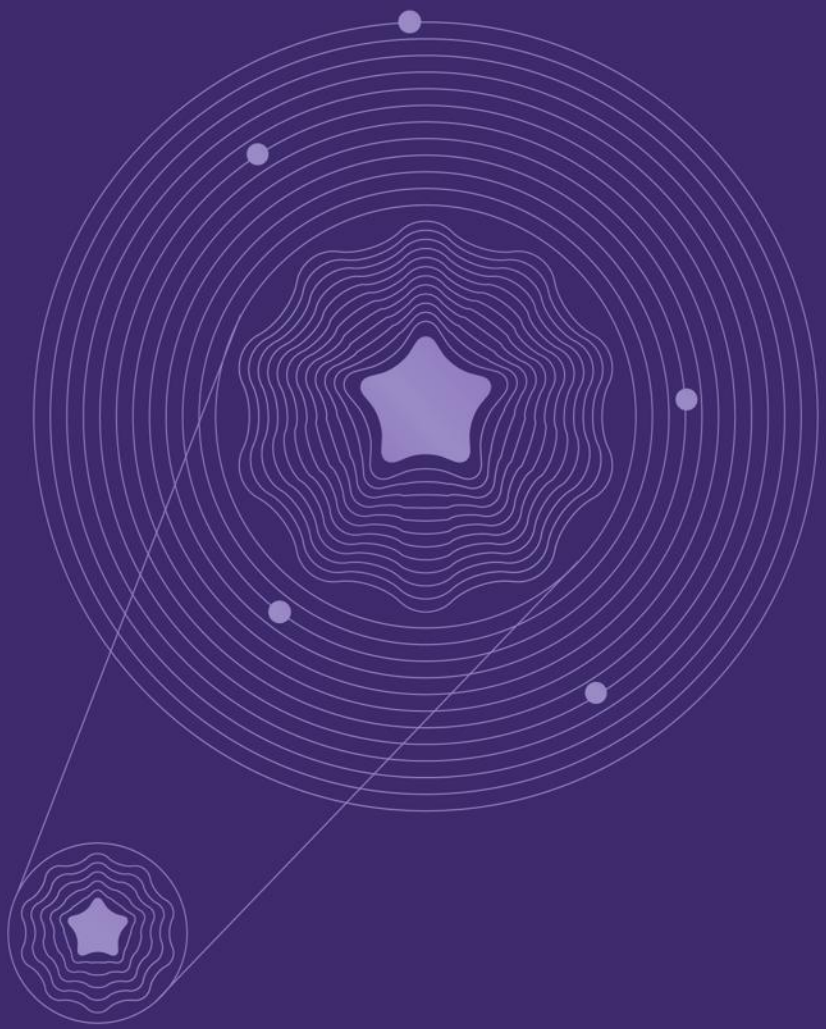
PENTA

区 块 链 世 界 的 连 接 器

技术白皮书

梵塔网络



V1.1.1 | 2018

摘要

区块链技术的蓬勃发展构建了纷繁多样的区块链世界和体系，这些体系却并不相互贯通且与链下场景缺乏交互，从而影响了整个真实世界与区块链世界的有效连接。如何基于多样化的区块链生态，衔接好区块链的分布式、去中心化世界与现存的中心化世界，实现区块链与未来一切的连接，是新一代区块链网络追求的目标。

Penta（称“梵塔网络”或“PNT”）是新型的区块链底层网络。Penta 源于五芒星（Pentacle），寓意“五回交错”的诞生，而对应到区块链世界则是主体、信任、价值、场景、流通五个维度的连接。

梵塔网络将通过上述五个维度的构建，让众多区块链网络和体系可与之衔接，让分散的中心化系统与之融合，并贯穿彼此，最终高效、便捷地连接链上及链下世界。这将让区块链成为普惠的技术，让基于此技术的应用可以更简便地开发，最终实现未来区块链世界的连接。

梵塔网络，连接未来！

目 录

1. 概述

Penta（称“梵塔网络”或“PNT”）是下一代区块链价值互联网的底层基础链与协议，旨在基于 5 个维度（主体、信任、价值、流通和场景）实现 3 大连接（链与链的连接、链与中心化的连接、链下与链上价值的连接），并为此制定了具体的 10 大核心技术路线，让区块链世界互联与普惠。梵塔网络的核心成员来自全球顶尖的科学、金融组织和机构，NASA、维基解密、Google、摩根斯坦利、荷兰银行、德国银行等，对科技、社会、经济的发展及生命周期有着深刻认知和解读。当区块链逐渐成为未来世界秩序之钥时，探索未来区块链世界的终极成为梵塔网络建设的初衷。

本文将阐述梵塔网络的核心架构以及对应主体、信任、价值、场景、流通这五个维度的连接，以及梵塔网络将如何作为区块链世界的连接器，引领未来的区块链世界。

2.五维之连接

Penta 源于五芒星（Pentacle），寓意“五回交错”的诞生，而对应到区块链世界，则是主体、信任、价值、场景、流通五个维度的连接，Penta 将作为区块链世界的连接器，引领未来的区块链世界。

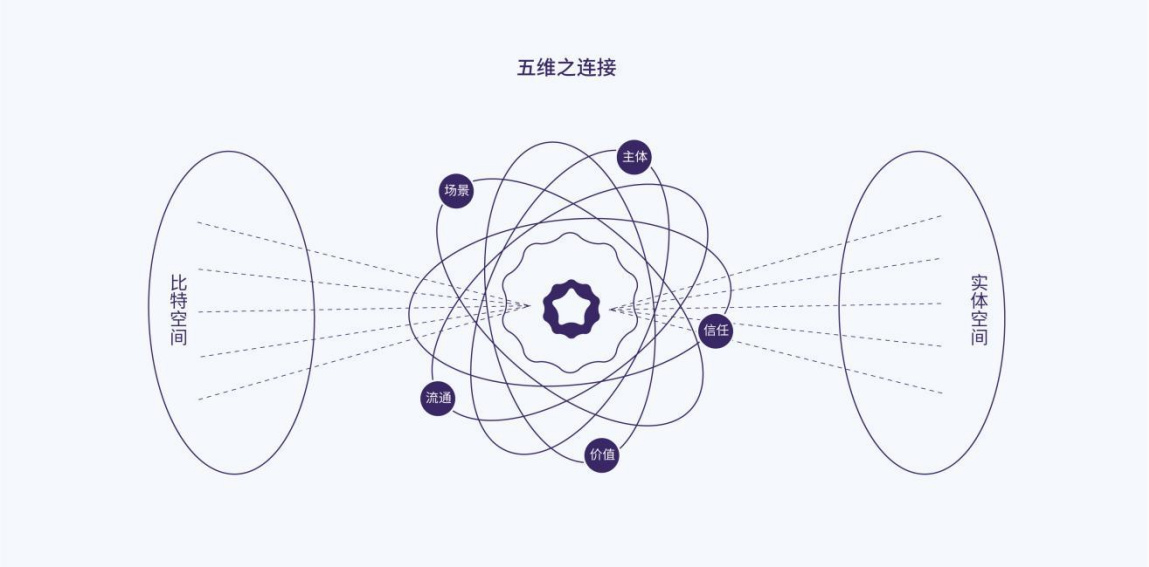


图 2 梵塔网络五维之连接

2.1.主体

所有参与主体，包括一切人、物、组织、系统等在梵塔网络中使用统一的身份标识，梵塔网络根据身份标识权益管理与业务处理，梵塔网络支持主体的多身份标识管理。

身份标识使用去中心化的方式进行管理，包括身份标识产生、使用、验证、存储，以实现隐私保护与安全交易。

- 产生：每个身份标识采用非对称加密 PKI 加密机制生成，产生对外公开的地址信息。身份标识的所有者保管地址与私钥信息。此外支持部分参与主体选择数字认证中心颁发的证书进行标识。
- 使用：身份标识的主体通过私钥信息，操作其在梵塔网络所有权益或数字资产进行交易，并向梵塔网络发起申请。

- 验证：梵塔网络进行所有权益检查与交易验证，通过后形成网络共识。
- 存储：产生的身份标识相应的公开信息，将被作为公开信息存储在梵塔网络的分布式账本中。

此外身份标识支持智能合约拓展，以实现更丰富的身份标识管理，满足不同业务领域的身份管理要求。如在金融业务领域资产交易的场景，需要满足业务主管地区的 KYC 需求，采用扩展的智能合约进行 KYC 内容的设置与存储。

2.2.信任

区块链的繁荣发展比较重要的一个原因是区块链技术实现了去中心化的信任机制，使其成为信任的机器。梵塔网络通过信任主体、信任网络、信任交互，建立了分布式信任机制。

- 信任主体

  每个参与主体在梵塔网络中都存在利用 PKI 建立的身份标识，并且通过分布式账本进行公开信息记录与存储。部分参与主体，可使用认证证书的方式进行管理。

- 信任网络

  采用共识算法，达成梵塔网络全网交易确认，并记录账本，一经确认，无法进行任何形式的交易撤销。

- 信任交互

  其他区块链平台、中心化系统，可采用密钥或者认证证书进行授权，达成跨链交易。梵塔网络支持智能合约进行跨链交易，在关联链或系统达成共识后完成梵塔网络共识，实现信任交互事务控制与管理。

2.3.价值

区块链本质上实现了去中心化的数字资产价值转移，登记在梵塔网络上的所有资产都以特定价值的形式存在，参与主体之间的交易，实现价值的转移。梵塔网络的价值管理，包括价值产生，价值交换，跨链交易。

梵塔网络的价值产生通过每次共识达成后释放 PNT 给参与共识的节点。此外支持参与的信任主体进行线下资产映射上链。

产生的价值资产，基于梵塔网络进行价值交换。梵塔网络使用柔性链路协议支持与其他链的交易与价值互换，并通过智能合约进行锁定交易并完成事务管理。

2.4.场景

梵塔网络支持与各个区块链网络，分散的中心化系统，各参与主体的连接，实现商业场景的支持与连接。梵塔网络作为价值交换的枢纽，结合云计算、大数据、人工智能技术为商业场景提供完善的支持。在第 4 章节将详细描述梵塔网络在部分业务领域的应用方式。

2.5.流通

梵塔网络定位未来区块链世界的连接器，不仅支持新型的业务场景，更将为传统商业进行流通，实现区块链连接一切商业，为未来的商业提供信任与价值互换的基础。

为此梵塔网络提供 DApp 应用开发组件与 SDK，简化 DApp 的开发，组合的工具包不需要专注于业务与场景的开发人员熟悉区块链的底层技术。此外梵塔网络提供 ChainStore，为 DApp 使用与推广提供平台。

3.梵塔技术

区块链技术得益于去中心化、不可篡改、价值转移等特征，正在受到越来越多行业的青睐。然而，区块链的技术发展中仍然存在诸多痛点，如性能不甚理想、商业场景难以支持、共识呈现中心化趋势、区块膨胀日益加剧、区块链平台间缺乏有效交互等等。

1、 性能不甚理想

现存的各种区块链平台交易速度及吞吐量均较低，部分支持智能合约的平台只能运行简单的合约代码，运行复杂 DApp 记账效率会急速下降，当前的区块链技术的性能还不足以支撑一个完备的系统并在其上运行丰富的 DApp，无法满足用户实际需求，故亟待一个高性能平台的出现。

2、 难以支持复杂商业场景

当前限制区块链商业应用的另一个原因是其还不能适用复杂商业场景的需要。商业应用场景一般业务逻辑上特点各异，从而需要更灵活的解决方案。因此，当前主流的区块链平台就面临着难以适配不同业务场景需求。

3、 共识呈现中心化趋势

比特币首创的 POW 共识机制目前看来容易被掌握挖矿技术的芯片巨头所垄断，而 DPOS，DBFT 等非 POW 共识机虽然能够提供比起 POW 算法更高的效率,却无法回避超级节点带来的中心化问题。区块链的核心价值在于通过有效的共识机制在缺乏信任协作网络中建立信任体系，而不是一味的为了追求高效率牺牲民主化。

4、 区块链平台间缺乏有效交互

区块链技术的快速发展，诞生了很多区块链平台，这些区块链平台之间却难以相互贯通，且与链下场景缺乏交互，从而影响区块链有效地服务实体商业。如何基于多样化的区块链技术，实现区块链平台间的连接，区块链与现存中心系统的连接，以及区块链与链下实体资产与商业的连接，是新一代区块链网络需要解决的痛点。

梵塔网络旨在承载真实的商业应用场景，并打造成为区块链世界的连接器，为未来分布式智能商业应用提供平台支撑。基于此目标，梵塔网络在技术上构建梵塔链、梵塔 DLOS、高性能 DApp 平台与连接器。

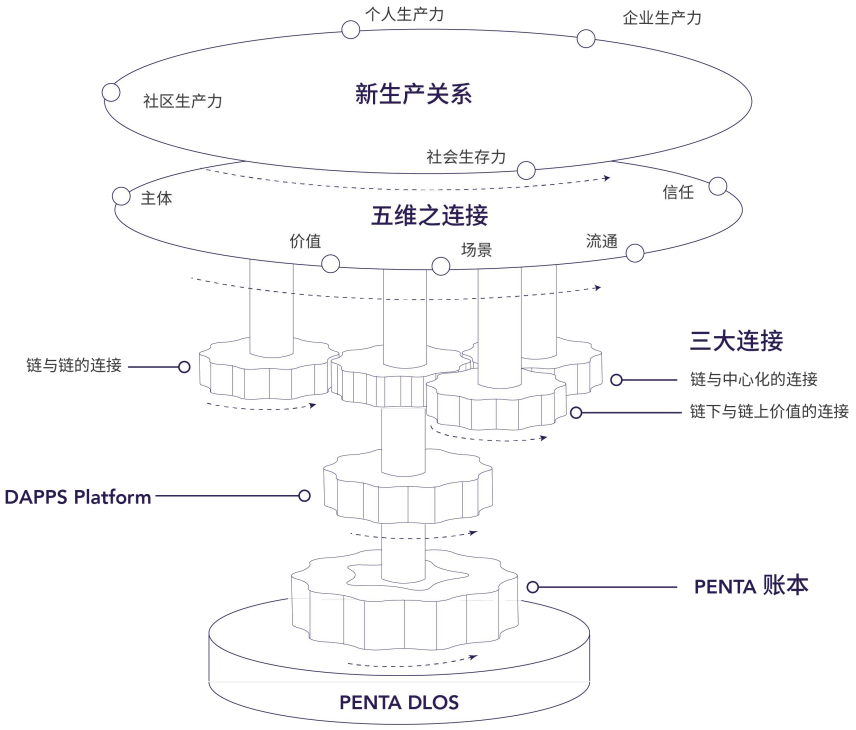


图 3 梵塔技术体系

梵塔链：采用动态权益共识协议（Dynamic Stake Consensus, DSC），通过散列抽签算法（Random Sorting Algorithm，RSA）确保共识过程的公平性，是平衡了效率、规模、安全性、一致性、可用性的民主化共识机制。

梵塔 DLOS：提供区块链平台的底层技术实现，包括存储、网络、企业应用组件、UI 组件等。

DApp 平台：目标是构建高性能的 DApp 运行平台，提供 DApp 运行所需的环境、数据库、文件系统及应用市场、开发 SDK 等，提升 DApp 运行性能简化 DApp 开发。

连接器：建立链与链的连接、链与中心化系统的连接、链下资产与链上的连接。

梵塔网络是由众多梵塔节点参与的多链网络，梵塔链是梵塔网络的主链，由梵塔基金会与技术社区重点维护。基于梵塔 DLOS 提供底层技术支持， DApp 平台实现商业应用，通过连接器构建三大连接，最终满足区块链应用场景所需的五个维度，从而实现对新商业中生产关系的重构。

3.1.梵塔网络-技术架构

梵塔网络采用了模块组件化的底层架构，在用户搭建区块链应用或区块链子链的时候，大部分组件都被设计成可以像乐高积木一样通过相互引用而组装起来使用。所有组件都支持可插拔技术，例如共识组件就支持 POW、POS、dPOS、PBFT 等，加密算法支持 RSA、SM2 等，用户也可以在其之上进行扩展。

图 3.1 梵塔技术架构图

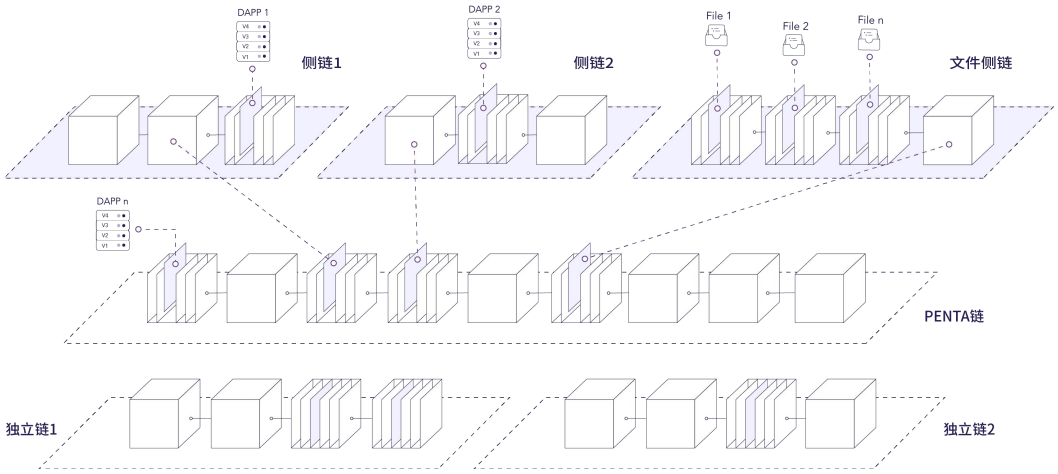
存储组件和通讯组件是所有区块链系统的基本组件。在存储组件方面，梵塔网络在普通的区块存储之外，还实现了世界状态和区块数据的文件存储和数据库存储等存储组件，以适应机构用户的高可用要求以及对数据查询的高并发要求；在通讯组件方面，梵塔网络在实现了基本的 P2P 网络之外，还扩展了分布式私有通讯网络和柔性链路协议。

在安全组件方面，有别于以太坊的完全匿名和 Hyperledger 的证书认证，梵塔网络将身份认证作为一个可选项，用户在运行特定的区块链应用时才可能需要展示

自己的身份认证信息。在应用组件方面，梵塔网络已经提供了智能合约、数字资产、激励机制、成员管理和权限管理等创建智能合约和区块链的应用组件。

3.2.梵塔网络-账本体系

梵塔网络将构建一个以梵塔链为核心的多链平台，梵塔网络由梵塔链、侧链、其他应用链、DApp State 数据、文件等共同组成梵塔网络账本体系，用于承载梵塔网络中重要的应用功能和跨链协作功能。



PENTA网络账本体系

图 3.2 梵塔网络账本体系图

梵塔网络的账本体系各种商业场景的 DApp 应用，也可以基于梵塔网络发布侧链或独立链。侧链与独立链采用插件化的共识组件，为不同商业场景提供差异化技术支撑。梵塔网络将根据同步用户下载的 DApp，仅同步关联的侧链或独立链账本数据。

3.3. 梵塔链

梵塔链采用独创性的 DSC 共识算法, 结合合理的治理结构、有效的激励机制以及底层分片技术，将有效提升区块链平台的效率、安全性和一致性，能够有效承载梵塔网络中重要的应用功能和跨链协作功能，实现以梵塔链为核心的梵塔网络账本体系。

3.3.1.共识机制

共识机制是区块链网络的核心，因为区块链的数据散布在网络中各个参与节点中，这些分散的数据必须通过一种算法来保持一致性。目前区块链技术在性能、公平性、安全性方面难以兼得，区块链网络就是通过有效的共识算法，实现多方博弈环境下的有效协作，构建了一个安全、平衡、稳定的点对点价值传递网络。

由此梵塔链独创性的设计了 DSC 共识协议，通过散列抽签算法，平衡民主、效率与安全，并且梵塔网络设计了插件化的共识组件支持侧链或独立链多样的共识算法。设计上将梵塔链记账共识和 DApp 交易运行与结果验证所依赖的侧链或独立链共识进行分离，对平台层和业务层进行解耦，提升梵塔网络运行的效率，灵活支持多样的商业应用场景。

3.3.1.1. 梵塔链 DSC 共识协议

DSC 协议（动态权益共识协议）是一种不产生分叉的共识机制。DSC 算法并非追求超高效率，而是在重点关注效率的同时，采用散列抽签算法，实现了共识过程的公平性。

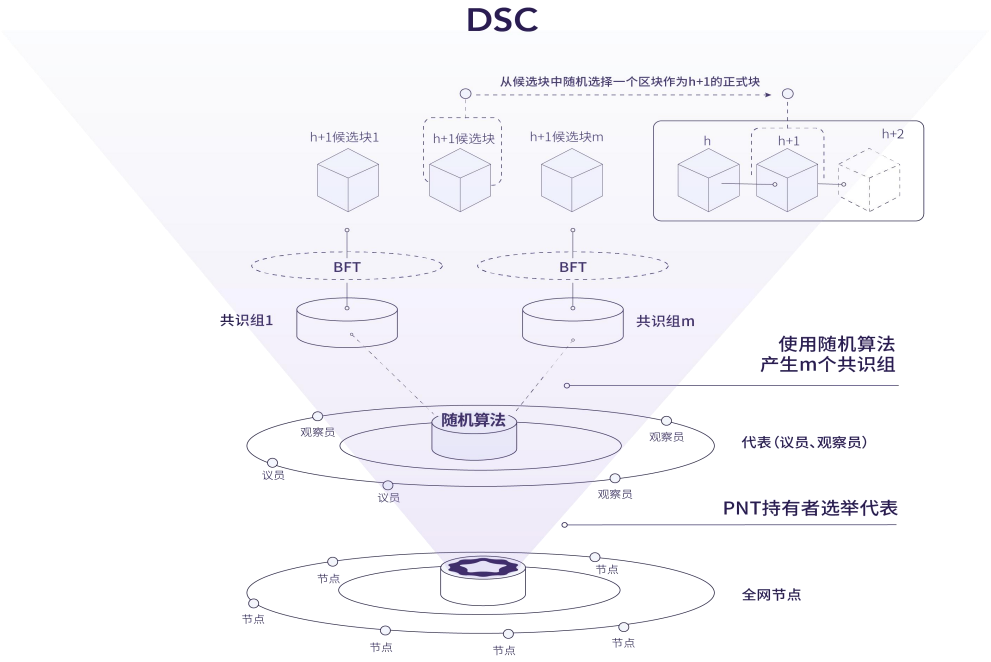


图 3.3.1.1 DSC 共识协议示意图

DSC 共识流程描述如下：

1、首先从全网节点中进行代表选举，包括选举持有较多 PNT 的议员和持有较少 PNT 的观察员。

2、通过散列抽签算法挑选议员和观察员组成若干共识组，每个共识组的议员或观察员占比不得少于 1/3。每个共识组进行 BFT 共识，从议员中选举议长，由议长提议区块，其他议员和观察员节点进行验证，2/3 以上节点验证通过后，生成该共识组对应的候选区块。共识组数量根据网络情况动态调节。

3、通过散列抽签函数从所有共识组产生的候选区块中选取正式块。

若区块共识一定时间内无法达成，将启动 RESET 机制，所有议员进行一轮 BFT 共识，产生一个 RESET 块，重新生成共识组成员，以便恢复网络正常运行。

DSC 共识过程利用散列抽签算法，保障共识过程的安全与公平性，只消耗非常少的时间和计算即可达成共识。由于共识小组是基于散列抽签算法随机生成的，所以相比起几十个较为集中的记账节点，DSC 可以更好地防范攻击也更加安全。

3.3.1.2. DApp 共识

DApp 共识由 DApp 发布方确定，在 DApp 元信息描述中进行指定，DApp 共识算法可以是平台默认提供的 DSC, POS, dPOS, PBFT, POA, Notary 等任何一种，也可以在现有共识算法基础上定制适合自己场景的共识算法。梵塔网络负责协调 DApp 交易的共识过程，提供 DApp 交易的并行和串行执行的调度机制，并对 DApp 交易共识结果进行合法性检查，得到确认后登记到区块中。

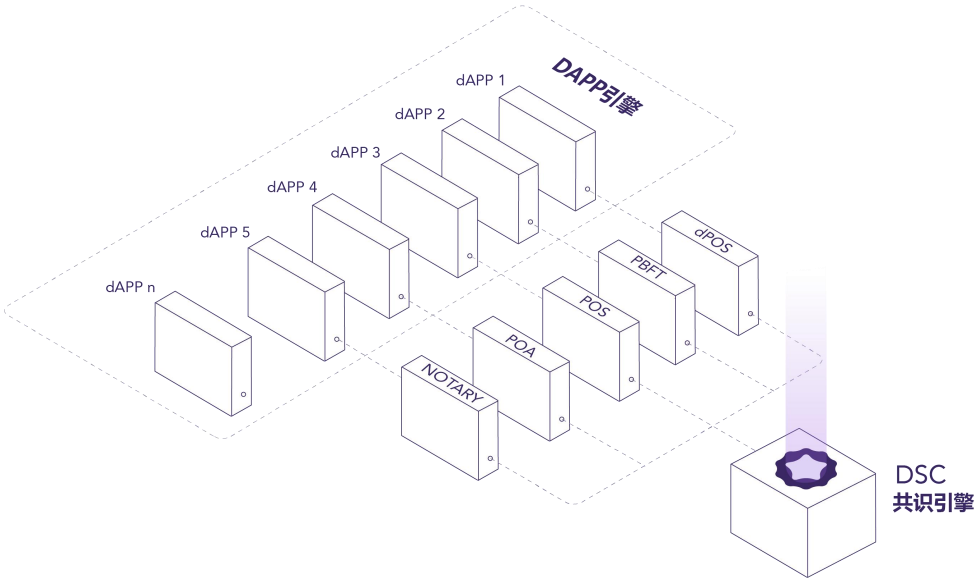


图 3.3.1.2 DApp 引擎与共识引擎

在梵塔网络中，创新性地采用多共识算法并存的机制，智能合约的执行确认与区块生成各自采用独立的共识机制，以便减少区块生成过程中夹杂处理的额外环节，更合理的利用平台资源，提高平台整体共识性能。

梵塔网络是一个多链平台，且支持插件化的共识算法，如：DSC, POS，dPOS，PBFT，POA, Notary 等。

POS 主要思想是节点获取记账权的难度与节点持有的权益成反比

dPOS 节点选举若干代理人，由代理人验证和记账

PBFT 是一种采用许可投票、少数服从多数来选举领导者记账的共识机制

POA 就是使用一组权限来允许人们在区块链上创建新的节点并确保区块链的安全

Notary 多重签名的见证人模式

3.3.2. 治理结构

梵塔链定义如下角色：

议员：由持有 PNT 的节点主动发起申请，其他节点进行投票。议员需要获得超过一定数量的投票，并质押指定数量的 PNT，议员间获取记账的机会是均等的。

观察员：由持有 PNT 的节点主动发起申请，其他节点进行投票的方式选举产生，观察员仅需要获得少量的投票，并持有与质押少量的 PNT。观察员数量较多，分布较广。

议长：BFT 共识过程中从议员中产生，负责区块的生成。

议员人数采用动态增长模式，初始议员数量与最低 PNT 质押量，根据参与节点与 PNT 持有排名的整体情况设置，根据梵塔链运行期间议员与观察员的总量进行动态调整；观察员数量则不设上限，且 PNT 质押量较低。加入记账与退出流程设置如下：

图 3.3.2 梵塔网络加入与退出记账流程

通过散列抽签算法从议员和观察员中随机选择组成共识组，每组记账人数为 n，n 是一个动态数值，每组记账人中议员的数量（n1）：n/3<n1<2n/3, 每组记账人中观察员的数量：n2=n-n1。

参与记账的节点需要在账户中质押一定的保证金，对于故意破坏系统运行的节点将进行一定的惩罚。如议长提出两个及以上的区块 BFT 共识提案，其他节点可以举证，该议长将受到数倍于收益的惩罚。

若退出记账，保证金会在 7 天后解锁。

梵塔链具有相应的协议升级机制，包含：议员和观察员人数上限、共识组节点上限、交易手续费上限、保证金最低限额等参数调整。协议升级需由全体议员进行 BFT 投票，(2n+1)/3 以上议员赞成后，在指定的区块高度自动切换新协议，可以保障协议升级不产生分叉。

3.3.3. 激励机制

为了鼓励更多参与者参与记账，维护梵塔链的正常运行，每次达成共识生成区块后，参与记账的节点，包括产生备选区块链的共识组成员都将得到相应的 PNT

激励。PNT 激励来自两部分：梵塔链预留了 50%的 PNT 用于共识记账激励；其次可以获得每个区块包含的交易手续费收益。

3.3.4. 分片

区块链系统中，交易存储在一个串行的链式结构中，每个区块都按照一定的时间周期定时生成，考虑到区块生成周期和 P2P 网络传播的速度，一般区块大小都有一定的限制，进而限制了整个平台的吞吐量。随着平台交易量的暴涨，区块链平台的可扩展性会成为平台一个重要瓶颈，如何提高并行处理能力也是每个平台必须考虑的问题。目前区块链平台在可扩展性方面，技术社区已经有一些讨论和尝试，基本分为：状态通道、侧链、分片等几种方法。

分片通常分为两种：提高交易并行处理能力，提高平台的存储能力。梵塔链的共识算法有比较高的处理效率，但是依然规划了并行处理方案，来应对未来随着交易量不断增长可能引起的可扩展性问题。梵塔链中将采用交易分片的方式提高平台的并行处理能力，使用以主链为核心特殊的账本结构 PSG（Penta Sharding Graph）提升交易处理的扩展性和安全性，并通过分片与主链的 Sync Point 技术，保障跨分片交易的一致性。平台对不同地址或 DApp 的交易采用动态分组的方式实现区块的并行处理，并自动协调交易的并行和串行处理。

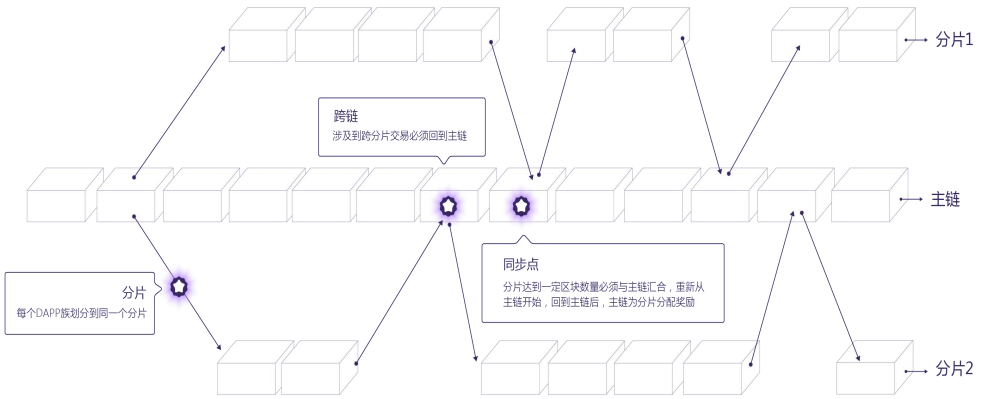


图 3.3.4 梵塔链 PSG 分片示意图

3.4. 梵塔 DLOS

DLOS 是梵塔网络的基础设施，是一个高可伸缩性、微服务、分布式框架。梵塔网络中参与节点使用 DLOS 接入，梵塔网络是以梵塔链为核心、同时包含侧链、独立链组成的多链网络。DLOS 需要支持支持各种多元化的网络结构、多样化的账本结构、以及众多共识算法，因此 DLOS 对计算、存储、网络、共识等进行分离，每一层进行了接口的抽象，然后通过服务管理和事件组件将各大服务组件连接起来，有效的实现了基础架构与具体应用的解耦，具体的应用链或 DApp 只需要实现自己特有的部分，而无需过多关注与应用场景无关的底层技术。

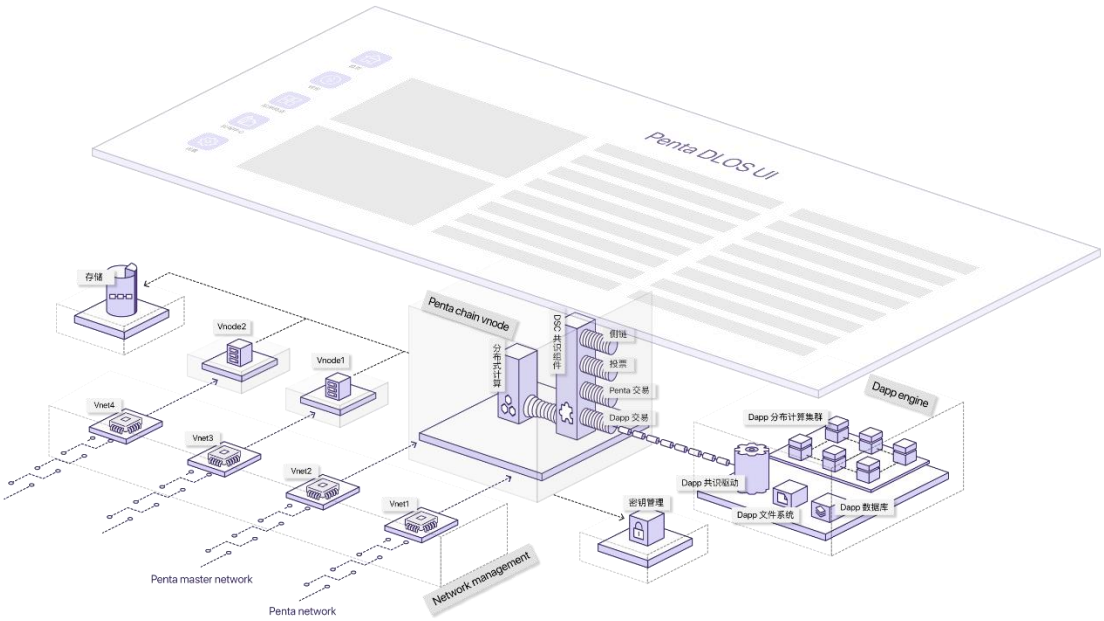


图 3.4 DLOS 逻辑架构图

3.4.1. 分布式计算框架

分布式计算框架是 DLOS 核心，用于处理整个节点的所有服务管理和事件管理。DLOS 各大组件通过分布式计算框架实现互相协作，连接成为一个有机的整体。

DLOS 在企业级应用中各大组件都可以在不同主机上运行，形成集群运行环境，有效提高单节点的可扩展性，为企业级用户构建高可用系统架构环境。

3.4.2. 存储

梵塔网络中应用场景多样，账本结构存在多种形式的可能，如：侧链、DAG 等。DLOS 对账本存储层进行抽象，并实现常用的账本存储组件，一般情况下只需要设置区块结构，即可使用。特殊情况下才会新增账本存储组件，扩展出新的账本结构。

对分叉和不分叉的链分别实现了多个存储引擎支持不同的 DApp State 数据组织形式。为分叉的场景设计了 MPT 数据存储引擎；为不分叉的场景设计了专有的数据存储引擎。

3.4.3. 网络

梵塔网络是一个多链平台，每个梵塔网络节点可能同时参与多个链。DLOS 网络层设置网络管理器管理多个虚拟 P2P 网络，每个虚拟网络都分配到具体的链，负责网络的消息的收发。由于对于 P2P 网络的需求不同，DLOS 中初期实现 Kademlia P2P 网络组件，同时不断增加新的 P2P 网络结构技术组件。应用开发者也可以自行扩展新的 P2P 网络结构技术组件。

3.4.4. DLOS UI

梵塔 DLOS UI 是工作在梵塔网络展示层的 UI 框架，为用户提供友好、易用、一致性的用户体验，同时为开发者提供统一的、低难度的 DApp UI 开发框架和技术组件。DApp UI 采用了 MVVM 架构，除封装了标准 UI 组件还封装了与 DLOS 服务层交互的 API，控制 DApp UI 访问服务层，特别是账号相关 API 的访问，与服务层配合提高客户端节点的安全性。

3.4.5. MPT 树

默克尔-帕特里夏树(Merkle Patricia Tree，MPT)是一种经过改良的、融合了默克尔树和前缀树两种树结构优点，其包含了键值的映射关系，提供了一个基于密码学的，自校验防篡改的数据结构，具有确定、高效和安全的特点；

1、确定性:查找数据时，相同的键值，将查找到同样的结果，并且有相同的根哈希；

2、高效性:当数据发生改变时，能快速的计算出新的树根，无需重新计算整棵树，对数据的插入、查找和删除具有较高的效率；

3、安全性:当攻击者恶意制造大量交易，发起 DOS 攻击，试图操纵树的深度时，限定的树深将使攻击无法实现。

梵塔网络中交易的验证、数据存储等环节大量使用 MPT。

3.4.6. 企业应用组件

梵塔网络的参与者既可以是个人用户，也可以是企业用户，但是个人用户和企业用户的需求有较大差异。个人用户更多考虑的是易用、轻量等特性，企业用户则对系统各项系统指标都有严格要求，特别是金融相关的系统更是苛刻。DLOS 企业版符合 COBIT（Control Objectives for Information and related Technology）标准，满足企业 IT 审计的要求。

DLOS 将增加安全中心、秘钥管理、成员管理、授权管理、运维、审计等组件，以便更加容易的开发企业区块链应用。

3.5.梵塔 DApp Platform

梵塔网络中 DApp（区块链应用）是实现梵塔网络场景应用服务的核心，一般分为：展示层、业务逻辑层、数据层。

DApp 数据层是 DApp 运行产生的状态数据，存储在梵塔网络账本中，数据以文件和数据库的形式存在各个节点中。梵塔网络客户端一般只同步区块数据，区块数据中一般只包含 DApp 状态数据的版本号和指纹信息，不包含 DApp 的状态数据，只有当用户在梵塔网络客户端的 ChainStore 中下载了 DApp 后，对应 DApp 的状态数据才会从其他节点同步到本地。

DApp 业务功能层可以是简单智能合约，也可以是复杂的系统。业务功能层对外接口一般分为三类：控制类（初始化、元数据等）、查询类（只做查询，不修改数据层数据）、变更类（业务逻辑会修改数据层数据，需要记账节点达成共识后数据才会生效）。

DApp 展示层运行于梵塔网络客户端中，负责与用户的交互。展示层开发必须满足梵塔网络展示层的开发规范和框架要求，才能在其客户端中正常运行。梵塔网络 DApp 展示层框架采用 MVVM 架构，有效分离 UI 布局和前端逻辑处理，提高展示层代码的可维护性。DApp 可以没有展示层，以纯接口模式提供服务。

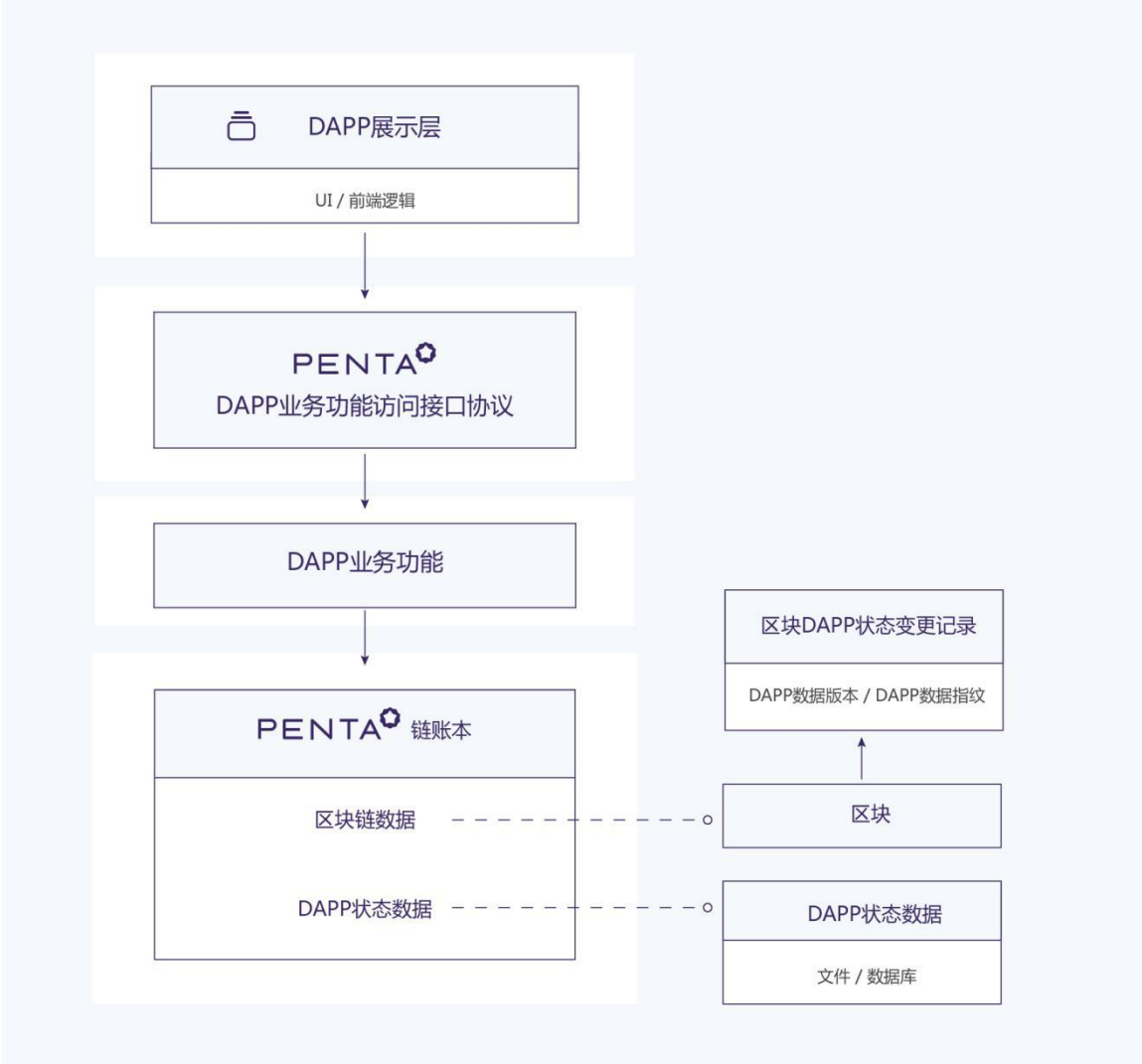


图 3.5 梵塔网络 DApp 结构原理图

3.5.1. DApp 运行环境

梵塔界（PDW）为智能合约及其他区块链应用提供完整的、独立的虚拟智能运行空间，梵塔界会为区块链应用提供独立计算资源、数据库、文件存储等应用运行所需资源，区块链应用所有资源访问权限限制在梵塔界中，不可以跨梵塔界访问其他区块链应用的数据或文件。

梵塔界中的计算、数据库、文件存储资源分别由 DARE、CLDP、MLDFS 分配，区块链应用使用 MLDFS 和 CLDP 提供的专用 API 进行资源访问，在运行结束时生成状态版本指纹，并记录在区块中。

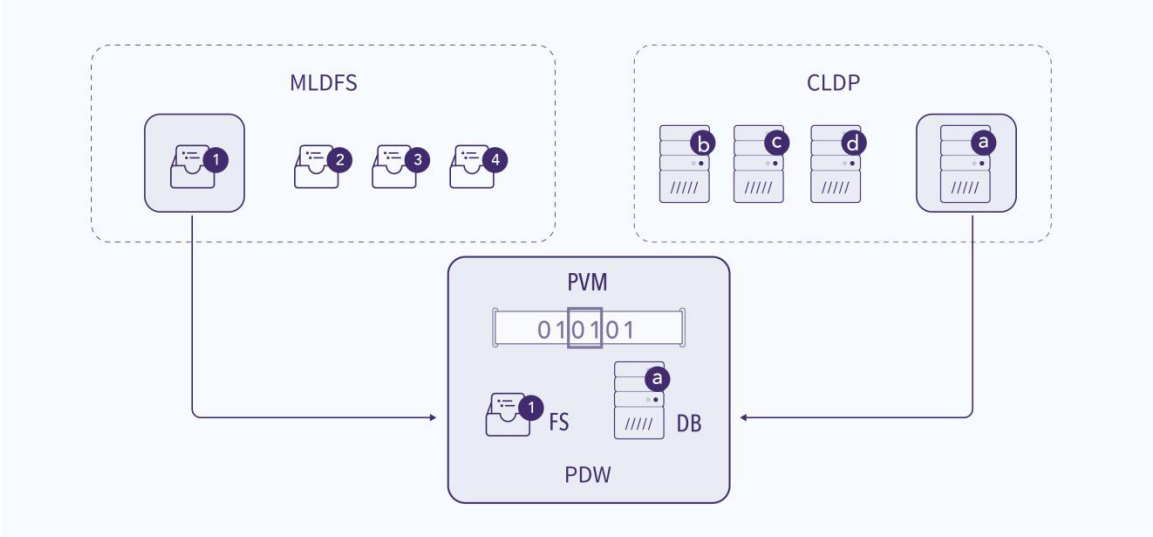


图 3.5.1 梵塔界示意图

3.5.2. DApp 数据库

容器级数据库协议（CLDP）是针对梵塔网络开发的分布式数据库存储引擎，是一个面向集合的存储引擎，介于关系数据库和非关系数据库之间，兼具关系型和非关系型数据库优点，同时提供 SQL 引擎以简化复杂区块链应用开发。为满足智能合约数据及事务日志隔离，以便区块链应用数据高效同步和复制，提供虚拟化机制。它的特点是高性能、易部署、易使用，存储数据非常方便，既适合个人用户的轻量级应用，也满足企业级苛刻性能要求。

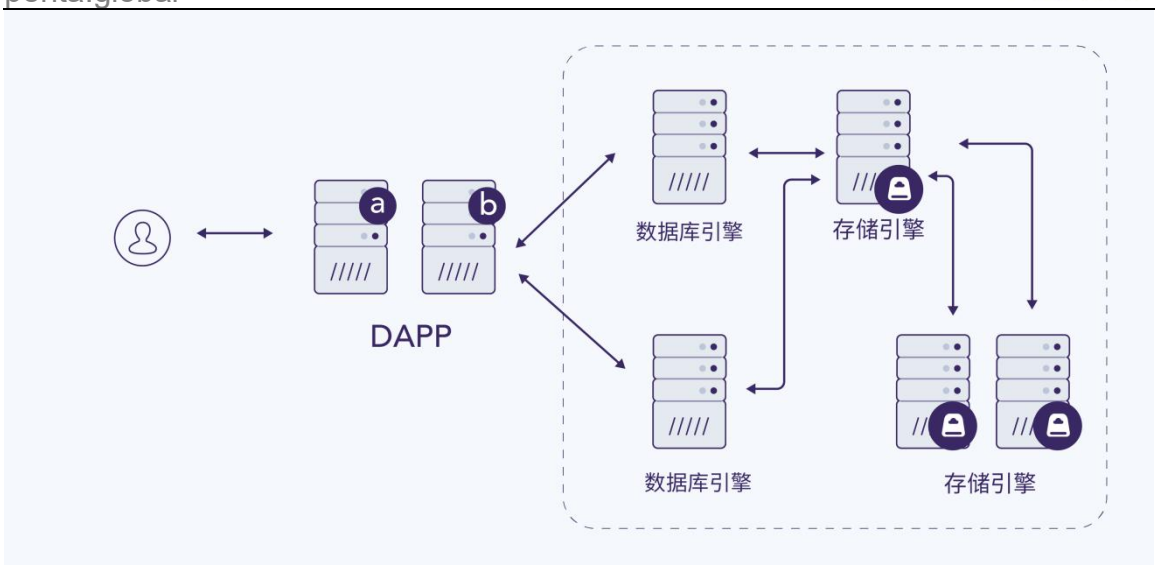


图 3.5.2 容器级数据库协议示意图

3.5.3. DApp 文件系统

层级多版本分布式文件系统（MLDFS）是一种分布式文件系统存储协议，由命名空间和数据空间组成，命名空间用于管理文件命名空间，数据空间用于存储具体数据，数据文件被分隔为若干个块存储在数据空间上。数据块支持使用传统文件系统进行分布式存储或使用 MLDFS 进行存储。

MLDFS 对文件的存储采用版本管理，对于区块链应用的每次共识事务提交后形成唯一的版本号，版本号是本次版本的 hash 值，可用于校验版本数据。每个版本记录本版本变更的数据，版本号会登记到区块中，用于其他节点同步 DApp 状态数据中的文件部分，同时版本号用于校验同步到的数据完整性。其他用户节点同步数据时可以增量同步（只同步本次版本变更的差异部分数据），有效节省流量和时间，提高整个区块链网络的性能。

MLDFS 使用虚拟化的技术，每个区块链应用运行时都会由 DARE 分配独立的文件存储环境，所有的文件修改记录都是在智能合约或区块链应用维度进行管理的，文件存储版本变更也是针对每个区块链应用变更的。

MLDFS 支持分布式事务管理，由于参与共识的节点都会运行区块链应用，校验结果，然后签名，区块链应用运行时会修改文件，但是在共识形成并提交前，数

据不能写入文件系统，直到共识完成事务提交后，才会形成文件存储新版本，每个版本最终形成分层的效果。

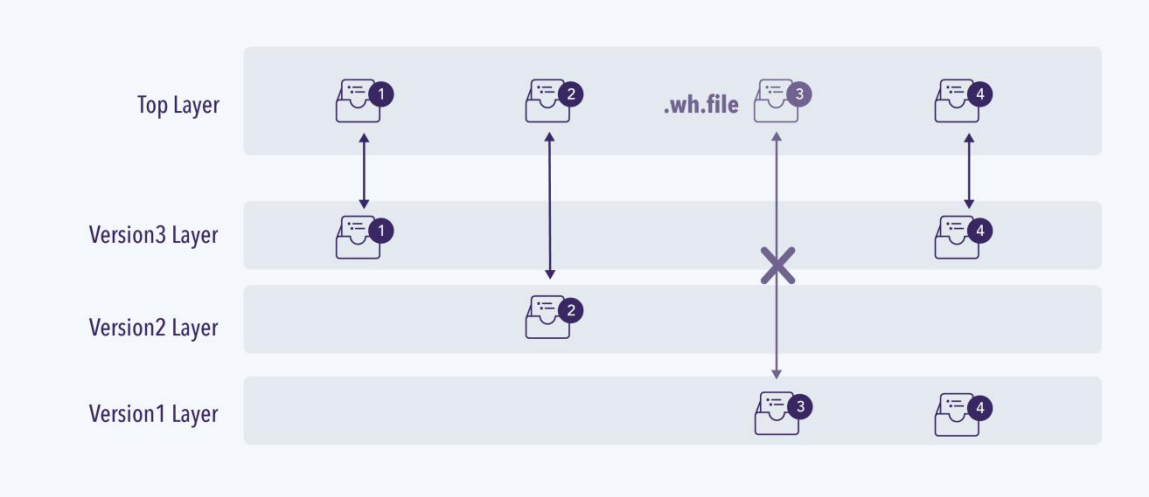


图 3.5.3 层级多版本分布式文件系统示意图

3.5.4. DAppStore

梵塔链应用市场（ChainStore）是梵塔网络中登记链和链服务（智能合约、其他 DApp 应用）的信息中心，ChainStore 的数据部分存储在梵塔链账本中，ChainStore 展现层逻辑由梵塔网络客户端提供。用户可以在梵塔网络客户端的链应用中心下载 DApp 应用，下载链应用后梵塔客户端自动根据 ChainStore 中登记的 DApp 信息下载 DApp 展示层程序，同时自动同步 DApp 的状态数据到本地。

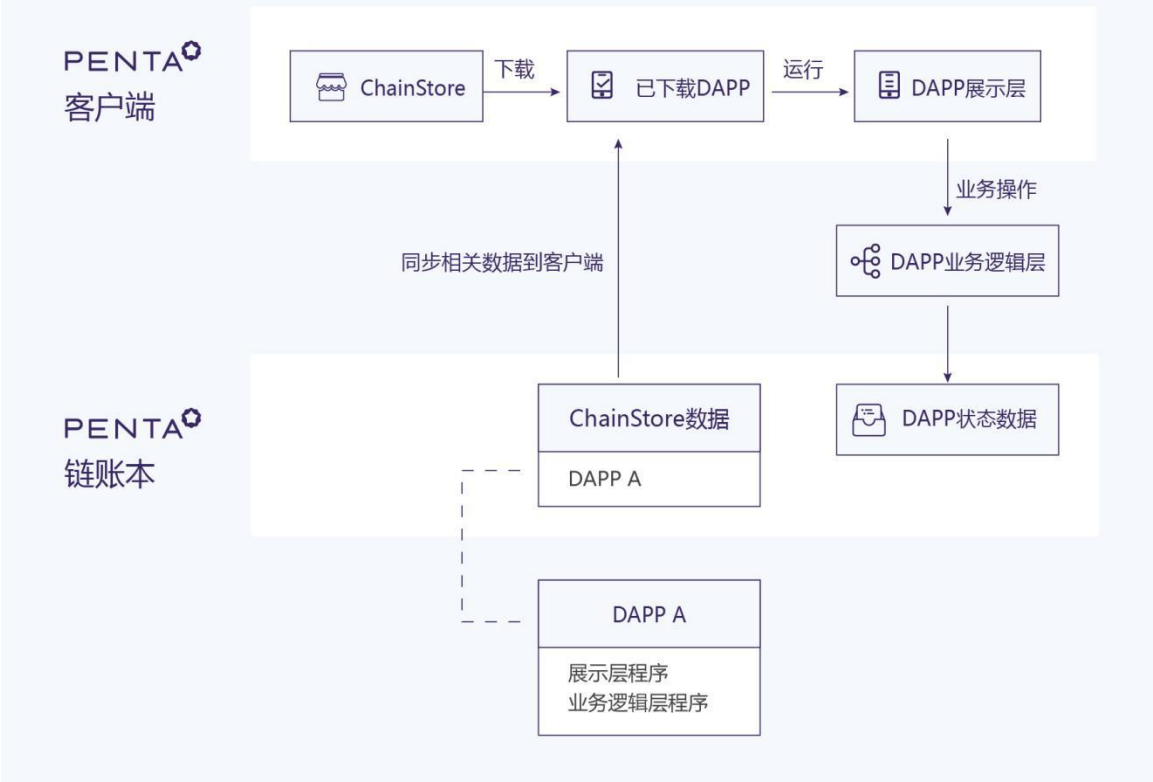


图 3.5.4 梵塔链应用市场（ChainStore） 原理图

3.5.5. DApp IDE

DApp 开发过程中调试和测试比传统系统开发复杂很多，梵塔网络将为 DApp 开发人员提供集成了代码编写、分析、编译、调试、发布等一体化的 DApp 集成开发环境，让开发更加快捷方便。通过提供工具和各种功能来帮助开发者组织资源，减少失误。

3.5.6. DApp SDK

梵塔 DApp 运行环境中 SDK 中按照层次提供了多种 SDK，以便开发者可以比较容易地开发出符合实际场景的应用。SDK 为 DApp 提供存储、验签、账户、身份、连接器、数字资产等 API。

3.6. 连接器

梵塔团队认为区块链等分布式账本技术并不是万能的，并非所有场景都适合区块链，主要会应用在一些缺乏信任的场景中。在一些场景中人们更相信中心机构，

所以未来应该是中心系统、联盟链、公有链互联互通协同为用户提供服务的工作模式。梵塔网络连接器以具有很好效率、安全性、一致性的梵塔链作为其核心，致力于实现链与链、链与中心系统、链上链下的连接，并提出包含通讯链路层、信任层、价值层、应用层的四层连接器协议架构。

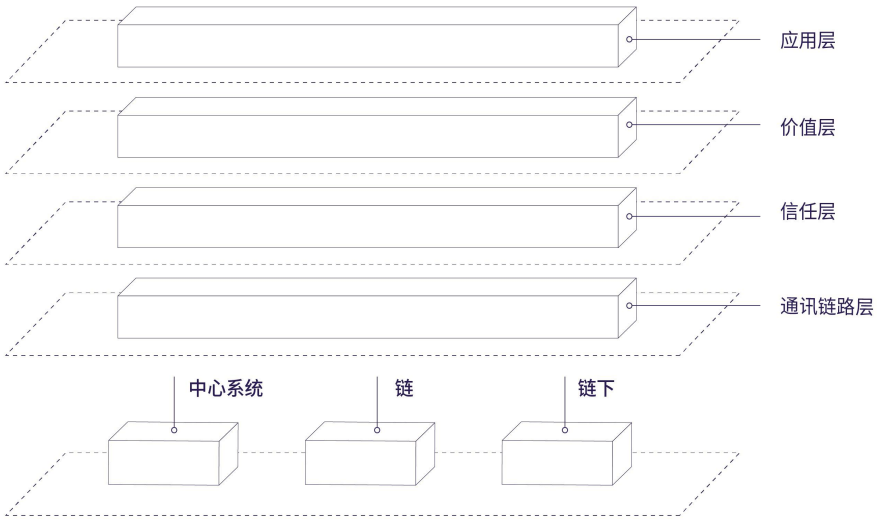


图 3.6-1 连接器协议架构

- 通讯链路层：实现与其他链平台和中心化系统的信息互通，解决通讯传输和数据格式问题。
- 信任层：提供各种主体的信任机制，实现价值在不同平台间转移中间方的信任，包括技术信任和主体信任。技术信任：HTLC、多重签名、分布式秘钥控制、智能合约、侧链等； 主体信任：身份认证、信息认证、担保、保险、时间戳、公众评价、信用评级等。
- 价值层：这一层主要负责链内外价值转移过程中的价值承载，可以包括：单主体托管、联盟托管、合约账户、记账人、公证人等方式。
- 应用层：根据场景选择合适协议组合实现价值传递、服务商业场景。

连接器协议支持柔性事务机制，以便分布式应用进行事务控制。梵塔网络核心运行环境 DApp SDK 中提供了调用其他链标准 API，也提供了调用现有主要区块链平台（BTC、ETH、Ripple、Stellar、NEO、Dash、Hyperledger 等）的 API，开发

者在 DApp 中调用这些 API 即可实现与其他链交互，也可以实现与传统中心系统的交互。功能组件层提供统一身份认证，以及链服务注册、链服务发现、链服务质量评价等功能，以便链服务与链服务、链服务与中心系统提供的服务协作运行。梵塔网络提供融合客户端，融合目前主要区块链客户端（BTC、ETH、Ripple、Stellar、NEO、Dash、Hyperledger 等），为用户提供统一的使用体验，融合客户端同时提供其他链访问这些链的统一 API，其他链通过融合客户端可以以统一的方式、非常容易地实现与梵塔网络的链或其他链的连接与协作。

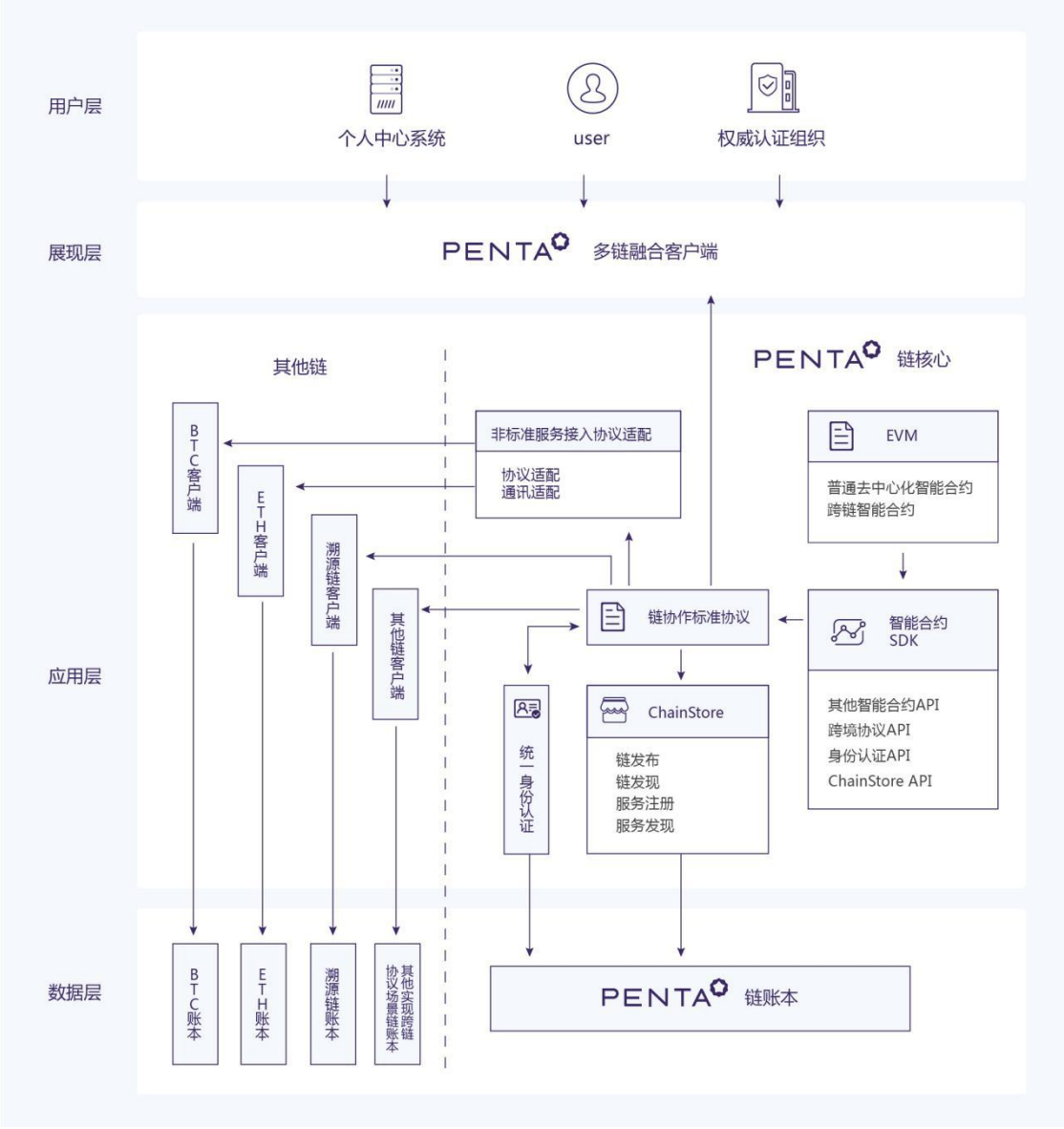


图 3.6-2 跨链服务协作工作原理

3.6.1. 柔性链路协议

区块链非中心化系统发展非常快，但是区块链系统应用也是有其特殊的场景，传统集中式系统会长期存在，区块链系统应用于更广泛的领域必然需要与现有集中式系统交互。如何能够快速、稳定、高效地与现有集中式系统进行对接，正是设计柔性链路协议（SXA）的目的。柔性链路协议分为三层：通讯层、协议层、业务层，通过三层协议配合，可以快速适配传统集中式系统。

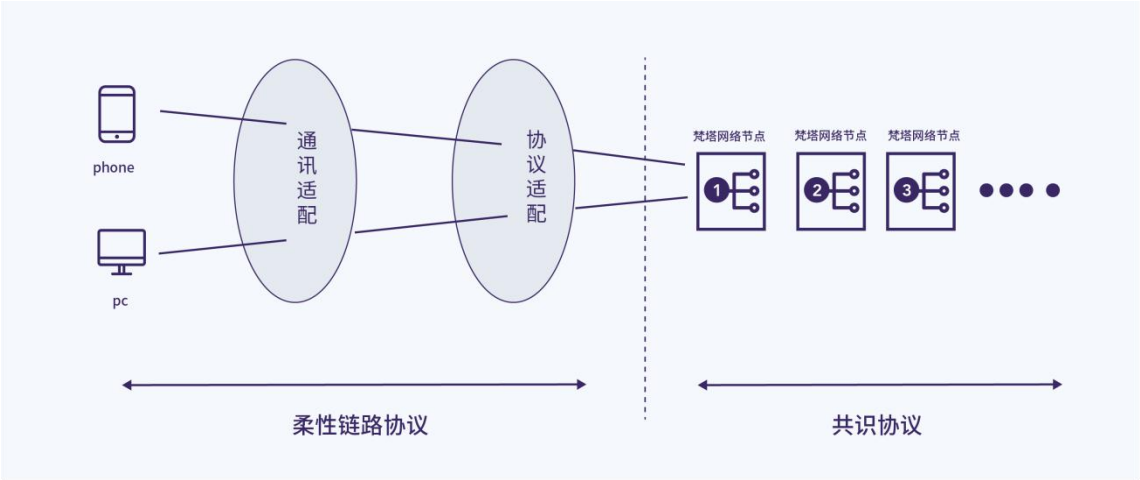


图 3.6.1 柔性链路协议示意图

3.6.2. 分布式私密通讯协议

区块链默认 P2P 网络是一个信息公开的，对数据进行广播的通信系统，发布到区块链上的数据，所有区块链参与者都可以查看，但是在很多现实交易过程中往往有一些数据不希望向交易无关者公开，这就用到了梵塔通信网络，梵塔通信网络在现有网络节点中构建一个特殊的通信网络（DPCP），两个参与节点如果需要传输私密信息，梵塔通信网络会在网络中建立起一条特殊的通信渠道，渠道中的所有数据只有通信双方可以看到，其他第三方都不能进行窥探。梵塔通信网络提供路由、渠道建立、流量控制、证书交换、数据秘钥交换、加密数据交换、渠道销毁等机制。

图 3.6.2 分布式私有通讯协议示意图

3.7. 技术路线

梵塔网络目标是实现区块链世界的连接器，首先完成实现分布式信任层梵塔链，然后逐步实现 DLOS 梵塔网络技术基础设施、承载去中心化应用的 DApp 平台、连接器协议架构，并完善各个层次的技术，构建梵塔网络。

梵塔技术社区将首先实现梵塔链，包括：DSC 共识算法、投票中心、梵塔 PC 钱包、区块链浏览器等，发布首个版本，支持用户进行 PNT 交易。

在梵塔链技术组件的基础上完成第一个版本 DLOS 核心部分的整理，使得其他用户可以基于 DLOS 更加容易地创建自己的链，同时推进梵塔网络节点承载多链。

DApp 平台是梵塔网络中非常关键的一层，使梵塔网络能够支持复杂分布式应用场景，平台将逐渐实现 DApp 运行环境、DApp 专用数据库、DApp 文件系统、DApp UI 框架、DApp 开发运维支持等一系列的技术。

连接器是梵塔网络的一个关键节点，实现链与链、链与中心、链上链下的连接，连接器的核心是标准、协议、规范和最后是技术组件的实现，需要行业共同推进，梵塔社区将在未来相当长的时间里不断推动连接器技术的完善和应用，从而实现梵塔网络区块链世界连接器的愿景。

3.8. 安全策略

梵塔网络采用多重安全策略保护平台安全运行，底层提供多种加密技术供选择，如：ECC，SM2 等，根据项目进展适时引入可以抵御量子计算暴力破解的加密算法，规避量子攻击，如 Lattice-based cryptography 。

梵塔网络中使用的 ECC 加密算法是一种主流的非对称加密算法，公开密钥算法总是要基于一个数学上的难题。比如 RSA 依据的是：给定两个素数 p、q 很容易相乘得到 n，而对 n 进行因式分解却相对困难。而 ECC 算法基于的难题：

考虑等式： K=kG [其中 K,G 为 Ep(a,b)上的点，k 为小于 n（n 是点 G 的阶）的整数] 不难发现，给定 k 和 G，根据乘法法则，计算 K 很容易；但给定 K 和 G，求 k 就相对困难了。这就是椭圆曲线加密算法采用的难题。我们把点 G 称为基点（base point），k（k<n，n 为基点 G 的阶）称为私有密钥（private key），K 称为公开密钥（public key）。

现在我们描述一个利用椭圆曲线进行加密通信的过程：

1、A 选定一条椭圆曲线 Ep(a,b)，并取椭圆曲线上一点，作为基点 G。

2、A 选择一个私有密钥 k，并生成公开密钥 K=kG。

3、A 将 Ep(a,b)和点 K，G 传给用户 B。

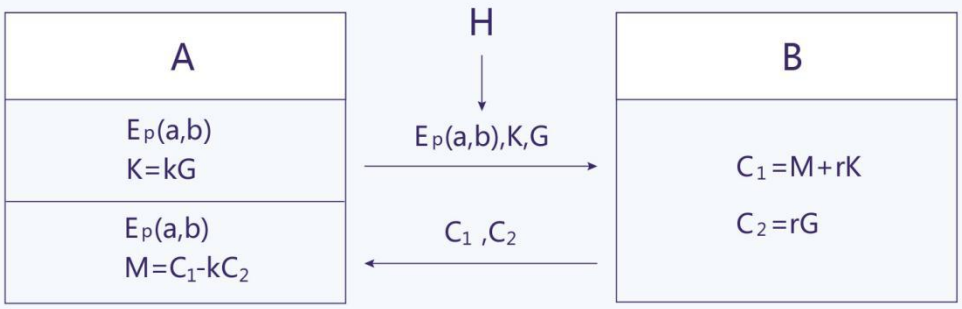
4、B 接到信息后，将待传输的明文编码到 Ep(a,b)上一点 M（编码方法很多，这里不作讨论），并产生一个随机整数 r（r<n）。

5、B 计算点 C1=M+rK；C2=rG。

6、B 将 C1、C2 传给用户 A。

7、A 接到信息后，计算 C1-kC2，结果就是点 M。因为 C1-kC2=M+rK-k(rG)=M+rK-r(kG)=M 再对点 M 进行解码就可以得到明文。

在这个加密通信中，如果有一个偷窥者 H，他只能看到 Ep(a,b)、K、G、C1、C2 而通过 K、G 求 k 或通过 C2、G 求 r 都是相对困难的。因此，H 无法得到 A、B 间传送的明文信息。



密码学中，描述一条 Fp 上的椭圆曲线，常用到六个参量：

T=(p,a,b,G,n,h)。

（p 、a 、b 用来确定一条椭圆曲线， G 为基点， n 为点 G 的阶， h 是椭圆曲线上所有点的个数 m 与 n 相除的整数部分）这几个参量取值的选择，直接影响了加密的安全性。参量值一般要求满足以下几个条件：

1、p 当然越大越安全，但越大，计算速度会变慢，200 位左右可以满足一般安全要求；

2、p≠n×h；

3、pt≠1 (mod n)，1≤t<20；

4、4a3+27b2≠0 (mod p)；

5、n 为素数；

6、h≤4。

梵塔网络中支持的 SM2 算法是中国国家密码局基于 ECC 算法基础上发展而来，是中国商用密码标准，在中国商用广泛，特别是金融领域被强制应用，梵塔网络支持 SM2 算法后适用区域和领域更加广泛。

梵塔网络设置了身份认证体系，以便能更加容易地和对安全性、信息敏感、参与方有严格要求的联盟链或中心化系统跨链协作。梵塔身份认证体系中由传统权威认证机构对参加用户身份信息认证，然后将对用户数据进行脱敏后的身份验证信息和授权信息存储在梵塔网络账本中，供其他使用方进行信息验证。

为了防止梵塔网络上的资源被滥用，产生过多垃圾交易，以及提高平台安全性。梵塔网络对网络转账和智能合约使用者的运行和存储扣减一定量的 PNT，PNT 持有者可以投票确定是否对上述行为实施 PNT 扣减机制及扣减额度。

4.梵塔网络应用

在过去两年多的时间中，梵塔网络团队与全球多个行业企业、机构合作并落地数个区块链项目。未来，梵塔网络将深耕行业拓展，为更多的应用场景提供坚实的区块链基础设施，提升行业效率，降低业务运营成本。

梵塔网络将从社会、经济等维度构建区块链普惠的应用网络。梵塔网络将结合人工智能、大数据、虚拟现实、机器人、物联网、云服务等新科技，在健康医疗、交通运输、IP、新能源汽车、有机农业、分布式能源、时尚、食品、商业、金融、游戏等行业推广落地应用。

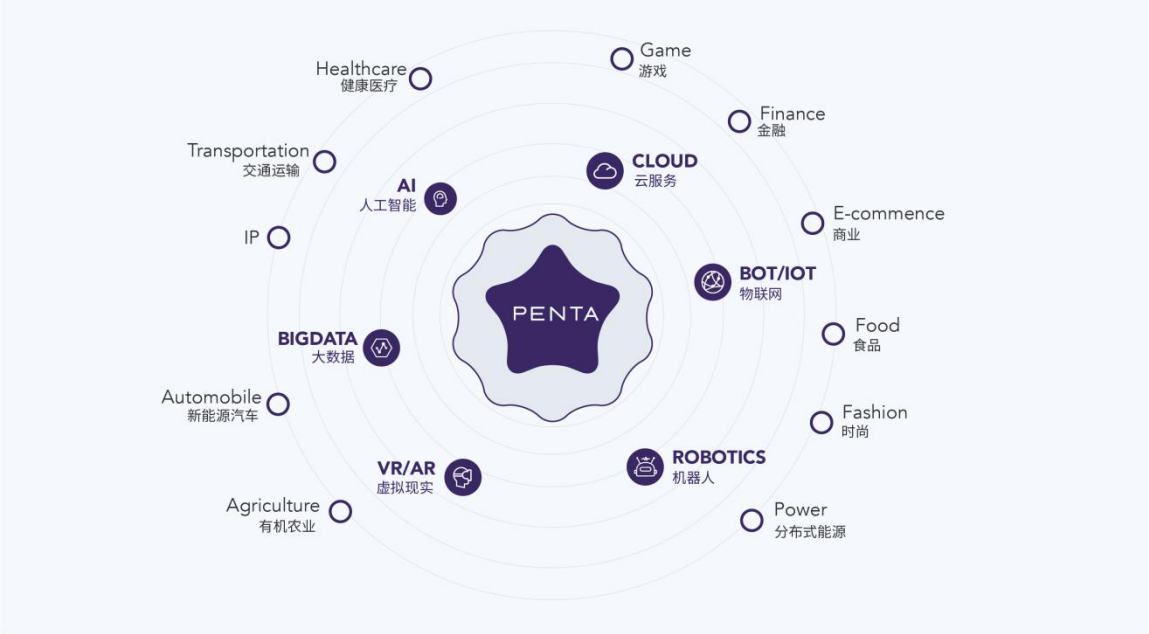


图 4 梵塔应用网络

4.1.社会

4.1.1.医疗/健康

健康医疗行业正经历着一个重大转变：药物、设备、服务和商业模式的数字化，此过程中使得医疗系统大众化，并产生新的价值。大多数国家都制定了以数字健康医疗为目标的政策，增加其数字健康记录，比如电子健康记录、电子医疗记录以及其他健康系统或设施。

目前围绕安全性、完整性以及对个性化健康数据的访问权限的限制成为医疗交付创新的关键。医疗保健行业难以找到风险与回报之间的平衡，区块链技术的潜在应用提供了一种及时的解决方案来缓解这些迫切的需求，并且可以从以下方面助力医疗行业：

1)数据安全

不同于现有的安全系统，区块链使用内置的密码学技术在分布式网络上运行，技术保障了数据的不可修改性。由此医疗系统、医疗设备制造商以及医疗技术公司可以利用区块链技术增强其设备识别管理功能，对病人生成的健康数据提供选择性的访问权限。

2)健康医疗数据交换

健康医疗数据的共享不仅仅是信息交换，而是两个或两个以上的系统或实体之间基于彼此的信任来使用共享的问责性信息，梵塔网络可提供一个不可变的、受信任的工作流，在健康数据交换中形成“单一数据源”，从而保证系统和模型的完整性。

3)药品安全

采用基于区块链的分布式医疗体系，可以加强药品防伪，公开药品价格等。

4)精准医疗

制药公司在证明其药品价值方面面临着越来越大的压力。根据行业估计，每年约有 3000 亿美元的药物因没能提供预期的效果而被浪费，同时也使患者遭受了药物带来的副作用。因此，制药行业必须转向以病人为中心的药物开发模式，以实现未来的靶向治疗。精准医学概念预示着医护交付领域的范式转变。

区块链技术以其完善的安全基础设施可以实现健康数据的无缝交换，推动更大规模的基因组学研究，从而促进精准医疗的发展。随着药物开发行业不断在精准医疗上押注，基于区块链的、不可变的记录可能会消除临床试验数据校正的负担和成本，并促进研究成果的共享。

梵塔网络未来与健康医疗行业的结合与商业推广，可有效提升医疗体系运作、管理效率，构建诚信、可追溯、透明、安全的医疗保障体系。

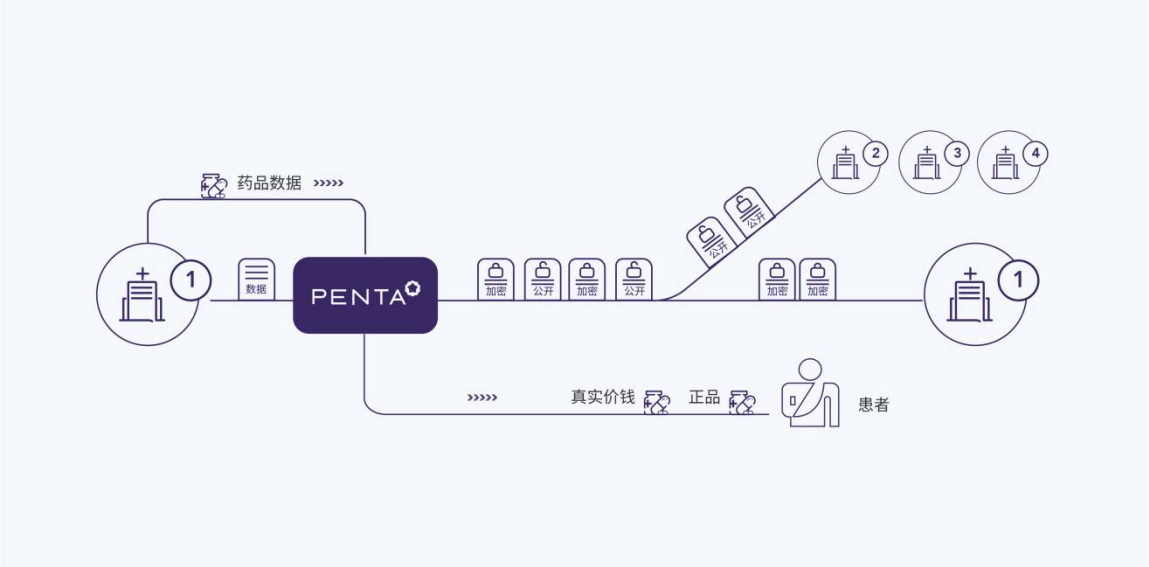


图 4.1.1 梵塔网络区块链药品应用体系

4.1.2.能源

传统能源的日益短缺以及带来的环境污染，已经成为世界性难题，另外一方面，人类可以利用的可再生能源（如风能、太阳能）技术虽然在逐渐成熟，但是却没有得到普遍使用，据行业调查，风能在发电量中仅占比 4%，太阳能占比 1%。究其根本，在于传统大电网（国家电网、南方电网等）在集中化经营模式下，输配电场景复杂、设备多种多样、电力调度和管控难道大，因此，分布式能源的大规模利用存在着很多技术上的障碍和商业利益冲突。

随着当前互联网通信和处理技术的快速发展，美国学者杰里米·里夫金在《第三次工业革命》中提出了“能源互联网”的概念，迅速获得广泛传播。2016 年，中国国家电网发布《城市能源互联网发展白皮书（2016）》，首次提出构建以电为中心的城市能源互联网 UEI（Urban Energy Internet），将城市作为一个自治主体，实现城市能源的高效资源配置，推动城市能源清洁化、电气化、智能化。

在新的形势和背景下，分布式能源的接入、交易和使用，我们可以从自主构建一个微型电网的角度出发，重新思考和设计，而不是在传统的大电网下进行整体规

划和考虑，在一个区域内形成一个“多能互联、多能互动、多能接入、多能交易、多能响应”的社区能源互联网 CEI（Community Energy Internet），再由 CEI 组合一个 UEI，最终与传统电网进行交互，形成一个能源互联网生态。这不仅需要在物联网领域进行突破，也需要在信息平台和商业模式变革上进行创新，其中一个关键突破口就是建立一个去中心化电能交易平台 SPX（Smart Power Exchange），推动一个物理区域范围内的电能提供方和电能消费方自主透明化交易和信息共享，并通过设定多方共赢的奖励机制，提高能源传递和利用效率。

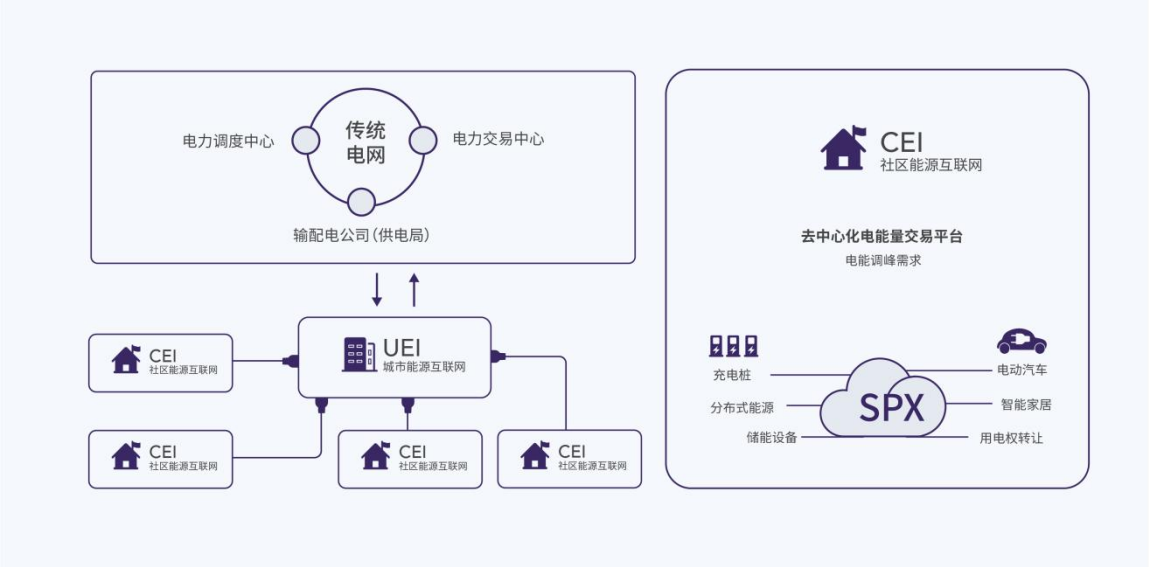


图 4.1.2 SPX 为核心的社区能源互联网

基于梵塔网络开发的去中心化电能交易平台 SPX（Smart Power Exchange）致力于通过信息平台的搭建和商业模式的重构，建立一定范围内的、虚拟化的社区能源互联网。其应用架构包括：可用资源发布、能源查找和需求发布、智能撮合、订单执行、智能电表和计量数据传送、电子钱包、订单结算等功能。

4.1.3.物联网

随着物联网技术、智能硬件和区块链技术的发展，万物互联（IOT， Internet of Things）的时代必然会发展向智能万物， 物链网（BOT， Blockchain of Things）。梵塔网络致力于最终实现设备自治（Things Autonomy），价值互通（Value Transfer），人工智能（AI）与机器人（Robotics）技术融合的物链网时代

拓展。

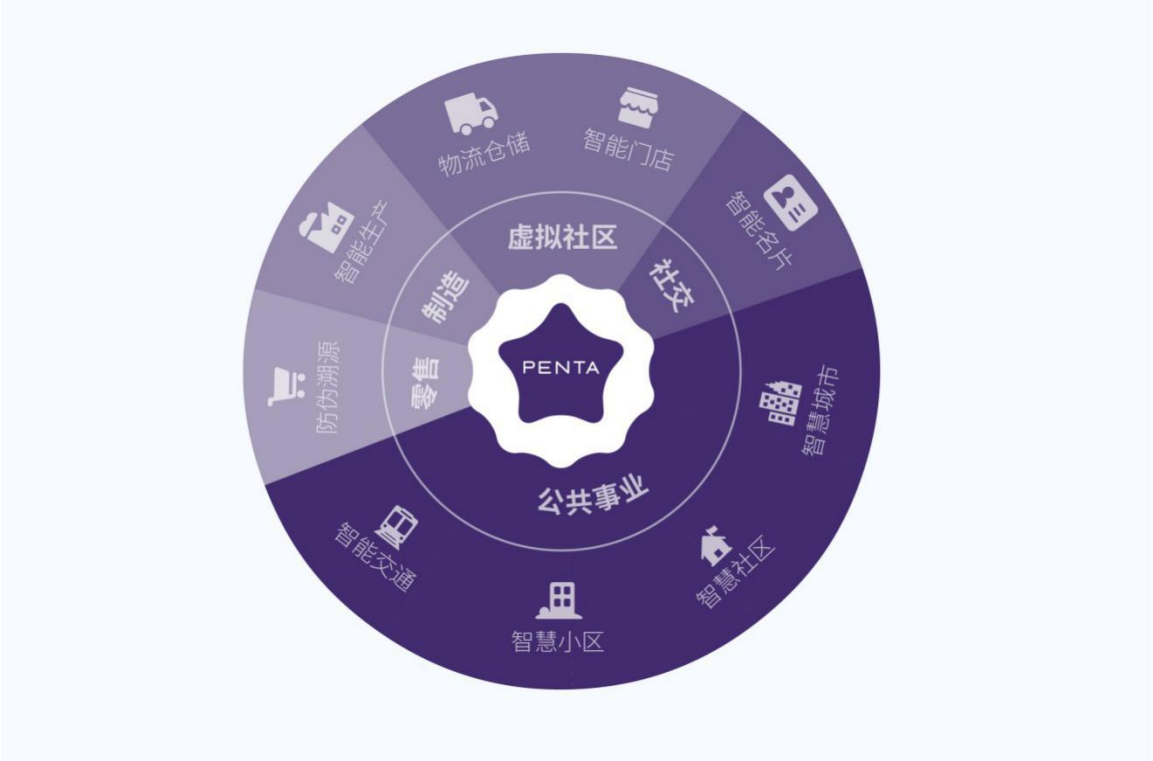


图 4.1.3-1 梵塔网络物联网体系

以物链网（BOT）在分布式充电桩（DCP）的应用场景为例，由于电动汽车的低碳化特性，全球范围内已经逐渐形成由政府主导的“去油车”趋势，据公开报道，德国计划在 2030 年停止生产汽油和柴油车，英国计划在 2040 年禁止汽油车。电动汽车的发展已经成为不可阻挡的历史潮流，但是，目前影响其推广的一个关键因素是充电的便利性。据某媒体记者调查：“对某城市核心的 42 处公共充电站进行实地调查，共有 340 个充电桩，其中，正在充电的充电桩有 61 个，占比 17.9%，损坏和故障的有 35 个，占比 10.2%，被占位有 92 个，占比 27%“。其症结在于这些充电设施是由电网公司和电动汽车公司、充电桩运营公司进行集中化的投资、建设和运营，在经营动机、互联互通、可持续发展等方面存在着较多的弊端，难以满足日益增长的电动汽车对充电的刚性需求。

充电难的主要原因是对充电桩（快充和慢充）的依赖性过强，而且大量私人投资的充电设施不能对外共享，其他潜在的电能提供方（如社区便利店、停车场）也

无法对电动汽车提供充电服务，其本质是缺乏一个有效的电能交易方式，包括供需撮合、计量、结算手段。

通过梵塔网络搭建 SPX 平台，向潜在的电能提供方（如私人充电桩、停车场和便利店）提供智能计量装置、智能快充和慢充设备，使其具备提供充电服务的能力，并在 SPX 上发布可用资源，用户可以通过各种渠道（包括：电动汽车公司 APP、SPX APP）快速找到充电点和完成交易，将极大地促进电能的高效传递和利用。

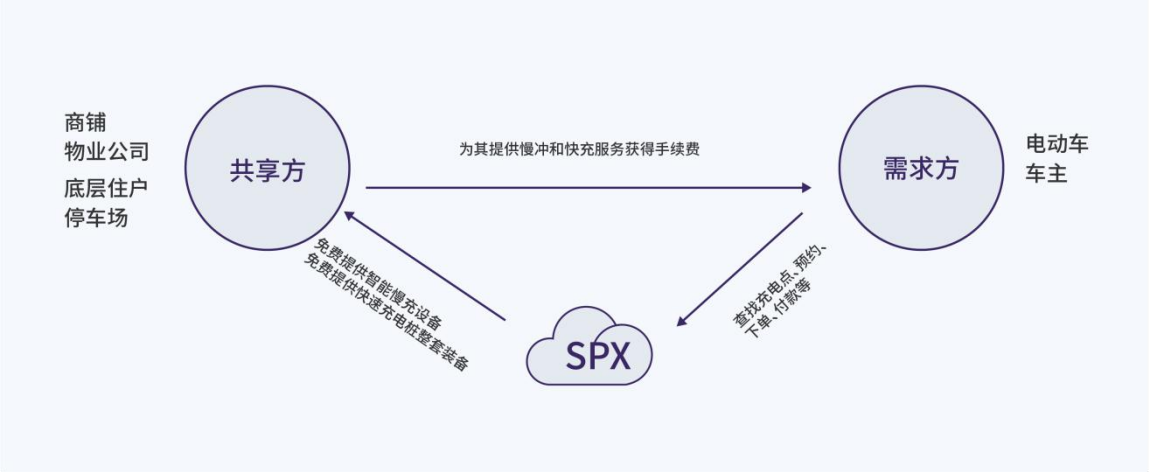


图 4.1.3-2 以 SPX 为核心的共享充电模式

需求侧响应：

需求侧响应（DemandResponse，DR），是指通过提供资金奖励引导用户改变原有的用电模式，达到减少或推移某时段的用电负荷而响应电力供应，从而保证电网系统的稳定性。

在目前的电网集中管理下，需求响应是集中化管理，参与需求响应的组织和个人需要提前提出申请，进行用电设备监控装置改造，并签订电力需求响应合同，造成手续繁多和要求高，广大的小散"用户参与难度大，难以形成规模效应，影响需求响应的实际效果。

图 4.1.3-3 以 SPX 为核心的需求响应

去中心化电能交易中心 SPX 可以在需求侧响应中承担负荷集成商的角色和职能。它从电网公司获得需求响应合同和事件，在 SPX 中设置智能合约并发布，让 CEI 内的主体进行负荷抢单或预约。通过这个过程，SPX 将从电网公司获得需求响应总量进行任务分解和执行主体分散化，让更多的"小散"主体可以参与到需求响应过程，发挥长尾效应。另外，在智能合约中设置容忍度函数，使得少数部分违约行为不影响整体需求响应的及时和准确性。在执行需求响应过程中，SPX 通过事先提供的免费智能终端监控需求响应情况，也可以基于信用评估，在不安装智能终端的前提下，由参与主体基于信任关系主动进行响应。SPX 作为负荷集成商，获得电网公司的需求响应奖励，并实时以代币的方式返还给参与方。

4.2.经济

区块链作为一种新兴技术，发展迅速，通常金融体系使用新技术要滞后于其他行业，但从各个区块链组织的成员来看，金融机构参与度是最高的，数量也是各行业最多的。主要源于区块链与金融有天然的融合性，在金融领域可以落地的场景较多。部分场景列举如下：

- 在资产交易业务方向，可以在同业资产交易、商业票据、供应链金融、ABS 资产化等方向进行实际项目落地；
- 支付清算方向，可在银行间清结算、跨境支付、积分等业务上进行应用；

- 信贷业务方向，可在征信、抵、质押、贷款、供应链金融等业务上进行应用；
- 其他业务方向，可在 P2P，众筹等领域结合区块链进行应用。

图 4.2 金融场景

梵塔网络过去的时间在金融行业的区块链结合应用上已经积累了丰富的经验，其中征信、积分、资产证券化、供应链金融业务上已有具体实践。

4.2.1.征信

近年来全球信贷规模与信贷人口规模不断持续增长，持续增长的信贷业务规模拉动了征信需求，同时征信技术的支持及社会大众对信用资质的重视，为征信快速发展提供了必要条件。

当前征信市场，部分问题较为突出：

1) 当前央行征信门槛较高，主要覆盖银行及其客户群体，其他如小贷公司，融资租赁等机构无法接入共享征信数据。
2) 征信机构之间缺乏数据共享，征信机构与用户信息不对称现象较为严重。
3) 正规市场化数据采集渠道有限，数据源争夺战耗费大量成本。
4) 数据隐私保护问题突出，传统技术架构难以满足新要求。

区块链具有去中心化、去信任、时间戳、非对称加密和智能合约等特征，在技术层面保证了可以在有效保护数据隐私的基础上实现有限度、可管控的信用数据共

享和验证。针对目前征信行业现状与问题，梵塔网络认为区块链可以在征信的数据共享交易领域着重发力，并构建了基于区块链的征信服务平台，以促进参与方最小化风险和成本，加速信用数据的报送、查询、结算。

梵塔网络基于区块链打造的征信平台，其节点成员包括征信机构、用户、其他机构（小贷机构、银行、保险、政府部门等），实现了信贷机构与征信机构，征信机构与征信机构的数据共享。

为解决征信信息滥用问题，梵塔网络利用区块链的智能合约，建立了征信查询授权机制，并利用区块链追溯特性记录授权与查询，区块链不可逆属性，可严格防范信贷机构不规范使用征信行为。此外在区块链记录的敏感信息已进行加密，仅在授权后可以查阅。

当前该平台已在上线运行，已有部分小贷机构接入，支持信贷数据、抵押物数据、黑名单数据、其他监管机构、三方机构提供的数据报送、查询。此外梵塔网络设计了积分奖励与消费机制，鼓励接入机构更多的分享数据。

图 4.2.1-1 梵塔网络区块链征信平台

该平台上线以来运行良好，不断增加新的机构与节点接入。基于区块链的征信服务平台的交易区块监控图如下：

图 4.2.1-2 区块链的征信服务平台交易区块监控图

4.2.2.供应链金融

随着经济与产业的发展，各国企业的应收账款逐渐增加，假如用这些应收账款当作银行贷款的潜在抵押品加以充分利用，可以预见未来供应链金融发展市场潜力巨大。

梵塔网络过去已为多家银行、财务公司等金融机构提供供应链金融系统解决方案，在服务的过程中，梵塔网络深刻理解供应链金融业务的复杂性，其中多方合同、交易支持材料等核验的繁琐，操作流程冗长，效率低下。主要源于供应链金融的参与方较多，信息互通与信任难以建立，以典型的订单融资场景而言，涉及到买方、卖方、买方开户行、卖方开户行、物流公司、监督机构、海关（跨境订单融资）等。

此外供应链金融产品类别较多，贯穿整个贸易环节，覆盖企业从生产计划到货物签收与资金交割的各个环节，支持的产品也是从订单融资，到流动资金贷款与资金结算等。

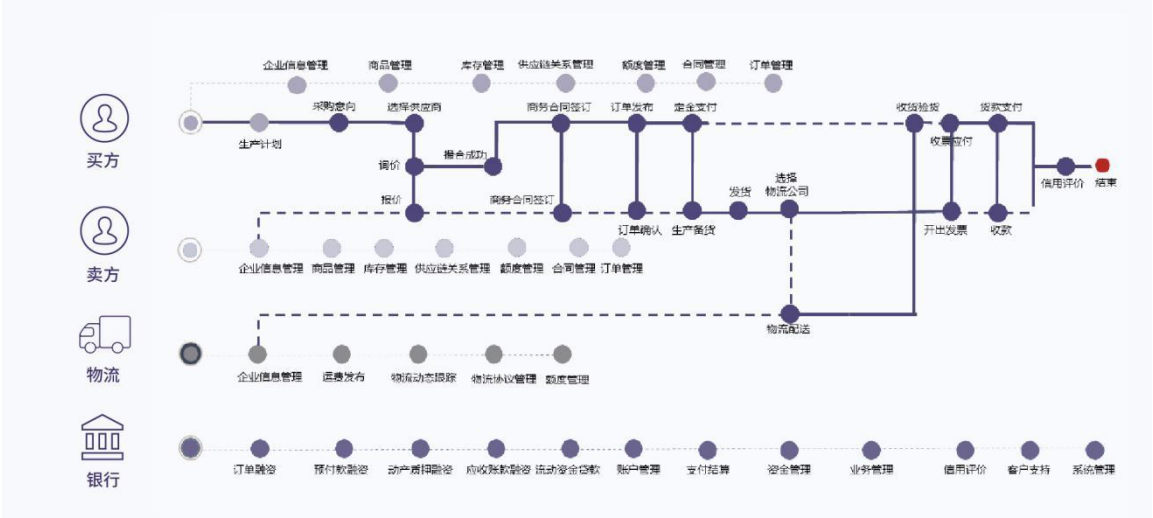


图 4.2.2-1 供应链金融

通过区块链技术与供应链金融业务相结合，可以将订单、信用证与提货单、贸易流程的文件放到区块链上，通过区块链进行认证与不可篡改的验证；同时，基于区块链的数字化解决方案，达到完全取代现今的纸笔人工流程，实现端到端完全的透明化，提高处理的效率并减少风险。

为此梵塔网络针对订单融资场景，曾为某金融机构构建基于区块链的供应链订单融资平台，其中业务场景与区块链记录处理描述如下：

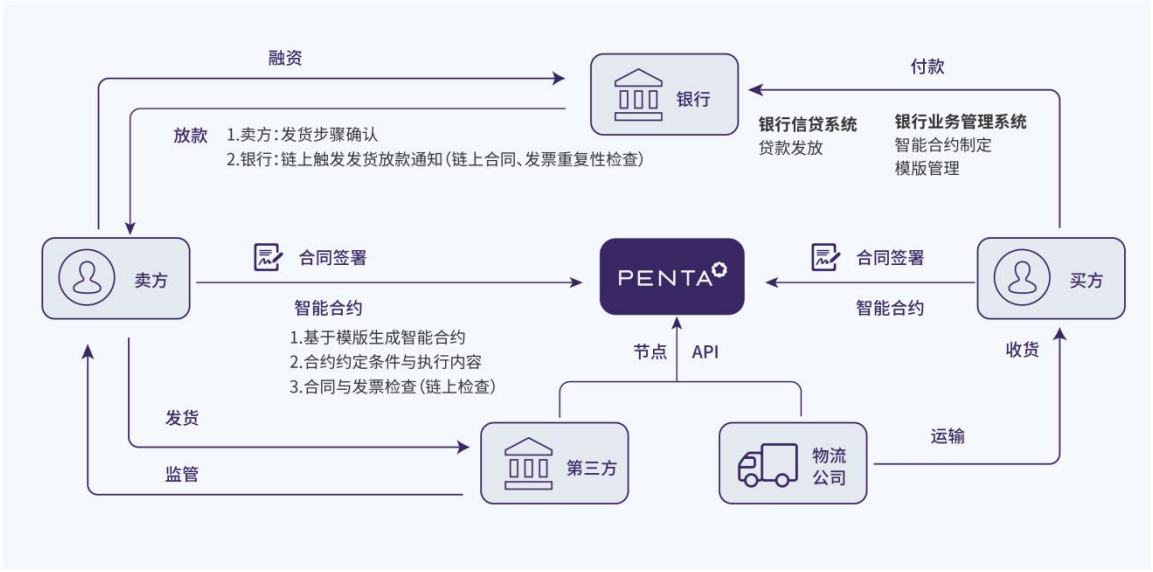


图 4.2.2-2 订单融资场景

此场景参与方包括买卖双方，双方合作银行，物流公司，第三方监管机构等，具体流程如下：

1)订单融资场景合同签订环节将条款记录至智能合约；

2)金融机构根据合同签订，发货情况进行不同程度的授信，贷款；

3)买方可以根据订单情况进行融资，到期后智能合约自动执行进行付款；

4)过程中，物流公司、监管公司将其业务处理状态更新至链上。

4.2.3.资产证券化

资产证券化过程繁琐，参与方较多，且需要设置专门的 SPV（专项资管计划）进行主体风险隔离。如下是典型资产证券化的交易结构：

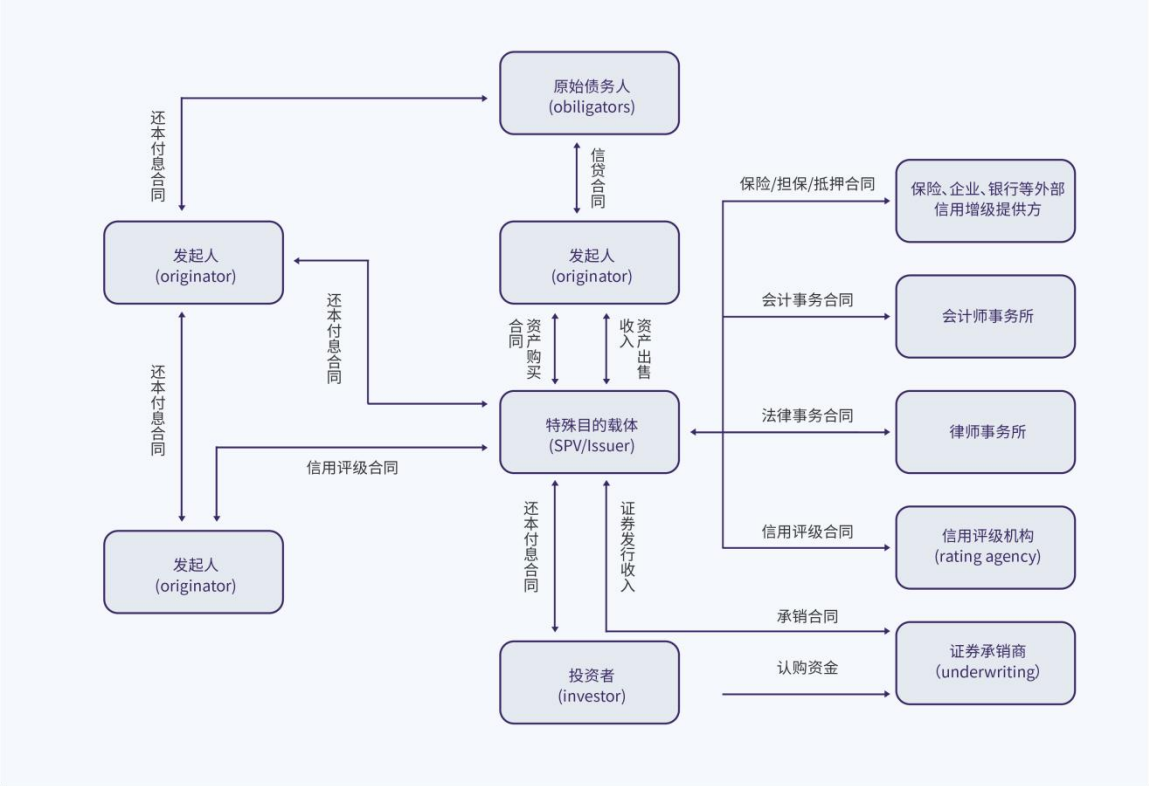


图 4.2.3-1 基本交易结构

覆盖特殊目的载体、发起人、原始债务人、投资者、托管人、服务商、会计事务所、律师事务所、信用评级机构、证券承销商等，相互之间信息互通成本较高，信息核验耗时较长。通过区块链连接 B 端所有机构，C 端投资者，保证资产包数据可信、各个参与主体资产分配可查、三方机构评级结果透明。上链数据可信，可有效降低各机构间的沟通与核验成本，信息透明更有利于投资者利用准确信息进行风险投资，做出适当决策。

为此梵塔网络曾构建基于区块链的智能资产证券化平台，使用区块链进行底层资产承载，并将每轮的资产评估、审计、交易信息记录在区块链上，资产穿透更有利于资产证券化业务良性发展，也可简化监管成本。

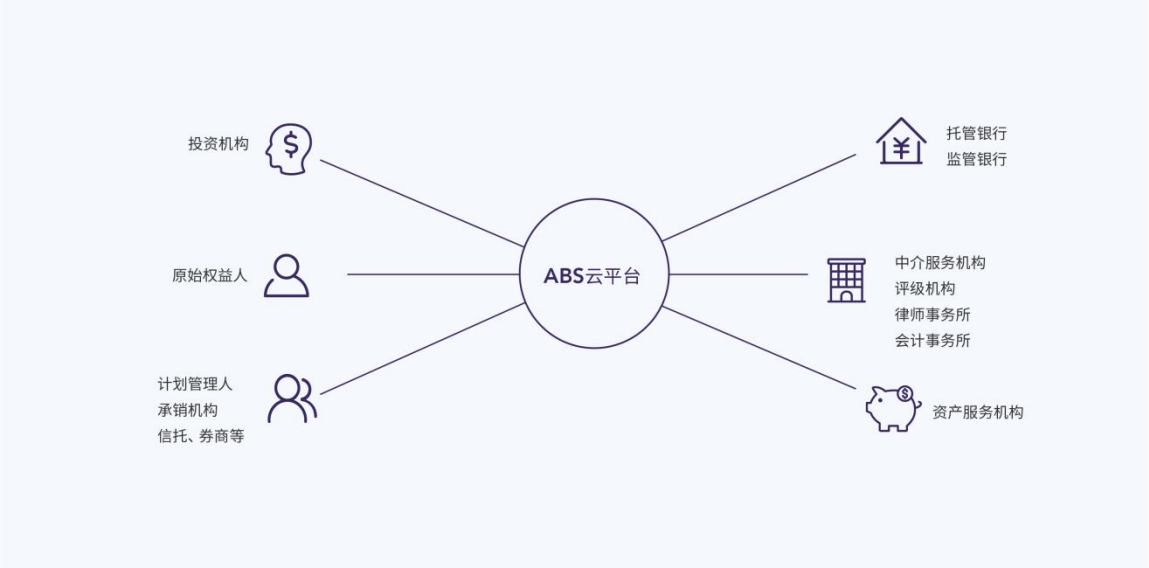


图 4.2.3-2 资产证券化智能云平台

已构建基于区块链的智能资产证券化平台，支持资产证券化参与的各方进行资产的管理与操作，各家机构可构建自己的数据记账节点，提升数据可信性。

5.术语解释

1)比特币：比特币是一种加密数字货币，在 2009 年由化名的开发者中本聪（Satoshi Nakamoto）以开源软件形式推出。

2)以太坊：英文名 Ethereum，是一个有智能合约功能的公共区块链平台。

3)超级账本：英文名 Hyperledger，是 IBM 发起的专注于联盟链的开源社区。

4)以太坊虚拟机：以太坊虚拟机设计运行在点对点网络中所有参与者节点上的一个虚拟机，它可以读写一个区块链中可执行的代码和数据，校验数据签名，并且能够以半图灵完备的方式来运行代码。它仅在接收到经数据签名校验的消息时才执行代码，并且区块链上存储的信息会区分所做的适当行为。

5)图灵完备语言：一个能计算出每个图灵可计算函数（Turing-computable function）的计算系统被称为图灵完备的。一个语言是图灵完备的，意味着该语言的计算能力与一个通用图灵机（Universal Turing Machine）相当，这也是现代计算机语言所能拥有的最高能力。

6)智能合约：智能合约是由时间驱动的、具有状态的、运行在一个复制的、分享的账本之上的、且能够保管账本上资产的程序。

7)代币：除了比特币以外的数字货币。

8)公有链：公有链是任何人在任何地方都能发送交易且交易能获得有效确认的、任何人都能参与其中共识过程的区块链。

9)联盟链：与公有链相比在开放程度和去中心化程度上有所限制，参与者均早已达成共识并互相信任。

10)POW：（Proof of Work，工作证明），就是说，你获得多少货币，取决于你挖矿贡献的有效工作，大部分的虚拟货币，比如比特币、莱特币等等，都是基于 POW 模式的虚拟货币（算力越高、挖矿时间越长，你获得的货币就越多）。

11)POS：（Proof of Stake，股权证明），就是一个根据你持有货币的量和时间，给你发利息的一个制度，在股权证明 POS 模式下，有一个名词叫币龄，每个币每天产生 1 币龄，比如你持有 100 个币，总共持有了 30 天，那么，此时你的币龄就为 3000，这个时候，如果你发现了一个 POS 区块，你的币龄就会被清空为 0。

12)PBFT：Practical Byzantine Fault Tolerance 的缩写，意为实用拜占庭容错算法。该算法是 Miguel Castro（卡斯特罗）和 Barbara Liskov（利斯科夫）在 1999 年提出来的，解决了原始拜占庭容错算法效率不高的问题，将算法复杂度由指数级降低到多项式级，使得拜占庭容错算法在实际系统应用中变得可行。

13)QOS：（Quality of Service，服务质量）指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力，是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。

14)RSA：Rivest、Shamir、Adleman 于 1978 年首次发表的国际通用的公钥密码算法，公钥密码系统与只使用一个密钥的对称传统密码不同，算法是基于数学函数而不是基于替换和置换。公钥密码学是非对称的，它使用两个独立的密钥，即密钥分为公钥和私钥，因此称双密钥体制。双钥体制的公钥可以公开，因此称为公钥算法。

15)国密算法：国家密码局认定的国产密码算法。主要有 SM1，SM2，SM3，SM4。密钥长度和分组长度均为 128 位。SM1：对称加密。其加密强度与 AES 相当。该算法不公开，调用该算法时，需要通过加密芯片的接口进行调用；SM2:非对称加密，基于 ECC。该算法已公开。由于该算法基于 ECC，故其签名速度与秘钥生成速度都快于 RSA。ECC 256 位（SM2 采用的就是 ECC 256 位的一种）安全强度比 RSA 2048 位高，但运算速度快于 RSA；SM3:消息摘要。可以用 MD5 作为对比理解。该算法已公开。校验结果为 256 位；SM4:无线局域网标准的分组数据算法。对称加密，密钥长度和分组长度均为 128 位。

16)负载均衡：英文名 Load Balance，建立在现有网络结构之上，它提供了一种廉

价有效透明的方法扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性。

17)P2P：对等网络，即对等计算机网络，是一种在对等者（Peer）之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。“Peer”在英语里有“对等者、伙伴、对端”的意义。因此，从字面上，P2P 可以理解为对等计算或对等网络。

6.参考文献

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song. Remote data checking using provable data possession. ACM Trans. Info. & System Security, 14(1), May 2011.

[2] M. T. Goodrich, M. Mitzenmacher, O. Ohrimenko, and R. Tamassia. Privacy-preserving group data access via stateless oblivious RAM simulation. In SODA, 2012.

[3] H. Shacham and B. Waters. Compact proofs of retrievability. Proc. Asiacrypt 2008.

[4] C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, and S. Yekhanin. Erasure coding in Windows Azure storage. In G. Heiser and W. Hsieh, editors, Proceedings of USENIX ATC 2012. USENIX, June 2012.

[5] L. Rizzo. Effective erasure codes for reliable computer communication protocols. ACM SIGCOMM Computer Communication Rev., 27(2):24–36, Apr. 1997.

[6] M. Liskov, R. Rivest, and D. Wagner. Tweakable block ciphers. J. Cryptology, 24(3):588–613, July 2011.

[7] V. Buterin. Ethereum, Apr. 2014.

[8] V. T. Hoang, B. Morris, and P. Rogaway. An enciphering scheme based on a card shuffle. In R. Safavi-Naini, editor, Proceedings of Crypto 2012, LNCS. Springer-Verlag, Aug. 2012. To appear.

[9] Nakamoto, S. 31 October 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System". Also known as the Bitcoin whitepaper.

[10] Kyle Randolph. "A Next-Generation Smart Contract and Decentralized Application Platform". Also known as the Ethereum whitepaper.

[11] Christopher Ferris. "Hyperledger fabric Protocol Specification".

[12] Miguel Castro, Barbara Liskov. "Practical Byzantine fault tolerance and proactive recovery".

[13] Hal, F. "Reusable proofs of work" http://www.finney.org/~hal/rpow/.

[14] Tushar Deepak Chandra, Vassos Hadzilacos, Sam Toueg. "The Weakest Failure Detector for Solving Consensus".

[15] Manos Kapritsos, Yang Wang, Vivien Quéma, Allen Clement, Lorenzo Alvisi, Mike Dahlin: All about Eve."Execute-Verify Replication for Multi-Core Servers"

[16] ZMWorm[CCG]. ECC 加密算法入门介绍

[17] Michael Rosing. Chapter5《Implementing Elliptic Curve Cryptography》，Softbound，1998