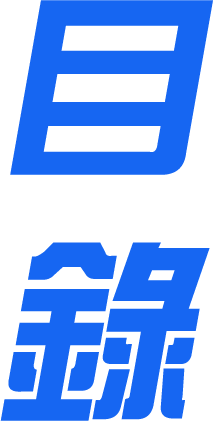


*前言*

*介紹*

*Zorro概述*

*Zorro理念*

*Zorro設計理念*

*Zorro價值觀*

*技術框架*

*Zorro模型*

*可信分佈式計算平臺（可拓展性）*

*Zorro架構*

*共識協議*

*多鏈並行模型*

*價值*

*Zorro優勢*

*Zorro發展*

*Zorro初衷*

*Zorro可拓展性*

*核心*

*區塊鏈基礎設施*

*商業化落地*

***Token分配***

***團隊***

***路線圖***

***免責聲明***

*價值網路*

*生態模型*

*Zorro生態圈*

*Zorro生態主推*

前言

2020年，危機四伏的一年，全球都陷入動盪與不安。澳大利亞大火，東非南亞蝗災，全球新冠疫情，美股熔斷，東京奧運會停辦，歐盟全境“鎖國”，第三世界國家外貿陷入困境，讓本已岌岌可危的經濟形勢，進一步惡化。“股神”巴菲特表示，經濟危機不是即將到來，而是已然降臨；唯一懸念在於，經濟崩壞程度是否能超越1929年的金融危機。

危機面前，各國紛紛自救。美國、日本、香港紛紛上馬大規模現金分發計畫刺激消費，20國集團線上峰會更就5萬億美元經濟激勵計畫達成共識；曾經打著協作、自由、共用、反壟斷的互聯網巨頭，為了自己的商業利益，成為了新的更大壟斷者，壟斷了本該屬於用戶自己的數據。並將這些數據封閉在自己的平臺中，形成一個個的數據孤島，甚至用這些數據來操縱傷害用戶，每一個服務商通過封閉的中心化帳戶體系，增加用戶遷移難度和成本，把用戶死死地鎖定在自己平臺上。

每個人都嚮往一個更加智能、更加公平、更有希望的未來。

我們希望條塊分割的數據能夠被打通，而不是把數據分散在不同的地方，存在大量的冗餘和矛盾，浪費了大量的資源卻形成不了整體合力。

我們希望人與人之間能夠更加信任地進行協作，而不是相互構陷，勾心鬥角、爾虞我詐。

我們希望有一個去中心化的可信平臺為世界提供安全優質的服務，而不需要花費大量時間去選擇比較。

我們希望這個世界更加開放包容，讓每個角色都能夠被平等對待，在這個世界上都有一席之地，有尊嚴地活著。

我們希望未來的規則能夠統一公開透明、數據資訊能夠更加可信、價值能夠更加充分流通、信用能夠在更大範圍內傳遞。

覆巢之下，焉有完卵。災情面前，受害最深的，不是達官貴人，不是富商巨賈，而是黎民百姓，經濟崩壞導致大範圍失業，無限制的量化寬鬆勢必引發嚴重的通貨膨脹，銀行收緊貸款額度浪潮即將來臨。我們這代人很難想像巴菲特所說的“史無前例的1929年”是什麼光景，但此刻卻很可能是我們要面臨的最艱難的歲月。

財富上的損失只是其次，最讓人痛心的是，為了度過這一艱難歲月，我們要在未來很長一段日子裏，背負著沉重的財務乃至債務壓力，不斷地為溫飽而奔波，不再有任何眺望詩與遠方的自由。

什麼是自由？巴爾扎克說：“一個有思想的人才是真正力量無邊的人”。泰戈爾遊歷八方，飽嘗世間百態，最終在不朽的《飛鳥集——新月集》中寫到：“弓在箭要射出之前，低聲對箭說道——你的自由就是我的自由。”因為他知道，如果努力不是為了自由而戰，那麼我們所有的努力都不過在鞏固我們頸項上的枷鎖；薩迪也在《薔薇園》中寫到“即使鳳凰從此在世界上絕跡，人們也不願在貓頭鷹的影子下麵棲息。”任何的成功如果不能用自由加冕，都不過是鏡花水月。因此，斯特林貝格在《戲劇選》中振臂高呼：“到光明中去尋找自由是一個人的義務!”

我們只是平平眾生，但我們也有不為五鬥米折腰的渴求，也有追尋屬於我們平反的自由的天賦人權！

遺憾的是，自由雖是天賦人權，其實現卻避不開荊棘之路甚至“鐵與血”，裏斯科夫就在《大堂神父》中寫到，“自由不是恩賜的，要爭取。”在這個為自由而奮鬥的風暴即將席捲而來的十字路口，我們何其希望，能有一位蒙面黑俠從天而降，路見不平亮劍挺身，警惡懲奸，鋤強扶弱，加快全人類同享自由偉大願景的到來。

“俠之大者，天下大同”，Zorro公鏈正是有感於西方傳說裏的正義蒙面黑俠佐羅（Zorro）的光輝想像以及寶貴的精神傳承，致力於通過尺度的公允、財富與創作的自由，全方位解放用戶群體乃至全人類的靈魂。

“The fate of all is always dust”，但自由的靈魂除外。



介紹

1、Zorro概述

Zorro深耕去中心化、分佈式記賬等核心技術，實現面向全球行業組織間的全新電子互信體系，並首先將這一體系應用在實體商品的全球貿易中，優先在國際貿易行業進行落地實踐。Zorro將秉承開放共贏的原則，打造區塊鏈世界的數字貨幣支付系統，推動智能支付的發展。Zorro還將打造涵蓋各種生態應用的公有鏈以及鏈接各個企業聯盟的私有鏈，並利用Zorro Token(ZRO)打通各聯盟、各行業、各用戶之間的鴻溝，解決目前支付行業的眾多痛點問題，是國際區塊鏈最新頂級架構理念指導下的一個具有全球性應用場景和雄偉理想藍圖的區塊鏈專案。

Zorro希望，能夠通過將經濟社會萬物的全面數位化上鏈、數位化確權、數位化交易與投資並基於區塊鏈技術分佈式存儲、資訊不可篡改等優異性能，實現所有經濟活動的真正公平、公正、公開，杜絕任何的不合理剝削現象以及對個人價值的無理剝奪，打造一個沒有營私舞弊空間的全新社會，讓全人類都能夠在其中暢享財富自由、創作自由、價值自由與思想自由！

2、Zorro理念

2.1 用信任鏈接與驅動世界

不論世界如何發展演進，“信任是剛需，共識是基石，合作是動力”的主旋律不會改變。Zorro為最大範圍的信任、共識和協作而生，作為能夠支撐起海量應用和用戶的區塊鏈基礎設施，面向大規模的商業應用，提供便捷友好、高效安全的開發部署環境，讓萬事萬物都能夠輕鬆上鏈，打造鏈接一切、協同世界的分佈式商業新生態，用信任鏈接和驅動世界。

2.2 構建智能進化生態

比特幣的發展和演進過程，讓我們看到一群平凡的人可以做一個不平凡事業的底層邏輯，讓我們看到組織基業長青、跨越不連續性的可能性。Zorro將探索打開組織邊界的方式，激勵和吸引越來越多的成員參與其中，高效協同、形成合力。構建一個良性發展的生態圈，能夠不斷向前迭代、自我進化，通過持續引入“負熵”破解熱力學第二定律的“熵死”問題，成為真正去中心化的智能進化生態，具有強大的反脆弱性，在持續演進的過程中，不斷地破繭成蝶，直到永恆。

3、Zorro設計理念

通過觀察過去十年中加密貨幣的發展，我們發現去中心化的想法並不新鮮，有理由認為，Zorro是有能力打造一個完整的生態、一個全新的次元；我們相信Zorro不但承載著一種貨幣或一個產業，還能夠為全世界帶來真正、全面的公平、公正與公開，讓每一個參與者都能夠享受私隱、財富與思想的全方位自由。

但是上述願景的實現，需要每一個Zorro用戶的共同支持。信仰無價，但信仰本身吸引力並不充足。我們不但要創造公平、公正的環境，更要用鐵一般的事實去給普羅大眾展示，絕對的公平與公正能為他們帶來什麼。因此為實現Zorro的願景，就有必要去為用戶提供持續性的有利可圖的機制，從而讓他們自發地參與到Zorro業務網路的搭建中。

從金融市場基礎邏輯的角度出發，Zorro認為任何商品的價格，都與流入市場的現金流成正比，而與當時市場可交易總數成反比。因此只要能夠開啟平臺的裂變迴圈，就能為平臺注入龐大的現金流，實現平臺規模的擴張與用戶的持續獲益；同時為進一步提升用戶的參與積極性，Zorro還將設立嚴密的機制，對為平臺發展做出突出貢獻的用戶進行額外的獎勵，尤其是輕節點、超級節點的參與者們，從而充分彰顯平臺的公平與公正。

隨著Zorro價值的不斷提升，大量用戶將會參與到Zorro網路的擴張中。為提升用戶對平臺的忠誠度，同時也是為了不浪費龐大用戶量所天然蘊藏的巨大價值，Zorro將會進一步開發注入去中心社交、去中心交易所、去中心城市生活功能等諸多應用板塊，不但為平臺注入全新活力，也能為用戶帶來巨大的便利。

在Zorro收益驅動與大量用戶的共同作用下，Zorro網路將會迅速在全球鋪開，讓公平與公正的種子在全世界的每一個角落生根發芽，為實現“給全人類帶來自由”這一宏偉願景提供最有力的保障。

無數先賢曾為追求自由顛簸半生，拋頭顱，灑熱血，但從未有一人真正得償所願；我們並不比先賢偉大，但是時代賦予了我們先賢從未擁有的工具。Zorro，必將成為全人類追求自由歷史上最高，也是最後一座里程碑。

因為此碑之後，再無束縛。

4、Zorro價值觀

***公正、平等、自由***



技術框架

1、Zorro模型

為了理解區塊鏈本質，首先定義基於交易的區塊鏈模型，量化安全性、一致性、去中心化等參數指標，並提出相關的函數，構建可量化分析的區塊鏈模型。

區塊鏈系統Ω由五個部分組成，包括：f是共識函數、V是節點集合、T是交易數據集合、S是消息集合、B是區塊集合。區塊鏈系統是指，節點集合V通過共識函數f把不斷產生的交易數據集合T寫成區塊集合B，並產生消息集合S的系統。共識函數f包括消息共識函數fs和區塊共識函數fb，是由系統決定的。節點集合V隨著時間而變化。t表示當前的時間，Vt表示t時刻系統Ω的節點集合，Vt−in表示t到t+1時刻新加入系統Ω的節點集合，Vt−out表示t到t+1時刻退出系統Ω的節點集合，那麼：



交易數據集合T:={Tv|v∈V}隨著時間變化。對任意v∈Vt∩Vt+1，Ttv表示t時刻v尚未處理的交易集合，Tt−inv表示t到t+1時刻v收到的消息集合，Tt−outv表示t到t+1時刻被處理的交易集合：

Tt+1v=Ttv+Tt−inv−Tt−outv

下麵先從理論角度來闡述區塊鏈，從基本模型出發來分析，再談系統模型的構建，然後是具體演算法機制的設計實現。希望通過體系的、由簡入繁的、抽絲剝繭的方式，更加清晰的描述區塊鏈的技術邏輯、發展路線、本質、優點和缺點，體現Zorro技術的先進性、蘊含的魅力和無窮的潛力。

消息集合S:={Sv|v∈V}隨著時間變化。對任意v,u∈Vt∩Vt+1，Stv表示t時刻v的消息集合，Stv,u表示t時刻到t+1時刻v從u收到的消息集合，St−out表示t+1時刻之後不再影響共識函數f的消息集合，那麼：

St+1v=Stv+Stv,u−St−outv+Ttv

同時由消息共識函數生成t+1時刻v向u發出的消息集合Mt+1u,v=fs(Stv,Btv,u)。

區塊集合B:={Bv|v∈V}隨著時間變化。對任意節點v∈Vt∩Vt+1，Btv表示t時刻v確認的區塊集合，且Btv滿足鏈式結構。區塊共識函數生成t+1時刻v的區塊集合為：

Bt+1v=fb(Stv,Btv)

消息集合S:={Sv|v∈V}隨著時間變化。對任意v,u∈Vt∩Vt+1，Stv表示t時刻v的消息集合，Stv,u表示t時刻到t+1時刻v從u收到的消息集合，St−out表示t+1時刻之後不再影響共識函數f的消息集合，那麼：

St+1v=Stv+Stv,u−St−outv+Ttv

同時由消息共識函數生成t+1時刻v向u發出的消息集合Mt+1u,v=fs(Stv,Btv,u)。

區塊集合B:={Bv|v∈V}隨著時間變化。對任意節點v∈Vt∩Vt+1，Btv表示t時刻v確認的區塊集合，且Btv滿足鏈式結構。區塊共識函數生成t+1時刻v的區塊集合為：

Bt+1v=fb(Stv,Btv)

1.1 共識演算法的去中心化

區塊鏈系統的去中心化體現在多個層面，其中的關鍵是共識的去中心化。共識去中心化是區塊鏈系統與傳統互聯網系統最重要的區別，也是決定區塊鏈的民主性安全性的重要因素。

評判一個共識協議是否去中心化，是一個見仁見智的問題，現在沒有一個被廣泛認可的標準。去中心化的主要目的有兩個：系統的結構分散，使其不會因為少數節點的掉線、叛變或遭受攻擊而失效；共識由系統參與者共同完成，這種民主性增加了系統的透明度和可信度，避免系統被寡頭控制。

每個參與者在系統中應該有多少發言權需要考慮兩個方面：中心化可能性、公平性。

區塊鏈是一個去中心化的系統，任何一個節點都可能成為階段性的中心，但不具備強制性的中心控制功能。首先，系統需要根據節點v的計算能力、系統貢獻度或是網路傳輸能力賦予其權值wv。一個公平合理的權值評價體系，可以激勵系統的運行，提高合作效率，增強系統性能，促進生態發展。例如，在工作量證明機制（Proof of Work, PoW）中wv就是v所擁有的算力比例，在權益證明機制（Proof of Stake, PoS）中，wv就是v所擁有的代幣比例。我們用：

W(U):=wv

表示節點集合U在系統中的權值和。

在區塊鏈系統運行過程中，系統中的節點可以從打包交易、生成區塊，或其他過程中獲利。節點v在系統中的權力av定義為v的期望的獲利比例。在一個完全去中心化的系統中，每個節點的權力和他的權值是相符的，那麼系統Ω的中心化程度σ可以定義為：

σ:=|av−wv|

系統Ω的σ值越低，說明系統去中心化程度越高。

1.2 系統安全性與一致性

區塊鏈是一個去中心化系統，沒有一個中心節點來維護區塊集合B。共識函數f的設計使不同節點之間維護區塊集合是同一個，從而達成一致性。然而系統中可能存在節點v，它不按照共識函數f，故意給u發送錯誤消息Mt+1v,∗≠fs(Stv,Btv,u)，從而影響其他節點的操作和全網的一致性，我們稱這樣的節點為壞節點。壞節點集合：

Ht=v∈Vt|∃u∈Vts.t.Mt+1v,u≠fs(Stv,Btv,u)

如果在任意時刻t，滿足W(Ht)≤η⋅W(Vt)，我們稱系統Ω的滿足容錯參數η，這裏W是節點權值函數（見4.1.1）。給錯參數η，我們定義在時刻t的有效節點集合：

Utη=argmaxU⊆Vt|W(U)≥（1−η)W(Vt){|∩v∈UBtv|}

和系統區塊集合Btη=∩v∈UtηBtv。如果在任意時刻t，任意區塊b∈Btη都滿足：

∀k≥t+τPr[b∈Bkη]≥1−2−c

我們稱系統Ω的滿足確認參數τ，這裏c是給定的一個常數。給定參數η，定義τ(η)為系統能滿足的最小的確認參數。分佈式系統中的一致性包括：強一致性（τ=0），弱一致性（τ≤τ∗），最終一致性（τ<∞）。在區塊鏈系統中，由於網路延遲和共識等因素，無法保證任意時刻全網節點數據的強一致性，只能退而追求弱一致性。給定確認參數τ∗，對於某個容錯參數η，如果系統Ω滿足確認參數τ∗，我們稱系統Ω滿足一致性。這樣我們把系統Ω安全性ζ定義為能滿足確認參數τ∗的最大容錯參數η，即：

ζ=max0≤η≤1ηs.t.τη≤τ∗

1.3 系統性能

區塊鏈系統的性能主要體現在系統確認交易所需的時間，一般用兩個參數刻畫：確認時間（只有一筆交易時需要的時間）和吞吐量（單位時間內確認交易的最大數目）。確認時間是用戶進行一筆交易的最短週期，如果一個系統的確認時間很長（例如比特幣需要大約1小時），會造成用戶體驗不佳，限制系統的應用場景。如果吞吐量太小，不足以處理所有交易請求，就會有一些交易被堵塞或丟棄，造成整個系統的延遲提高。

更一般地，給定一個交易集合T，定義d(T)為T中全部交易被確認所需要的等待時間（delay），該時間的期望值：

D(T):=𝔼[d(T)]

反映了系統處理T中交易的能力；這裏取期望值是為了反映系統和環境的隨機性。當T中只包含一個交易，D(T)即為系統的確認時間。當T中包含很多交易，D(T)可以反映出系統的吞吐量；和吞吐量這種單一指標不同，對於同樣大小的集合T，D(T)可能會根據T中包含的具體交易而改變（甚至劇烈變化）。

對性能的討論只有在系統具有足夠的一致性和去中心化時才有意義。因此，提高性能的問題就是在保證系統的中心化程度σ≤σ∗和安全性ζ≥ζ∗的前提下（其中σ∗和ζ∗是系統常數）對函數D進行優化。這裏的定義允許我們考慮實際應用中的交易模式，並針對性地進行分析和優化。

在一個區塊鏈系統確認一筆交易，需要保證所有參與者的共識。為了優化性能，應該改進共識演算法的計算複雜度和通訊複雜度。

經典的PoW共識機制，要求節點進行大量的額外運算來爭取打包的許可權，在保證系統的安全和穩定的同時也極大地增加了計算複雜度。後來提出的PoS、DPoS和它們的一些變種，避免了PoW的額外開支，但節點仍然需要進行驗證和簽名，而智能合約也增加了處理交易所需的運算量，並且這些運算是無法避免的。

共識演算法的通訊複雜度，分為兩個部分：共識的參與者需要先達成共識，然後廣播到全網的所有全節點。為了在去中心化的前提下實現安全性，即允許網路中存在一定數量的惡意節點，每筆交易被確認之前要得到一定數量節點的驗證，這需要所有共識節點都收到該交易。廣播可以在達成共識後進行，不會影響確認速度，但如果網路中有很多全節點，廣播需要的帶寬和時間可能會影響網路的性能。

1.4 高效共識機制

對一個交易集合T，全部交易被確認所需要的等待時間為：

dT=hdcompT,dcommT,dempoTσ≤σ∗,ζ≥ζ∗

其中dcomp表示共識計算的延遲，dcomm表示共識通訊的延遲，dempo表示共識許可權分配的延遲，σ,ζ表示系統的去中心化程度和安全性，σ∗,ζ∗為系統常數。為了提高共識機制的效率，需要對性能函數中的dcomp,dcomm,dempo進行優化。

1、dempo

dempo主要由共識許可權的分配方式決定。現有的區塊鏈系統中，分配共識許可權的方法主要包括：基於算力分配（PoW）、基於股權分配（PoS、DPoS）、基於身份認證分配等等。

基於算力分配共識許可權的區塊鏈系統，為了保證系統的去中心化程度，使每個節點都可以獲得和它權利wv相匹配的影響力av，需要算力證明函數使Gwork(wv)=av，此時σ=0。但Gwork需要大量的計算，dempo較高；

基於股權分配共識許可權的區塊鏈系統，存在容易計算的股權證明函數Gstake滿足Gstake(wv)=av，此時σ=0，dempo較低；

基於身份認證分配共識許可權的區塊鏈系統，需要引入第三方的認證來保證影響力分配的公平公正，這種方式更適用於聯盟鏈類型的區塊鏈，並不適宜於基礎公鏈。

2、dcomm

主要由共識節點集合規模決定。在共識演算法不變的情況下，參與共識的節點集合越小，需要傳輸的數據量越低，dcomm越低。共識的節點集合大小受到系統安全性的限制。假設系統Ω的節點集合為V，Ω的安全性係數為ζ，共識過程由一個子系統Ωc完成，Ωc的節點集合為U，Ωc的安全性係數為ζU，Ωc中壞的節點的比例z。此時共識子系統Ωc安全的概率為：

Pr(z≤ζU)=ζ|V|i(1−ζ)|V||U|−i|V||U|

當|U|很小時，雖然dcomm很低，但對應的共識系統安全的概率也變得很低，整個系統可靠性下降。

為了保證系統安全性滿足ζ≥ζ∗，共識節點集合大小應滿足|U|≥k∗。

3、dcomp

dcomp主要由節點的計算性能決定。在共識演算法不變的情況下，參與共識的節點計算性能越高，完成共識所需的時間越短，dcomp越低。在共識過程中，節點v的計算性能為ev，節點v的影響力為av，那麼整個系統Ω的計算性能上限eΩ滿足：

eΩ≤

由這個公式可以看出，可以通過提高節點的影響力a或提高節點的計算性能e來提高系統的計算性能上限。

提高節點性能：當系統中影響力為a的節點平均計算性能提高了m倍，系統的計算能力上限提高了ma倍。雖然可以通過提高影響力節點的計算性能來提高系統計算性能的上限，但由於摩爾模型的限制，在一個性能需求快速增長的系統當中，單純通過提高節點計算性能無法滿足整個系統的性能要求。

提高節點影響力：傳統的單鏈系統中σv∈Vav=1，而通過多級分層的方式，m條分鏈同時運行，可以大大增加節點的影響力。假設節點v在第i條分鏈的權利為av,i，σv∈V,i∈[k]av,i=m，那麼：



即使在一個性能需求快速增長的系統當中，仍然可以通過增加分鏈的數目來滿足系統的性能要求，降低dcomp。

2、可信分佈式計算平臺（可拓展性）

從系統角度來說，區塊鏈是一個可信分佈式計算平臺，它可以充當共用計算資源。客戶可以將此平臺視為新一代計算設施。他們向其發送任何請求。當平臺收到請求時，首先檢查它的合法性，然後在某些節點上處理請求，並將結果返回給客戶端。通過該過程，數據和消息在平臺上傳輸，以分佈式方式管理計算節點和資源。特別的，一個有效的區塊鏈設計應具有以下屬性。

1、安全性(Safety)

所有結果是正確的。

2、活躍性(Liveness)

每個有效請求都會在一個固定（小）的時間內處理。在這裏，我們假設該平臺具有一個統一的可信介面，允許客戶端發送請求和接收結果。此外，還需要共識協議以確保在不同計算節點上運行相同的內容。

最相關的經典模型是狀態機複製機（state machine replication）。然而，與SMR模型（需要許可[9]）不同，區塊鏈平臺允許任何節點在無需獲得許可權許可的情況下加入。在無權限的設置中（permissionless），節點是不可信的，這引入了一個具有挑戰性的問題，也就是“女巫攻擊”。在“女巫攻擊”中，攻擊者能產生大量計算節點，然後可以輕鬆控制大多數計算節點以達成共識。為了防止女巫攻擊，一種常見的方法是使用工作量證明（POW）[8]或者權益證明（POS）。

在我們技術相關的白皮書中，描述了系統模型，從一致性、可靠性和安全性、可擴展性等面進行了定性分析，提出了一個分析區塊鏈系統可擴展性的框架。

吞吐量是一個重要的系統性能指標，它表示系統處理請求的能力。但是，這個指標還並不充分。當系統達到其處理瓶頸時，它必須丟棄客戶端請求的多餘請求，使系統的可用性降低。因此，我們需要有另一個性能指標來評估系統限制，即可擴展性（Scalability）。

區塊鏈可擴展性不只是表明當系統中計算節點的數量增加時，系統吞吐量可以單調增加。除此外，可擴展性還包括：

1、負載可擴展性，系統適應更重或更輕負載的能力；

2、功能可擴展性，通過添加新功能增強系統功能的能力；

3、更新可擴展性，通過使用新一代組件進行擴展的能力。

我們提出了一個分析區塊鏈系統可擴展性的框架，它類似於分佈式系統。給定系統的配置C，我們使用FC來評估系統的性能和成本：

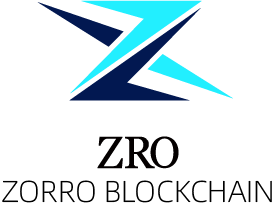
FC= F（T,S,Q）= T⋅Q/S

其中T和Q分別表示系統的吞吐量和服務品質。S表示系統總體成本，包括節點成本，網路帶寬成本等。對於區塊鏈，其Q主要由平均確認時間d和目標確認時間෠d決定。為了將Q標準化為（0,1）間隔，我們設置Q=然後當d→∞時Q=0，當d→0時Q=1

給定初始配置C，我們可以通過縮放因數k將系統的配置擴展到Ck。策略σ指定如何擴大配置。例如，當初始配置C具有n個節點，並且策略σ將節點數量增加k時，配置Ck中的節點數量等於k·n。然後，我們可以定量計算可擴展性：

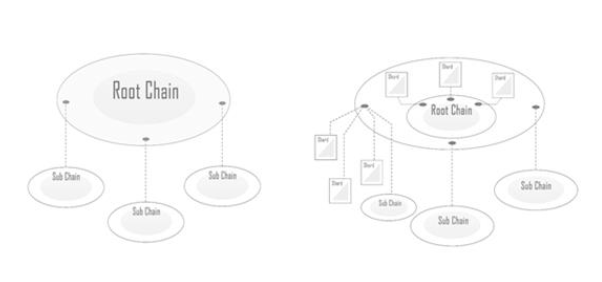
ψσ(k)=FCkFC

如果ψσ(k)等於1或隨k增加而單調增加，我們說系統在策略σ下具有完美的可擴展性。

3、Zorro架構

3.1 分層多級鏈結構

從實現的角度來看，我們的鏈結構是分層多級鏈結構。



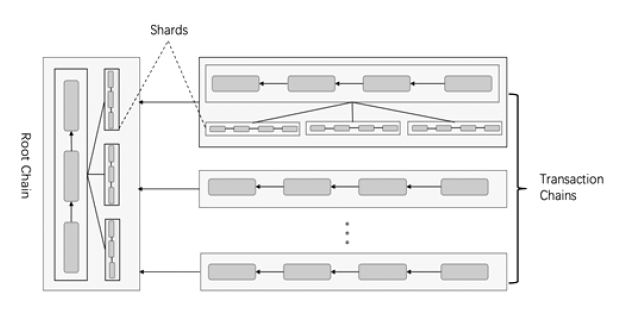
Zorro的鏈按功能分為主鏈和業務鏈兩種，每條鏈都是具有自己狀態的完整系統。主鏈充當整個系統的領導者和協調者，它作為業務鏈的切入點和信任來源，記錄每條業務鏈已確認區塊的元數據和摘要，產生所有鏈的委員會選舉中使用的隨機種子，並記錄選舉結果。同時，來自業務的工作負載由所有業務鏈共同承擔，並使用基於Actor模型的消息驅動協議進行合約並行計算。系統中的所有節點都保持主鏈的狀態，通過更新和驗證主鏈的區塊，節點可以驗證已經包括在主鏈中的業務鏈的任何區塊數據。該結構具備以下主要優點：

1、節點加入系統只需要從可信源獲取主鏈的當前狀態，或者從創世塊重建，並不需要同步整個系統的所有數據，這使得整個系統的負載大大降低。

2、每條鏈的共識是獨立和並行執行的，大大降低了對網路帶寬和計算處理要求。

3、主鏈可以充當系統的協調器，它提供跨鏈同步，並允許整個系統拓撲是動態調整的。

4、節點可以使用主鏈中的摘要和Merkle證明來驗證從另一個業務鏈發起的事務。因此，業務鏈的區塊生成者不需要來自其他業務鏈的任何資訊來處理鏈間交易。



我們可以按照不同的事務類型或商業主體，劃分出不同的業務鏈進行單獨運行。他們之間可以完全無關的獨立運行，通過主鏈提供的佐證進行跨鏈通信，也可以把有從屬關係的鏈組成有依賴的父子關係鏈，其中子鏈繼承部分父鏈的屬性，例如在這條鏈上的帳戶餘額的貨幣類型、鏈的選舉方式等。

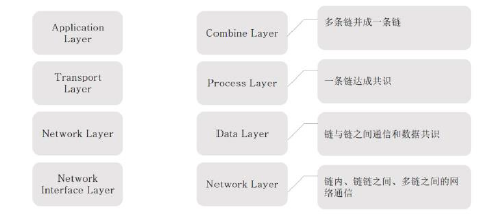
這種關係在邏輯上是相關的，對鏈的屬性以及網路連接產生直接影響，這使得兄弟鏈之間可以更容易的進行數據交換。Zorro的設計原則是允許每條業務鏈向下擴展自己的子鏈，但實際使用中，基本在三層以內都可以解決問題。

無論是主鏈還是業務鏈，都有可能因為請求過多而擁堵變慢。當發生擁堵時，可以通過將該鏈分片的方式，把請求分散到不同的分片上，以求提高該鏈的吞吐能力，隨著分片的數量增加，該鏈的吞吐量線性增加。分片本身也是一條獨立運行的鏈，分片之間會有針對跨分片交易請求的優化，大大提高分片鏈間的跨片交易執行速度。

這種分層多級的結構具有很好的靈活性和可擴展性，並且可以動態調整，因此每個鏈都不會成為整個網路的性能瓶頸。此外，隨著鏈的數量增加，整個系統的吞吐量線性增加，而不會產生太多的冗餘消息。

3.2 四層系統結構

基於上面的分層多級鏈結構，我們從系統角度設計了一種四層實現框架，以方便系統將來的可擴展和升級。



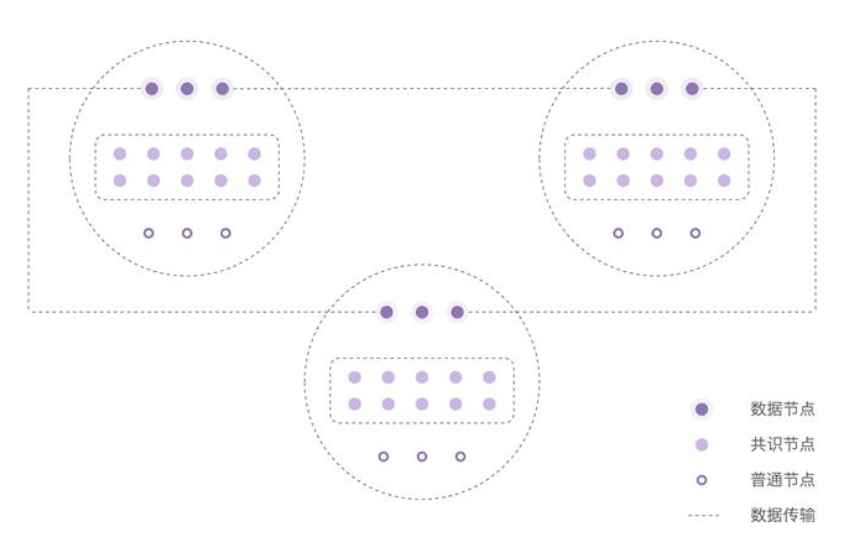
第一層是整合層，主要解決全系統總體共識，主要負責劃分請求和節點，並將不同的請求分配給特定的委員會進行處理。所有請求首先發送到整合層，在那裏它們將被分割並分配給不同的委員會進行並行處理。由於並非所有請求都可以並行處理，因此需要根據其類型進行劃分。此外，所有活動節點都在整合層註冊。這些節點以隨機方式被劃分到不同的委員會，並被分配不同的請求。我們需要確保每個委員會都是可信的，即每個委員會內部的惡意節點比例不會超過系統設定的某個閾值。

第二層是處理層，主要解決單鏈共識問題，需要處理分配的請求並生成日誌。每個委員會包含一組節點，當委員會收到給定請求時，它需要處理請求，達成共識並生成日誌。由於每個委員會的可信度由上層保證，因此該層只需要考慮如何儘快在委員會中達成共識。

第三層是數據層，主要解決多鏈之間的共識，每個委員會生成的日誌和請求數據會根據特定的編碼方法進行聚合，以形成單一的日誌。系統的目標是每個節點生成一致的日誌。因此，需要聚合演算法來集成委員會中節點生成的所有日誌，並達到統一日誌。還需要編碼方法來減少每個節點的存儲。此外，由於節點會不時地加入和離開委員會，因此必須使來自數據層的相應數據進行同步。

第四層是網路層，主要解決不同屬性和任務節點之間的通信。該層是整個系統的基礎，為計算節點之間建立通信。在網路層內，我們可以構建一個多層網路，為每個委員會建立一個共識網路層。

4、共識協議

在Zorro系統中，每一條鏈中都存在三類節點：數據節點，共識節點，普通節點。數據節點負責其所在鏈全部數據的存儲以及鏈與鏈之間資訊的交互，共識節點的主要職責為所在鏈的運算、打包以及共識，普通節點則只是承載業務。下圖展示了多鏈間不同節點的的關係。

每次參與的共識節點是隨機分配的，他們會隨著時間的變化而不斷重新選拔。

4.1 委員會選拔

為了抵制對無權限系統的女巫攻擊，我們使用基於股權證明（PoS）的選舉演算法。

比特幣、以太坊等早期區塊鏈專案使用工作量證明共識（PoW）。共識參與者通過"挖礦"，即進行一些特定的複雜計算，競爭記賬的權力。挖礦需要消耗大量的電力、佔用大量的計算時間，但這些資源並沒有為提高系統的效率作出貢獻。事實上，由於確認一筆交易需要全網的大多數節點的接收和驗證，隨著節點數量的增加，在網路中廣播資訊所需要的時間也會增加，效率反而會降低。

此外，如果共識演算法要求每筆交易都要消耗每個參與者的帶寬、計算和存儲資源，系統的性能瓶頸取決於每一個維度中最弱的參與者。在這種情況下，要提高系統性能，只能要求參與共識的節點均為"超級節點"，反而形成了事實上的中心化。

因此，我們選擇了基於權益證明（PoS）的共識機制。在PoS機制中，共識參與者的記賬權取決於其擁有的資產。在我們的共識演算法中，共識參與者通過提交押金的形式證明自己的權益。系統通過隨機演算法，定期按照押金的比例選取一定數量的參與者組成委員會負責一段時間的出塊。

由於每次出塊只需要選出來的委員會成員參加，因此在多鏈系統中，每條鏈的委員會可以同時存在，相互獨立地運行。隨著網路中的節點數量增加，可以支持同時運行更多的子鏈，從而高效地利用節點的資源。

和PoW相比，PoS共識不需要挖礦，大大降低了參與共識的門檻和能源消耗，更有可能實現真正去中心化。另一方面，與DPoS固定的超級節點出塊不同，委員會由隨機的選舉產生，這既保證了公平性，又讓所有人都有權力參與出塊和獲得獎勵，也防止了超級節點壟斷可能產生的各種問題。和PoW類似，PoS演算法的安全性只需要假設大多數權益不屬於惡意攻擊者以及網路滿足弱同步性。

選擇演算法需要以下安全屬性。

假設所有參與者中誠實節點所占的股權比例為δ0，每次選舉中當選的委員會成員中至少δ1比例是誠實的。此外，演算法應該是公平的，因為每個參與者被選擇的概率（大致）與參與者所投入的股份數量成比例。

委員會成員應該是流動和不可預測的，以便對手不能通過腐蝕委員會成員來攻擊系統（假設腐敗的時間超過了委員會的壽命）。

在Zorro中，我們通過以下過程實現上述屬性。首先，在選舉之前，由於所有節點只監聽主鏈，所以當需要選擇下一個委員會時，子鏈必須在主鏈上發出信號。所有鏈的選舉都在主鏈上進行，通過主鏈上的摘要資訊，主鏈可以收集到各條鏈的選舉狀態，進行匯總發佈。同時，主鏈上會週期性地生成隨機種子，用以保障各條鏈選舉的隨機性。

願意參與共識的節點需要通過發送特殊類型的交易在主鏈上註冊。該交易還規定了股權金額，該金額將轉移到特定的股份帳戶並被凍結，直到該節點退出並撤回股權。

主鏈發佈選舉資訊後，共識參與者可以在主鏈上看到選舉資訊，使用對應的隨機種子和自己的私鑰計算一個可驗證隨機函數的值，以此決定自己是否被選中。當一個節點發現自己有權力加入某條鏈委員會，它會先加入這條鏈的網路，在其中發送自己的ID和可驗證隨機函數證明，這些資訊會被當前的委員會記錄。同時，新加入的委員會成員需要為參與共識進行準備，加入委員會的網路。他們還開始同步子鏈的狀態。接收到的區塊和狀態都可以使用主鏈上的摘要進行驗證。

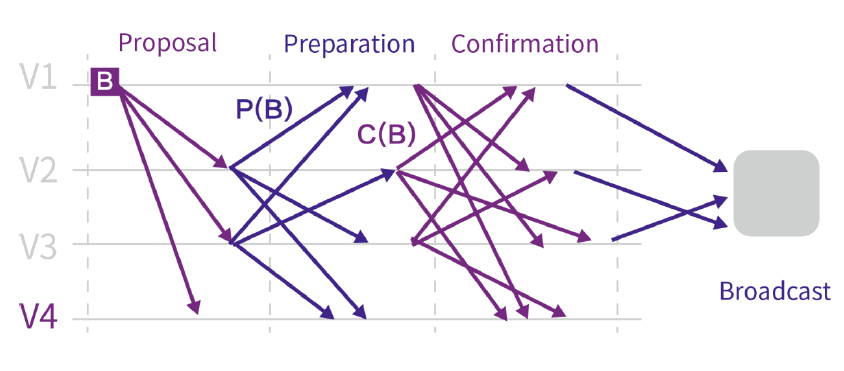
選舉產生的節點將建立一個小型共識網路，用於委員會內部的溝通。擁有專用網路可減少委員會成員之間點對點通信和廣播的延遲和帶寬消耗。另一方面，如果設置不當，網路可能不太穩定，更容易受到攻擊。需要確保網路拓撲是健壯的，並且使用加密安全地交換節點資訊。到下一個紀元開始時，新委員會應該生成新密鑰，同步並更新了鏈的當前狀態，在新的共識網路中建立了聯繫。

選舉的公平性對於系統的安全至關重要：如果攻擊者可以在一個委員會中佔據多數席位，這個委員會就沒有辦法正常出塊。一方面，為了保證隨機種子不能被操縱，每個隨機種子由委員會中的一組成員通過門限簽名生成：相比於由出塊者獨立生成隨機種子，這種方式大大增加了攻擊者預測後面的隨機種子以及阻止隨機種子生成的難度。另一方面，我們設計的激勵機制，使得誠實的委員會成員會願意記錄新的委員會成員，而不是通過破壞選舉來尋求保留自己的出塊權力。

4.2 委員會共識

我們假設委員會內部存在部分同步通信模型，其中存在有效的拜占庭容錯演算法，並為此設計量身定制的PBFT變體。委員會只占全網節點的一小部分，並且他們會自己組建一個規模更小的網路以降低廣播的延遲，因此得以穩定高效地出塊。由於PBFT演算法的性質，當委員會中的節點滿足弱同步假設時，在惡意節點不超過一半的情況下，出塊演算法就能安全地運行。因此，在選舉演算法安全的前提下，每個委員會出塊的活性、正確性和唯一性可以得到保證。此外，我們的押金和懲罰機制，使得委員會成員作惡需要付出很高的代價，由此鼓勵誠實的用戶不作惡並舉報其他人的惡意行為。

節點的執行可以以輪劃分。每輪包括三個階段：提案，準備和確認。



節點的執行可以以輪劃分。每輪包括三個階段：提案，準備和確認（如上圖）。狀態轉換是事件驅動的。為了在出現網路故障或惡意攻擊時保持系統活躍性，本地時鐘可能會觸發超時。

1、提案階段：委員會的負責人向其他委員會成員廣播擬議的議案。

2、準備階段：每個委員會成員收到建議的塊後，會廣播一條包含該塊的簽名的消息。如果在收到建議的塊之前觸發超時，則委員會成員簽署並向其他委員會成員廣播特別消息（表明領導者有缺陷）。

3、確認階段：在準備階段結束時，每個委員會成員簽署並廣播一份在準備階段收到的簽名。簽名聚合可用於顯著減少確認階段中的消息大小。

根據在確認階段收到的消息，每個委員會成員可以決定是否已達成關於該塊的協議，並廣播商定的區塊或空塊以及其決定的證據。

惡意節點懲罰。在檢測到明確行為不當的節點的情況下（例如，在同一階段向不同節點發送不同消息的節點），該輪將通過輸出空塊而中止。但是，行為不端的節點將受到大量的經濟懲罰，使得這種攻擊不可持續。

如果在準備階段收到的簽名數量意味著大多數誠實的委員會成員已收到相同的提議塊，委員會成員可能會達成“早期共識”：成員可以在確認階段之前使用簽名輸出該塊作為協議的證明（與常規協議相比的不同形式）。請注意，節點仍需要參與確認階段。

4.3 安全分析

設N是節點數，n是委員會中期望的節點數，m是委員會的數量。惡意節點的數量是λN。當委員會中的超過比例ρ的節點是惡意節點，我們說委員會選舉失敗。不失一般性，我們設置N=n·m。假設有一個完全隨機的oracle O:[N]→[m]。固定一個委員會，定義Ai成為委員會中惡意節點的比例i>ρ的事件。那麼對於每一個i∈[m]，我們都有



通過union bound，我們可以得到

Pr∪i∈[m]Ai≤m⋅PrAi

設定適當的參數設置，我們可以確保事件發生的概率是可以忽略不計。

5、多鏈並行模型

對於多鏈系統，當前單鏈系統的帳戶模型（例如，UTXO或者以太坊帳戶）不再適應新的需求，特別是在處理大量跨鏈操作時。我們設計了一種新的帳戶模型，它允許我們以非同步和無鎖的方式在多鏈系統上實現複雜的邏輯。在此模型中，我們將涉及到一組帳戶的交易以消息形式分離為多個步驟。每條消息都由唯一的主體接收，並由相應的鏈執行。最終執行所有消息就能實現交易。

5.1 通用並行模型

在並行計算中有很多機制，包括單機本地計算的，分佈式網路計算的，如加鎖等，但是這些對區塊鏈多鏈並行效果很差或者不適用。我們深入分析了Actor模型，由Hewitt等人[3]在1973年提出，這是一個處理併發計算的概念模型。它和很多場景結合，設計了新的並行應用，如部分電子郵件系統、Web服務和Java中帶有鎖的對象。

一個Actor指的是一個最基本的計算單元。它能接收一個消息並且基於其執行計算。它的重要特徵是Actor之間相互隔離，它們並不互相共用記憶體，每個維持一個私有的狀態，並且這個狀態不可能被另一個所改變。

在接收消息時，該計算單元可以同時：

1、向其他計算單元發送有限個消息;

2、創造有限個新的計算單元;

3、指定接收下一條消息時要使用的行為。

上述動作沒有假定的順序，它們可以並行執行。每個計算單元都可以接收來自其他計算單元的消息。消息以非同步方式發送給計算單元，每個計算單元按順序處理消息，對消息到達順序沒有限制。多個actor可以同時運行。

5.2 Zorro並行模型

我們設計一種基於Actor的並行模型作為我們的基本框架。在Zorro中，該結構主要包含以下資訊：

1、地址：區塊鏈帳戶的唯一識別字。

2、餘額：帳戶的當前餘額。

3、Nonce：標量值，等於從該地址發送的外部消息數。

4、代碼：處理消息的編程邏輯。

5、存儲：帳戶的內部狀態，可以為空。

每個帳戶都由私鑰控制。在代碼中，帳戶為其收到的消息定義了自己的處理方法，允許向其他帳戶發送消息，創建新帳戶並修改內部狀態。對於某些規範消息，每個帳戶都有相同的通用處理方法（例如“tran”和“add”）。每個帳戶還可以自定義其他消息的方法。

消息有兩種類型：外部消息（external message）和中繼消息（relay message）。外部消息由使用私鑰對其簽名的帳戶創建。中繼消息由在執行過程中執行send命令的帳戶產生，這有點類似於以太坊中的消息。最大的區別是中繼消息執行在我們的模型中是非同步的，在以太坊中是同步的。因此，我們模型中的這些消息支持跨鏈傳播。

Zorro中的消息主要包含以下資訊：

1、發件人：消息發送人地址。

2、收件人：消息接收人地址。

3、Nonce：標量值等於發送方發送的外部消息數，對於中繼消息為空。

4、輸入：指定消息調用的輸入數據組。

5、驗證數據：標識發送者外部消息的簽名，或中繼消息的證明。

對於外部消息，可以通過簽名和nonce進行驗證。對於中繼消息，它可以通過證明進行驗證。

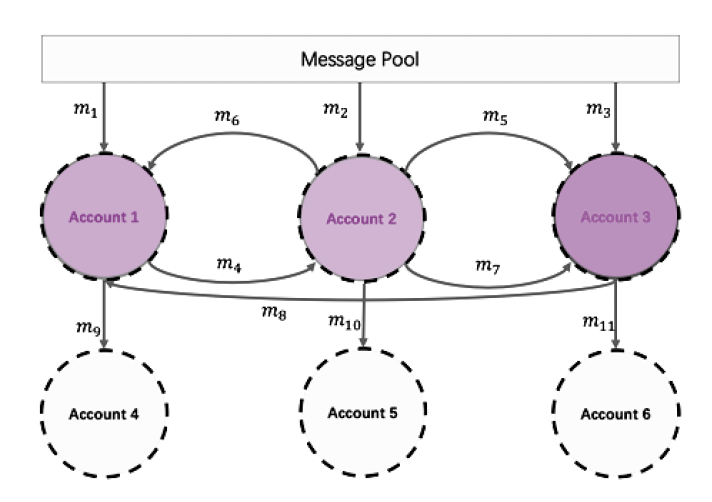
5.3 基於並行模型的區塊鏈計算

在我們的並行模型中，對於鏈C上的每個區塊，有三種消息：

1、輸入消息。這些消息當前未被確認，並且接收者帳戶都是在鏈C上，它們可以是外部消息或由其他鏈產生的中繼消息。

2、內部中繼消息。這些是在執行整個區塊期間生成的中繼消息，並且接收器同樣位於鏈C上，因此它們在本區塊上就會被確認。

3、外部中繼消息。這些是在執行整個塊期間生成的中繼消息，它們的接收器位於其他鏈上，這些消息將由其他鏈確認。



下麵介紹一個如上圖所示的例子。在C鏈上有三個帳戶1,2,3，在其他鏈上有三個帳戶4,5,6。特別是，有三個輸入消息（即m1,m2,m3），分別由帳戶1,2和3接收。

對於每個帳戶i，我們使用σi來表示處理消息的順序以及生成新消息。然後，我們有：

σ1=m1:m4m8m6:m9

σ2=m2:m5,m6m4:m7,m10)

σ3=m5:m11m3:m8m7

因此，σ1表示帳戶1按順序處理消息m1，m8和m6。通過處理m1產生內部中繼消息m4，並且通過處理m6產生外部中繼消息m9。然後我們有內部中繼消息集m4,m5,…,m8和外部中繼消息集{m9,m10,m11}。

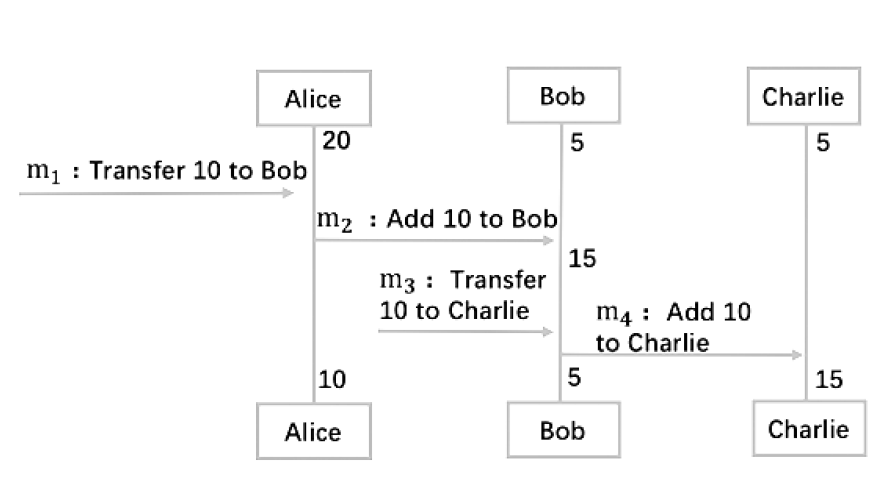
在收到負責人提出的區塊時，委員會成員需要驗證，防止有惡意負責人。在我們的系統中，節點驗證了三個部分：

1、每個輸入消息的有效性，即{m1,m2,m3}。

2、每個帳戶的處理有效期，即{σ1,σ2,σ3}。它們可以獨立並行地進行驗證。

3、處理消息順序的有效性，即順序σ=(σ1,σ2,σ3)。

為了驗證處理消息順序σ，我們建立有向圖Gσ。對於兩個事件e1和e2，e1→e2表示e1的發生時間在e2的發生時間之前。設mi表示事件帳戶i收到消息mi，mi表示事件帳戶i發送消息mi。然後我們有mi→mi對於每個σi，例如i=1，我們有m1→m8→m6。基於σ的這些關係，我們可以建立有向圖Gσ。



定理：當且僅當有向圖Gσ不存在環時，處理消息順序σ=(σ1,σ2,σ3)是有效。

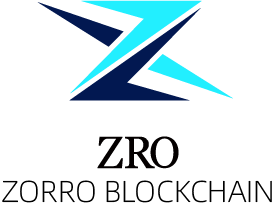
2.5.4 優化

我們設計了一些優化方法來降低通信成本和帳戶存儲。

1、避免重複存儲。對於某些特定消息，每種帳戶都有相同的通用處理方法。這些公共方法由系統設計，不需要由每個帳戶設計。

2、降低通信成本。通過合併一堆相同類型的消息可以降低通信成本。例如，如果有10個“add”消息發送到同一帳戶，則可以將它們組合成一個“add”消息。

對於“單一帳戶熱點”問題，單個帳戶涉及大量消息，可以通過上層應用程式的協同設計輕鬆解決，這類似於“熱點貓”問題，很多經常使用的帳戶可以放在多個鏈上。

相比同樣被用來做併發的其他方法，我們的模型具有更高的靈活度和效率。但是在使用此模型進行開發時，開發者需要清楚考慮如何跨鏈通信的規模，否則多次的跨鏈很有可能抵消掉由並行而產生的高效。



價值

1、Zorro優勢

Zorro本質上是用區塊鏈的技術，試圖解決行業內的各種痛點，構建一個“全球區塊鏈自由貿易區”。在自貿區裏，Zorro提供底層區塊鏈基礎架構，引入Zorro的Token體系作為中小商戶之間貿易活動價值傳輸的衡量標準。在各種應用場景下，Zorro將與全球眾多第三方服務機構一起，打造集電商+支付，電商+供應鏈溯源，電商+供應鏈金融，電商+社區直播，電商數據+數字貨幣交易所為一體的平臺。

Zorro希望，能夠用數位化的思想、不可篡改的分佈式時間戳體系以及無所不在、萬物互聯、即時上鏈的業務體系，妥善完成上述宏偉的目標，真正做到全方位、全覆蓋的公平、公正，為“全人類自由”的最高目標實現提供有力的支持。

Zorro將分步驟實施，並針對前述的電子商務市場現有的痛點提供相應的迅速到賬、快捷支付、跨境支付、通兌全球法幣、資訊溯源等服務；未來還可以擴展更多的服務，包括本地孵化服務以及在Zorro上發行區域性Token的服務等。

Zorro的設計充分考慮了開放性和合規性，將遵守當地監管要求和法規。由於Zorro區塊鏈的開放性，必要的時候監管可以在其上設立節點，或者通過Zorro提供交易記錄。由於區塊鏈不可篡改的特性，此舉將在必要時充分幫助監管提升其監管精度。

2、Zorro發展

隨著世界經濟規模的增長以及公平公正、自由平等觀念的深入人心，Zorro將迎來巨大的流通潛力與此同時，而由於Zorro數量有明確的上限，不存在隨意濫發的風險，因此Zorro將能憑籍穩定的流通量獲得越來越多人的認可，為其持有者帶來巨大其有持續性的收益。

Zorro的定位是，深耕區塊鏈技術，依託平臺龐大且卓著的綜合生態功能開發服務網絡，打造區塊鏈世界的綜合經濟平臺，為世界經濟貿易乃至整個支付環境提供迅速、保密、安全的交易服務。

Zorro敏銳地意識到，貨幣的本質在於信任與流通，信任必須由所有參與流通的人共同進行，而不應將決定權交予中心化運營的傳統機構；流通的關鍵在於自由，而不應受到過分的監管。而這也正是Zorro希望為社會提供的優質服務。

在Zorro發展的初期，Zorro將主要用於購買平臺旗下的各項服務，流通範圍將隨著Zorro市場能力的逐漸顯現而向Zorro的合作單位乃至整個線上交易擴散，最終成為世界線上交易最重要的支付手段。

3、Zorro初衷

想像一下，你無須信任任何陌生人就可與之進行交易；你無須信任銀行就可安心地把積蓄儲存在那兒；你不需要信任何的商家、經紀人與仲介，因為你知道它不得不公平、公正。那會發生什麼？

那會改變這個世界。

而這，正是區塊鏈的願景。當主流媒體還在忙於猜測加密貨幣價格及其黑市陰謀時，他們已經遺漏了這一切的本質事實。那就是，密碼學家們悄然發明了一套全新的技術原型。區塊鏈（以及支持它們的共識協議）的誕生，源於開發人員試圖解決一個大膽的難題：如何創造不可追溯的數字貨幣。通過將密碼學、博弈論、經濟學以及電腦科學相結合，他們成功創造出了一套全新的工具用於建立去中心化的系統。

區塊鏈並不再遙遠，已經來到觸手可及的眼前，它是互聯網的一部分，在交通、醫療、衣業、產權、支付、生活服務等領域已經出現諸多應用場景，區塊鏈讓互聯網浪潮再次升級，並逐步深入到更多的創新領域．在數字貨幣領域。區塊鏈並不僅僅是一種技術創新，其背後含的去中心化、去信任化思維更揭示了構建全新經濟模式的可能。在價值賦權和轉移領域，區塊鏈技術因其公開、透明、可追溯、不可篡改的特點，已經開始展現出巨大的優勢，最終，它將幫助我們完成資產數位化這一價值遷移，實現對自身財富的真正掌控。

遺憾的是，新興技術的出現總會因為會顛覆原有的經濟結構而遭到既得利益者的杯葛；而此種杯葛對新興技術的快速市場化、實用化進程所起到的阻礙更是數以倍增。截至目前，區塊鏈技術市場已經出現了過分重視新的數字貨幣發行、數字貨幣市場運營混亂等諸多亂象，對廣大投資人的經濟利益造成了嚴重的威脅，進而極大地打擊了大量潛在投資人的進場意願；而在第三世界國家市場，由於獨特的金融監管體制，區塊鏈技術的發展更是困難重重，而諸如市場規範、標準化流程、優質交易所等市場效率提升的必要元素的構建更是無從談起，使得截至目前全球區塊鏈市場仍處於“荒蕪”的待開發狀態。

而Zorro的立項初衷正是，在這個紛繁複雜的時代，在這個區塊鏈問世的意義、目的以及其前景都被極大扭曲的時代，高舉“公平公正、全民自由”的旗幟實現撥亂反正，重拾區塊鏈技術足以改變世界的力量，重塑這一前沿科技蒙塵已久的原始面貌，回到造福全人類、推動全人類社會公平公正、追求自由事業的正軌上。

4、Zorro可拓展性





核心

1、區塊鏈基礎設施

以區塊鏈技術為代表的去中心化，自主治理的系統，正在引起越來越多人的重視和研究。當前全球區塊鏈專案已經超過20000 個，全球加密數字資產總體價值達到2000億美元。區塊鏈/數字資產領域的用戶人群也正在快速增加。從2013 年初的全球200萬用戶，到2019年初的7500萬用戶。我們認為，在2020年左右，全球區塊鏈/數字資產用戶會達到或超過2億。在2025 年前後，全球用戶有望達到10 億規模。

隨著區塊鏈技術的普及，越來越多區塊鏈技術之上的應用場景被挖掘出來。區塊鏈技術的應用場景已經從最初的數位化貨幣本身逐步擴展到更多的場景及用戶群體中。例如，以以太坊為代表的社區在區塊鏈技術中引入智能合約的概念，Ripple 則使用區塊鏈技術實現了全球的結算系統。隨著應用場景的多樣化，用戶對區塊鏈技術的訴求也日益增加，我們已經看到很多挑戰：

1、價值尺度的缺失

我們認為，區塊鏈世界需要⼀個普適的價值尺度，來衡量用戶和智能合約的價值，上層應用可以在這個普適的價值尺度上結合自身場景挖掘更深層次的價值，這將帶來更多的商業模式的創新，就像Google 在互聯⽹世界的興起⼀樣。

2、區塊鏈應用生態環境的建立

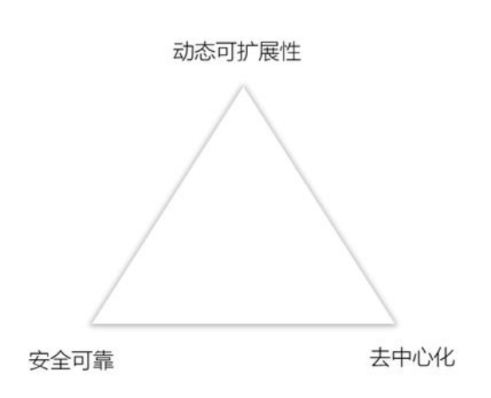
隨著區塊鏈上各種應用(DApp) 的快速增長，良好的生態環境是提高用戶體驗的根本所在。這包括用戶如何在海量的區塊鏈應用中檢索自己期望的DApp，如何激勵開發⼈員為用戶提供更多的DApp，以及如何幫助開發⼈員更快的構建更好的DApp。以以太坊為例，基於以太坊的DApp 總數已經數⼗萬個，試想如果區塊鏈世界中的DApp 接近蘋果AppStore應用總量規模的話，如何發現並找到期望的DApp 就是個很⼤問題。

3、創新不足

“為了區塊鏈而區塊鏈”是當前科技領域非常普遍的一個現象，因為“區塊鏈”三個字不但自帶流量，還自帶“高深莫測”屬性。如前段時間非常火熱的Ankr區塊鏈雲計算平臺，號稱利用自主研發的PoUW技術實現全新的基於區塊鏈技術的雲計算服務與工作量計算模式，但是業內人士深入分析其工作模式，發現Ankr與此前出現過的多個雲計算平臺相比同樣沒能利用區塊鏈計算真正實現雲計算平臺運行邏輯與商業模式上的突破。所謂的“自研PoUW模式”不過是將英特爾的SGX處理器加密技術用於資訊上載，而SGX技術本身即可充分實現Ankr聲稱的一系列平臺優勢，如工作量真實統計、工作量與品質無法作偽、實現按勞分配等。這些“偽區塊鏈”的氾濫，讓許多對區塊鏈技術感興趣的消費者與投資人逐漸對“區塊鏈”三個字望而生畏。

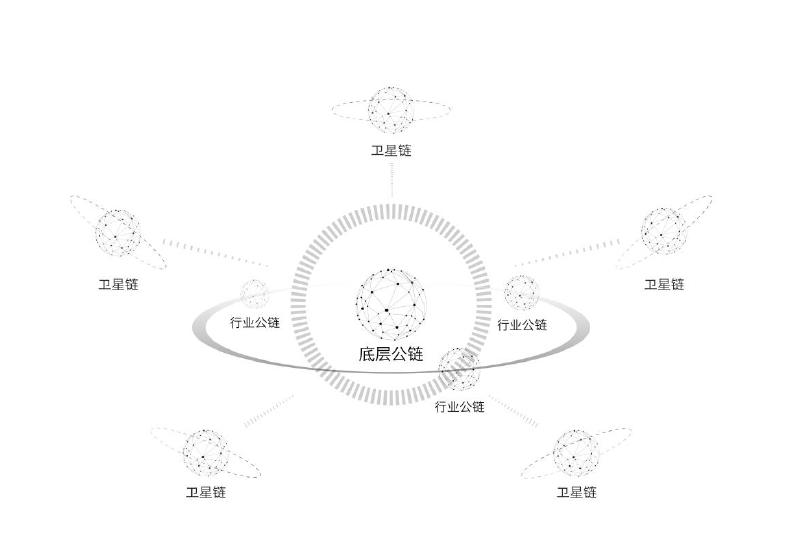
而秉著開放包容、互惠互利的心態，Zorro將全球領先的公鏈、聯盟鏈、隱私保護三大技術創新優勢賦能給開發者，讓開發者不再受制於技術，可以基於Zorro底層開發自己的行業公鏈、聯盟鏈或者應用，為他們找回初心，迎接夢想。

2、商業化落地

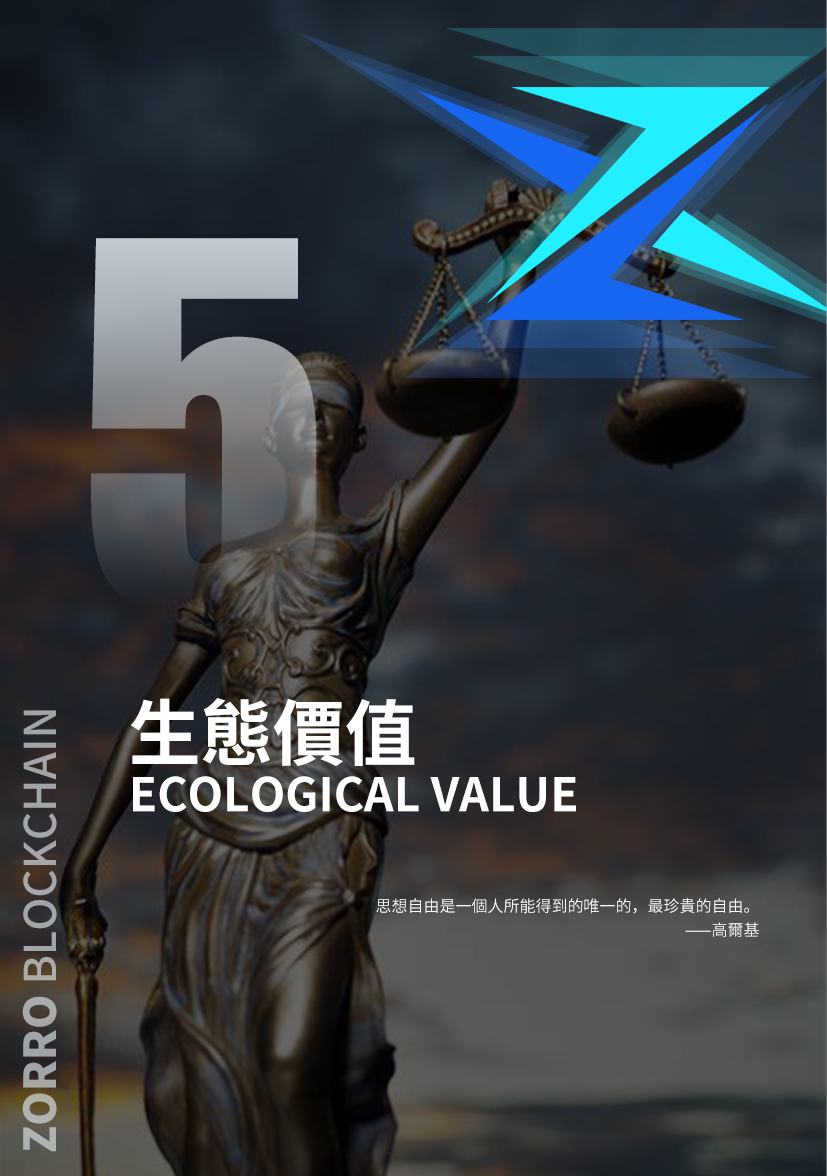


Zorro通過分層多級的架構以及自主研發的分層共識協議棧技術，在保證整個系統的安全性與一致性的條件下，支持了橫向和縱向的雙向動態擴展，從根本上解決了區塊鏈“不可能三角”的問題。在解決不可能三角問題的基礎上，Zorro還創新性地提出基於Actor模型的帳戶體系，完美支持複雜任務的高併發處理，讓區塊鏈能夠更高效承載大規模的交易，能夠支撐起海量用戶規模的應用運行，使得原本由於受限於技術成熟度的區塊鏈商業專案的落地變為可能。

3、價值網路

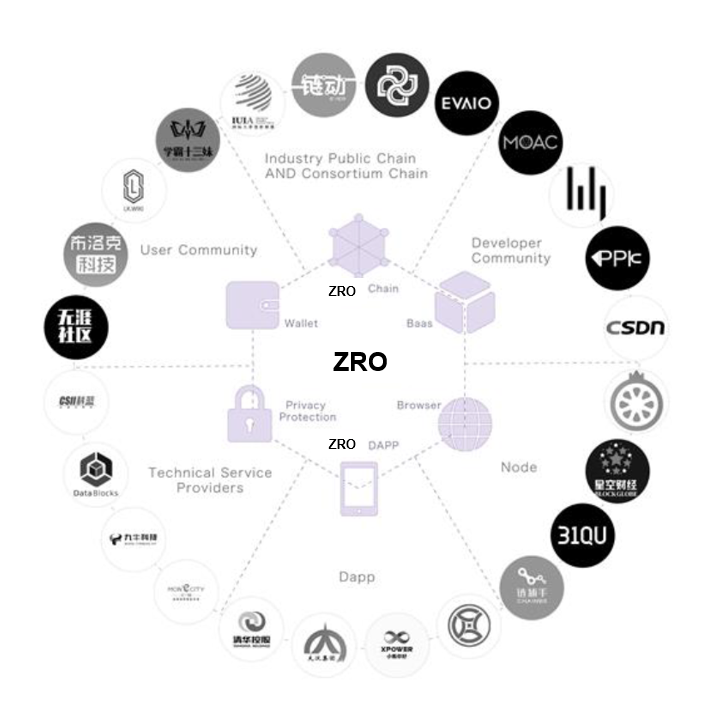


Zorro的整個價值網路可以理解為由Zorro的底層公鏈+可擴展的衛星鏈組成。Zorro的底層公鏈上可以再搭建行業公鏈，衛星鏈是聯盟鏈。如果是行業公鏈，其底層安全性和Zorro的底層公鏈及其上的其他行業公鏈是一致的，價值可以直接傳遞；如果是聯盟鏈，底層安全性是不一致的，價值傳遞過程需要額外的協議保障。開發者可以在Zorro底層公鏈上直接開發DAPP，也可以在行業公鏈上開發DAPP，同時也可捕獲已經與Zorro鏈接的衛星鏈的部分價值。開發者還可以在衛星鏈上開發DAPP，可以通過Zorro來傳遞不同衛星鏈之間的部分價值。



生態模型

1、 Zorro生態圈



Zorro商業生態圈包括Zorro公鏈、聯盟鏈、隱私保護和DAPP、錢包、流覽器等區塊鏈應用，同時為行業公鏈、行業聯盟鏈、去中心化應用、開發者社區等大規模商業應用提供便捷友好、高效安全的開發、測試、部署、運營環境。

Zorro可以比擬為一個互信商業協作引擎，它催生了一個對生態所有參與者即可信又安全的商業環境，在這樣的商業環境中，所有商業主體之間的協作摩擦將會大大降低，從而使得所有的商業協作更加高效可靠。

2、Zorro生態主推

市場早已經證明，簡單的發揮區塊鏈的金融屬性，通過激勵早期參與者的方式是無法實現區塊鏈的大規模商業落地的。Zorro從金融、電商、行銷、遊戲、AI、IoT等領域做了大量實踐和理論研究，致力於提供底層技術基礎設施的同時，為生態參與者提供傳統資訊技術互通、大規模商業應用落地路徑，並構建全新的金融底層。



2.1 Zorro去中心化金融服務

DeFi，去中心化金融，是目前區塊鏈技術的最佳落地場景之一。DeFi的核心原則是提供一個全新的、無需許可的金融服務生態系統，沒有任何中心化權威，世界上任何人都可以使用。在這個生態系統中，用戶就是自己資產的託管人，對自己的資產擁有完整的控制權、所有權，他們可以自由進入市面上所有的去中心化市場。DeFi最重要的願景就是將所有資產通證化，在全球市場上實現無國界交易，創造出一個更開放的金融系統。Defi業務的發展一方面將顛覆現有金融業組織結構和商業模式，實現“去銀行的眾融和自融”；另一方面將提高主流數字貨幣流動性並擴大價值認同，促使其最終成為穩定的“貨幣”，構建全新的商業和金融體系。這為真正的普惠金融提供了可行性，讓每個人、每個企業的信用變成財富——Banktheunbanked,Servetheunderserved.

當前DeFi還處於初期，但它的發展空間是不可想像的。要成功靠DeFi改變未來，不僅需要開發出豐富的有價值的應用產品，而且需要億級用戶的大規模使用，還要幾乎“零出錯”的絕對安全性。Zorro作為未來全球可信結算層，就是為世界提供了一套低成本、高效率的支付結算系統，滿足高效率的支付和交易，並保證整個分佈式帳本的絕對安全，構建分佈式金融的基礎設施。

去中心化金融產品往往都是大眾需求，如去中心化保險、去中心化借貸等。Zorro採用分層多級的架構，從而支持性能、存儲和應用的無限擴展。各行各業都可以在自身業務基礎上基於Zorro開發滿足市場需求的DeFi應用，面向海量用戶，實現高效的借貸、交易和支付。

1、協議靈活組合

DeFi的關鍵創新在於把金融的基本要素模組化，並通過這種模組化實現信任的商品化。Zorro自身就會開發類似於錢包、支付、身份認證、資產發行等一系列基礎協議，並引入越來越多的開放式金融協議。應用層可以根據自身團隊的基因和對市場機會的發現，來自由組合需要的協議層，並且去實現應用的落地。比如去中心化交易所，可以由一個錢包協議、借貸協議、託管協議和交易所協議組合來實現。

2、安全可靠

DeFi業務涉及到大量數字資產的交易和存儲，其安全問題尤為重要。Zorro採用分層共識協議棧從而保證協議、合約、數據、網路等全方面的安全。

3、良好的用戶體驗

DeFi本質上是一類應用，是幫助用戶解決問題、創造價值的，需要保證良好的用戶體驗。Zorro具有動態可擴展的計算存儲能力，TPS能夠輕鬆擴展到10W，確認時間短，有效解決解決網路擁塞問題；Zorro採用超低手續費模式，不會將調用網路資源的負擔轉嫁到用戶身上；並且Zorro採用多種方式存儲數據，面對海量數據可以快速讀取和處理。

凱文·凱利說，金融應當演變成為人們的一種生活方式，只有真正將金融融入到人們生活的方方面面，才能真正讓金融變得與往常不同，最終完成蛻變。未來人類商業活動中將有越來越多的商品通過區塊鏈開放性協作組織來創造，包括越來越多的文化、娛樂、遊戲等等數字產品，而商品創造過程中產生的融資需求通過鏈上金融業務來解決，並最終通過區塊鏈“貨幣”來支付。這將是人類商業和金融體系的一次顛覆性的變革。Zorro去中心化金融提供了這種可能性，去中心化金融的目標不是去中心化本身，而是更加開放和公平。DeFi的發展會對Zorro生態的發展會有積極的促進作用：

4、吸引眾多的開發者

DeFi應用場景的多樣性以及對未來高增長的預期，會吸引大量的開發者和專案方基於Zorro提供的框架和模組來進行開發。

5、吸引海量的用戶

DeFi沒有准入門檻，不用擔心隱私被審查和利用，一切數據公開透明的優勢，使得用戶有了更加廣泛的參與度，把握新時代財富分配和增長的方式。用戶規模的不斷擴大會正向激勵更多有意義、有價值應用的開發落地。

6、有效賦能

DeFi是可信世界數字經濟的血脈，能夠促進基於Zorro開發的DAPP、應用公鏈的繁榮發展。在Zorro生態中，各種應用互聯互通互融，使得鏈上鏈下的資金流、資訊流、信任流、物流等融為一體，加速分佈式商業世界的精彩綻放。

2.2 Zorro去中心化用戶體系

基於Zorro構建的可信協作網絡、Zorro的真實ID系統、Zorro的可信結算體系，勢必會引發一場新的行銷革命。當前商業主體的價值成長主驅動因數已經轉變為自身用戶的價值成長，而Zorro提供的技術使得可以將用戶的價值儲藏在各個分佈式的網路中，最終還能完成整合，提供了一種可行的用戶價值管理模型，我們將它定義為CVM（Customer Value Management）。

CVM也可以理解為一種新的用戶忠誠度革命，它可以將用戶的所有行為資產化，並且可以歸集並永久存儲用戶的價值，我們會為每個用戶提供一個私有的價值記憶體（除去資產、還會包含一些核心的私有數據）。

在新的行銷體系下，傳統的拉新和留存模型都發生了巨變：

1、由原有的商業主體主動滲透及激勵、用戶被動接受，逐步轉化為，用戶自身的價值成長驅動，用戶會因為自身的個性化價值被得到認可而更自主的加入價值網路（也可以定義為社群）。

2、留存：由原有商業主體更多的單方面主體的維繫和激勵，逐步轉化為用戶跟商業主體之間的持續互動形成共同的價值共同體，用戶因為價值沉澱而變得更忠誠。

隨著用戶同商業主體的共同價值成長，推動各自的價值網路相互間進行價值傳遞，而且這種交互是建立互信的商業環境底層上，使得如流量互換、廣告等最基本的行銷活動變得無需再擔憂流量陷阱、結算風險等。

未來的產品服務還會持續升級，但行銷始終是商業活動不可避免的難題，而基於Zorro技術構建的互信行銷網，將大大降低行銷成本、且更高效的覆蓋到更廣的範圍。

2.3 Zorro分佈式電商

分佈式電商指的是基於Zorro區塊鏈技術構建可信平權的供需網路，在這個互信網路中各參與方的行為按照共識的標準被資產化，同時可按照共識的規則進行自主協作並交換價值。

隨著社交電商的興起，以及近些年對私域流量的深度挖掘，看似已經不存在結構性創新的的電商市場，其實單從供需兩端的宏觀角度來看：

1、供給端：行業網路協同尚未形成，通過整合提升效率大有可為。

2、需求端：消費需求從大眾轉向個性化，個性消費催生柔性供應鏈。

基於供需兩端的痛點出發，Zorro的分佈式電商核心目標旨在：

1、通過區塊鏈技術整合供給端形成協同的供給網路：在idea、生產、加工、定價、銷售（預售、正式銷售）等各個環節，各參與方進行自主協作，並根據貢獻的價值決定最終的收益。

2、基於共識的標準，將用戶的行為資產化，並將其存儲在區塊鏈上形成一張新的價值網路，價值的延續可以保護用戶的個性且激發個性。

3、因為共同的價值體，進而將用戶（需求方）跟供給端進行更深度的捆綁，智能合約可以保障不同參與者之間的利益分配。

在這樣新的互信分佈式電商網路中，參與的各個角色的協作摩擦大大減小，進而大大提升效率和降低信任成本，同時Zorro的新行銷革命也賦予整個電商網路新的商業勢能，使得各個角色的價值被得到更合理的分配以及被持續存儲下來從而自主實現各自的能力升級、角色轉化：

1、用戶：從單純的消費者升遷為價值投資者，消費即投資，這種消費可以是直接的金錢、可以是社交關係資產、可以是行為資產等等。

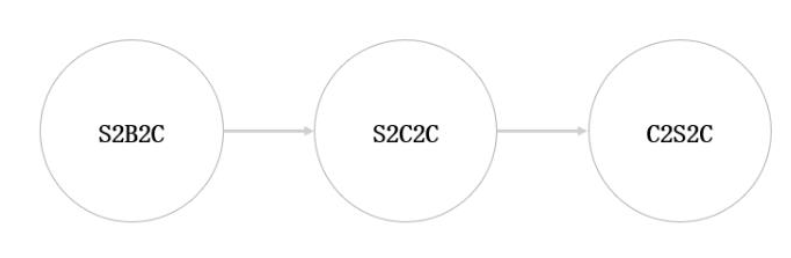
2、服務者：（銷售、客服、內容生產者）進行更專業的分工切割，各自從事更加符合自己人格的產品服務工作，服務者的服務經驗、創造的內容、經營數據等被資產化,並存儲在更大範圍的價值網路內，也使得服務者的服務邊界被打破。

3、品牌主：品牌是具有經濟價值的共識資產。在新的互信商業環境下，品牌主跟用戶共同創造、維護品牌，共用品牌收益，使得品牌的成長路徑縮短且更加穩固。

4、生產者：可以更加真實全面的掌握整個供需網路中的數據，進而實現按需生產、按需定制，使得更貼近消費者個性化的同時，保證足夠的生產效率和極低的浪費。

5、開發者：數據與程式分離，數據所有權歸還給用戶本身，開發者的由原來的收集用戶數據變現的盈利模式轉變為協同用戶共同創造價值的新模式。

隨著用戶價值的主體地位逐步提升，同步推進分佈式電商的模式演進:



在基於Zorro的互信的分佈式電商網路中，S指的是通過區塊鏈技術整合的超級供應鏈平臺，這種整合下的S2B2C不再是簡單的B2B2C的變種，而是一種真正意義上的基於技術鏈動和數據驅動的協同網路生態系統。傳統的供應鏈都是線性思維的，這樣的供應鏈根本無法同時應對低成本、快反應、高定制這三個完全衝突的核心指標，只有可信網路的結構，才具備足夠的靈活性來實現這三個指標的動態優化。通過區塊鏈構建的這個產業價值協同網路是任何一個產業內的單體都做不到的，平臺的價值就是這個網路的形成和底層架構者。它從賦能的角度出發，突破傳統加盟體系的“交易”思維，實現S和產業鏈上的各類小B共生共贏。隨著用戶的價值成長，用戶扮演的角色越來越重要，逐步成為整個供需鏈路上的主導者。

這個演進模式並不是指的要直接推翻所有的資源主導的業態，它在很長一段時間內均是一個融合模式的形態。只是在Zorro構建的分佈式電商網路中，各角色可更大規模的進行互信協作，共同創建更巨大的商業價值共同體。



Token分配

發行量：3.3億枚

分配比例：

3%，發展基金;

7%，穩定基金；

20%,保障基金；

30%，礦層基金；

40%，激勵基金；

20%保障基金6600萬通證，每天釋放6600枚，該部分購買的ETH全部流入驗證池為投資者提供保障，發展基金對撞結束，開始釋放保障基金。發展基金用作白名單交易所上幣、媒體宣發、多元生態構建等之用。激勵基金開啟，共識基礎形成，自治聯盟俱樂部將陸續回購最初釋放的此部分幣量（990萬枚），並將之打入黑洞，永久銷毀。穩定基金用於通證價值及生態維護，激勵基金用於持幣算力及推廣算力的激勵。礦層基金前期凍結，後期升級公鏈，映射後用於礦機挖礦。



團隊

Zorro 濫觴於對當今全球數字經濟、實體經濟所存在痛點的反思。而 Zorro 的主體運營思路則深受暗網運營模式的啟發。暗網（不可見網，隱藏網）是指那些儲存在網路資料庫裏、不能通過超鏈接訪問而需要通過動態網頁技術訪問的資源集合，不屬於那些可以被標準搜索引擎索引的表面網路。邁克爾·伯格曼將當今互聯網上的搜索服務比喻為像在地球的海洋表面的拉起一個大網的搜索，大量的表面資訊固然可以通過這種方式被查找得到，可是還有相當大量的資訊由於隱藏在深處而被搜索引擎錯失掉。絕大部分這些隱藏的資訊是須通過動態請求產生的網頁資訊，而標準的搜索引擎卻無法對其進行查找。傳統的搜索引擎“看”不到，也獲取不了這些存在於暗網的內容，除非通過特定的搜查這些頁面才會動態產生。於是相對的，暗網就隱藏了起來——而 Zorro 團隊，則是一群來自於暗網生態網路頂層的天才駭客！

佐羅，為什麼專案會叫佐羅？是因為現在的大環境受疫情、病毒、政治環境等的影響，導致民不聊生，人們壓抑、痛苦、絕望，所以一群技術極客充當正義的使者，像佐羅一樣亮正義之劍，還世界以正義、自由、平等,所以這個團隊叫佐羅。



路線圖

2017.06

2018.01

2019.03

2019.06

2019.08

2020.01

2020.02

2020.03

2020.04

2020.06

2020.08

2020.12

2021年

Zorro創世團隊成立

Zorro底層核心模組開發完畢

Zorro應用層模組完善

Zorro鏈上智能合約部署

Zorro全球主節點部署

Zorro測試網上線，全球暗網內測

Zorro白皮書發佈

Zorro全球共識計畫啟動

Zorro亮劍計畫

Zorro財富自由計畫

Zorro正義之戰計畫

Zorro和平之旅計畫

Zorro星辰繁榮



免責聲明

文檔僅作為傳達資訊之用，文檔內容僅供參考，不構成在Zorro 及其相關公司中出售股票或證券的任何買賣建議、教唆或邀約。本文檔不組成也不理解為提供任何買賣行為，也不是任何形式上的合約或者承諾。

鑒於不可預知的情況，本白皮書列出的目標可能發生變化。雖然團隊會盡力實現本白皮書的所有目標，所有購買 Zorro的個人和團體將自擔風險。文檔內容可能隨著專案的進展在新版白皮書中進行相應調整，團隊將通過在網站上發佈公告或新版白皮書等方式，將更新內容公佈於眾。

本文檔僅供主動要求瞭解專案資訊的特定對象傳達資訊使用，並不構成未來任何投資指導意見，也不是任何形式上的合約或承諾。

Zorro明確表示不承擔參與者造成的直接或間接的損失包括：參與者一旦參與 Zorro分發計畫，即表示瞭解並接受該專案風險，並願意個人為此承擔一切相應後果。專案團隊明確表示不承諾任何回報，不承擔任何專案造成的直接或間接損失。本項目涉及的 Zorro是一個在交易環節中使用的虛擬數字編碼，不代表專案股權、收益權或控制權。由於數字資產本身存在很多不確定性(包括但不限於：各國對待數字貨資產監管的大環境、行業激勵競爭,數字貨資產本身的技術漏洞)， 我們無法保證專案一定能夠成功，專案有一定的失敗風險，本項目的 Zorro也有歸零的風險。

雖然團隊會努力解決專案推進過程中可能遇到的問題，但未來依然存在政策的不確定性，大家務必在支持之前瞭解區塊鏈的方方面面，在充分瞭解風險的前提下理性參與。

團隊將努力實現文檔中所提及的目標，但基於不可抗力的存在，團隊不能做出完全承諾。在適用的法律允許的最大範圍內，對因參與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、商業資訊的丟失或任何其他經濟損失，本團隊不承擔責任。