 基礎</td><td rowspan="2">海量技術和 時間 成本 必需的
在 A 3-6年 基礎</td></tr>
<tr><td>主鏈生態開發者</td><td>硬幣 圈子</td><td>DApp</td></tr>
<tr><td>金融鏈生態開發商</td><td>金融 圈互聯網 圈硬幣圈</td><td>Parallel chains
DApp</td><td colspan="2">Modularized configuration of parallel chains
Hundred times lower technical and time costs On a weekly or even daily basis</td></tr>
</table>

Fin-Chain具有高度模組化和可配置的架構(無限可擴展的平行通道)，針對銀行、金融、保險、醫療、元宇宙、人力資源、供應鏈甚至數位音樂交付等行業案例提供了靈活的創新和優化。Fin-Chain中的CA、資料庫和共識演算法都是可插拔的，鏈代碼透過Docker實現。

透過獨特的平行鏈架構，解決了區塊鏈無法同時滿足可擴展性、安全性和去中心化要求的問題。系統提供了一套完整的解決方案，幫助想要擁有屬於自己的公鏈的企業用戶建立專屬的應用鏈。

未來，開發者只需在手機上輸入應用鏈所需的應用鏈節點數、保證金、共識機制等參數，幾分鐘就可以部署一條應用鏈，之後只需在區塊瀏覽器上註冊應用鏈的合約位址、連接埠等訊息，就可以監控新鏈的出塊狀況和運作情況。

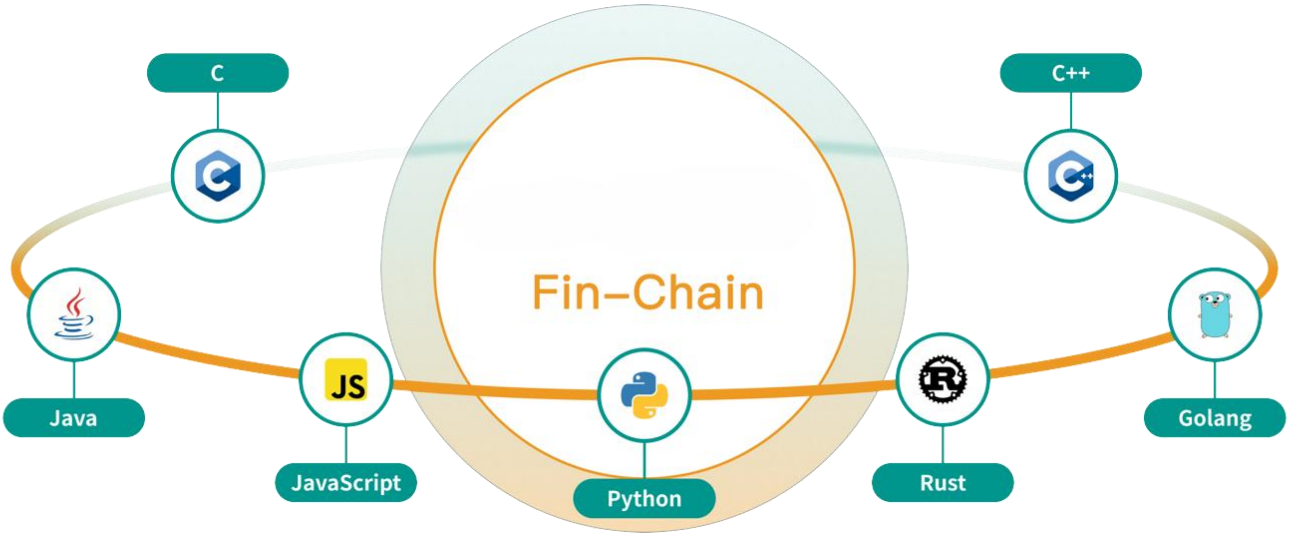
平行鏈支援的選用共識模組有PBFT、APoS、PoS、PoW。
平行鏈的典型配置：

已創建 和 設定檔.yaml 文件 和 配置工具。用法 的 配置根：
-chainCreateTxBaseProfile 細繩
指定 底層 交易 的 設定 文件 , 需要 與'
outputCreateChainTx' -chainID 字串一起 使用
鏈 姓名（不能 是 重複）-配置路徑 字串配置 文件 小路 –
檢查區塊 細繩
堵塞 貯存 小路 -inspectChainCreateTx 細繩
區塊鏈 交易 貯存 小路 -outputCreateChainTx 細繩 -outputCreateChainTx 字串路徑 書面 什麼時候 這 區塊鏈 創造 配置 -版本
版本 資訊

9. 通用程式設計合約開發

Fin-Chain的平行鏈虛擬機(FVM)是圖靈完備的，可以運行任何程式語言編寫的程序，讓非區塊鏈開發者可以輕鬆為新興的Web 3.0產業創建自訂智慧合約和DApp。FVM支援Java/Go/C++/JS等主流程式語言所創建的智慧合約。

企業可以節省Soldity/Rust等技術人員的成本，非區塊鏈企業也可以低成本開發去中心化應用，結合模組化的平行鏈服務，傳統企業上鏈門檻可以降到最低。



10. AUT 治理與激勵

AUT 是AUTHERIUM 的原生代幣，基於AUT 代幣進行治理和激勵。

10.1 AUT保險與設立

AUTHERIUM（AUT）總發行量為10億。

10.2 AUT 代幣分配策略

IDO：25%，全部由市場IDO產生，不鎖倉，上線前全部釋放。

技術：15%，鎖倉5年，之後每年釋放1%，直到全部釋放。

營運：15%，由基金會審核，不定期發行，具體釋放比例會在社區公佈。

基金會：19%，鎖倉2年，之後每季釋出1%。這部分代幣主要用於公關、社群建立、市場推廣，以及獎勵對平台有突出貢獻的用戶和機構。

空投：10%，有條件空投給活躍用戶或符合特定條件的用戶，鼓勵社區參與和生態建設。

挖礦：16%，透過用戶資料挖礦產生，鼓勵用戶積極參與生態活動，貢獻價值。

11. AUT 金融基礎設施

AUT 是一條金融公鏈，擁有支撐現代金融體系和麵向未來金融的基礎服務和基礎設施，這些基礎設施建立在AUT 核心技術之上，以協議層和服務層的形式提供給AUT 生態系統使用。

11.1 FinSwap 跨鏈資產交易

加密產業已進入跨鏈時代，隨著Web3.0世界公鏈和聚合層的激增，許多應用都建立在不同的孤立生態上，部分應用雖然在多條區塊鏈上部署試驗，但其流動性難免碎片化。一旦涉及跨鏈交易，用戶就必須透過CEX或笨拙的跨鏈橋進行資產轉移，操作複雜，Gas費用高，隱私性差，流程過於冗長，給駭客提供了更多可乘之機。

AUT作為專注於加密金融服務的公鏈，將基於自身雙股閃電互動架構和原子互換服務，推出示範級創新應用－跨鏈互換FinSwap，解決去中心化跨鏈流動性的產業挑戰。

FinSwap是一個可組合的全鏈流動性聚合協議，資產跨鍊和互換過程對用戶來說快速且瞬時。此外，處理交易的合約在Fin-Chain 上執行，TPS 高達80,000+，使用戶能夠享受接近CEX 的交易體驗，這在傳統互換中是不可想像的。
值得注意的是，FinSwap 使用ALLIM 訊息跨鏈框架聚合來自所有區塊鏈的流動性，同時允許其他DApp 存取深度，以幫助他們從不同的區塊鏈中獲取流動性。因此，使用者可以從最深的流動性中受益，以最低的成本實現最佳匯率和最小滑點互換。

在做市演算法的基礎上，FinSwap 將是唯一一個LP 可以透過第三代AMM 自動做市商機制精細控制資金配置價格區間的跨鏈交易所，從而進一步提高資金效率，減少滑點，防止資產暴跌。

經濟學家Robin Hanson 在2002 年研究數位市場評分規則時首次提到了AMM 演算法。2016 年，Uniswap 將自動做市商有效地引入了加密領域，提出了恆定乘積做市商(CPMM) 模型，以確保以太坊的代幣交易恆定且具有流動性，其公式如下：

$$(Rx - \Delta x)(Ry + (1 - f)\Delta y) = k$$

其中，Rx、Ry分別為各類型Token的儲備量，f為交易費，k為常數。簡化公式如下：

$$x * y = k$$

其中x 為Token1，y 為Token 2，k 為常數。
本質上，AMM 將兩種正在交易的資產組合到一個流動性池中，旨在確保無論交易規模如何，流動性池的資產規模都保持不變。

CPMM 模型是AMM 的範式轉變，是一種去中心化的機制，它完全消除了中間人，同時實現了流動性、快速交易和鏈上機制的結合，以正確的價格報價。然而，它也存在明顯的缺陷，例如滑點、無常

損失和安全風險。

2020 年左右，新一代AMM 開始快速成長，CPMM 模型逐漸與CSMM 模型融合，形成混合CPMM。此公式使得流動性呈指數級密集。此曲線大部分屬於線性匯率：

$$An^n \sum x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$$

其中，x 為每種資產的儲備量，n 為資產數量，D 為不變量（儲備量的總價值），A 為放大係數（類似“槓桿”，代表曲線的曲率程度）。

接下來，FinSwap 將以更複雜的解決方案將互換演算法提升到更高的水平。我們將引入中心化流動性、基於第二代AMM 的多個費用等級，以及使用主動做市機制和Pyth 預測機。第二代AMM 將消除流動性池對套利者的依賴，以保持價格準確，並大幅降低不可預測損失的風險。

未來，FinSwap 將允許流動性定價到固定頭寸，使中心化流動性更進一步，讓DEX 的運作體驗接近CEX 的流暢度。

11.2 去中心化信用證明

信用是金融業的核心，信用的建立和擴展需要可靠的機制來保證其真實可信。AUT公鏈作為一條金融公鏈，透過區塊鏈技術、智能合約等技術手段，為金融業去中心化的信用拓展提供了基礎設計，實現了信用資訊的高度安全可信的共享管理，從而為客戶提供更優質、高效率、便利的金融服務。

鏈下客戶的信用資訊可以透過零知識證明的方式上鍊到AUTHERIUM，具體步驟如下：

1) 鏈下客戶向信用機構請求產生信用證明：客戶向信用機構提供其個人資訊、信用歷史等數據，請求信用機構產生相應的信用證明。
2) 信用機構產生信用證明：信用機構用自己的私鑰對客戶提供的資料進行簽名，產生數位憑證作為客戶信用證明的標識，同時將數位憑證上傳到鏈上，儲存在指定的智慧合約中。
3) 客戶產生零知識證明：客戶利用零知識證明技術，根據其個人資訊和信用歷史產生零知識證明，該證明不包含任何具體的個人信息，只是客戶擁有的對應數字證書的證明。
4) 客戶上傳零知識證明：客戶將自己產生的零知識證明與自己的數位憑證識別一起上傳到鏈上。
5) 鏈上智能合約驗證證明：鏈上智能合約在收到客戶的數位證書和零知識證明後，首先驗證數位證書的有效性，再透過零知識證明核對客戶的信用訊息，最終確認客戶的信用證明是否有效。

AUT去中心化信用證明使用AUTHERIUM中的互動式零知識證明方法來驗證客戶的信用，具體流程如下：

- ·客戶將其信用資訊儲存在本地設備中，並對資訊進行加密，產生加密雜湊值。
- ·客戶產生一組隨機數，並使用加密演算法加密，產生加密隨機數。
- ·客戶使用加密隨機數和信用資訊的加密雜湊值產生非互動式零知識證明。

- ·客戶將零知識證明發送給AUTHERIUM的智慧合約，智慧合約驗證證明的正確性，如果驗證成功，則將加密雜湊值儲存在鏈上。
-
- 上述方案中，非互動式零知識證明過程：
- 假設客戶想要證明自己知道自己信用資訊的雜湊值H，但不洩漏資訊本身，則證明過程如下：
-
- ·客戶產生一組隨機數r，並以加密演算法加密，產生加密隨機數R。
- ·客戶產生兩個值：s1 = H^r和s2 = r，其中^表示異或運算。
- ·客戶使用零知識證明系統證明s1和s2，在證明過程中不洩漏H和r的值。
- ·客戶將證明結果發送到鏈上，合約驗證證明的正確性，如果驗證成功，則將H儲存在鏈上。

上述方案中，客戶利用零知識證明系統證明自己知道H和r的值，但又不透露H和r的具體值，這樣既保證了客戶的隱私不被洩露，又證明了客戶確實知道信用信息的哈希值。

以上所有信用機構均須為AUTHERIUM的節點，並符合以下條件：
1）節點獎勵機制：節點每次成功產生信用證明並上傳到鏈上，即可獲得一定數量的AUT作為獎勵。獎勵數量可根據節點的信用等級和信用證明的複雜程度動態調整，以確保對節點的積極性和貢獻給予合理的獎勵。
2）懲罰機制：若發現節點產生的信用證明被偽造，則節點將受到對應的懲罰。具體而言，若發現節點被偽造，則節點將失去先前獲得的所有獎勵，並扣除一定的信用等級分數。同時，該節點也會被從節點清單中移除，不再被允許產生信用證明。
3）信用評等機制：節點的信用評等可以透過多種因素計算得出，包括但不限於節點產生的信用證明數量、真實性和複雜度等，評級結果作為節點獎懲機制的參考，以更好地調整節點的行為。
節點獎懲機制使得信用機構作為節點，透過信用評等機制不斷優化調整節點行為，確保信用證明的真實性和可信度，提高整個系統的信任度和效率。

11.3 金融靈魂綁定代幣（FinSBT s ）

SBT 是去中心化網路中描述使用者出身、學歷、薪資、消費水準、信用狀況等的不可轉讓的NFT，簡單來說就是「證明你是誰、你做過什麼、你取得了什麼成就、你的人脈網」等等。

SBT 可以分為很多類，在區塊鏈世界中，一個人可以擁有多個SBT。AUT 的關鍵功能之一就是為每個AUT 帳戶建立金融SBT，即FinSBT，該功能使用戶能夠在區塊鏈網路中映射自己現實中的完整金融身份，為用戶建立金融身份體系。

這意味著FinSBT 由AUT 位址原生承載，是整個AUTHERIUM 的底層基礎設施。
AUTHERIUM 建置SBT 的詳細方案如下：

1) 定義FinSBT的內容：FinSBT包含使用者的基本個人資訊、學歷、職業、收入、財務狀況、信用評級等，這些資訊都需要透過使用者授權和機構驗證進行收集和驗證。

2) 確定SBT的標準：根據FinSBT的內容，制定標準，包括資料格式、儲存方式、加密演算法等。
3) 開發智慧合約：根據SBT的標準，開發智慧合約，實現FinSBT資訊的使用者授權和機構驗證，以及FinSBT資訊的儲存和更新。
4) 與信用機構和節點合作：AUTHERIUM需要與信用機構合作，獲取其用戶信用評級數據，並將其添加到FinSBT中。
5) 實施隱私保護：由於FinSBT包含用戶的敏感訊息，因此需要實施隱私保護。使用零知識證明等技術防止用戶資料外洩。
6) 發行SBT：根據FinSBT的內容，發行相應的SBT，每個用戶可以擁有多個SBT，包括金融身分、信用評級等。
7) 使用SBT：用戶可以使用SBT在AUTHERIUM上進行交易、借貸、投資等金融活動，在這些活動中，用戶的FinSBT資訊可以作為信用評級、身份驗證的依據，提高交易的安全性和效率。
8) 更新SBT：用戶可以隨時更新自己的FinSBT訊息，如職業變化、收入增加等，更新後，相應的SBT也會隨之更新。

透過以上方案，AUTHERIUM可以建立完整的金融身份體系，提高金融活動的效率和安全性；同時，SBT可以體現用戶的金融身份，幫助用戶獲得更多的金融服務和機會。

11.4 原生穩定幣(FinUSDs)

AUT發行一種原生穩定幣，我們稱為FinUSD，簡稱FUSD。AUT透過一套智慧合約來管理、發行和銷毀FUSD，並維護FUSD的運作。

FUSD的發行必須有足夠的抵押物作為後盾，其具體的鑄造和發行流程如下：

1）用戶透過在AUTHERIUM上質押AUT、BTC等主流數位貨幣來獲得相應的FUSD。

2）要獲得FUSD，抵押物需要達到一定價值，該比例由AUTHERIUM的質押率結合用戶SBT的信用評級來控制。

3）當用戶還清FUSD貸款後，就可以拿回抵押物。

4）抵押物價格的波動可能帶來貸款風險，如果抵押物價值跌到一定水平，系統會強制平倉，賣出抵押物來彌補借款。

5）為確保抵押品的價值足以支付FUSD的發行費用，AUTHERIUM會定期審核抵押品的價值，並根據市場波動做出必要的調整。

用戶在質押鑄造的穩定幣後可以獲得以下收益：

1）投資收益：平台利用穩定幣的抵押品進行投資，如購買債券、股票、數位資產等，並從投資中獲得收益，部分收益可分配給穩定幣持有人。
2）借貸收益：平台可以以穩定幣抵押品發放貸款，並向借款人收取利息，部分利息可作為穩定幣持有人的收益。

3)穩定幣交易手續費收益:平台可以收取穩定幣交易的佣金,並將部分佣金作為穩定幣持有人的收益。
4)FinPAY支付收益:FinPAY在傳統銀行系統之間進行支付結算,並將部分手續費作為穩定幣持有人的收益。
5)抵押品價格波動收益:由於穩定幣的抵押品包含一定比例的加密貨幣,因此抵押品價格的波動可能會對穩定幣的收益產生影響。如果抵押品價格上漲,平台可能會出售部分抵押品以獲得收益,並將部分收益分配給穩定幣持有者。相反,如果抵押品價格下跌,平台可能需要注入額外的抵押品來維持穩定幣的價值。然而,這也可能為穩定幣持有者帶來額外的抵押收益。

總而言之,AUT FUSD的回報率預計在年化率20%至300%之間。

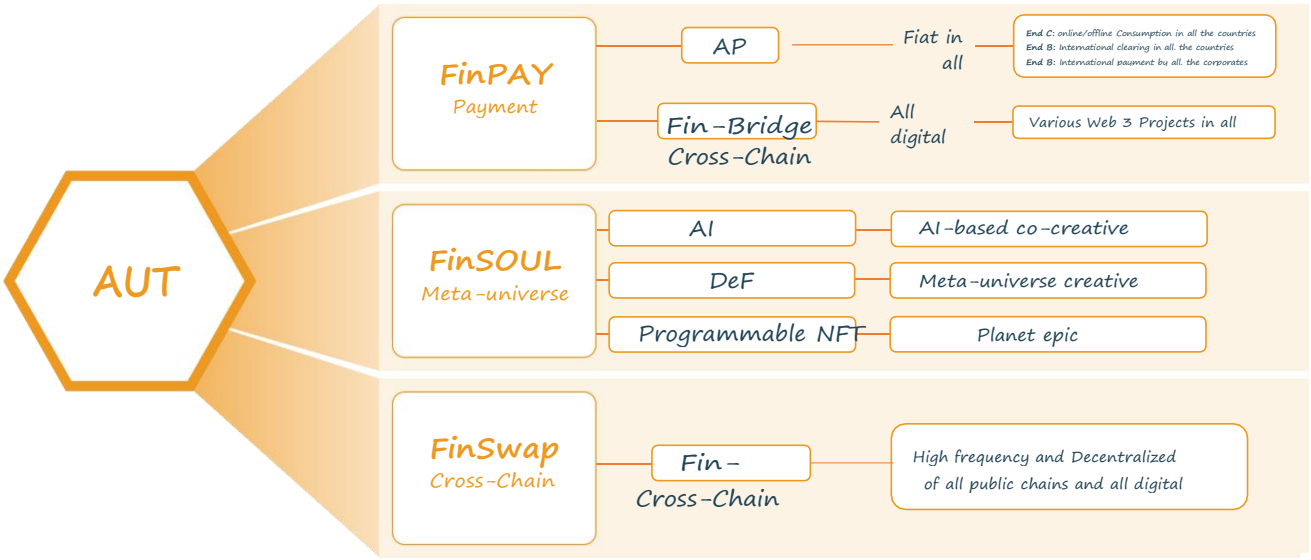
12. AUT生態應用

作為一條劃時代的金融公鏈，AUT不僅建構了堅實的雙鏈底層共識，還在應用層開發了先進的演示平台，包含超級支付網關、跨鏈兌換、AIGameFi、Defi、NFT五大模組，其中後三者被整合到FinSOUL平台。

12.1 FinPA Y 支付app

FinPAY是基於AUT的去中心化跨域跨鏈支付網關，現階段主要配合AUT用於銀行體系間的支付結算。

可視為SWIFT+PALPAY+VISA的超級融合協議，目前已與華爾街富國銀行、匯豐銀行、花旗銀行、高盛銀行等跨國銀行達成初步合作夥伴關係，FinPay可透過安全匿名的方式實現各國法幣與公鏈資產之間的低成本、高效率的轉帳。



其應用場景具有革命性，如：

1) 歐元可以在POLYGON公鏈專案A上3秒內快速兌換成Ax代幣。
2) 以太坊公鏈B項目上的Bx代幣可以快速兌換成印度里拉或俄羅斯盧布。
3) 日本銀行/企業的大筆日圓可以快速兌換成等值的美元或其他國家的法定貨幣。
4) X公鏈Y專案的治理代幣可用於在各國的商店、便利商店或線上商城購買商品和消費服務。
5) 各公鏈上的各類Defi項目都可以接收FINPAY支持的任何法定貨幣和Token來開展業務。

我們以SWIFT來做對比分析。SWIFT（全球銀行間金融電信協會）成立於1973年，是一個全球銀行間國際合作組織，其功能是在組織成員之間傳遞國際清算、支付等金融資訊。

雖然SWIFT在收費標準、資金到帳速度等方面取得了進步，但仍存在非免費、非即時、數位貨幣不可轉讓等問題。而這些正是FinPAY要解決的問題：

1）系統運作成本低

FinPAY是一個去中心化的架構，核心理念是「共識」、「共享」、「去信任」、「自由」。SWIFT是中心化機構，維護成本極高，例如係統內的薪資、伺服器叢集等設備成本、信任溝通成本，導致其跨幣種、跨境、跨地區的營運費用、收費標準一直居高不下。而FinPAY系統內任何幣種都可以近乎零成本自由兌換，異地、跨行、跨境支付無差異。

2）閃電般的轉帳速度

FinPAY系統下的轉賬速度和發郵件一樣快，大概3秒就到賬，而SWIFT國際匯款則需要一到兩天，相差幾千倍。對於分秒必爭的金融業來說，FinPAY系統是一個現象級的創新。

3）任意貨幣流動

FinPAY是數位貨幣與法幣任意轉換的超級網關，而SWIFT只適用於各國國家法幣，只要有匯率，任何貨幣都可以在FinPAY系統內自由兌換。

4）支援匿名交易

FinPAY提供了匿名交易的選項，而SWIFT交易必須公開雙方身份，可選匿名性對於WEB3.0金融非常重要。

5）API自由接入

無論是加密產業專案方、傳統銀行、網路公司，甚至是離線實體或個人機構，只要符合系統規則，都可以自由接入FinPAY的API，享受一站式網關服務，無需嚴格的准入門檻和冗長的審核流程。同時，API也會對基於智慧合約的惡意行為實施安全防禦和相應懲罰，識別惡意商家，並隔離至黑沙盒，確保系統整合運作。

此外，與成熟的開放支付網路Ripple相比，FinPAY還具有以下幾個面向的應用優勢：

Items to compare	Ripple	FinPAY	插圖 的 這 比較
TPS	1500+	7500+（主鏈） 80000+（金融鏈）	這 極佳的 規模 的 5 到 53 次 並發性 表現 差距
單身的 同時 交易	5秒-10秒	<3秒	A 堵塞 同步 時間 的 少於 1 第二 能 是 出色地 應用 面向各種支付場景， FinPAY擁有更全面的業務應用
商業 重點	國際的 銀行 清算	國際的 銀行 清算 全部 國際 的 交易 小額法幣支付 數位的 貨幣 在 A 小的 數量 支付	
跨鏈 交易	跨帳協議協議，在 一般的	閃電 狗 閃電鏈並行跨鏈原子交換	FinPAY執行跨鏈交易 更多的 有效 地
程度 的 權力下放和品牌可信 度	XRP發行總量1兆 創始團隊 擁有 更多的 比 200 百萬。銷售 and cashing out are extremely serious	Open, fair, scientific consensus output mechanism	In Oct. 2020, SEC filed a lawsuit against Ripple till now

從瑞波幣網路上XRP價格幾乎崩盤的事件中，我們體認到科技是創新的基礎，但公平的製度和不作惡的心才是平台長遠發展的支柱。

我們可以預見，FinPAY將成為跨境、跨鏈支付的終極解決方案，成為人類邁向未來金融文明的必

備基礎建設。

12.2 跨鏈金融票據交易市場(FinBills)

票據是用於支付目的的有價證券，傳統銀行票據業務是現代金融體系的核心，事實上，在許多國家，現金票據本身可以看作是跨銀行承兌的本票。

傳統金融票據業務分為以下幾類：

Types	Description	Difference
Bill of exchange	一個 樂器 發布 經過 這 抽屜，世界衛生組織 委託 這 付款人 到 支付 A 定數量 到 這 收款人 或者 持票人 無條件地 在 視線 或者 在 A 指定的 日期。	不同的 的人 看 這 帳單
本票 筆記	一個 樂器 發布 經過 這 抽屜 世界衛生組織 承諾 到 無條件地 支付 A 定 數量 到 這 收款人 或者 持票人 在 視線。	
查看	一個 樂器 發布 經過 這 抽屜，世界衛生組織 委託 這 銀行 為了 查看 訂金 to unconditionally pay a definite amount to the payee or bearer at sight.	

匯票依出具單位不同，可分為銀行匯票及商業匯票兩大類：

Types	Description	Difference
Bank draft	由以下機構發行的文書 這 發卡銀行 是無條件的 有薪資的 到 收款人 或者 持票人 在 視線 在 按照 和 這 實際的 沉澱 數量。	不同的 發行人
商業的 草稿	一個 樂器 發布 經過 這 抽屜，世界衛生組織 委託 這 付款人 到 無條件地 pay a definite amount to the payee or bearer on a specified date.	

FinBills作為AUT公鏈的基礎生態，將以WEB3.0的概念，以去中心化的方式實現上述三大金融票據業務。

FinBills將為客戶提供以下服務：

1) 發行金融工具NFT：金融機構可以在AUT上發行各類金融工具NFT，如商業匯票、貿易融資票據等，每個金融工具NFT都有唯一標識，確保不可複製、不可竄改。

2) 交易金融工具NFT：金融機構可以將發行的金融工具NFT投入市場進行交易，持有金融工具NFT的用戶可以透過交易市場進行買賣、質押，獲得收益。

3) 提供流動性支援：AUT可以透過提供流動性池來支援金融工具NFT的交易，使用者可以將AUT、BTC、ETH等數位貨幣質押到流動性池中，換取相應的流動性代幣。這些流動性代幣可用於交易金融工具NFT，而對應的數位貨幣則可隨時贖回。

4) 實現去中心化：AUT的金融票據市場採用去中心化設計，即金融機構直接與使用者進行交易，無需中介機構的參與。這種去中心化的模式可以降低交易成本，同時提高交易的透明度和安全性。

5) 提供信用評估服務：AUT可以利用平台上的使用者數據，結合FinSBT的基礎設施，為使用者提供信用評估服務。它有助於幫助金融機構更了解借款人的信用狀況，降低違約風險。

6) 提供資料查詢服務：AUT可以提供查詢服務，幫助金融機構查詢使用者的信用資料、借款記錄等信息，以輔助決策。同時，使用者也可以查詢自己的數據，以保障自己的權益。

12.3 衍生性商品交易所(FinEX)

FinEX是AUT的去中心化衍生性商品交易所，FinEX將提供多種衍生性商品供交易，包括期貨、選擇權、差價合約等。用戶的數位資產將儲存在智能合約中，以確保安全性和透明度。用戶可以透過錢包連接到FinEX，並使用自己的數位資產進行交易。

FinEX具有以下特色：

1)保證金交易：用戶在交易前需要存入保證金，以確保交易順利進行。保證金可以是數位貨幣或穩定幣，但係統建議使用FUSD。FinEX將提供多種保證金比例供用戶選擇，以滿足不同的風險偏好。

2)交易撮合：FinEX將採用去中心化的撮合機制，確保交易公平、透明、有效率。交易數據將儲存在區塊鏈上，以確保其不可篡改的特性。

3)費用結構：FinEX的費用結構將包括交易費、平台使用費和提現費。具體費率將根據交易類型和交易量而定，並在平台上揭露。

4)風險管理：FinEX將實施全面的風險管理措施，包括限制用戶的最大交易金額、即時監控交易風險等。同時，FinEX將提供風險保險，確保用戶的數位資產受到保障。

5)用戶支援：FinEX將提供7*24小時的用戶支援服務，幫助用戶解決交易過程中的任何問題。同時，FinEX將提供交易教育和技術支持，幫助用戶更好地了解和使用平台。

FinEX採用混合交易撮合機制，既確保了去中心化，也保證了效率。

首先，FinEX發揮了去中心化交易的優勢，所有交易都在鏈上執行，用戶的資產由用戶自己掌控，沒有中心化機構參與，確保了安全性和可信性。

同時，為了提高交易效率，FinEX還引入了基於混合CPMM的中心化流動性和多級費用交易撮合機制，可以更快地匹配交易對手，並提供高流動性和低交易費用。這種混合機制既保證了交易的去中心化，也保證了交易的效率。

此外，FinEX還採用了許多其他技術手段，進一步提高交易的效率和使用者體驗。例如，引入了閃電網絡，以加快交易確認速度並降低交易費用。

12.4 WEB3.0社群平台(FinBox)

FinBox是一個去中心化的即時通訊和內容社交平台，是AUT公鏈支援的首個WEB3.0社群平台。
FinBox可以在APP中一鍵連接錢包、匯入和建立新的錢包ID和AUT SBT，並加入FinBox的社群網路。

即時通訊：用戶可以使用錢包ID登錄，與其他用戶聊天並發送訊息。

社群功能：使用者可以建立個人資料、發布狀態和圖片，並追蹤其他使用者。

錢包連接：用戶可以連接自己的數位錢包，以便在平台上進行交易和轉帳。

AUT NFT支援：FinBox將支援AUT公鏈上的NFT，並允許用戶購買、交易和展示自己的NFT。

FinBox透過以下技術實現WEB3.0去中心化聯網：

1）區塊鏈技術：利用AUT公鏈支援FinBox的加密貨幣交易與NFT功能。

2）IPFS：使用IPFS作為檔案儲存和傳輸的協議，確保分散式網路中資料的安全可靠。

3）加密技術：使用加密技術保證使用者聊天、交易和資料儲存的安全。

12.5 FinSOUL下一代GameFi

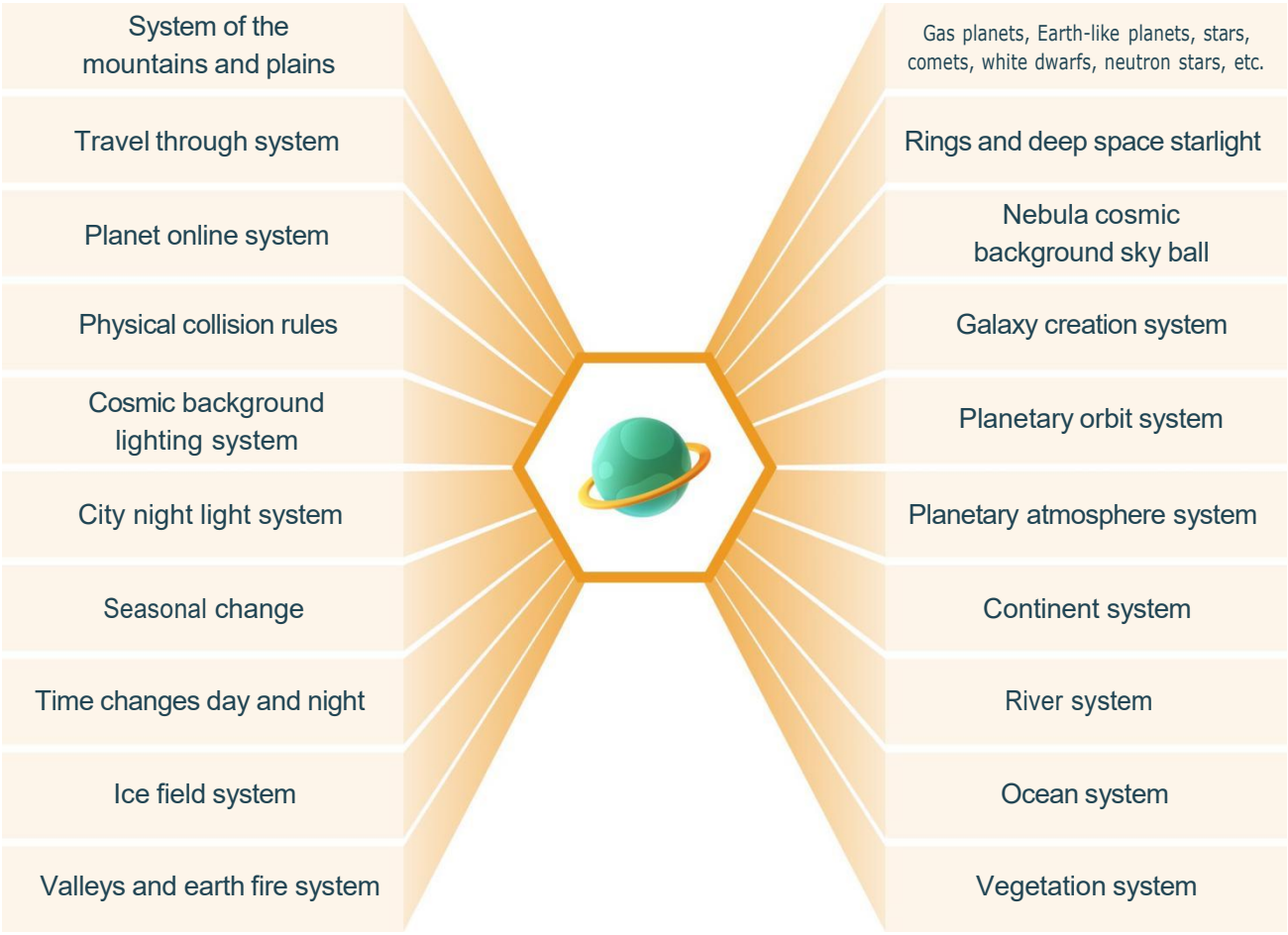
FinSOUL是集共創AIGameFi、可程式化NFT、元宇宙DeFi於一體的鉅作創新力作，目前尚無直接對標產品，可以理解為元宇宙2.0的先鋒專案。

2021年被稱為元宇宙元年，但在AUT團隊看來，先前的項目更多的是炒作和市值操作，因為概念領先於技術，大部分項目的核心依然只是傳統遊戲，一些鏈改項目也不過是一層WEB3.0的噱頭，離理想的元宇宙還相去甚遠。

AUT團隊將基於雙股基因，開發出有靈魂、有吸引力、有價值感的元宇宙2.0世界FinSOUL。

FinSOUL基於一個接入ChatGPT核心的可編程NFT星球，每個玩家都可以在其中創建獨一無二的AI夥伴，與更多玩家一起體驗波瀾壯闊的星際冒險，並在冒險過程中收穫頹廢的SOUL代幣。
FinSOUL基於虛幻引擎5開發，每個玩家先透過治理代幣鑄造自己的AI夥伴和NFT星球，然後進入元宇宙市場玩各種免費或付費遊戲副本，購買各種遊戲NFT資產。

使用者可以根據自己的喜好對夥伴的性別、外貌、妝容、體型、服飾、技能等數百項參數進行精細定制，並在經過針對性訓練的ChatGPT-NPC感知庫中匹配夥伴的性格和行為，然後與夥伴共同探討打造玩家的NFT星球，可製定的範圍包括但不限於：



FinSOUL將向業界開放遊戲編輯器和API，讓全球創意團隊可以開發各種沙盒世界玩法和FinSOUL宏大宇宙的複製品，競技不僅限於多人遊戲，還有旅行體驗、社交、MMORPG、槍戰、空戰、動作冒險、星際貿易、星際殖民、城市建設、模擬經營、競猜遊戲...

這是一個真正具有持久生命力的元宇宙，也許有一天，FinSOUL會成為我們的第二人生。

13. 差異化核心競爭力總結

13.1 技術能力分析

	Bitcoin	Ethereum	BSC	AUTHERIUM	AVAX	Solana	Polkadot
Two Chains Structure	No	No	No	Yes	No	No	No
Modular Parallel Chain	No	No	No	Yes	不	不	不
閃光 平行線 跨鏈	不	不	不	是的	不	不	不
可擴展性	低的	低的	高的	高的	高的	高的	中等的
去中心化	高的	高的	高的	高的	中等的	中等的	高的
安全	高的	高的	中等的	高的	中等的	中等的	高的
實際的 TPS	7	18	100	主鏈7500金融鏈彈性沒有 限制	4500	2900	400
交易確認 時間	30-60分鐘	5分鐘	75秒	3秒	3秒	1秒	30秒
平均的 氣體 費用	12 美元	3 美元	0.01 美元	0.0001 美元	0.001 美元	0.0001 美元	0.15 美元
合約開發語言	/	堅固性	松露 索爾克	JAVA/GO/Solidity ETC	堅固性 去	鏽	鏽
類型	第1層	第1層	第1層	第1層	第1層	第1層	Sharding
Energy Efficiency	No	No	Yes	Yes	Yes	Yes	Yes

13.2 財務預測

AUTHERIUM的收入來源如下：

1）超級節點挖礦獲得的AUT

2）鏈上交易消耗的Gas費用利潤3）FUSD質押發行利息4）FinEX交易撮合佣金5）FinBox社群平台廣告收入

同時產生以下成本費用：

1）節點營運成本2）行銷營運成本3）風險準備金成本

4）公鏈技術開發維護成本

AUT公鏈用戶數量目前在千萬級，預計最終將達到數億級。

AUT公鏈在加密貨幣市場的份額將從零到數十億美元，預計最終將達到數百億美元。

假設市場規模為ETH的十分之一，利潤率為30%，PE為30倍，財務預測表如下：

Year	Revenue (USD million)	Profit (USD million)	Growth rate	Total market capitalization (USD billion)
2024	300	90	300%	9
2025	900	270	300%	27
2026	2700	810	300%	81

我們預計AUTHERIUM 的總市值將在2026年達到810 億美元。

14. 發展路線圖

2020年1月核心團隊成立大會。

2020年2月由史丹佛大學畢業生Bob Lambert和William Thompson以及他們的好友Bruce等共同創立於2019年。

2022年1月全新的HyBriid安全技術問世。

2022年12月HyBriid技術的突破，讓AUT團隊榮獲泛美區塊鏈高峰會DeFi技術貢獻獎。

2023年3月在摩根士丹利副總裁Jorge的撮合下，兩家公司完成簽約程序，準備成立新公司。AUT團隊聲名鵲起，受到市場廣泛關注。

2023年4月由摩根大通注資，DF提供技術，摩根DF AUT正式成立。

2023年5-6月AUT公開徵集全球各大金融公司及機構作為監管節點，包括華盛頓Coin Center、加州BitGive、澳洲Cryptos、新加坡LinkCove等100個平台，共同守護用戶資金安全，將風險係數無限接近於零。

2023年6-7月AUT舉辦特別訂閱合作夥伴活動，邀請100位合作夥伴訂閱者見證AUT的輝煌。

2023年7月AUT正式上線。

2023年8月發放100萬美元金融優惠券，惠及全球更多用戶。

2023年9月AUT逐步建立全球社區服務中心，為各國社區舉辦會議及市場發表會。

2023年10月AUT成立專門基金會，培養區塊鏈相關領域的技術人才，舉辦黑客馬拉松，獎勵幫助優化AUT安全性、研發創新安全技術的團隊。

2023年11月AUT在全球進行路演及發表會，包括矽谷、倫敦、多倫多，以及新加坡、吉隆坡、東京、首爾、香港、澳門等亞太重點城市。

2023年12月HyBriid 2.0智能合約協議升級，支援大部分主流幣種借貸，最高支持5倍槓桿借貸，提升資金利用率。

2024年1月為累積大量用戶數據，持續提升金融公鏈效能，回饋參與者，AUT為社群用戶提供了為期6個月公鏈內測參與機會，讓用戶不僅能搶先體驗AUT金融公鏈的功能與便利性，還能在未來的加密世界站穩腳步，實現資產收益最大化。

2024年1月中東王室注資10億美元入股18%，公司開始重組，王室資金支持加速上市進程。

2024年2月原Morgan DF AUT LLC完成重組為AUT LLC，William Thompson擔任董事長。

2024年2月-6月計畫與富國銀行、匯豐銀行、花旗銀行、高盛等跨國銀行進行深入談判，為華爾街的重要資本搭建橋樑，無縫銜接傳統中心化金融與去中心化金融，讓區塊鏈金融市場更加成熟。

2024年6月AUTHERIUM（AUT）全球上線。

2024年6月-12月AUT全力與第三世界國家企業及商家建立策略夥伴關係，承擔社會責任，利用區塊鏈協助其追趕。

2024年底Finton社區用戶將達到1億規模的里程碑，覆蓋全球100多個國家和數千個城市，實現AUT合作共贏的願景。

2025-2026年AUT走向全球，全球用戶量突破數億，並在納斯達克上市，成為全球引爆區塊鏈金融的獨角獸。

15. 參考附錄

AUT是一條集區塊鏈前沿技術於一體的超級公鏈，在金融領域的核心應用上有著不可取代的優勢。我們非常感謝業界先行者和精英們用智慧的探索。在此附錄獻給為產業發展與AUT技術架構做出過巨大貢獻的專家學者：

A Proof-of-Work Parallel-Chain Architecture for Massive Throughput
https://neironix.io/documents/whitepaper/6793/chainweb-v15.pdf

會議記錄 的 這 2018年 國際的 座談會 在 溝通 工程 & 電腦 科學https://www.atlantis-press.com/proceedings/cecs-18/25902503

實用拜占庭容錯https://pmg.csail.mit.edu/papers/osdi99.pdf

複製理論與實務https://link.springer.com/book/10.1007/978-3-642-11294-2#toc

區塊鏈的耐攻擊協議演算法https://ieeexplore.ieee.org/abstract/document/8639577

互動式證明系統的知識複雜性
https://dl.acm.org/doi/abs/10.1145/3335741.3335750

Pinocchio：近乎實用的可驗證計算https://dl.acm.org/doi/abs/10.1145/2856449

沒有廢話的樣子 在 L1 表現
https://medium.com/dragonfly-research/the-amm-test-a-no-bs-look-at-l1-performance-4c8c2129d581

在 這 尺寸 的 基於配對 非互動式 參數
https://link.springer.com/chapter/10.1007/978-3-662-49896-5_11

Bulletproofs：機密交易等的簡短證明 https://eprint.iacr.org/2017/1066.pdf

可擴展，透明的，和 後量子 安全的 計算性的 誠信
https://eprint.iacr.org/2018/046

P2PTradeX：加密貨幣之間的 P2P 交易
https://bitcointalk.org/index.php?topic=91843.0

Alt 鏈與原子傳輸
https://bitcointalk.org/index.php?topic=193281.msg2003765#msg2003765

Solidity 0.8.18 文件https://docs.soliditylang.org/en/v0.8.18/

比特幣：A 點對點 電子的 現金 系統https://bitcoin.org/bitcoin.pdf

原子跨鏈互換https://dl.acm.org/doi/abs/10.1145/3212734.3212736

去中心化金融作為加密貨幣市場子行業的現狀回顧
https://static1.squarespace.com/static/553d790de4b08ceb08ab88fd/t/5f5c2a4d381d4c58ce97cde2/1599875 662625/DeFi_P2_SciPaper_3.

A 新一代 聰明的 合約 和 去中心化 應用 平台。
https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

A 民調 的 區塊鏈 從 這 觀點 的 應用、挑戰和 機會https://ieeexplore.ieee.org/abstract/document/8805074

值得信賴 和 有擔保 電子投票 選舉 系統 基於 在 堵塞 鏈 技術

https://link.springer.com/chapter/10.1007/978-3-030-43192-1_9

金融 和 經濟學 討論 系列
https://www.federalreserve.gov/econres/feds/decentralized-finance-defi-transformative-pottial-and-linked-risks.htm

Bidl：資料中心網路的高吞吐量、低延遲許可區塊鏈框架https://dl.acm.org/doi/10.1145/3477132.3483574

股權證明（權益證明）
https://ethereum.org/en/developers/docs/consensus-mechanism/pos/

使用分片解決區塊鏈中的可擴展性和儲存問題https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3446547

固定 股權證明 區塊鏈 協議
https://link.springer.com/chapter/10.1007/978-3-319-67816-0_17

以太坊生態系的初步證據https://www.nber.org/papers/w30949