Dimension Blockchain

Whitepaper

2019

Enterprise-grade Blockchain
Network Service

Dimension

目录

I 哲學

沒有人知道一張紙幣從哪裡來到哪裡去，而區塊鏈卻可以讓數位資產的每一筆動向都清清楚楚有“鏈”可查，同時還可以保護參與者的隱私。區塊鏈技術可以構建一個高效可靠的價值傳輸系統，推動互聯網成為構建社會信任的網路基礎設施，實現價值的有效傳遞，並將此稱為價值互聯網。我們注意到，區塊鏈提供了一種新型的社會信任機制，為數字經濟的發展奠定了新基石，“區塊鏈+”應用創新，昭示著產業創新和公共服務的新方向。

1.1 動機

我們在應用過程中，意識到區塊鏈發展還受到一些因素制約。例如可擴展性急待提升，隱私保護方案不夠完善，分散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演算法，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于商業應用帶來障礙。

- 區塊鏈由多種技術構成，學習成本高、實施難度大，商用行業方案欠缺。讓商業用戶快速理解區塊鏈，選擇適合的區塊鏈技術快速應用到不同行業的企業級業務中去，目前來看還有很大的挑戰。缺少可持續且針對性強的商業化落地案例，大多數案例還停留在理念或 POC 階段。

- 區塊鏈需要適應多樣化的業務需求，滿足跨企業的業務鏈條上的資料安全高效共用，要求區塊鏈行業解決方案具備較好的通用性。目前的區塊鏈網路大多採用特定的共識演算法、密碼演算法、帳戶模型、存儲類型，缺少可插拔能力，無法靈活適應不同場景要求。

- 在資料存儲能力方面，由於區塊鏈的資料只有追加而沒有移除，資料只增不減，隨著時間推移，區塊鏈系統對資料存儲大小的需求也將持續增大，在處理以幾何倍數增長的企業資料時這一趨勢增長更甚，以及鏈外資料如何接入區塊鏈網路。目前區塊鏈網路需要採用分散式資料存儲設計，需要探索更為有效的大資料存儲方式。

- 很多方案不是從解決業務痛點出發，導致案例缺少有效價值，不能高效地拓展業務邊界。難以適應業務系統快速開發的要求。涉及到企業業務協作時，跨企業的事件通知機制顯得尤為重要，但少有區塊鏈平臺進行了相關功能支持。

1.2 維度

作為區塊鏈領域發展及推動的重要組成部分，區塊鏈社群煥發出巨大的號召力和創造力，社群成員

就區塊鏈技術、治理機制、商業模式等方向分享著經驗和建議。積極活躍在區塊鏈社群中的意見領袖與貢獻者們，針對當前區塊鏈領域存在的各類問題，提出了專業性思考及前瞻性建議，其中特別就關於如何構建更具商業價值的區塊鏈應用網路進行了長期深入溝通和探討。

我們社區核心成員來自不同行業和領域，有知名區塊鏈風投機構全球合作人，排名前十區塊鏈專案全球社群負責人，前華爾街私募投資機構高管，金融支付及資訊安全顧問，傳統 IT 領域如摩根士丹利，華為等大資料項目目負責人，大型商用系統架構師等。大家就未來區塊鏈如何結合商業，服務於分散式商業提出了新的設想，在創新區塊鏈治理模型，靈活易用底層架構以及自我調整區塊鏈商用框架三個方面提出了解決思路並達成了共識。

我們的項目取名為 **DIMENSION**，意為維度。從廣義上講：維度是事物“有聯繫”的抽象概念的數量；從哲學角度看，指代觀察、思考與表述某事物的“思維角度”。項目寓意從技術多個維度的創新推進區塊鏈技術的不斷演進；從商業應用層面理解，為商業價值進行升維，提供更高視角的商業洞察和商業應用模型。實現技術與商業價值的多維度連接，因此 Dimension 致力於構建新一代區塊鏈分散式應用服務網路。

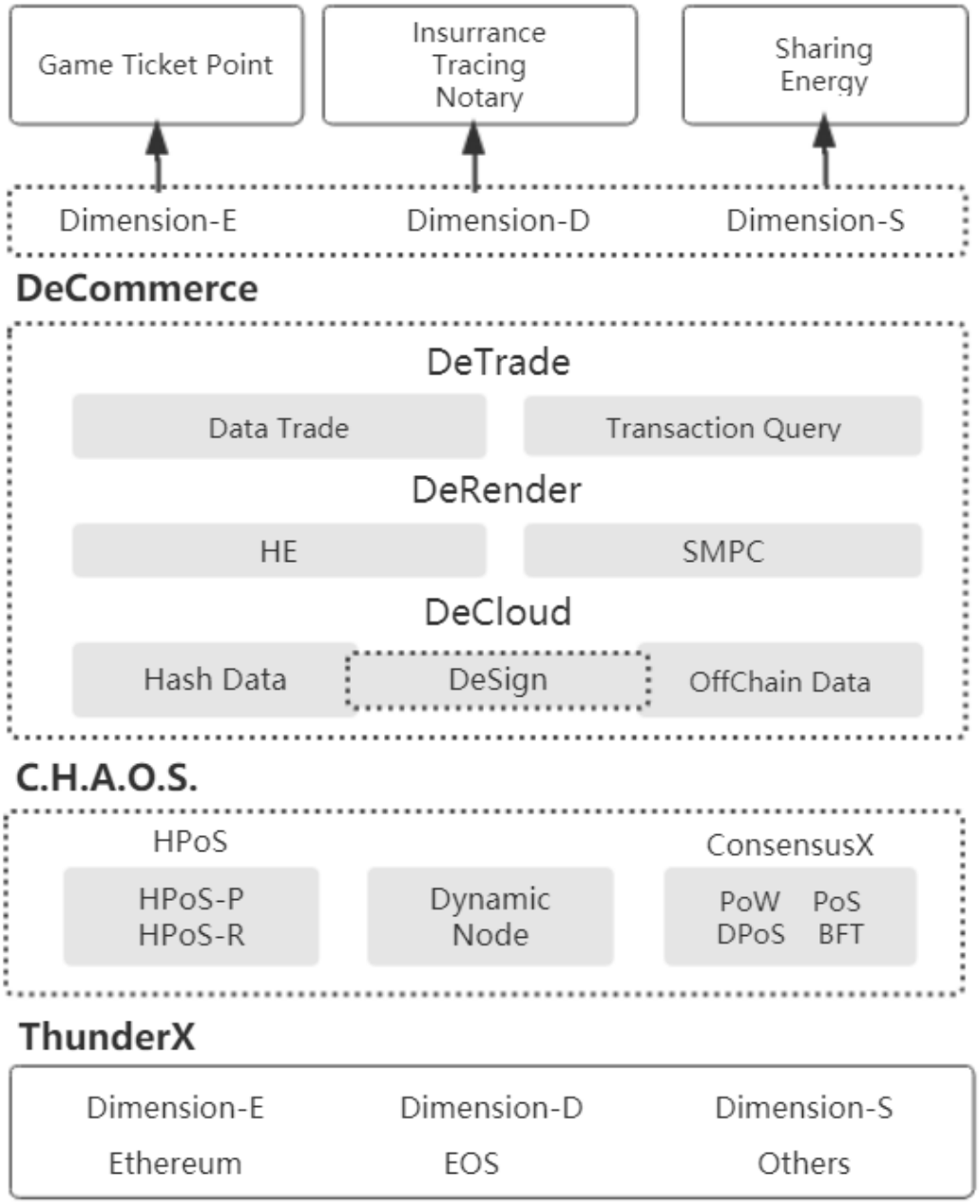
1.3 願景

基於區塊鏈技術的分散式商業正在加速探索及逐步落地。區塊鏈去中心化、開放性、自洽性、不可篡改、匿名性的特性，結合分散式商業有多方平等參與、智慧協同、價值分享、運行透明等特點。實現資料在多源異構的網路架構中自由流動，資料共用的價值通過生產關係的重構被無限放大。並形成節點之間，鏈之間的多維度連結，構建高度複雜的共用網路。

分散式商業藍圖也有巨大的想像空間，如分散式能源、分散式電商以及各類共用經濟。在分散式商業模式中，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復驗證下，Dimension 致力於實現區塊鏈全網間的商業價值互聯，構建新一代企業級區塊鏈應用服務網路。

因此我們希望 Dimension 通過結合分散式存儲、混合共識機制、隱私保護、加密演算法等技術支撐可快速適配的跨共識引擎、跨鏈資料互聯介面、快速部署發佈鏈，從而實現跨鏈的資料共用及價值傳遞，為更多的企業提供商用級的區塊鏈應用服務網路。

II 維度網路



圖例 1. Dimension 架構圖

2.1 經濟

Dimension 注重區塊鏈治理模型設計。經濟模型作為驅動區塊鏈專案和社群的重要引擎，專案將採用回購通縮模型及可調節定量增發機制，實現項目權益價值的長期增益的正回饋，同時對項目反覆運算及社群發展激勵的重要方式。

2.1.1 回購

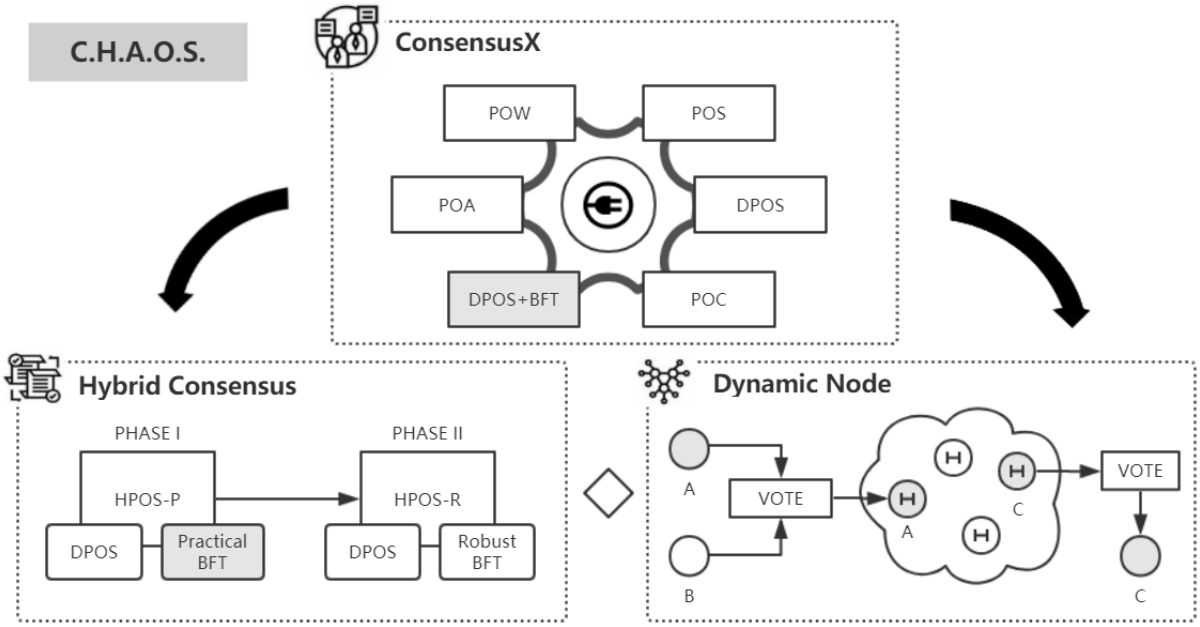
Dimension 採用代幣回購方式減少流通中代幣總量，提升代幣稀缺性，在生態流通供給關係趨緊的情況下，代幣的價值將會加速上升。DIMENSION 基金每年會通過生態項目如數位交易所，科技授權等收益，作為對社區的代幣進行回收銷毀，銷毀記錄會第一時間向全網公佈，用戶可通過區塊鏈流覽器查詢，以確保公開透明，全程可監督和透明化。

2.1.2 增發

隨著 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。以及專案長期穩定發展，和所有專案參與方的利益回饋。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迴圈。
每年增發市場流通量的 3%，分配方式如下：
節點獎勵為 1%
開發者獎勵 1.6%
治理激勵 0.4%

2.2 技術

我們提出的混沌系統 C.H.A.O.S.是指代 Cross-Hybrid Automated Operating System，即跨共識混合作業系統。混沌系統包含核心模組有：混合共識 HPoS，動態節點 Dynamic Node，跨共識引擎 ConsensusX。它結合了多個共識演算法的優勢；實現了可伸縮的網路節點，能適應使用者網路的快速變化，允許多重共識組合相互切換。



圖例 2. C.H.A.O.S. 框架

2.2.1 HPoS

我們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，因此我們提出了新型的混合共識機制 HPoS。

HPoS 結合授權股權證明 DPoS，在保證網路安全的前提下更快的確認速度，整個網路的能耗進一步降低，網路運行成本最低。同時，共識節點採用拜占庭共識演算法 BFT 出塊並達成共識。惡意節點將被取消其作為共識節點的資格，並給與一定的計算貢獻值扣除及經濟懲罰。共識節點在執行打包交易時，將交易中的計算邏輯拆分到多個計算節點平行計算，每個計算節點在回饋計算結果的同時返回正確執行的證明。共識節點將結果與證明打包到區塊中，其他節點只需驗證證明確定區塊的合法性，可以大大減少區塊驗證時間，提高交易性能。混合共識 HPoS 在性能和健壯性上得到了極大的提升，為有效服務于企業級應用的區塊鏈網路提供了共識基石。

HPoS 將分為兩個階段實現，HPoS-P 和 HPoS-R。

我們在混合共識第一階段採用 HPoS-P 演算法，實現了一種採用許可投票，少數服從多數的選舉代理人領導並記帳的共識機制，並且該混合共識機制支持拜占庭容錯，允許監管節點參與，具備許可權分級能力，性能更高，耗能更低。採用混合共識 HPoS-P，能有效支撐 Dimension 為企業級應用提供高性能且穩定的區塊鏈服務網路。

我們發現目前基於 PBTF 的副本容錯系統在某些特定場景下，不能很好地解決拜占庭機制中因節點故障所引發的穩定性問題。若單個故障節點提交的一系列請求、有問題的主程序或副本，則可能會給 HPoS-P 可用性帶來影響。因此我們將在混合共識二階段中使用混合共識 HPoS-R，設計並實現了以穩健性、簡潔性為核心的高性能魯棒拜占庭共識演算法 RBFT（Robust Byzantine Fault Tolerance)。將重點從構建最大化最佳性能的高掛接系統轉移到使用 RobustBFT 構建系統，盡可能廣泛的環境下(包括發生故障時)提供足夠和可預測的性能(10K+TPS)，以便支持可部署的大規模企業級應用服務。

Consensus	Peak Throughput	Faulty Client
PBFT	60982	0
Query/Update Protocol	21873	0
A Hybrid Quorum Protocol	6983	N/A
Zyzzyva Speculative BFT	56287	0
RBFT	**38873**	**38873**

表格 1. 基於 BFT 的共識對比

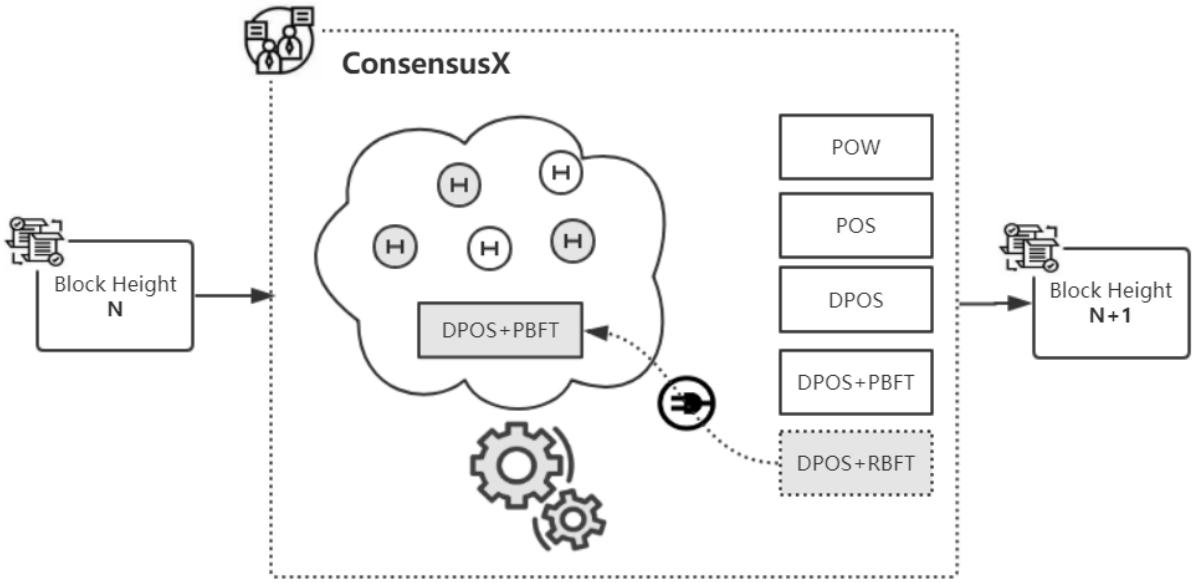
2.2.2 Dynamic Node

縱觀現有區塊鏈平臺若想新加入一個節點，舊的節點需要宕機後重新修改設定檔，並重啟網路後生效。但這樣的操作對於絕大部分商用場景是不可接受的。如何確保商用級區塊鏈網路的高可用、高擴展、高性能等問題。

借助動態節點 Dynamic Node 機制，實現區塊鏈網路授權節點的動態加入及調整。動態節點 Dynamic Node 機制則是通過建立授權代理人鏈上共識節點審批機制，多個節點的相互驗證投票。當贊成票超過或等於現有授權代理節點數量的三分之二時，視為新節點變更提案生效。Dimension 網路將按調整後的授權代理節點共同維護全網記帳任務。這種完全在不宕機的情況下，動態的增加或者減少節點，不僅實現區塊鏈節點變動的靈活性，而且保證原有區塊鏈網路的平穩運行，降低開銷和規避潛在變動可能引發的風險。

2.2.3 ConsensusX

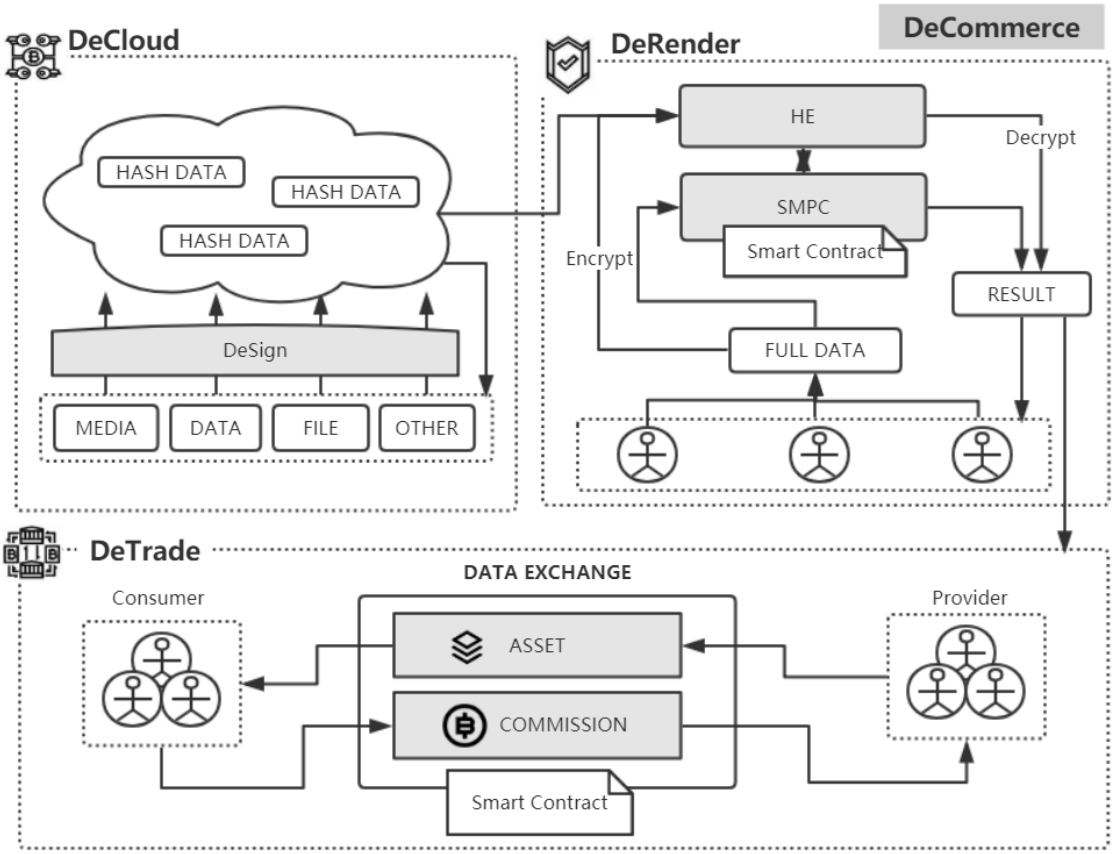
跨共識引擎 ConsensusX 可解決主網運行中演算法不可輕易動態切換的問題。在啟動區塊鏈網路前，如果在區塊鏈網路運行中，當業務場景發生變化時需要切換其他共識演算法，則可通過跨共識引擎 ConsensusX 快速穩定的切換至其他共識演算法，並且當切換至 DPOS 共識時，還可通過動態節點 Dynamic Node 實現節點調整的動態切換。實現區塊鏈網路共識機制的快速插拔，極大降低區塊鏈商用網路在初期共識選型上的風險，共識引擎 ConsensusX 面向企業級應用網路提供高效靈活，低成本的共識解決方案。



圖例 3. ConsensusX 運作圖示

2.3 應用

分散式商用框架 DeCommerce 聚焦於企業級分散式服務網路，借助其中的分散式資料存儲系統鏈雲 DeCloud，分散式運算框架 DeRender，最終實現資料交易框架 DeTrade，為商業用戶提供可多方協作參與，確保資料隱私安全的新型區塊鏈資料交易服務。



圖例 4. DeCommerce 框架

2.3.1 DeCloud

分散式存儲系統 DeCloud 結合 DHT 分散式雜湊表，實現資料上鏈，並基於創新區塊鏈存儲協定 DeSign，實現去中心化的更快、更安全、更開放的高輸送量內容定址塊存儲模型。將打包後的區塊資料通過 DeIPLD 進行異構處理，並掛載到 DeCloud 的連結上，讓網路承擔存儲和 P2P 檢索的邏輯，方便不同系統之間的資料交換和交互操作。通過資料存儲的節點化網路，為商業提供企業應用級數據存儲服務，為實現不改變資料所有權下的企業級資料共用及交易提供技術支撐。

2.3.2 DeSign

在 BitTorrent 基礎上優化了 P2P 資料交換及存儲協定 DeSign。從不屬於本檔的其他檔獲取資料塊，只要資料塊的雜湊值一樣，那麼資料內容必然是一樣的。從全域來看 DeSign 的效率遠優於 BitTorrent。同時通過信用體系，激勵節點樂於分享資料。如果當一個節點只接收資料而不分享資料，信用值會降低直到被其他節點忽略。

2.3.3 DeRender

分散式運算框架 DeRender 通過疊加同態加密（HE）和安全多方計算（SMPC），實現真正的隱私計算，保證輸入資料以及計算邏輯本身的隱私。同時，通過可驗證計算等提高單個交易的處理性能，交易輸送量也得到相應的提升。具備可擴展、隱私性並可驗證的 DeRender 滿足企業級商用對資料隱私及安全保護的全面訴求，為資料共用交易提供基礎計算框架支撐。

同態加密（Homomorphic Encryption）是一種無需對加密資料進行提前解密就可以執行計算的方法。Dimension 通過同態加密技術與區塊鏈結合，對資料進行加密處理後在鏈雲 DeCloud 持久化，通過智慧合約對指定加密資料提取做複雜運算處理，僅將最終結果資料解密後回饋，並明文顯示給資料使用方，使用方可通過驗證演算法對結果資料做真實性和準確性驗證。

安全多方計算（Secure Multi Party Computation）允許多個使用者各自持有部分資料登錄，協作完成對全量資料的計算，同時要求每個用戶除計算結果外均不能夠獲知其他使用者的任何輸入資訊。資料持有方可通過私密共用資料到 DeRender 分散式運算框架中，同時授權 DeCloud 可接入新資料來源，當新計算需求被發起後，協同計算網路 DeRender 確認計算申請，並傳遞執行代碼到多個計算參與方，將回饋結果資料給多方確認。這個流程均通過隱私計算協定傳輸，從而實現了各個計算節點在資訊隱私保護的前提下實現資料協同計算。

2.3.4 DeTrade

我們構建了一個去中心化資料交易框架 DeTrade，建立可信任的資料資產交易環境，破除資料被任意複製的威脅，保障資料擁有者的合法權益，促進資料要素流通融合。資料交易框架 DeTrade 為企業級商用區塊鏈提供完備安全隱私權原則，提供符合不同場景需求的區塊鏈資料交易服務。

資料交易框架 DeTrade 提供兩類資料交易模型。第一類原始資料交易，當資料需求方提出資料訴求時，消息通過 DeTrade 向全網進行廣播，而資料來源通過查詢自身離線資料庫，如有匹配資料則通過智慧合約進行點對點數據交易。第二類資料查詢交易，即資料需求方並不關心明細資料，而是僅需要回饋資料計算後的結果，僅按智慧合約執行代碼返回結果集給需求方即可。

此外，DeTrade 基於大資料和彙集眾多服務節點，還可延展為對資料的深度挖掘，如數據趨勢分析、商業智慧分析、資料智慧預測等，及全網計算能力的交易，最大化發揮 DeTrade 作為資料服務網路的核心價值。

III 側鏈

3.1 Dimension-E

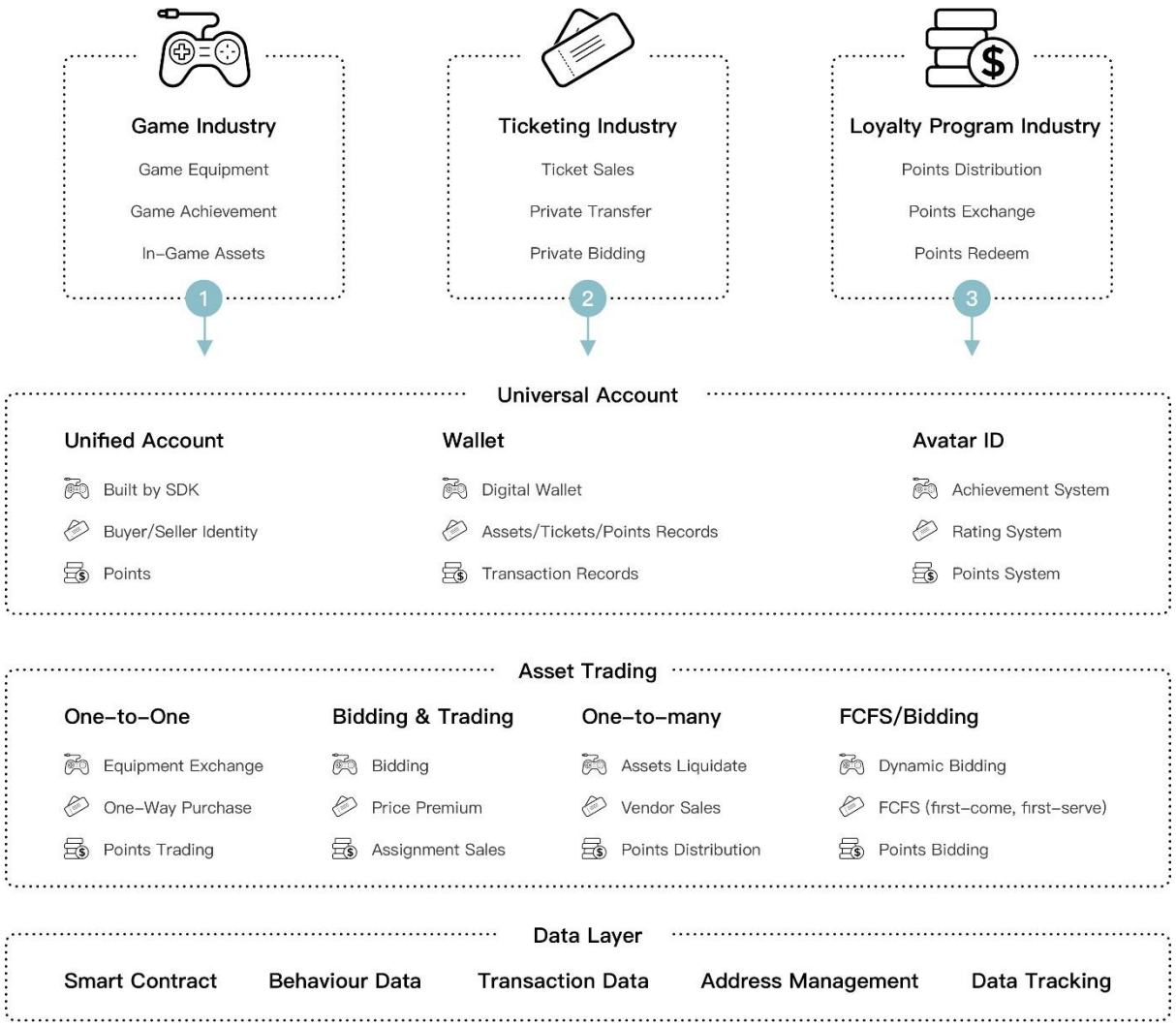
我們以遊戲為突破口，通過核心的三層結構系統 1 通用帳號系統，2 虛擬數位資產交易系統，3 垂直行業的虛擬資產貨幣化系統，解決了行業資料霸權問題，保證交易的安全和透明，同時非常好的解決了廠商盈利模式單一的問題，保障了玩家、cp、管道等多方共贏，為泛娛樂企業的數字資產提供更多應用價值。

帳號系統是玩家進入平臺的最基本的服務。我們通過構建統一的帳號體系，通過遊戲 SDK，將遊戲資料上鏈。用戶使用錨定在區塊鏈上的帳號系統，將關鍵資訊保存到區塊鏈網路中，保障了系統的安全性。用戶的帳戶成為不受任何機構控制的私人所屬，一方面提升玩家的遊戲體驗，使得玩家可以低成本的體驗不同遊戲，另一方面玩家通過帳戶可以綁定分散式平臺內任意的資料資產，通過秘鑰證明其歸屬，並可以在平臺的交易所中方便的管理或者轉移。

團隊聯合了遊戲聯盟進行針對性的改造，既考慮到玩家對遊戲道具、裝備的交易需求，又不對原有的經濟體系進行過多的干涉。以此為基礎，玩家通過建立自己的虛擬商品商店，並進行買賣交易，鏈上以市場撮合競價的方式，通過智慧合約，實現不同遊戲間的虛擬資產轉移， 交易透明，結果不可逆轉，永久可查。 聯盟平臺將極大的改善玩家的體驗，保證玩家的利益，並逐漸建立併發展出虛擬商品經濟體系。

隨著鏈生態的不斷發展，平臺將進入第三階段的發展，即數位資產貨幣化。簡單而言，加入我們的各大企業，無論是遊戲公司，還是跨行業公司，如文娛行業，金融行業等，都可在平臺上發行自己的數字資產，說明其積分、IP 等數字資產化。

Dimension-E 適用於各類擁有虛擬資產的商業應用場景，如積分、票務、遊戲、動漫等多個行業。



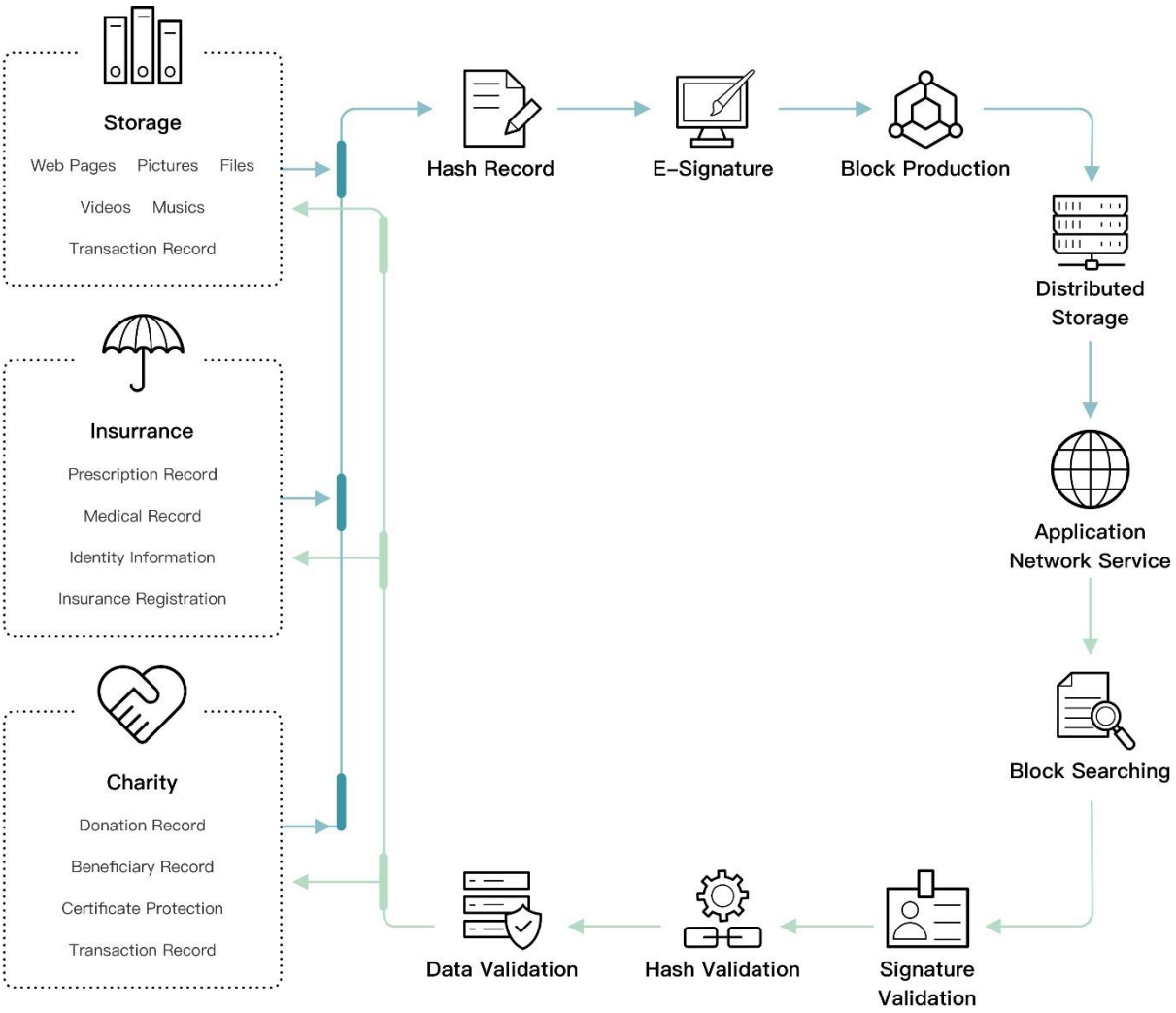
圖例 5. Dimension-E 架構

3.2 Dimension-D

互聯網的最顯著特點是對資訊處理的高效率和低成本，任何人都可以不受任何時間和地點的限制，輕鬆的通過互聯網發佈、傳遞和獲取各種資訊。如何確認和判定網路中交互資訊的真實可靠，以及對電子證據及時、有效的固定，確保文件不被篡改，一直是“互聯網+”大戰略中亟待解決的問題。Dimension-D 運用區塊鏈理論實現公證系統的構想，完成資料上鏈：通過散列演算法把任意長度的輸入變換成固定長度的輸出，再通過原始金鑰進行長度驗證的演算法，從源頭上完全杜絕了資料和檔被偽造和篡改的可能性。同時，我們用分散式存儲的方式，處理鏈上資料，方便讀取，達到商業應用級別。

1.雜湊運算：電子檔案、合同、圖片、著作等電子資料經過雜湊運算後，生成一段固定長度的原資料的唯一特徵資料，稱為原資料的“數位指紋”，無法由“數位指紋”推出原資料的內容；原資料的任何一點改動後，重新生成的“數字指紋”是不可預料的。2.電子簽名：利用非對稱加密技術，存儲方對資料經過私密金鑰簽名後發送到區塊鏈網路，明確資料的來源不可抵賴，並保證傳輸過程不可篡改。3.寫入區塊：發送到區塊鏈網路的存證資料會經過一次共識後打包成區塊，並同步給網路中的各個節點分散式存儲。4. 出證：當使用者需要對存儲的資料進行證明時，可聯繫對應公信力機構出具證明報告

Dimension-D 適用於各類需要資料存證並驗算的商業應用場景，如公示、保險、信託、慈善公益等多個行業



圖例 6. Dimension-D 架構

3.3 Dimension-S

對於實體經濟企業來說，其面臨的商業模式的創新壓力越來越緊迫，它不僅需要簡化原有的商業模式，更是需要從新的技術、新機遇中獲得競爭優勢，而共用經濟就是一個很好的解決方案。另一方面，由終端設備產生、人與終端共同行為產生的資料越來越多，但資料的價值及所屬權從未被真正的歸屬、評估、量化和使用。使用者作為資料的生產者卻從未擁有它並因此而受益，且資料價值被割裂成孤島沒有形成有效的互通機制。

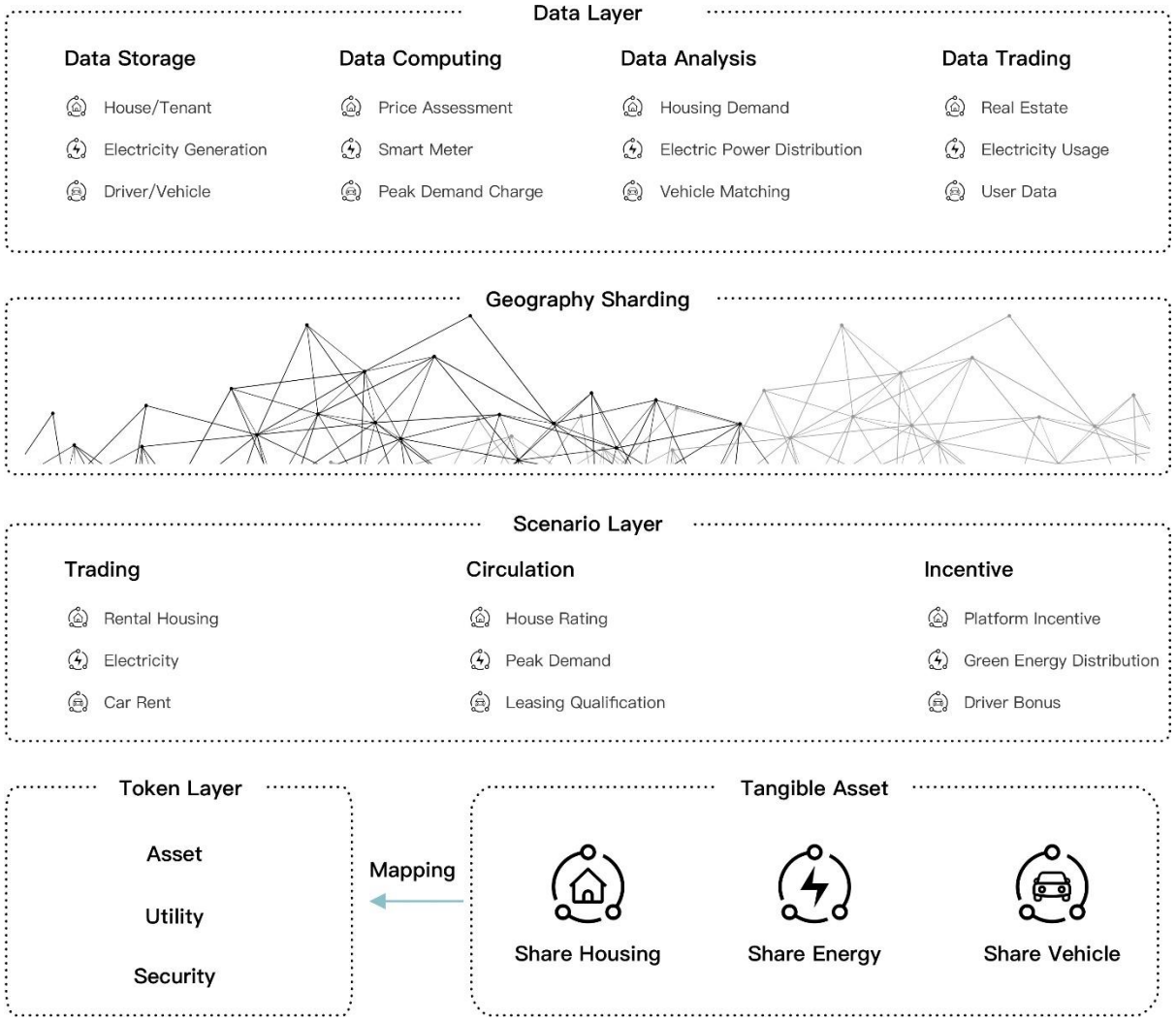
Dimension-S 將實現所有實體經濟資產到數位世界的映射和切分，並提供全套的交易系統，說明企業完成經濟共用及行為資料交易，從而提升經濟效益。

- 實體資產映射上鏈，構建實體經濟價值生態系統。 Dimension-S 是基於實體經濟行業應用特性開發的側鏈，並支援多種行業應用，構建安全、去中心化的、支持高併發的區塊鏈網路。

- 建立交易平臺，實現資料價值流通。 Dimension-S 將解決實體經濟終端的資料價值問題，通過去中心化交易平臺實現使用者的資料權利和價值交易，保護使用者以及設備的資料價值。

- 通過區塊鏈同態加密技術，在保護隱私資料的前提下擴大交易範圍，從資料所有權交換到資料使用權交換，進一步彙集並共用使用者行為資料，為共用經濟模型優化不斷提供資料支撐。Dimension-S 的願景是基於可信區塊鏈網路釋放最大共用效益，促進共用生態長期有效的發展。

Dimension-S 適用於各類需要將實體經濟映射到鏈上進行交易、存儲的商業應用場景，特別適合共用經濟、綠色能源等行業。



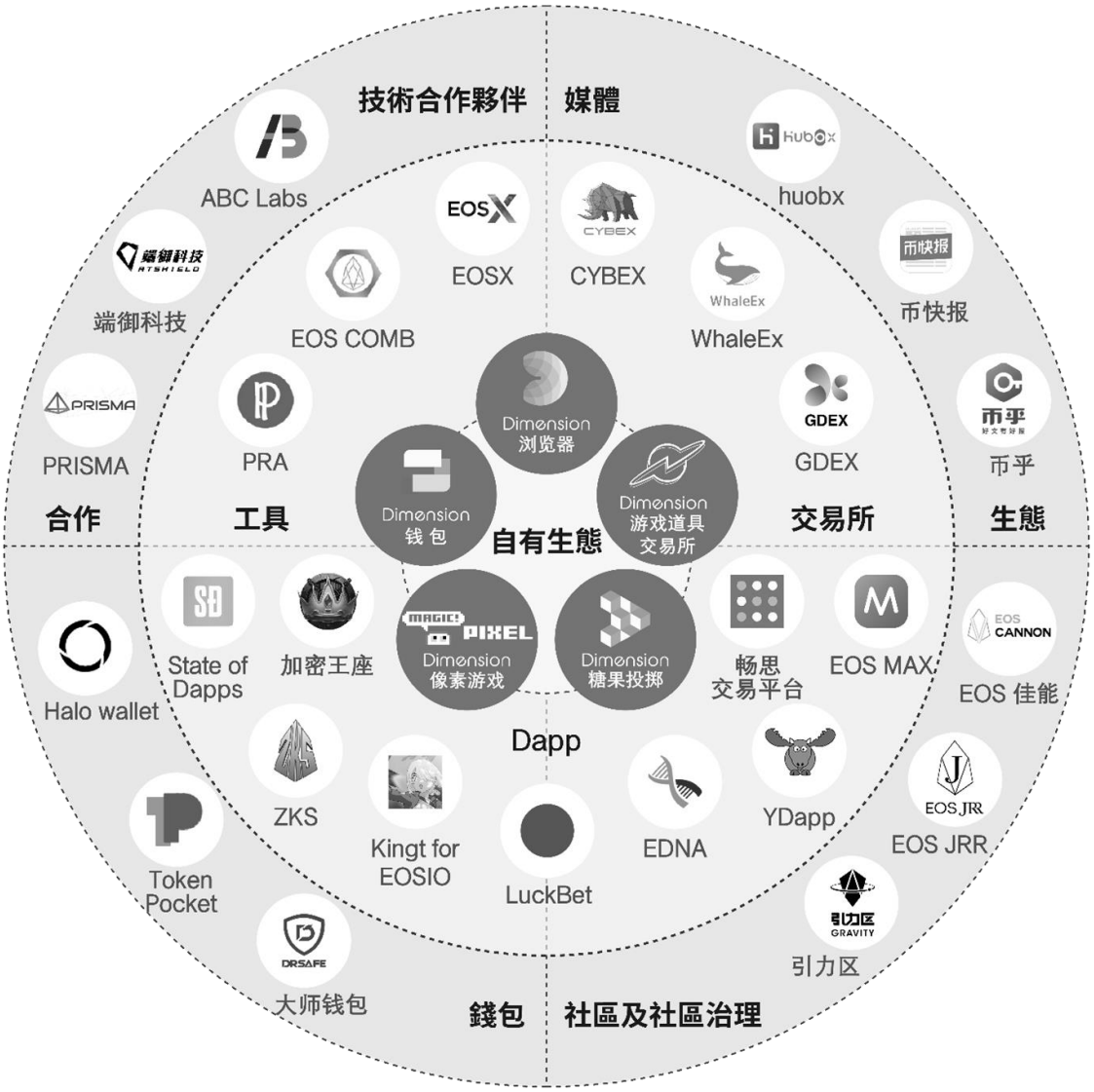
圖例 7. Dimension-S 框架

IV 治理

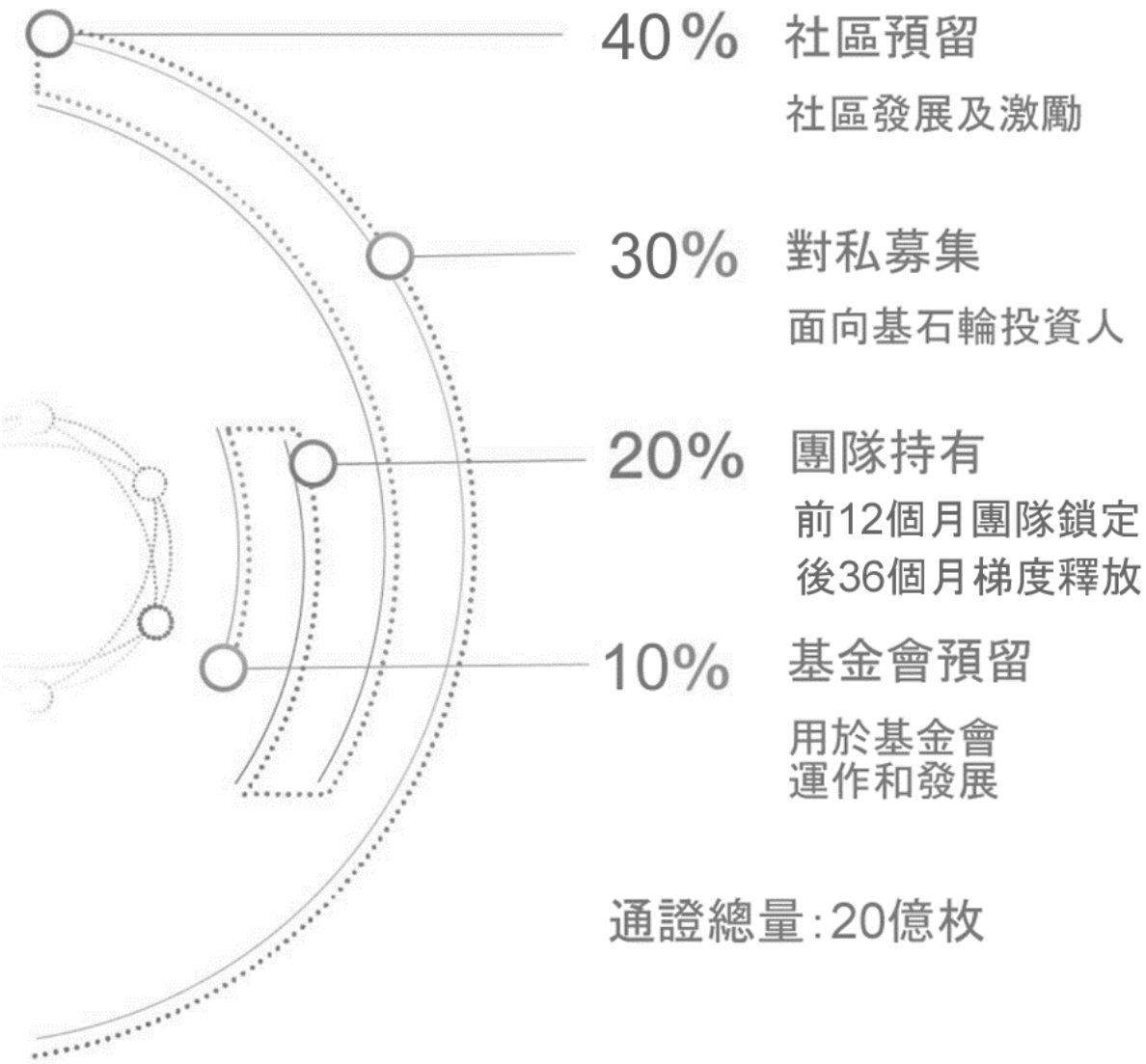
4.1 路线图


2018 Q2
Dimension項目啟動
Dimension-E白皮書
POC技術驗證開展
2018 Q3
測試網1.0啟動上線
各節點穩定出塊運行中
核心合作方參與開放測試
流覽器及錢包反覆運算開發
2019 Q1
流覽器及錢包正式發佈
混合共識演算法HPoS開發
萬向區塊鏈等 機構參與節點共建
DeCloud框架實現階段一功能
生態DApp MagicPixel發佈
2019 Q3
Dimension主網啟動
更多生態DApp持續發佈
分散式商用DeCommerce搭建
Dimension-D框架反覆運算
2020 Q1
Dimension-S應用
C.H.A.O.S.階段測試
分散式計算DeRender階段開發
ThunderX跨鏈機制測試
2020 Q3
C.H.A.O.S.開放應用測試
生態DApp商用擴展
DeCommerce階段性應用測試

4.2 生態


技術合作夥伴
媒體
ABC Labs
huobx
EOSX
CYBEX
端御科技
EOS COMB
WhaleEx
币快报
PRISMA
PRA
GDEX
币乎
Dimension 浏览器
Dimension 钱包
Dimension 游戏道具交易所
合作
工具
自有生態
交易所
生態
State of Dapps
加密王座
Dimension 像素游戏
Dimension 糖果投掷
畅思交易平台
EOS MAX
EOS 佳能
Halo wallet
Dapp
ZKS
Kingt for EOSIO
EDNA
YDapp
EOS JRR
Token Pocket
LuckBet
引力区
大师钱包
錢包
社區及社區治理

4.3 分配


40%
社區預留
社區發展及激勵
30%
對私募集
面向基石輪投資人
20%
團隊持有
前12個月團隊鎖定
後36個月梯度釋放
10%
基金會預留
用於基金會
運作和發展
通證總量:20億枚

4.4 團隊

Fernando Liu
Chief Executive Officer

Randall Foster
Director of Global R&D

Aditi Saxena
Data Scientist

Edwin Liu
Marketing Director

Oliver Church
Director of Fintech Security

Martyna Basara
Strategic Partnership Manager

Melvin Adams
Director of Community Management

4.5 投資者及顧問

Jon Carnes

Investment Director of Eos Holdings LLC (A private equity investment fund founded in 2004)

ZENG Liang

Internet Entrepreneur Angel Investor

Ex-Microsoft and Baidu Executive

Alvin Chan

CEO & Founder of Magic Oranges & JRR EOS

Guest lecturer of Fudan University