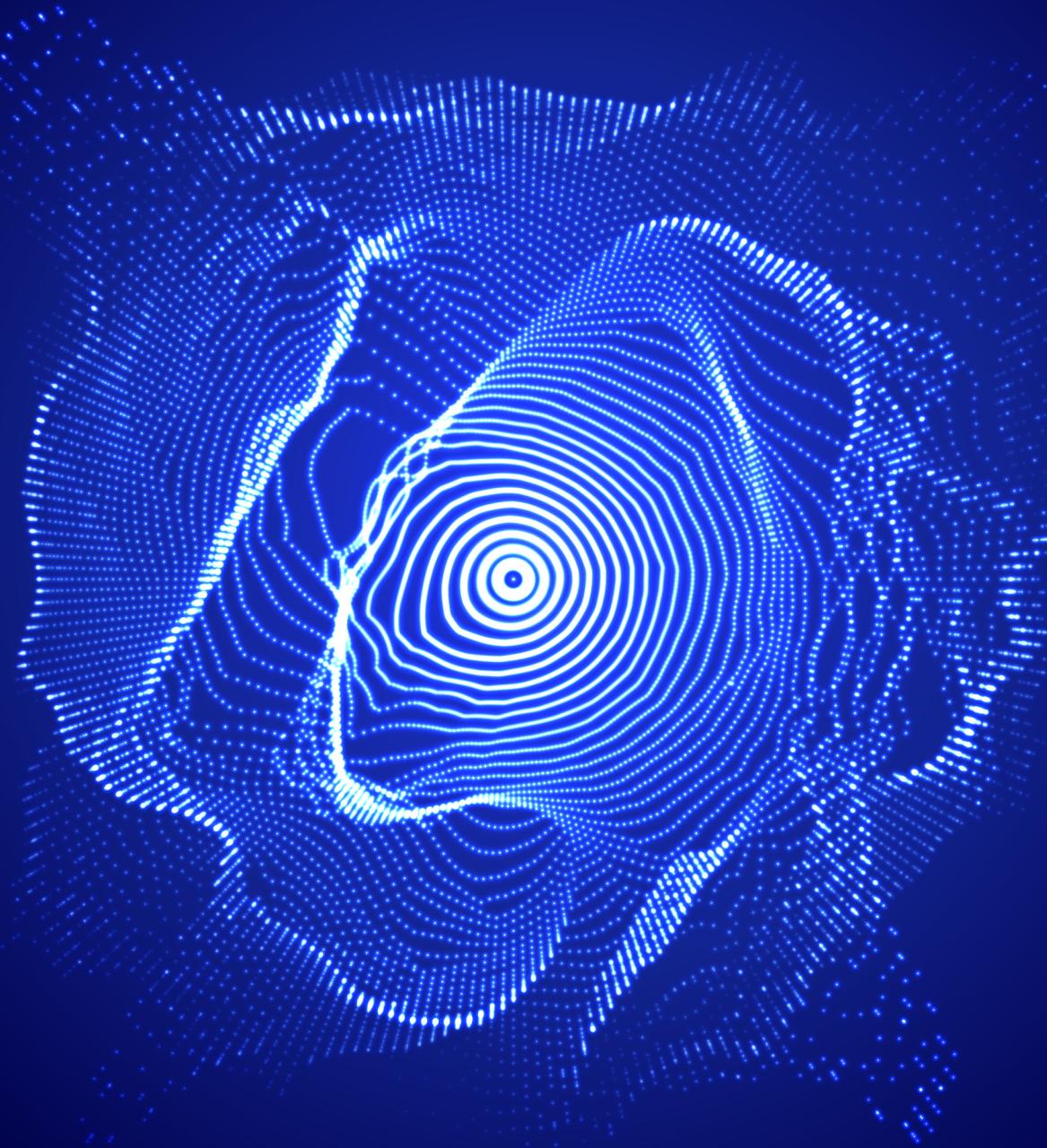


2019

Dimension白皮书



Dimension 出品

目 录

Contents

01

設計理念

- 1.1 區塊鏈發展
- 1.2 區塊鏈面臨問題
- 1.3 維度鏈使命與願景

02

應用服務網絡

- 2.1 維度鏈概述
- 2.2 設計架構
- 2.3 迭代演進

03

維度鏈特性

- 3.1 石墨烯框架
- 3.2 分佈式存儲
- 3.3 混合共識機制
- 3.4 隱私保護
- 3.5 跨鏈互聯
- 3.6 開發中間 SDK
- 3.7 數據交易

04

治理架構

- 4.1 基金會及治理框架
- 4.2 核心團隊
- 4.3 經濟模型
- 4.4 分配方案
- 4.5 治理機制
- 4.6 披露事項
- 4.7 法律及免責

05

實施及迭代

- 5.1 維度鏈路線圖

06

生態應用

- 6.1 結合行業場景應用
- 6.2 生態應用

摘要

ABSTRACT

DIMENSION 致力於構建新一代區塊鏈分佈式應用服務網絡。DIMENSION 採用多項革新性技術用於結合區塊鏈，如全同態加密，安全多方計算，可驗證算法，零知識證明等，通過分佈式數據存儲協議，混合共識機制等協議與共識算法，並結合去中心化社區治理機制，提供了從多個技術維度支撐面向商業應用的高效、便捷的區塊鏈服務網絡。

DIMENSION 底層功能，如通用賬戶、智能合約等，解決了數字資產確權及可編程控制，保證交易的安全性和透明化。基於數據隱私保護及跨鏈互聯的技術方案，可實現跨共識共存，實現在多個主鏈上的運行和交易，最終可實現支持 EOS、ETH 等主鏈之間的數據互聯及共享。通過數字資產交易平台為用戶提供了數據共享及交易，實現了區塊鏈上資產輕所有權，重使用權的價值共享嶄新商業模式。通過 DIMENSION 服務網絡結合商業訴求，最大限度地挖掘數據潛在價值。

同時，DIMENSION 通過面向商業應用場景，提供針對企業級區塊鏈應用的服務接口，企業可根據業務需求，快速靈活部署所需區塊鏈應用組件，極大降低區塊鏈應用實施開發成本和縮短實施週期。DIMENSION 作為面向區塊鏈技術的企業服務中間件，通過敏捷開發組件、且支持靈活配置的區塊鏈套件，可針對不同企業的所屬行業特性，快速實現具有高適配性的區塊鏈主網及應用開發。借助 DIMENSION 自適應框架，跨共識數據並行方案，推動區塊鏈技術在商業場景的快速落地及應用。实现具有高适配性的区块链主网及应用开发。借助 DIMENSION 自适应框架，跨共识数据并行方案，推动区块链技术在商业场景的快速落地及应用。

DIMENSION

具有強大的核心競爭力

技術優勢

擁有強大的區塊鏈技術團隊，同時作為萬向區塊鏈實驗室技術合作夥伴，DIMENSION 致力於在區塊鏈技術上不斷尋求創新和突破。

生態優勢

DIMENSION 擁有強大的資源優勢與生態支持，如數字貨幣交易所、數據交易市場、全球四大審計合作方及律所、社群自治組織、頂級安全團隊、區塊鏈研究中心、空投平台、冷熱錢包等生態資源。DIMENSION 與區塊鏈各頭部項目均有著密切合作，眾多優秀區塊鏈項目團隊作為 DIMENSION 合作方深度參與生態共建。

關鍵詞

Key Words

分佈式應用

混合共識

區塊鏈

企業中間件

服務網絡

數據共享

跨共識引擎

I. 設計理念

CONCEPT

1.1 區塊鏈發展

中本聰自 2008 年發表的《比特幣：一種點對點的電子現金系統中》中提到區塊鏈（BLOCKCHAIN），並作為比特幣的核心技術得到全球關注。廣義的區塊鏈技術是指，利用塊鍊式數據結構來驗證與存儲數據、利用分佈式節點共識算法來生成和更新數據、利用密碼學的方式保證數據傳輸和訪問的安全、利用由自動化腳本代碼組成的智能合約來編程和操作數據的一種全新的分佈式基礎架構與計算方式。其主要特徵包含：分佈式（Decentralized）、免信任（Trustless）、時間戳（Timestamp）、非對稱加密（Asymmetric Cryptography）、智能合約（Smart Contract）、共識機制（Consensus）。

■ 區塊鏈演進的三個階段

區塊鏈 1.0 -- 數字貨幣

最具代表意義的比特幣（BitCoin），用區塊鏈作為底層技術，實現區塊鏈的最初始應用。

區塊鏈 2.0 -- 數字資產和智能合約

以太坊（Ethereum）為代表的區塊鏈技術引入了智能合約，圖靈完備虛擬機，提供更豐富的應用場景。

區塊鏈 3.0 -- 服務應用

區塊鏈引入分佈式存儲、數據隱私保護等技術，將被廣泛應用於商業場景和社會生產的各個方面，如資源共享、版權保護、物聯網、供應鏈金融、資產數字化等。

1.2 區塊鏈面臨問題

毋庸置疑，區塊鏈擁有巨大的潛力，除了技術上的快速發展，如點對點傳輸、共識機制、加密算法等技術。區塊鏈更帶來了商業模式的變革，分佈式商業模式作為全新商業應用場景，改變了目前商業供給側的關係，打破了現有的商業模式。借助區塊鏈的去中心化、不可篡改、安全可靠等技術特性，區塊鏈技術可適用多類應用場景。

於此同時，區塊鏈的技術發展也同樣受到如下因素的製約。例如可擴展性急待提升，隱私保護方案不夠完善，分佈式存儲技術不夠成熟，去中心化且安全高效的共識機制待改進，缺乏統一且公認的治理標準，跨鏈互聯技術有待突破，無法針對不同業務適配最佳共識算法，區塊鏈開發及部署技術難度大等等。這對區塊鏈技術能否廣泛有效服務於商業應用帶來障礙。

本白皮書將在後續篇幅中闡述，DIMENSION 作為區塊鏈分佈式商業應用的服務網絡，如何從技術突破及分佈式商業應用提出解決之道。

1.3

使命與願景

■ 勾勒區塊鏈服務網絡

DIMENSION 通過結合分佈式存儲、混合共識機制、隱私保護、加密算法等技術支撐可快速適配的跨共識引擎、跨鏈數據互聯接口、快速部署發布鏈，從而實現可支持多區塊鏈間的數據共享及價值傳遞的立體服務網絡。

區塊鏈技術實現並塑造了全新的分佈式商業理念，分佈式商業的本質是一種開源的分享經濟。現有商業實體是基於所有權設置的封閉式商業形態，而分佈式商業中商業組織的參與門檻被降低，只要基於某種共識機制，各方都可以參與到組織的運營中，分享或使用區塊鍊網絡資源，通過將自身利益與組織發展綁定實現商業組織的持續運轉。所有參與者基於共識共同完成組織目標獲取回報。通過通證激勵機制，分佈式商業實現了參與者利益與組織利益的統一，形成參與與發展的正循環。

■ 激發分佈式商業價值

隨著全世界數字化進程加劇，數據的採集與生產、存儲與計算、分發與交換、分析與處理已經普遍存在於跨地域、跨領域、跨主體、跨賬戶的各種組織與企業之中，追求多方參與和對等合作的分佈式商業就逐漸凸顯價值。

基於區塊鏈技術的分佈式商業正在加速探索及逐步落地。區塊鏈去中心化、開放性、自治性、不可篡改、匿名性的特性，結合分佈式商業有多方平等參與、智能協同、價值分享、運行透明等特點。實現數據在多源異構的網絡架構中自由流動，數據共享的價值通過生產關係的重構被無限放大。並形成節點之間，鏈之間的多維度鏈接，構建高度複雜的共享網絡。

在區塊鏈網絡中，每個節點都分佈式地存在，在信息透明的環境參與競爭。在區塊鏈分佈式商業模式中，所有權中佔有、使用、收益、處置分離程度大。區塊鏈分佈式商業模式是符合市場規律的模式，對於發揮市場機制有促進作用，提高市場的激勵作用。這種權益分解導致原有的權責利關係發生變化，從而形成新的商業模式。

分佈式商業藍圖也有巨大的想像空間，如分佈式能源、分佈式電商以及各類共享經濟。在分佈式商業模式中，各個參與方能夠在公開、透明的基礎上開展合作，並按各自貢獻來獲得收益。基於 DIMENSION 對區塊鏈的信念與技術的長期探索和積累，在對區塊鏈發展方向進行思考和技術實現的反複驗證下，DIMENSION 致力於實現區塊鏈全網間的商業價值互聯，構建新一代區塊鏈互聯協作的服務網絡。

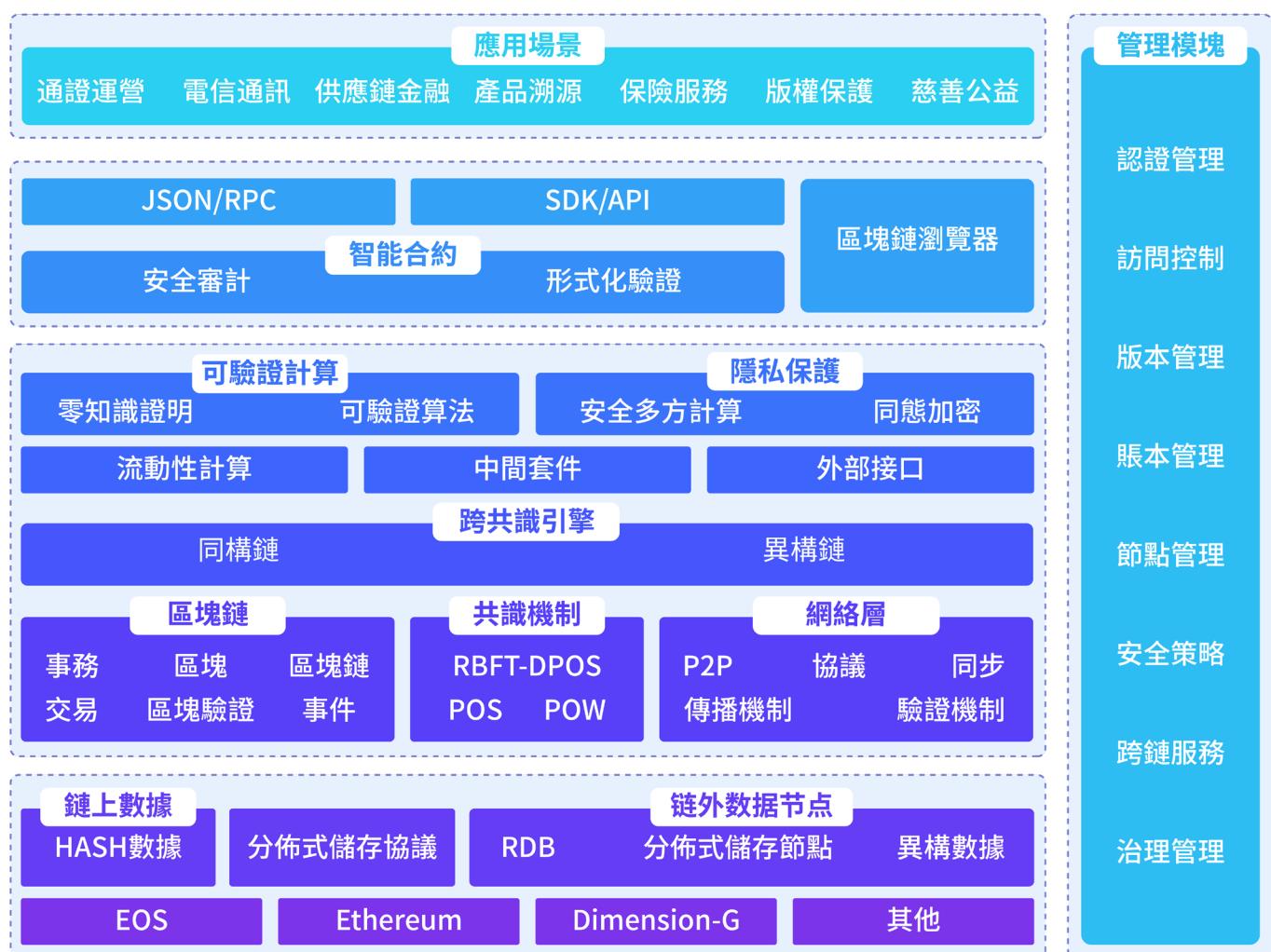
II. 應用服務網絡

APPLICATION

2.1 概述

DIMENSION 是一個非盈利的開源社區項目。從技術層面 整合區塊鏈多項基礎特性，實現區塊鏈的分佈式數據存儲，可行性混合共識機制，數據加密算法，數據隱私保護等功能，從而提供可插拔共識引擎和通用應用及數據交換接口，實現區塊鏈跨鏈互聯的中間件框架。並從底層架構、業務重構、生態治理及應用運營上實現全面革新的多元化、開放化、信任化、分佈式的商業應用服務網絡。

2.2 設計構架



2.3 迭代演進

■ 迭代路徑

泛文娛網絡搭建

泛文娛主網 DIMENSION-G 上線為泛文娛垂直領域服務網絡提供基本功能，包括通用賬戶系統、區塊節點搭建、分佈式賬本記帳、區塊鏈瀏覽器等。平台用戶可以通過內容創作獲得通證獎勵。

多側鍊及生態應用

基於底層主網突出的性能優勢，通過跨共識互聯方案，以代幣及主流數字貨幣錨定，實現 DIMENSION 生態體系內多種數字資產在跨鏈間的高效流通與交易，打通 DIMENSION 與生態側鏈間的完全互聯。

數據共享及交易平台

基於區塊鏈分佈式數據存儲框架，數據隱私保護，採用全同態加密，安全多方計算等創新技術，實現數據在區塊鏈上的革新性共享及數據交易，構建不改變數據所有權的數據共享及數據交易區塊鍊網絡。

分佈式商業賦能

通過跨鏈消息傳遞機制，實現區塊鍊網絡間的資產及數據跨鏈功能。更多參與 DIMENSION 生態的合作方均可安全高效的共享或交易數據，借助人工智能 AI，物聯網 IOT 等關鍵技術，參與對數據的深度挖掘，創建動態模型，快速適配新型分佈式商業場景。實現不同角色、不同行業、不同類型側鏈均可獲取 DIMENSION 生態的全方位支撐和生態化發展，最終構建成全行業立體互聯的嶄新分佈式商業體系。

■ 泛文娛網絡搭建

已落地並推進中的 DIMENSION -G 聚焦泛文娛垂直領域，通用的賬號系統，並支持通證經濟。通過多場景化的智能合約，可進行消費交易、平台內支付、數字貨幣兌換等行為或通證激勵。不僅涵蓋遊戲，也包括 IP、視頻、小說等，平台用戶可以通過內容創作獲得通證獎勵。用戶可將已授權 IP 進行二次創作，通過智能合約自動與創作者及原 IP 所有方進行分成。從而保障了玩家、CP、渠道等多方利益，實現分佈式泛文娛領域生態共贏。

通用賬號系統

賬號系統是 DIMENSION 提供的基礎模塊，用戶使用錨定在區塊鏈上的通用賬號系統，這是一種去中心化的通用賬號，將關鍵信息保存到區塊鍊網絡中，分散在全球的完全等價的區塊鏈節點保障了系統的安全性。

通證交易與智能合約

DIMENSION 代幣可用於鏈上通證經濟系統，通證交易建立在智能合約上進行，智能合約具有自動執行、不可篡改、安全可靠的特性，可替代傳統中心化服務提供商，實現去中心化組織公開公平的自治機制。通過可編程的智能合約，不僅能適配不同應用場景，快速、便捷的完成通證交易，更可解決

現有合約不可監控，甚至無法履約的諸多問題。

■ 多側鍊及生態應用

基於 DIMENSION 構建的應用服務網路，通過 DIMENSION 所提供的各類服務接口，以及服務網絡的突出性能優勢。實現高吞吐量，支持百萬級 TPS；免手續費，針對區塊鏈不合理機制進行改良，解決如 CPU/RAM 質押搶占資源等問題，提升分佈式應用的性能擴展。

DIMENSION 應用服務網絡可承載各行業不同應用場景的 DApp 應用，並消耗 DIMENSION 代幣在整個生態體系的正常運轉形成閉環。服務生態體係將採用社群自治機制，鼓勵並推動優秀應用的持續發展，減少無效應用對生態資源的浪費，促進服務網絡的多向循環、良性發展。

與此同時，服務網絡還將通過對應用大數據收集及分析，輸出及共享關鍵數據和動態趨勢，用於行業和關聯應用的運營支持。此外，側鏈上不同類型數據更可通過 DIMENSION 獨有的數據交易平台實現價值共享。

■ 數據共享交易平台

DIMENSION 基於分佈式存儲，隱私保護，安全多方計算等技術，可提供數據資產應用交易平台，實現生態內多種數據資產的流通與交易。用戶通過平台的智能合約設定交易條件，智能合約將自動完成數據標的、數據使用權交易、加密多方計算、結果驗證及反饋等一系列行動。

通過數據應用交易平台，數據持有方不僅通過區塊鏈匯集、分析、挖掘自有應用數據，也可同時從其他數據持有方購買、交換、消費指定數據。數據的所有權和使用權從而得到有效剝離，在不改變數據所有權的前提下，即數據明細仍歸原數據持有方所有，數據的使用權則被視為獨立數據資產進行交易。

基於數據輕所有權、重使用權的機制下，數據價值得到確認和放大。數據不再類似傳統模式下，隨著數據的交換而失去數據所有權，在數據應用交易平台上僅是數據使用權的交易。並且，通過完全公開透明的數據驗證規則，失效數據和造假數據將被智能合約和結果驗證算法直接捕獲，導致無法獲得數據使用方的交易確認；從此數據所有方將更為重視數據質量，確保數據的真實性、有效性。

借助維度鏈數據 應用交易平台，極大降低數據使用方的交易風險，且支持更為靈活可控的數據交易，有效減少數據的使用成本。數據使用權交易帶來的益處顯而易見，勢必將改變傳統數據交易模式，成為區塊鏈應用網絡上最為基礎應用場景，大幅度提升數據的流轉和使用，充分發揮數據在共持共享的嶄新商業價值。

■ 分佈式應用賦能

伴隨著分佈式應用服務網絡的不斷迭代，更多運行在不同類型鏈的應用，希望藉助一個可跨鏈並性能優異立體異構網絡的，整合分佈式多維信息系統。通過完善的跨鏈消息傳遞機制，實現區塊鍊網絡間的資產及數據跨鏈功能，實現數字資產的自由流通和相互賦能。

作為應用服務網絡生態化的倡導者和持續實踐者，不斷吸納優秀的各行業應用融入到 DIMENSION 生態體系中，如文娛遊戲，金融保險，智能物聯等領域，結合可拓展的生態架構與應用接口，構建跨鏈、跨行業、跨應用的分佈式應用服務網絡。同時隨著生態應用的不斷搭建和完善，各類基礎服務和功能應用爆發式增長，如數字交易所、冷熱錢包、自治社群等，為各行業商業合作夥伴在 DIMENSION 生態體系中，實現區塊鏈創新性商業應用提供全面支撐和服務。

III. 項目特性

FEATURES

極速發展的區塊鏈技術，推動著加密算法、共識機制等關鍵技術的創新和突破，為支撐各類嶄新商業模式提供可能。DIMENSION 始終堅信，唯有融合不斷創新和突破的技術方可構建性能優異和高擴展性的分佈式應用網絡。

3.1 高性能

DIMENSION 借鑒現有成熟區塊鏈設計框架，並不斷改進和優化算法，構建高並發性能的區塊鍊主網。較強的並發能力可達到 0.5 秒的平均確認速度和有限條件下實測 10000TPS 的數據吞吐量。為區塊鏈上有著高並發性訴求的商業場景提供了性能實現支撐。

DIMENSION 並發性還體現在，出塊速度快，理論上可以到 10 萬 TPS，甚至可以擴展到百萬 TPS。成熟的技術方案使得其穩定性能已得到長期驗證，自開發運行多年來暫未出現明顯漏洞和問題，這也是 DIMENSION 底層協議框架可支持更多生態應用的核心優勢和重要支撐。

3.2 分佈式存儲

受限於早期區塊鏈數據結構設計，鏈上賬本僅可用於存儲哈希數據，並不能有效用於存儲大量數據。因此對於區塊鏈涉及到海量數據持久化問題，成為區塊鏈能否結合區塊鏈商業應用至關重要的前提。

DIMENSION 結合分佈式哈希表，並通過分佈式存儲文件系統的點對點超媒體協議，實現 DIMENSION 對去中心化的存儲網絡的需求。在此存儲網絡中，DIMENSION 網絡中的每個節點都可以提供存儲空間，提供網絡中的其他節點進行存儲，同時也提供傳輸，依據規則向網絡中需要讀取該文件的節點發送本地存儲的文件，DIMENSION 更好地支持對原生數據的共享和流轉。借助分佈式存儲系統，可實現去中心化的更快、更安全、更開放的高吞吐量內容尋址塊存儲模型。可滿足行業應用的大數據存儲需求，如電信通訊，金融保險等等。

DIMENSION 分佈式存儲系統是一個旨在創建持久且分佈式存儲和共享文件的網絡傳輸協議，是一種內容可尋址的對等超媒體分發協議。它是一個面向全球的、點對點的分佈式版本文件系統，試圖將所有具有相同文件系統的計算設備連接在一起。帶有激勵機制的塊交換和自我認證命名空間，分佈式存儲系統有可能取代過去互聯網採用的超文本媒體傳輸協議（HTTP），或成為區塊鏈世界的核心傳輸協議。



3.3 混合共識機制

DIMENSION 在綜合分析現有主流共識時，注意到單一共識雖然在實現上的便捷和易維護，但是在區塊生成的效率和安全性存在諸多弊端，如出塊時間長及確認不及時，部分共識算法易導致分叉或雙發，無法有效提升區塊鏈性能。因此 DIMENSION 選取了混合共識機制，採取 DPOS（授權股權證明）和 RBFT（拜占庭 共識算法）結合的方式。實現原理為，每個見證人出塊時全網廣播，其他見證人收到新區塊後，立即對此區塊進行驗證，並將驗證簽名完成的區塊立即返回出塊見證人，不需等待其他見證人自己出塊時再確認，極大提升區塊出塊的性能及穩定性。

■ 共識概述

共識機制是確認區塊鏈記帳權的核心概念，用於分佈式賬本確保所存儲信息的準確性與一致性 而設計的一套確權機制，機制的設計需考慮到安全、性能和成本的需求。從 PoW 到 PoS 再到 DPoS 和各種拜占庭容錯算法，共識機制不斷創新，在確保所有節點能公平公正參與的前提下，區塊鏈出塊性能也得到大幅提升。

工作量證明（PoW）共識機制

最早應用於比特幣，區塊鏈中讓各節點通過算力比拼，進行哈希計算，使得獲勝節點確認記帳權的合法性。其缺點顯著，工作證明比拼算力，專業礦

池逐漸形成壟斷，排除了普通挖礦參與者，使得記賬權越發趨於中心化；並且挖礦耗費大量能源，造成大量資源浪費。

股權證明（PoS）共識機制

根據每個節點所佔通證的比例和時間折算成幣齡，從比拼算力演化為比拼幣齡。PoS的優點是相對PoW顯著提高了效率，缺點是依然需要耗費算力，浪費能源不適用於高並發的需求。

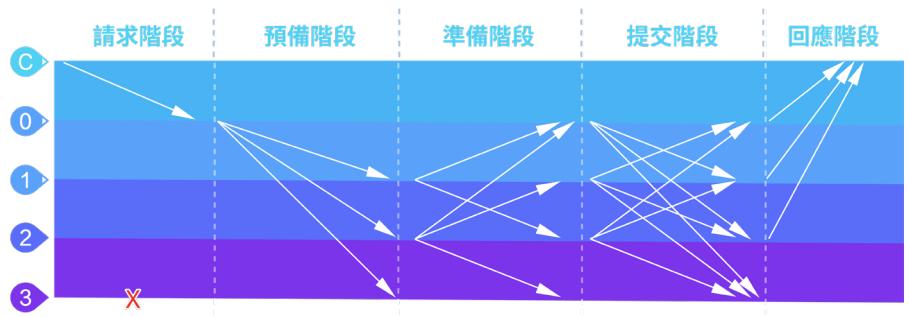
授權股權證明（DPoS）共識機制

是由被社區選舉的可信代理人來按順序輪流出塊。區塊鏈上持有通證的用戶均可通過投票持續選擇區塊生產者，任何人都有機會成為出塊見證人。每個代理人出塊時向全網廣播，需要等待輪到自己出塊時，才能通過生產區塊來確認之前的區塊，且要求三分之二以上確認後區塊才能生效。

■ RBFT 拜占庭

PBFT（Practical Byzantine Fault Tolerance）共識機制涉及拜占庭將軍問題，證明了在將軍總數大於 $3f$ ，背叛者為 f 或者更少時，忠誠的將軍可以達成命令上的一致，即 $3f+1 \leq n$ ，算法複雜度為 $O(n^{(f+1)})$ 。PBFT算法容錯數量也滿足 $3f+1 \leq n$ ，算法複雜度為 $O(n^2)$ 。因此拜占庭容錯能夠容納將近 $1/3$ 的錯誤節點誤差。RBFT（Redundant Byzantine Fault Tolerance）是多線程模型執行多個PBFT實例。

基於拜占庭將軍問題，一致性確認主要分如下三個階段：



預準備階段（Pre-prepare）

主節點分配一個序列號 n 給收到請求，隨後向所有備份節點群發預準備消息，請求本身不包含在預準備消息裡，可使預準備消息足夠小。因為預準備消息僅作為一種證明，確定該請求是在視圖 v 中被賦予了序號 n ，從而在視圖變更過程中可追溯。另外，將“請求排序協議”和“請求傳輸協議”進行解耦，利於對消息傳輸的效率進行深度優化。

進入準備階段（Prepare）

如果備份節點 i 接受了預準備消息則進入準備階段。在準備階段的同時，該節點向所有副本節點發送準備消息，並將預準備消息和準備消息寫入自己的消息日誌。

進入確認階段 (Commit)

當 (m, v, n, j) 條件為真的時候，副本 i 將向其他副本節點廣播，於是就進入了確認階段。

■ RBFT-DPoS

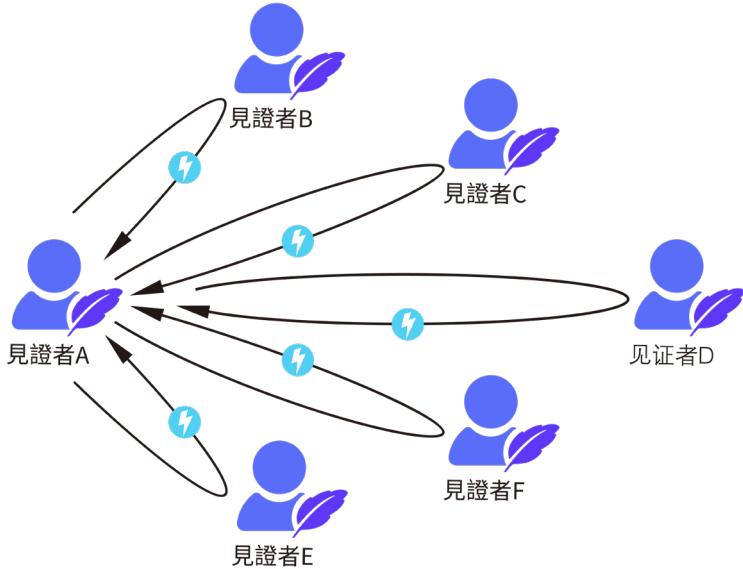
DIMENSION 綜合對現有多類單一共識機制的優劣分析得出，共識機制既要保證公平，安全的同時，也需要考慮到對性能的要求。因此，DIMENSION 創新性 採用混合共識機制（RBFT- DPoS）進行分佈式記賬，即通過授權股權證明機制（DPoS）持通證者投票選擇一定數量的代理出塊節點，代理全網節點進行驗證和記賬，並由代理節點全部參與出塊記賬。再結合拜占庭共識機制確認有效出塊則被寫入帳本，杜絕作惡節點和失效節點對記賬的潛在風險。

在混合共識機制中，每個見證人出塊時全網廣播，其他見證人收到新區塊後，立即對此區塊進行驗證，並將驗證簽名完成的區塊立即返回出塊見證人，不需等待其他見證人自己出塊時再確認。具有大幅縮小參與驗證和記賬節點的數量，可以達到秒級的共識驗證，符合維度鏈的高頻交易和高並發的業務需求，更是摒棄了比拼算力，浪費資源的問題，以及規避了單一代理節點因失效或作惡或對全網帶來的巨大潛在風險，為絕大多數業務高並發性需求的實現提供共識機制支撐。

DIMENSION 將已得到區塊鏈行業充分驗證的共識機制 RBFT 和 DPoS 進行有效結合，形成更具實用性和安全性的混合共識機制（RBFT- DPoS）。此混合共識機制分別結合了 RBFT 及 DPoS 共識機制各自優點，實現在區塊鏈出塊性能及安全性之間平衡方案。

對於 RBFT 共識機制，通過允許所有生產者簽署所有區塊，實用拜占庭容錯機制被添加到傳統 DPoS 中，只要沒有生產者簽署具有相同時間戳或相同區塊高度的兩個區塊。一旦達到閾值數量的生產者簽署了一個區塊，則這個塊被視為不可逆轉的。如果拜占庭式的生產者簽署了兩個相同時間戳或相同區塊高度的區塊，那麼系統會生成其不忠行為的密碼證據。在這一模式下，不可逆的共識可在 1 秒內可達成，安全性和穩定性得到提升。

對於 DPoS 共識機制，將原設定的隨機出塊順序升級為由見證人商議後確定的出塊順序，這樣網絡連接延遲較低的見證人之間就可以相鄰出塊，這樣可以大大降低見證人之間的網絡延遲，新區塊的生產和舊區塊確認的接收同時進行。絕大部分情況下，交易會在 1 秒之內確認並不可逆，其中包括了 0.5 秒的區塊生產，以及要求其他見證者確認所需時間，性能得到保證。



3.4 隱私保護

在區塊鍊網絡中，每一個參與者都能夠獲得完整的數據備份，所有交易數據都是公開和透明的，這個區塊鏈的優勢特點，從安全角度來講，特別是針對商業敏感數據，這個特點是致命的。隨著歐盟《通用數據保護條例》(GDPR)的實施，隱私保護對區塊鏈應用提出了訴求，就商業機構來說，很多帳戶和交易信息更是這些機構的重要資產和商業機密，不希望公開分享。DIMENSION 已將隱私保護作為區塊鏈公鏈開發的核心，通過保護個人隱私和商業機密數據的技術手段，推動商業需求在維度鏈應用網絡的落地。

區塊鏈技術快速發展和日趨成熟，在商業應用落地過程中，數據安全，隱私保護，加解密技術便成為區塊鏈能否成功擁抱商業應用的基礎。隨著區塊鏈技術的深入研究和技術迭代更新，DIMENSION 將前沿的隱私保護技術與區塊鏈應用結合，例如同態加密、零知識證明等，針對特定的商業應用場景提供技術支撐。

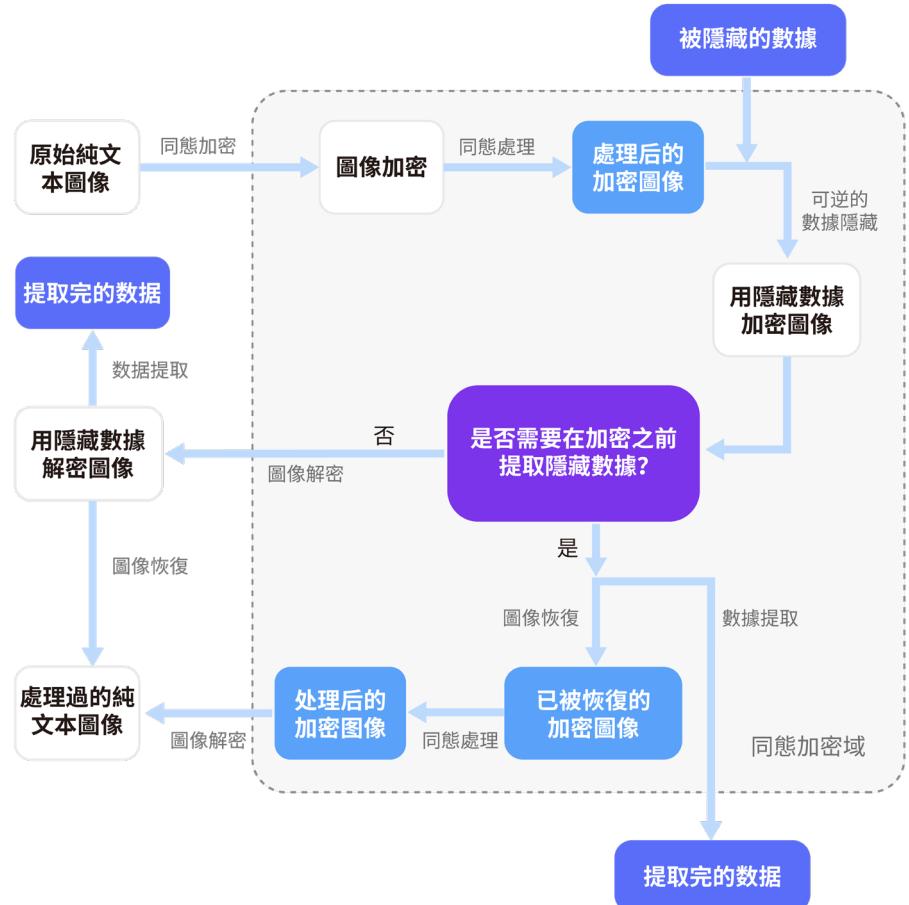
■ 全同態加密

全同態加密（Fully Homomorphic Encryption）是一種無需對加密數據進行提前解密就可以執行計算的方法，可以對加密數據做任意功能的運算，運算的結果解密後相應於對明文做同樣運算的結果。

與區塊鏈技術結合，通過使用同態加密技術在區塊鏈上存儲數據可以達到一種完美的平衡，不會對區塊鏈屬性造成任何重大的改變。特別對於公有區塊鏈，區塊鏈上的數據將會被加密，因此照顧到了公有區塊鏈的隱私問題，同態加密技術使公有區塊鏈具有私有區塊鏈的隱私效果。全同態加密方案是一個功能性和平安性的最佳方案，但存在計算開銷大，需結合特定場景應用。

DIMENSION 結合同態加密技術在數據存儲源頭對數據進行加密處理後持久化，確保數據的隱私保護。當數據有使用需求時，通過智能合約對指定加密數據提取做複雜運算處理，僅將最終結果數據解密後反饋，並明文顯示給數

據使用方。同時，使用方可通過驗證算法對結果數據做真實性和準確性驗證。同態加密方案可結合電信通訊，金融保險等敏感數據商業場景。



$$\forall m_1, m_2 \in \mathcal{M}, E(m_1 \odot_{\mathcal{M}} m_2) \leftarrow E(m_1) \odot_{\mathcal{C}} E(m_2)$$

其中， \mathcal{M} 表示明文的集合， \mathcal{C} 表示密文的集合， \leftarrow 表示可以從右式計算得出左式。特別的，有

$$\begin{aligned} \forall m_1, m_2 \in \mathcal{M} \quad E(m_1 +_{\mathcal{M}} m_2) &\leftarrow E(m_1) +_{\mathcal{C}} E(m_2), \\ E(m_1 \times_{\mathcal{M}} m_2) &\leftarrow E(m_1) \times_{\mathcal{C}} E(m_2). \end{aligned}$$

分別為加法同態，乘法同態。

■ 零知識證明

DIMENSION 採用非對稱加密來做身份認證，驗證方只要使用公鑰解出自己提供的隨機數，即可證明被認證方的身份，不需要其提供自己的私鑰。DIMENSION 服務網絡開放針對零知識證明的接口，可應用於保險理賠領域，例如保險公司在審核某被保人病史時，可通過調用接口查詢並反饋單一結果，但查詢人並不能獲得被保人的相關病史資料，也無法得知查詢結果是從什麼機構反饋的。實現了數據解耦，及數據的受控共享，或將成為應用服務網絡的典型應用場景。

零知識證明（Zero Knowledge Proof）

是一種無需洩露數據本身情況下證明某些數據運算的一種加密學技術，允許證明者和驗證者證明某個提議的真實性，且無需洩露除了真實性之外的任何信息。零知識證明具備如下特點：

完整性

如果論述是真實的，誠實的驗證者（也就是正確遵循協議的一方）將能夠通過一個誠實的證明者來相信該事實。

可靠性

如果論述是錯誤的，欺騙性的證明著無法讓誠實的驗證者相信它是真實的，除了一些小概率。

零知識

如果論述是真實的，欺騙性的驗證者無法獲得該事實之外的其它信息。

同態隱藏

我們現在可以建立一個“支持加法”的 HH - 這意味著 $E(x+y) = E(x) + E(y)$ 可以由 $E(x) = g^x$ 和 $E(y) = g^y$ 計算得到。我們假設 EE 中的輸入來自 $Z_p - 1$ 到 $Z_p - 1$ ，因此它的範圍是 $\{0, \dots, p-2\}$ 。我們將這樣的 x 定義為 $E(x) = g^x$ ，並稱這樣的 EE 是一個 HH：第一個特性表明，在 $Z_p - 1$ 中的不同 x 會映射不同的輸出。第二個特性表明，對於確定的 $E(x) = g^x$ ，很難計算出 x 。最終，使用第三個特性，對於給定的 $E(x) = g^x$ 和 $E(y) = g^y$ ，我們可以計算出 $E(x+y) = g^{x+y}$ 為：
$$E(x+y) = g^{x+y} \bmod p - 1 = g^x \cdot g^y = E(x) \cdot E(y).$$
$$E(x+y) = g^{x+y} \bmod p - 1 = g^{x+y} = g^x \cdot g^y = E(x) \cdot E(y).$$

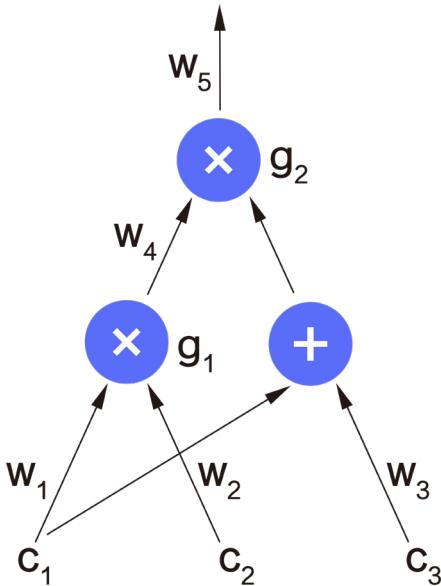
盲法評估多項式

我們看到了由 $E(x) = g^x$ 定義的 HHE EE，其中 g 是由一組難離散對數的結果而產生的。我們提到這個 HH “支持求和”的意義是 $E(x+y) = E(x) + E(y)$ 可以由 $E(x) = g^x$ 和 $E(y) = g^y$ 計算得出。我們注意到它同樣“支持線性組合”，這意味著，對於給定的 $a, b, E(x), E(y)$ ，我們可以計算出 $E(ax+by) = E(x)a + E(y)b$ 。因此得出計算方式為：

$$E(ax+by) = g^{ax+by} = g^{ax} \cdot g^{by} = (g^x)^a \cdot (g^y)^b = E(x)^a \cdot E(y)^b.$$

數字環路

一個數字環路由多個數字計算門組成，其功能類似於加法和乘法，通過使用線路鏈接門。在我們的應用場景中，環路的樣子如圖所示：



- 當相同的輸出先進入不同的門，我們將其視為同一根線 - 就像例子中的 $w_1 w_1 w_1$ 。
- 我們假設乘法門有兩個輸入線，我們將其稱為左側輸入線和右側輸入線。
- 我們並不為從加法門進入乘法門的線路標記標籤，也不為加法門設置標籤；我們認為加法門的輸出直接進入乘法門的輸入。因此，在例子中，我們認為 $w_1 w_1 w_1$ 和 $w_3 w_3 w_3$ 都是 $g_2 g_2 g_2$ 的右側輸入。

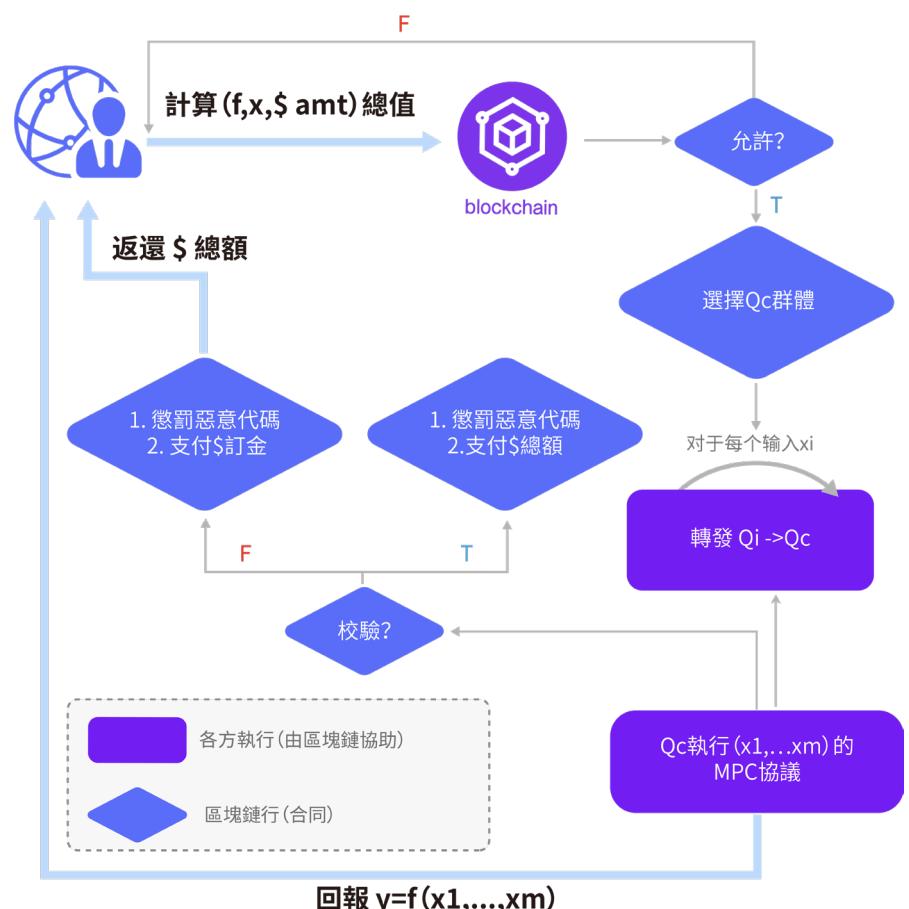
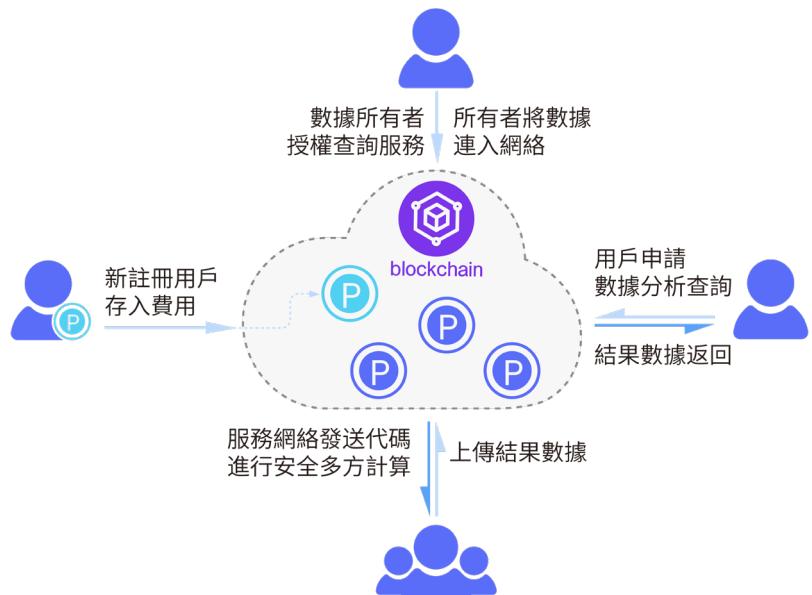
■ 安全多方計算

安全多方計算 SMPC (Secure Multi Party Computation) 在一個分佈式網絡中，多個用戶各自持有部分數據輸入，他們希望協作完成對全量 數據的計算，同時要求每個用戶除計算結果外均不能夠獲知其他用戶的任何輸入信息。

DIMENSION 通過建立面向數據的基礎傳輸層和基於人工智能的算法模型，通過協同計算傳輸協議，並結合圖靈完備編程語言和多方計算沙盒，確保了數據隱私和計算執行的安全可控，從而實現了區塊鏈的多方安全計算。

對於多方計算所需考慮其安全性、隱秘性、公平協作等因素，維度鏈搭建一套支持高並發的底層協同計算框架，面向參與計算方開放接口。數據持有方可通過私密共享數據到 DIMENSION 計算框架中，同時授權 DIMENSION 服務網絡可接入新數據源，參與多方計算任務。當新計算需求被發起後，協同計算網絡確認計算申請，並傳遞執行代碼到多個計算參與方，對目標數據執行處理和計算，最後反饋結果數據給多方確認。以上流程均通過隱私計算協議傳輸，從而實現了各個計算節點在信息隱私保護的前提下實現數據協同計算。

高階多方計算流架構如下：



上圖：計算內部的一個視圖。當服務將代碼送到云時會發生什麼。

(T: 正確 F: 錯誤)

1. 預處理，獨立數據的隨機性輸入及預處理的雙向共享在此階段執行，數據持有者僅在此階段參與處理，後續階段數據持有者不再參與。
2. 在線階段，實際的在線多方計算被調用，即為並行共享開銷，並且循環計算的深度是可調節的。
3. 處理後期，在誠實或惡意參與方（包括服務）的確認上，並且在分發相應酬勞和懲罰上，區塊鏈節點達成共識。

前兩個階段（離線和在線）包含了多方計算的標準預處理模型。唯一的差異在於輸入共享被推送到離線階段，因為在線狀態要求必須為同步執行。基於上述規則，缺少輸入並非是個問題，因為在線階段可以異步執行。

3.5 跨鏈互聯

DIMENSION 作為分佈式應用服務網絡，注重不同異構網路的互聯互通，DIMENSION 支持各種跨鏈協議，實現各類數字資產通過維度鏈高效流通，構建去中心化的區塊鏈服務網絡。

涉及到跨鏈互聯則需遵從兩個重要特性：第一，需要有及時最終性的共識算法，所謂及時最終性是指 遵從共識機制生成的新區塊，這個塊是不可逆的最終確定區塊。第二，交易的提交確認可通過高效且獨立的 Merkle 進行證明。對照 DIMENSION 網絡分析，其共識機制基於拜占庭容錯，通過分佈式的共識算法基於弱同步的投票機制，可以最多容忍三分之一的拜占庭節點。同時，基於 DIMENSION 混合共識形成的最新區塊就是最終區塊，符合及時最終性。



DIMENSION 將兼容支持多類不同的數據交換協議，以支持不同的業務場景需求。同時將數據交換協議與分佈式賬本結合，形成分佈式的數據交換流程，並提供系列的數據與隱私保護的密碼學組件支持。DIMENSION 將形成多代幣賬戶體系，網絡中見證節點負責共識和出塊，互聯鏈的通信協議跟 DIMENSION 進行連接，每個鏈都可完成特有功能，從而構成一個支持多鏈多幣的經濟高度集成的生態化服務網絡。

3.6 流動性算法

DIMENSION 基於數字資產流動性算法，使得智能合約在區塊鏈上代幣的價格發現和流動機製成為可能。這些新型智能代幣持有一種或多種其它代幣作為準備金，這些被持有的代幣，我們統稱為“準備金代幣”。持有這些智能代幣的人，可以即時的買入或賣出這些智能代幣用於交換它持有的某種“準備金代幣”。這些即時的買入或賣出過程則是通過智能合約實現。交易價格是通過一個以與交易量為變量的數學公式計算得出的。

智能代幣採用一種創新的策略促成價格發現，這種策略即恆定準備金率（Constant Reserve Ratio）策略，簡稱為 CRR。CRR 由智能代幣的創建者為每一種準備金代幣設定，並結合智能代幣當前供應量和準備金代幣餘額計算出代幣價格，公式如下：

$$Price = \frac{Balance}{Supply \times CRR}$$

3.7 中間件應用框架

DIMENSION 作為面向區塊鏈技術的企業中間件，通過敏捷開發組件、且支持靈活配置的區塊鏈套件，可根據不同企業針對所屬行業快速實現具有高適配性的主鏈。借助 DIMENSION 的兼容自適應框架，跨共識數據並行方案，推動區塊鏈技術在商業場景的快速落地及應用。

中間件應用框架開放各位 API 接口，供區塊鏈應用提供高效穩定的服務，如外部接口、用戶 API、管理 API 等，涵蓋開發、運營、安全、監控和審計等多個方面。



3.8 數據交易

DIMENSION 為一個去中心化數據服務平台，提供一系列的密碼學和數據安全組件支持，包括數據加密傳輸、密鑰分享協議、多方密鑰管理、環簽名組件、盲簽名組件等技術，為全網節點提供數據交易接口。並針對特定場景，提供特定安全組件，根據不同場景需求對數據交易平台進行不斷拓展和探索。

現今“數據驅動未來”已成共識，但數據造假、過期、敏感數據被非法倒賣等情況也屢見不鮮，傳統中心化的數據交易平台存在數據緩存、數據丟失的風險。借助區塊鏈技術，DIMENSION 將構建一個去中心化數據交易平台，是分佈式數據存儲、點對點傳輸、共識機制、加密算法等技術的集成應用。採用區塊鏈技術推動數據確權、數據溯源，通過共識算法建立可信任的數據資產交易環境，破除數據被任意複製的威脅，保障數據擁有者的合法權益，促進數據要素流通融合。數據交易可覆蓋如金融、通信、交通、營銷、商貿、機器學習等多個數據領域。

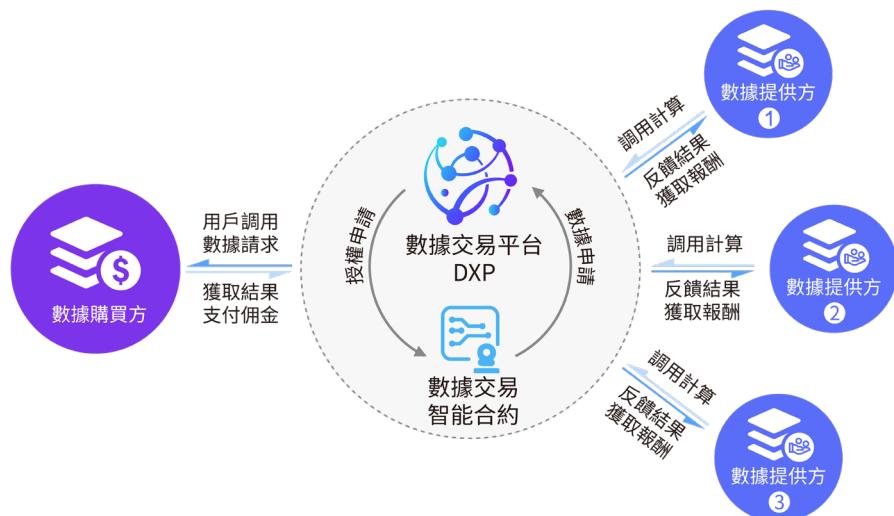
■ 數據交易多方網絡

區塊鏈點對點的傳輸機制及不可篡改性則是中心化的數據交易平台無法比擬的優勢。數據買賣雙方通過智能合約執行數據交易，數據通過點對點的方式進行傳播。建立基於區塊鏈的數據交易所，記錄交易數據，共同驗證交易，實現數據資產的可信交易，從而調動數據所有者積極性，讓數據要素廣泛而有序地流通。維度鏈服務網絡中的數據交易服務商可以在此基礎上實現各類別、各領域的數據交易。

■ 原生數據共享流轉

DIMENSION 提供兩類數據交易方式：第一類原始數據交易，當數據需求方提出數據訴求時，消息通過 DIMENSION 向全網進行廣播，而數據源通過查詢自身離線數據庫，如有匹配數據則通過智能合約進行點對點數據交易。第二類數據查詢交易，即數據需求方並不關心明細數據，而是僅需要反饋數據計算後的結果，這類需求則無需對數據明細進行傳輸，僅按智能合約執行代碼返回結果集給需求方即可，此過程可能涉及到多個數據持有方的參與計算，則需要對多個參與方提供有償或等價數據服務。

此外，數據交易平台基於大數據和匯集眾多服務節點，服務不僅限於數據資產本身，還可延展為對數據的深度挖掘，如數據趨勢分析、商業智能分析、數據智能預測等，及全網計算能力的交易，最大化發揮 DIMENSION 作為服務網絡的核心價值。



IV. 治理架構

ARCHITECTURE

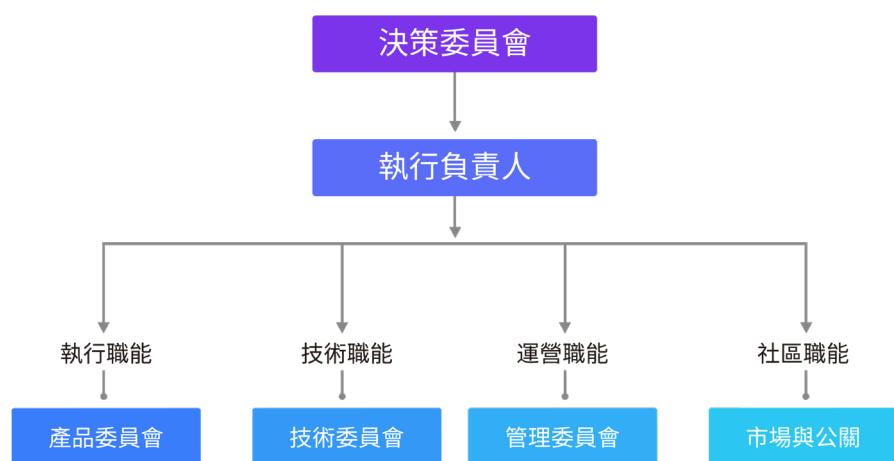
4.1

基金會及治理框架

DIMENSION 生態將由設立在新加坡的維度鏈基金會進行管理。該機構作為 DIMENSION 的法律主體，負責技術開發、業務推廣、社區運營，同時承擔所有的法律責任。基金委員會下設立有：

決策委員會

決策委員會是基金會最高決策機構，管理基金會旗下各個執行機構，有權決定基金會資金使用、獎勵、懲罰、凍結等，決策委員會成員由社區選舉產生。決策委員會任期為兩年，在任期滿後，由社區進行投票選舉產生。其中決策委員會下設立四個執行機構，如圖所示：



產品委員會

負責整體產品的設計規劃、業務推廣、商業拓展、生態搭建等。

技術委員會

負責技術開發管理、代碼開源管理、Github 開源代碼維護、社區技術更新評估等。

管理委員會

負責基金會管理，包括成員的日常補貼發放、正常財務支出、項目募集資金使用和審核等。

市場與公關委員會

負責社區運營和管理、活動策劃、資源對接、社區獎勵發放、社區懲罰執行以及公關問題處理。

4.2 核心團隊



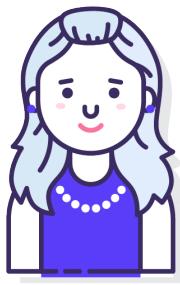
Alvin Chan | CEO & Founder

擁有 10 多年上移動互聯網、遊戲行業的經歷。曾任神州圖驥 MOC 總經理。13 年創立笨鳥網絡，製作發行了百餘款單機遊戲，其中包括太極等優質產品，總遊戲下載量過億。15 年初涉足區塊鏈行業，其創立的魔橙網絡獲得上海萬向區塊鏈股份公司國內投資（區塊鏈領域國際國內最頂尖最專業的機構）。作為萬向區塊鏈聯合創新團隊，主要負責人參與主導保險、慈善、公證等眾多區塊鏈項目的實施與落地。並建立了創新型分佈式流量平台—“星柚”，註冊用戶超千萬。



Step Tsou | CTO

擁有近 20 年的研發經驗，曾任神州圖驥技術中心總監，負責集團公司所有參與過多款移動 APP 開發及平台開發，擁有多年開發管理經驗。參與過多款移動 APP 開發及平台開發，參與底層鏈研發，擁有多年開發管理經驗。



Hanyu Tang | UI & PM

畢業於上海交通大學藝術設計專業，擁有同濟大學設計學及米蘭理工大學產品服務體系設計雙碩士學位。曾為阿斯頓馬丁，保時捷，華為，adidas 等多家知名品牌服務，主導並參與設計多款互聯網保險產品及區塊鏈產品。專註於品牌，視覺，用戶體驗等多個設計領域。



Daniel Huang

擁有 12 年 IT 技術、系統架構、研發管理經驗，曾服務於 Infosys 、 華為、摩根斯丹利、惠普等公司，主導及參與項目商業分析、實施，並主導參與多個區塊鏈產品設計，擔任項目管理 PMP 。

4.3 經濟模型

內置兩種原生代幣，管理代幣 Dimension Token（縮寫符號 DMCT）和 燃料代幣 Dimension Gas（縮寫符號 D GAS）。代幣流通，在去中心化生態中大家按照約定的基本規則自由流通，平台生態既不參與，也不監管。

DMCT 是 DIMENSION 管理代幣，在 DIMENSION 網絡的創世塊裡 20 億枚 DMCT 已經生成，總計發行數量為 20 億，永不增發。用於實現對 DIMENSION 網絡的管理權，包括投票進行記賬人選舉等。項目方也通過交易所回購 DMCT 來調控市場，以實現緊縮的通證市場。

DGAS 是 DIMENSION 燃料代幣，最大總量上限為 1 億枚，用於實現對 DIMENSION 網絡使用時的資源控制。DIMENSION 網絡對代幣轉賬和智能合約的運行和存儲進行收費，從而實現對記賬人的經濟激勵和防止資源濫用。

代幣回流，用戶在平台內消費所支付的手續費，除了部分獎勵給區塊鏈記賬者，其餘回流到基金會的通證池中，保障平台的穩定與發展。

4.4 分配方案

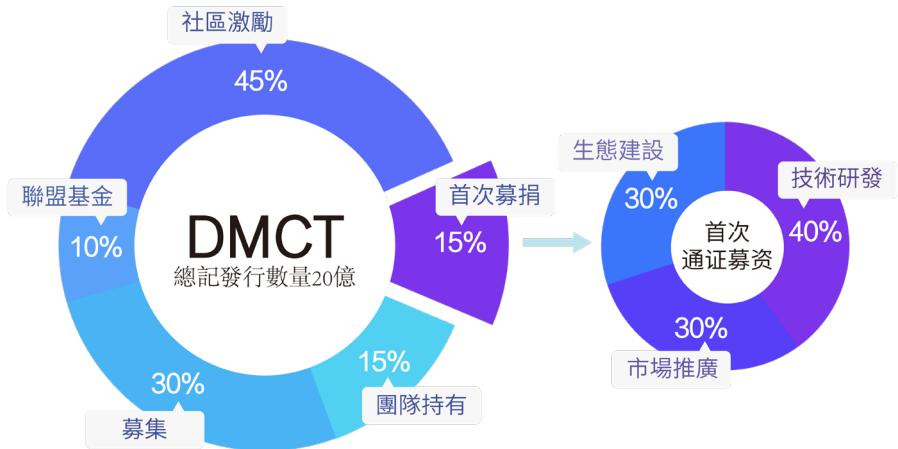
■ DMCT 分發

DMCT 總計發行數量為 20 億，永不增發，分發佔比如下：

- 30% 對私募集，僅面向基石輪和投資人等特定購買者，非公開售賣，籌集幣種為以太幣（ETH）。首輪募集 15%，硬頂 20%，剩餘部分在主網上線後啟動募集。
- 10% 聯盟基金，保留以支持基金會運做。
- 45% 社區激勵，社區生態預留，用於社區獎勵或售賣。
- 15% 團隊持有，鎖定期為 4 年，所得通證將分 48 個月發放。

首批通證募資 資金（15%）使用預算方案為下：

- 技術研發 40%
- 市場推廣 30%
- 生態建設 30%



目前不接受中國大陸國籍及美國國籍的個人投資者。如欲了解更多詳情，請參閱我們的服務條款及合規聲明。

■ DGAS 分發

DGAS 伴隨著每個新區塊的生成而產生，DGAS 初期總量為零，伴隨著新區塊的生成逐漸增多，直至約 20 年後達到總量上限 1 億。DIMENSION 每個區塊的間隔時間約為 3-5 秒，600 萬個區塊約合 1 年時間。

■ 鎖倉機制

DIMENSION 將對 ERC20 代幣和原生代幣進行一定期限的鎖倉，鎖定的代幣不允許在市場上流通交易，到期才能解鎖買賣。持幣者將代幣發送到項目方制定的錢包地址或者智能合約地址進行鎖定。

■ 回購機制

DIMENSION 基金會每年會對社區的代幣進行回收銷毀，銷毀記錄會第一時間向全網公佈，並且用戶可以查詢，全程可監督和透明化，直到銷毀總量 6 億 DMCT 代幣為止。

■ 增發機制

隨時 DIMENSION 生態發展的不斷提升，共識參與者和底層開發社群的不斷壯大。以及項目長期穩定發展，和所有項目參與方的利益回饋。可通過調節增發比例，調節共識參與者可以獲得的無風險收益比例，進而調節共識的參與度。達到項目生態長期收益及分配的正循環。

4.5 治理機制

DIMENSION 採用鏈上治理及鏈下治理並行模式。

鏈上治理

凡持有 DIMENSION 管理代幣的持有人，作為 DIMENSION 網絡所有者和管理者，可通過投票方式實行管理權。通過持有 DGAS 燃料代幣來實現對 DIMENSION 網絡的使用權。

鏈下治理

通過決策委員會，及其下設產品委員會、技術委員會、管理委員會、市場與公關委員會分別負責產品及生態決策、技術決策、基金會管理及市場運營。

4.6 披露事項

每年基金會將向社區披露 DIMENSION 的開發情況、服務網絡運營情況、代幣使用情況以及基金會的運作是否符合治理章程。

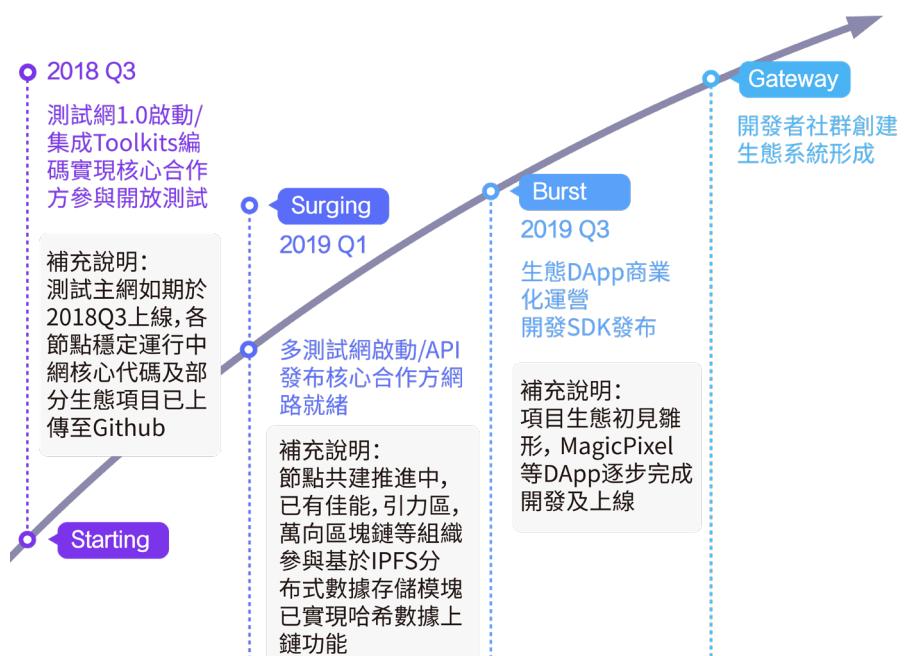
4.7 法律及免責

DIMENSION 基金會在香港成立，若出現需要尋求法律意見的事項，需要通過當地律師予以確認。

DIMENSION 基金會為非營利組織，鏈上用戶獲取的 DIMENSION 使用權，購買者應明白在法律範圍內，代幣不做任何明示或暗示的保證。此外，購買者應明白代幣不會在任何情況下提供退款。

V. 實施及迭代 IMPLEMENT

5.1 路線圖



VI . 生態應用

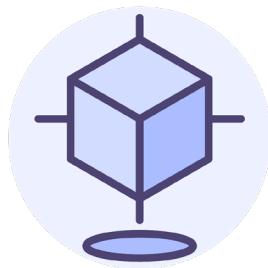
ECOLOGICAL APPLICATIONS

6.1

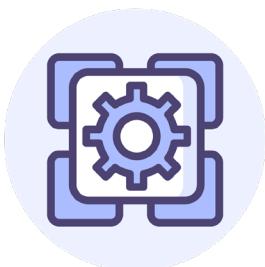
結合行業場景應用



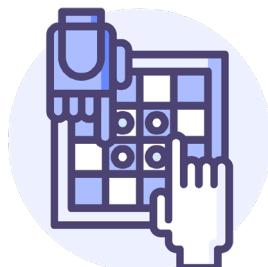
場景一
產品溯源



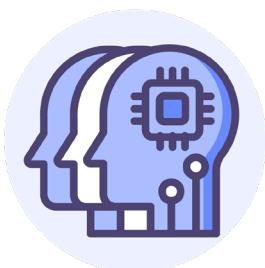
場景二
通證積分



場景三
公證



場景四
泛文娛

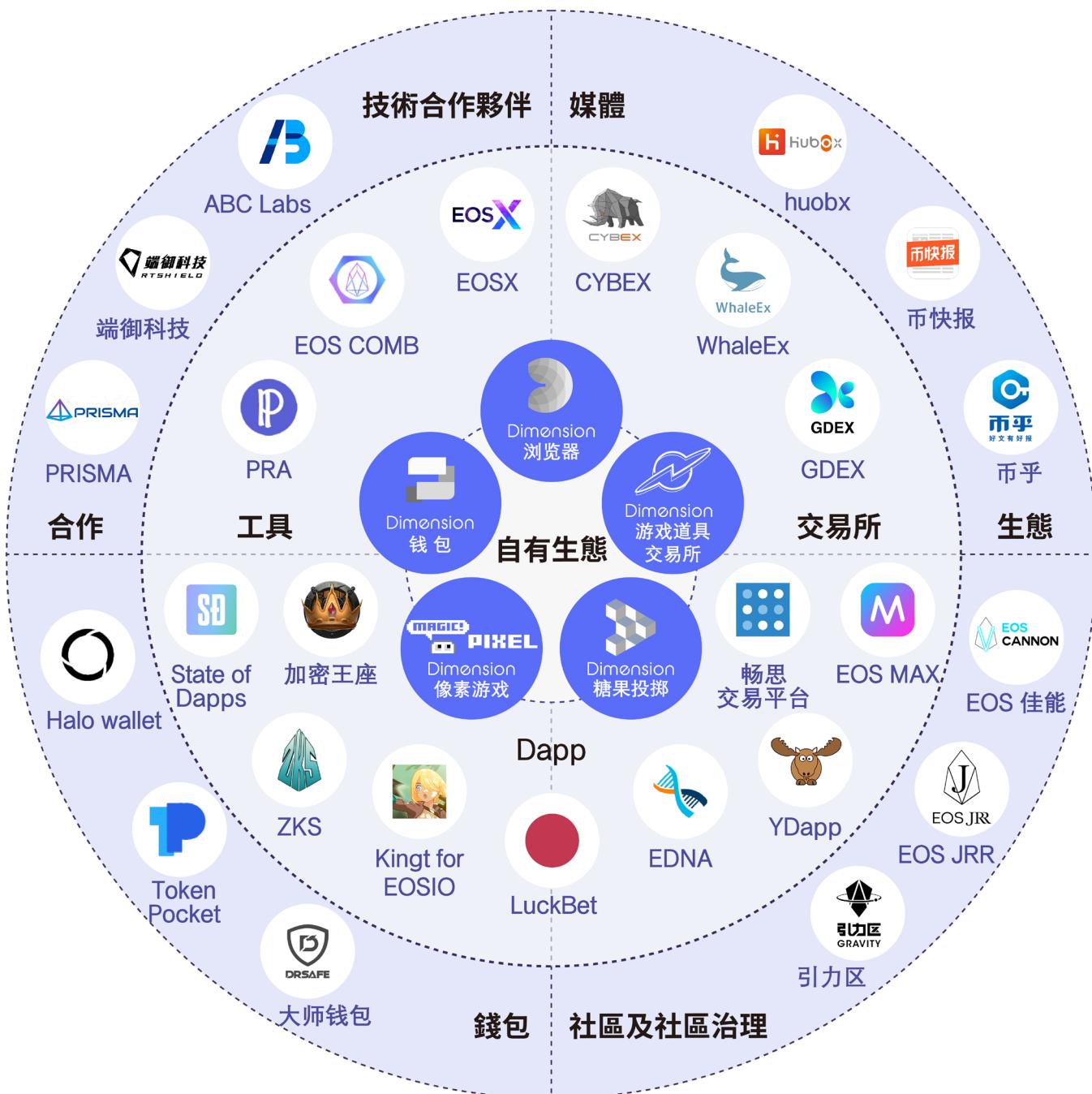


場景五
眾創眾包



場景六
電信通訊

6.2 項目生態





Dimension白皮书