WeBank 微众银行 | WeCross

WeCross 技术白皮书

区块链跨链协作平台

2020 年 2 月

微众银行区块链团队编著

前言

区块链作为构建未来价值互联网的重要基础设施，深度融合分布式存储、点对点通信、分布式架构、共识机制、密码学等前沿技术，正在成为技术创新的前沿阵地。全球主要国家都在加快布局区块链技术，用以推动技术革新和产业变革。经过行业参与者十年砥砺前行，目前区块链在底层技术方案上已趋于完整和成熟，国内外均出现可用于生产环境的区块链解决方案。其所面向的创新应用场景覆盖广泛，已在对账与清结算、跨境支付、供应链金融、司法仲裁、政务服务、物联网、智慧城市等众多领域落地企业级应用。

在广泛的场景应用背后，来自于性能、安全、成本、扩展等方面的技术挑战也愈发严峻。目前不同区块链应用之间互操作性不足，无法有效进行可信数据流通和价值交换，各个区块链俨然成为一座座信任孤岛，很大程度阻碍了区块链应用生态的融合发展。未来，区块链想要跨越到真正的价值互联网，承担传递信任的使命，开启万链互联时代，需要一种通用、高效、安全的区块链跨链协作机制，实现跨场景、跨地域不同区块链应用之间的互联互通，以服务数量更多、地域更广的公众群体。

作为一家具有互联网基因的高科技、创新型银行，微众银行自成立之初即高度重视新兴技术的研究和探索，在区块链领域积极开展技术积累和应用实践，不断致力于运用区块链技术提升多机构间的协作效率和降低协作成本，支持国家推进关键技术安全可控战略和推动社会普惠金融发展。微众银行区块链团队基于一揽子自主研发并开源的区块链技术方案，针对不同服务形态、不同区块链平台之间无法进行可信连接与交互的行业痛点，研发区块链跨链协作平台——WeCross，以促进跨行业、机构和地域的跨区块链信任传递和商业合作。

WeCross 着眼应对区块链行业现存挑战，不局限于满足同构区块链平行扩展后的可信数据交换需求，还进一步探索异构区块链之间因底层架构、数据结构、接口协议、安全机制等多维异构性导致无法互联互通问题的有效解决方案。作为未来区块链互联的基础设施，WeCross 秉承多方参与、共享资源、智能协同和价值整合的理念，面向公众完全开源，欢迎广大企业及技术爱好者踊跃参与项目共建。

风起于青萍之末，一场围绕区块链技术的变革正在徐徐拉开帷幕。与一个具备无限潜力的趋势共同成长，现在，正是最好的时节。

微众银行区块链团队

目录

目录

第一章 WeCross 设计背景与理念

1.1 设计背景：行业现状与挑战

近年来，区块链行业经历了高速发展，诞生许多形态各异的底层技术平台， 基于这些平台建设的区块链应用百花齐放。随着应用生态本身的发展壮大，越来越多应用在既有用户和价值积累基础上，为追求更大的网络效应，产生了与其他应用实现交互、建立关联的外延需求，于是整个区块链生态需要一个更加开放、易于协作、多方共赢的交互环境。由于目前区块链平台技术实现上存在多维异构性，在应用和数据上存在“孤岛效应”，无论是基于不同平台或者同一个平台构建的不同应用，都难以便捷地跨平台联通协作，区块链生态要向下一阶段演化需要“超越平台、链接应用”的创新性解决方案。

为了应对这一挑战，旨在搭建链与链之间可信交互渠道的跨链技术逐渐成为业界关注的焦点，业界普遍认同高效通用的跨链技术是实现万链互联的关键。跨链技术能够连通分散的区块链生态孤岛，成为区块链整体向外拓展的桥梁纽带。当前，业界在跨链领域已有初步的探索和积累，讨论较多的跨链方案有公证人机制、中继、侧链、哈希锁定和分布式密钥控制等。较早出现的 BTC-Relay 使用侧链技术来实现区块链数字资产之间的单向跨链。Ripple 提出的跨链价值传输协议 ILP 采用哈希锁定的方案来解决跨账本之间的支付问题。Cosmos 和 Polkadot，则关注如何建立通用跨链开发框架，分别提出了 Tendermint 和 Substrate 的开发框架，它们的跨链核心设计是基于中继链的思想。

上述跨链方案，仅适用于面向数字资产的跨链转移场景，难以扩展涵盖到更为广阔的应用场景。微众银行在 2018 年提出“公众联盟链”的概念，将联盟链进一步升华为面向公众提供服务的联盟链，公众作为“链”的服务对象，可通过公开网络访问联盟链提供的服务，联盟是“链”的属主和运营方，通过“链”实现信息与价值交换。公众联盟链并非单一区块链生态，而是一种全新的区块链商业应用跨域融合形态。要支撑这样的融合形态，需要能够支持多链并行、跨链通信以及处理来自互联网海量交易的能力。在公众联盟链的大生态中，必然需要应对底层平台异构化、应用场景多样化等特点，构建公众联盟链的可信跨链交互面临着更大的挑战。

底层架构不同，互通难：业内已有多种区块链平台，这些平台在整体架构设计上存在很大的不同，包括计算、存储、网络等各个方面。例如，Hyperledger Fabric 采用 Endorser-Orderer-Comitter 三层架构，交易先经过 Endorser 节点进行预执行背书，得到状态读写集 RW-Set 返回客户端，客户端再次打包交易发送至 Orderer，Orderer 打包排序后交给 Commiter 节点进行落盘存储。同为金融级、企业级的区块链平台 FISCO BCOS，交易在客户端完成签名之后被发送到区块链节点，节点将交易打包成区块，并且交给 EVM 执行，状态数据以 MPT 树状组织存储。不难看出，这两个底层平台在架构上存在巨大差别，不仅交易处理时序不同，计算与存储结构也不同，想让交易直接在两个平台互通，存在较大挑战。

数据结构不同，互认难：不同区块链平台的数据结构设计往往各不相同。例如，FISCO BCOS 的区块结构中，区块头包含三个默克尔根字段：世界状态根 state-root、交易根 tx-root、交易回执根 receipt-root，这些字段可用于交易和执行结果的存在性证明。而Hyperledger Fabric，以其最新发布的稳定版本（v1.4）为例，使用一个 DataHash 字段来标记该块的数据变化，其区块头设计中并没有默克尔根的相关字段，不容易实现类似交易存在性证明机制。基于默克尔树的存在性验证是常用的跨链认证手段，但由于不同区块链平台数据结构和预期的应用场景不同，并非所有平台都支持，所以想要实现数据互认依旧存在着一定挑战。

接口协议不同，互联难：常见的网络传输编码协议有 Protobuf、JSON 和二进制等协议。这些编码协议各有其优势与适用场景。例如，Protobuf 协议具备支持语言多、格式紧凑、易于扩展的优势，被 Hyperledger Fabric 选用为 P2P 网络传输消息包的编码协议。而二进制编码协议有编码速度快、格式紧凑和可自由定制的优势，被 FISCO BCOS 选用为 P2P 网络传输消息包的编码协议。除此之外，因为架构与数据结构的不同，不同平台暴露的访问接口在功能和格式字段方面也大不相同。综上所述，由于接口与协议的不兼容，这些平台间难以互联通信。

安全机制不同，互信难：区块链安全涉及面很广，包括共识记账模式的安全、数据传输安全、数据存储安全、准入机制安全以及接口访问权限安全控制等多方面。由于区块链设计的安全边界往往是以平台范围为界，以确保用这个平台建设的一个区块链实例内部是安全的。当涉及到链和链之间、平台和平台之间进行衔接时，会因为多种安全机制参差不齐，且敏感数据跨越安全边界，如共识者列表不同、准入机制严格程度有高低、权限配置差异等因素，导致平台之间的互信条件不成立。

业务模式不同，互访难：区块链技术已经在众多应用领域初露头角，以 FISCO BCOS 披露的落地场景为例，已经覆盖政务、金融、溯源、文化、游戏等众多行业。不同业务场景的合约逻辑千差万别，各个场景都是内在闭环的系统。要打通场景之间的互访，例如要实现金融场景区块链与政务场景区块链有关备案信息的互通跨链，会面临比传统数字资产跨链更复杂的业务逻辑，过程中任意一个环节的疏漏都可能导致异常使跨链失败，如何保障整体衔接过程中事务和事务之间的完整性和一致性将会是巨大的挑战。

除了上述由于不同平台架构差异而导致的挑战，基于相同区块链平台的多个区块链之间也存在着显著的跨链挑战。受限于区块链本身的架构特征，单链架构难以同时满足高安全、高性能和高扩展三个需求，无法应对需要承载海量数据的服务场景。尽管可以借鉴传统互联网海量服务的经验，采取多通道、多群组或多链架构等方式进行平行扩展，但有别于传统互联网服务，区块链应用作为多方参与的弱信任业务模式，多方之间既有协作也有博弈。即便对于构建在同一个平台上的区块链应用，也需要构建一个多方可信的渠道对平行扩展之后的通道、群组和多链进行可信数据互联。

因此，同 / 异构区块链平台都需要依赖于跨链解决方案来连接信任孤岛，实现信任在更大范围内的传递，推动区块链应用生态的深度融合发展。

1.2 设计理念：4S 原则

面对区块链应用生态中互联互通的诸多挑战，我们从底层平台的架构设计开始深层次思考，在众多主流平台中探寻可信融合连通所需的“最小化”抽象设计，充分考虑跨链交互的安全、扩展和可用性问题，提出跨链方案需遵循的 4S 原则。

Synergetic：跨链业务高效协同

跨链的目标是打通区块链业务之间的高墙，连接众多信任孤岛，让信任得到更大范围的传递。为了使这些基于众多区块链平台的业务能够无缝协同，首先需要设计普适通用的数据结构和交互协议，使不同区块链平台之间数据格式转化和网络协议适配所产生的代价降到最低。

WeCross 遵循满足跨链业务高效协同的设计理念，根据“一次适配，随处可用”原则，提炼跨链交互必需的“核心接口子集”，设计通用数据结构和网络协议，解决因设计目标不同而导致的各平台接口差异性难题。

Secure：跨链操作安全可信

区块链的重要特征之一是通过多中心化、共识机制以及密码学技术来实现数据可信存取。但这种安全机制往往只能在一个区块链平台内部形成闭环，在两个或者多个区块链平台之间进行交互访问时，需要进一步突破原有平台的安全边界，建立更强的安全保障机制。

WeCross 遵循保障跨链操作安全可信的设计理念，引入 CA 身份认证机制，对通信链路进行加密加固，严格限制访问权限，设计多维度的默克尔证明机制，以及多种原子事务机制，保障跨链交互全流程数据的可信性。

Scalable：跨链网络分层可扩展

跨链不仅能够支持异构区块链之间互联，也能够帮助同构区块链平台进行扩展。常见的多通道、多群组和多链等扩展方案都需要依赖跨链组件打通通道、群组以及链与链之间的交互。随着跨链业务协作的演进，越来越多的业务有相互连接的需求，一对一的跨链将演变成一对多、多对多、甚至更为复杂的拓扑结构。这就要求跨链组件本身具备足够的灵活性，能够应对多种复杂的网络模型和业务需求。

WeCross 遵循支持跨链网络分层扩展的设计理念，设计跨链路由协议与模块，支持多个区块链分布式互联，承载树型、星型等各种拓扑架构，支持多层次纵深跨链协作。同时，设计多方共建、共治的治理架构，实现跨链网络的可持续扩展。

Swift：跨链接入高效便捷

由于区块链平台存在多样化特性，开发者每接入一个新的区块链平台就需要学习一套区块链开发运维流程，跨越不同区块链平台的接入将导致学习成本的增加。

WeCross 遵循为开发者提供高效便捷接入方式的理念，设计通用 SDK、交互式控制台以及可视化浏览器等全套开发组件，简化跨链交互流程，设计“所见即所得”的运维工具，支持一键发起跨链操作。

综上，4S 设计理念以业务协同为核心，在多个关键维度上追求跨链操作的高安全性、高扩展性和高易用性，以应对未来形式多样、层出不穷的跨链应用场景。

第二章 WeCross 整体架构设计

以融合连通各大主流区块链平台（例如 FISCO BCOS 和 Hyperledger Fabric）为目标定位，基于对当前行业现状、应用场景和区块链技术发展的全面分析，WeCross 对主流区块链平台体系进行标准化抽象提炼，并以此设计跨链整体架构。

2.1 区块链体系抽象

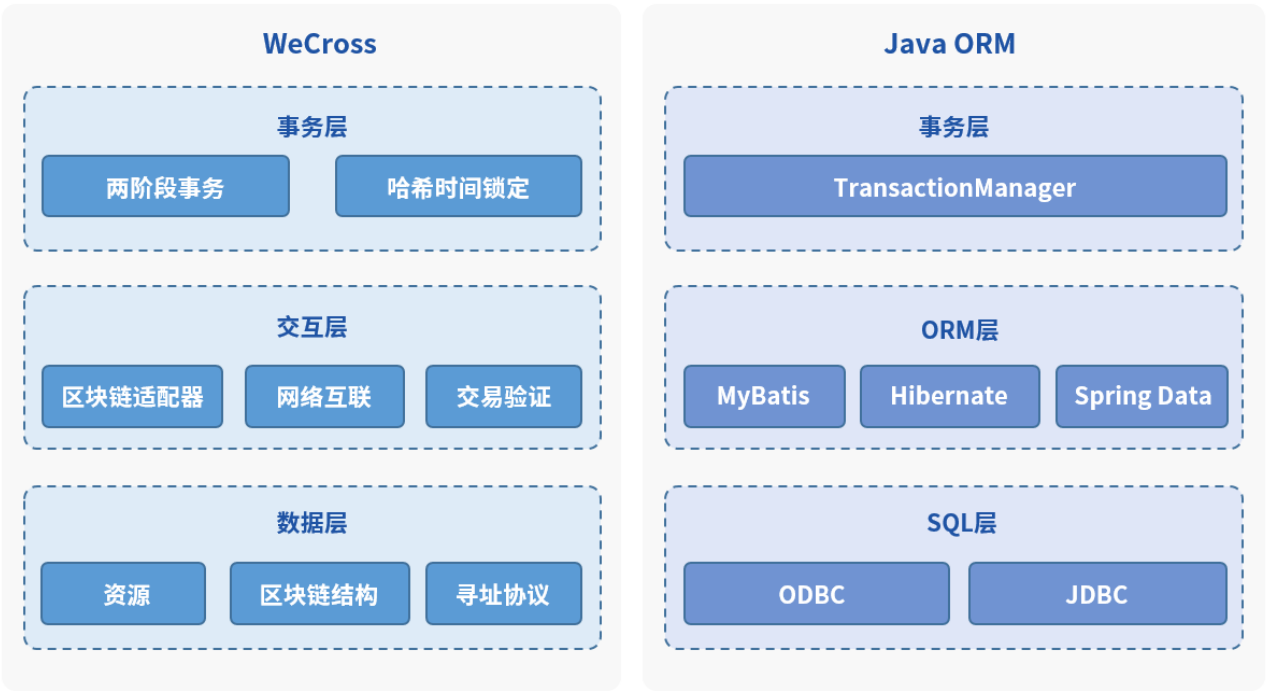
为打通异构区块链之间的交互，首先为这些异构区块链设计统一的“语言”，即统一的体系结构抽象。基于统一的体系结构，异构区块链之间找到双方都能理解的“语言”，互联互通才有可能实现。基于跨链所需的关键要求，WeCross 在核心数据结构、区块链交互模式和事务管理上提取业界主流区块链产品核心且必需的公共子集，对区块链平台进行多层抽象。

数据层：跨链交互的核心是数据在链间的流动，数据层的抽象就尤为重要。跨链涉及的数据维度包括区块、交易、合约、消息等多个方面。WeCross 以满足跨链基本要求为前提，提炼通用区块数据结构，将交易、合约和消息等抽象设计成资源类型，为资源设计通用的寻址协议。

交互层：不同业务场景有不同的跨链交互模型，基于抽象数据层，WeCross 建设通用区块链适配与路由中继网络，结合标准默克尔证明机制，实现跨链交互层抽象设计。

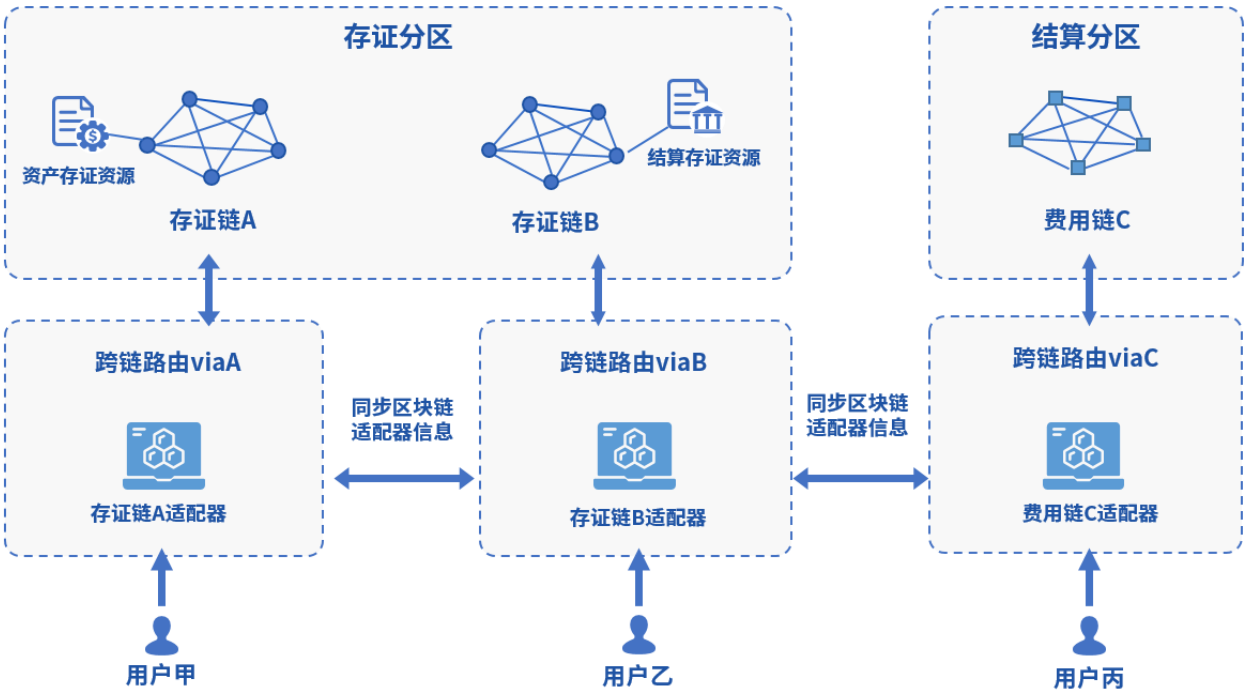
事务层：基于数据结构和交互的抽象层，实现跨链事务效果。目前支持两类机制：两阶段事务和哈希时间锁定事务。未来将依据场景需求设计更多事务机制。

WeCross 抽象体系结构中的任一层都是通用可替换的，无论底层技术实现如何替换，上层的逻辑都可以通用。WeCross 对区块链的多层次抽象可以类比 Java ORM（Object Relational Mapping）对数据库的多层次抽象。ORM 技术作为 Java 访问数据库的通用“语言”，可以将数据库层完全隐蔽，呈现给开发的只有 Java 对象。开发者只需要根据业务逻辑的需要调用 Java 对象的方法，即可实现对后台数据库的操作，无需关注后台采用什么数据库。相应地，WeCross 数据结构抽象可以对应 Java 中对 SQL 和数据库驱动的抽象如 ODBC 和 JDBC，WeCross 交互抽象类似于 Java 对数据库访问模型的 ORM 抽象如 MyBatis 和 Hibernate，而 WeCross 事务管理则与 Java 的事务管理类似，但支持更多事务模式。



2.2 跨链系统架构

WeCross 的跨链系统架构设计充分考虑跨行业、机构和地域的多区块链互联，无论是新部署的区块链平台还是已有的区块链平台，都可以基于上一节中的区块链体系抽象，在不改动原有区块链平台底层的前提下，无缝接入 WeCross 平台。



WeCross 系统架构包括以下组件：

跨链分区（Zone）指运行着同一类业务的区块链集合。WeCross 可以对这个区块链集合本身和内部的区块链资源进行命名和寻址。例如，图中存证业务的命名空间为“存证分区”，结算业务的命名空间为“结算分区”。存证分区里有两条存证链分别是存证链 A 和存证链 B，存证链 A 链上部署一个资产存证资源，产生的费用和相关的资产可能需要存证。于是，根据业务需要，跨链操作会产生分区和分区之间，以及分区内部的链和链之间。

跨链路由（Router）指用于桥接业务系统与区块链的服务进程。多个跨链路由之间可以相互连接，相互转发请求。用户通过向跨链路由发起请求来访问跨链分区中的资源。

跨链适配器（Stub）指连接一个区块链的接口实现，可由跨链路由加载。跨链路由可以配置多个区块链适配器，达到连接多条区块链的效果。跨链路由间会自动同步区块链适配器的配置信息，从而帮助用户寻址位于其他区块链上的资源。

跨链资源（Resource）指区块链上的智能合约、数字资产等用户可访问的数据对象。类似于区块链适配器的配置信息，跨链资源的元信息也在跨链路由之间同步。用户通过统一的接口对跨链分区中的资源进行寻址和调用。

为了满足未来多样化的业务互联需求，针对海量数据跨链的典型业务特征，WeCross 为网络交互和部署架构设定了以下关键设计目标。

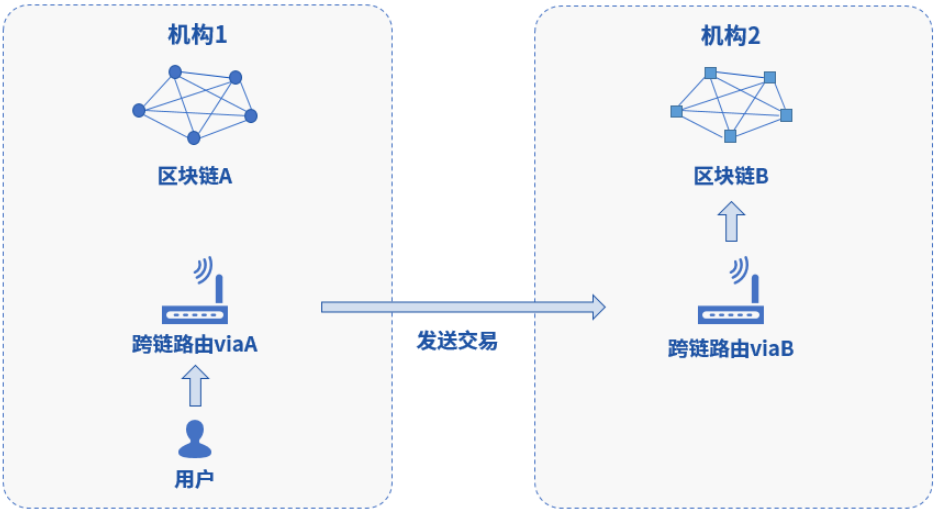
跨地域互联：作为多方参与的区块链应用，通常涉及多个服务机构，业务部署在多个跨地域的数据中心。WeCross 为跨地域场景设计安全、可靠和高效的网络架构，基于 TCP 长连接、心跳、自动重连和加密通信技术的网络机制来保证大范围跨地域互联的稳定性、及时性和安全性。

部署架构灵活：由于跨链需求通常源自成熟的区块链应用项目，跨链部署架构需要具备兼容现存区块链实例的能力。WeCross 采用 “非侵入式” 设计，跨链路由以独立进程的方式与区块链节点分离部署，无需变更既有的区块链网络架构，即可实现灵活的架构部署。跨链路由间使用网络传输跨链消息和区块链消息，结合网络自动寻路功能，只要跨链路由间有直接或间接可触达的网络链路，就能完成跨链交互。

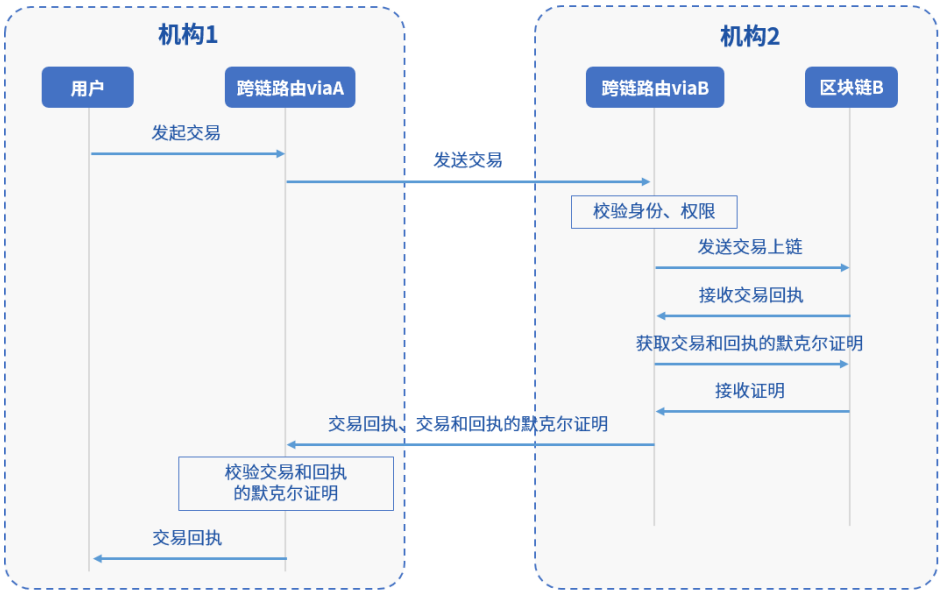
可自由定制：现实业务场景中的跨链需求千差万别，接入的区块链平台多种多样，因此定制化可裁剪的跨链能力不可或缺。WeCross 的区块链适配器和跨链资源支持自由定制，根据接入的区块链类型、系统资源和网络情况，选择不同的区块链适配器和跨链资源。

2.3 可信交互流程

区块链平台设计的基本安全假设是“每个参与者皆有可能作恶”，在此假设下通过密码学与共识算法等机制构建分布式可信环境。然而此可信环境往往只在区块链平台内部生效，无法简单被另一个区块链平台信任，需要引入额外的可信证明信息来实现跨区块链平台的可信交互。WeCross 在处理跨链交互时除了传输区块链交易信息外，还会额外传输区块链交易的相关证明数据，并使用这些信息进行交易和回执（交易执行结果）的存在性证明，以证明链上信息的真实与可靠。



以上图所示的跨链交互为例，机构 1 和机构 2 分别部署了区块链 A 和区块链 B，现在机构 1 的用户要访问机构 2 的区块链 B，并要求访问的结果真实可信，其跨链交互时序如下图所示。



与传统的区块链交易处理流程相比，WeCross 跨链路由除了传输交易和回执的信息，还额外传输交易和回执的默克尔证明，交易的发送方使用这些证明来进行跨链数据访问的可信验证，使交易的发送方能确认交易在目标区块链上真实发生且获得结果，保证交易和回执的真实可信。

WeCross 遵循跨链交互数据皆可自证的原则，要求交互响应消息同时携带数据和证明，该规则普遍适用于各类跨链场景，可用于保障整个交易流程的真实可信。

第三章 WeCross 核心技术与优势

为了实现跨链交互的高效可用、安全可信和便捷治理，WeCross 基于区块链体系的抽象、跨链系统的架构和可信交互流程的顶层设计，提炼四个技术点，以实现跨链的核心功能：

- **通用区块链接口（UBI，Universal Blockchain Interface）：** WeCross 设计一套通用的区块链数据协议，抽象提炼主流区块链共通的核心数据结构与资源定义，使多种区块链平台可以用统一的数据协议交互，极大程度减小区块链平台之间的交互难度。
- **异构链互联协议（HIP，Heterogeneous Interchain Protocol）：** WeCross 设计主流区块链平台通用的网络交互协议及统一的交互模式，通过简便适配，即可实现异构区块链平台的连通。
- **可信事务机制（TTM，Trust Transaction Management）：** WeCross 采用密码学技术和分布式算法，保证区块链平台之间交互数据的真实可信且难以篡改，保证业务逻辑的原子事务性，使得区块链平台之间任何关联的两个交易能够完全执行或完全回滚。
- **多边跨域治理（MIG，Multilateral Inter-Domain Governance）：** WeCross 设计一套可扩展、去中心的跨链治理架构，让多个区块链业务能够根据其特定需求共同搭建一条治理链进行跨链交互方面的治理。治理链承载了权限控制、事务管理、准入机制和监管介入等治理功能。

结合设计理念，用户体验以及平台特性等方面的综合考量，WeCross 具备以下三个主要优势：

- **开源开放：** WeCross 秉承开源、开放的原则，与社区共同维护平台的迭代升级，群策群力，共建更强大、更好用的跨链平台。
- **开发友好：** WeCross 提供多语言版本的 SDK 供开发者使用，提供可视化的管理工具，方便用户开发、调试以及运维。
- **安全可信：** WeCross 基于加密、准入、隔离以及追溯等多种机制保障跨链数据的机密性以及系统的安全性。

3.1 通用区块链接口

各家区块链平台有着各自的 SDK、智能合约框架和交互逻辑，开发者不得不针对性地学习每一种区块链平台的 API 和调用逻辑，做定制化开发。当两个异构平台存在跨链需求时，双边业务需要重新学习对方平台的 API 和调用逻辑，这不仅是对开发者精力和成本的巨大浪费，也是跨链落地难的一个重要原因。

区块链平台虽各有不同，但万变不离其宗，主流区块链的底层原理都有其共通之处。经过抽象后，大部分区块链平台的区块链逻辑、区块数据结构和交易数据结构等都具有较高的相似性。

以 FISCO BCOS 和 Hyperledger Fabric 的交易数据结构为例，两者有各自的 SDK、合约框架等接口规范。尽管它们之间有一定的差异性，但对于关键数据结构和合约调用接口，两者之间有很多共同点。

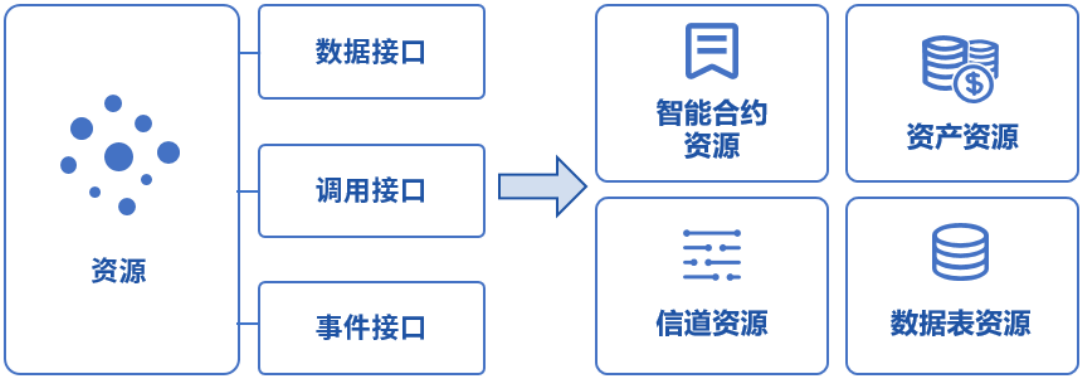
	相同字段	差异字段
FISCO BCOS交易	智能合约地址 智能合约方法名 智能合约参数 发送者签名	交易ID字段 交易防重字段
Hyperledger Fabric交易		

FISCO BCOS 和 Hyperledger Fabric 虽然使用不同的智能合约引擎，但智能合约的调用方式是类似的，都是通过给出智能合约的地址、智能合约的方法名和调用智能合约的参数，获得智能合约方法返回的数据。不仅是 FISCO BCOS 和 Hyperledger Fabric，其它主流区块链平台的智能合约调用也基本如此。

本着“求同存异”、“聚焦最大公约数”的基本思路，通用区块链接口（UBI）对交易、智能合约与资产等数据进行抽象包装，设计统一的资源范式，对主流区块链的关键数据结构进行提炼，设计普适跨链场景的抽象区块数据结构，为异构区块链的交互建立数据协议一致的基础，实现“一次适配，随处可用”的效果。

3.1.1 统一资源范式

各家区块链平台上的资源多种多样，有智能合约、资产、信道和数据表等，无论这些资源的功能如何多样，其核心接口主要可以归纳为数据、调用和事件三类固定的接口。为了更好地打通区块链平台资源交互，UBI 提出统一资源接口范式，使得用户在调用区块链智能合约、资产、信道或数据表时无需关心具体的智能合约语言和区块链的底层架构，只需传入通用的参数，并处理统一定义的返回值即可。



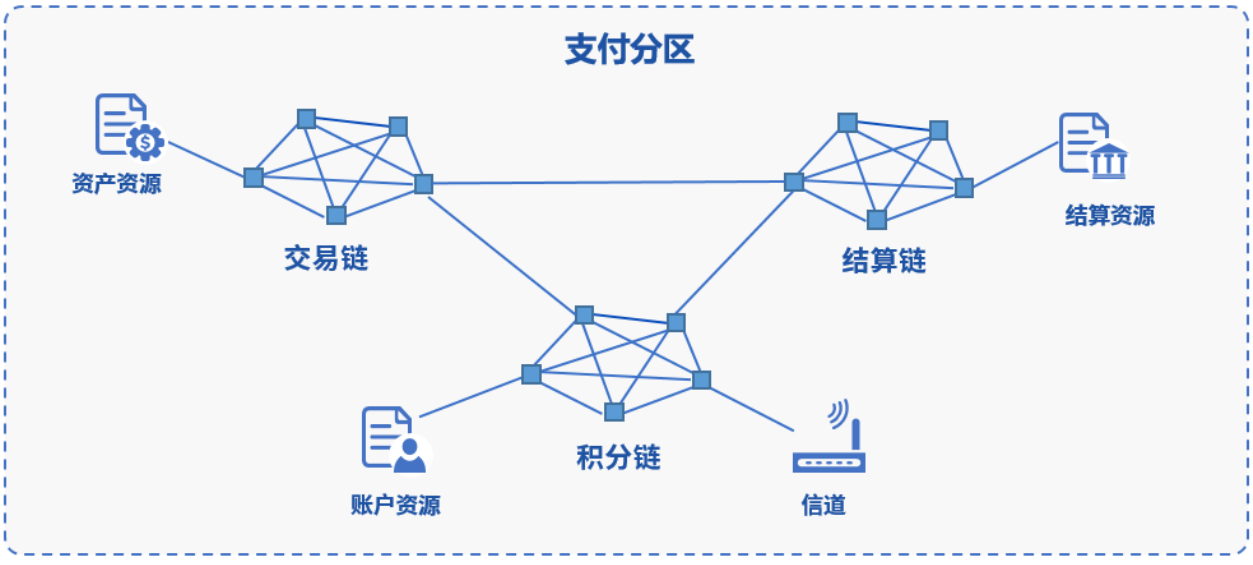
统一资源范式包括数据、调用和事件三类接口，如下表所示。

接口分类	接口功能	参数	返回值	说明
数据接口	获取数据	字段名	value:字段值	以键值方式获取资源的数据
	设置数据	字段名 字段值	无	以键值方式获取资源的数据
调用接口	调用智能合约接口	智能合约接口参数	智能合约返回值	只读地调用资源的方法，不改变链的状态
	向智能合约发送交易	智能合约接口参数	智能合约返回值	发送交易调用资源的方法，改变链的状态，需要出块
事件接口	注册事件回调	事件回调	无	注册资源事件回调，接收资源的事件通知

统一资源接口的定义如下（伪代码）：

```
public interface Resource {
  // 获取数据
  public String getData(String key);
  // 设置数据
  public void setData(String key, String value);
  // 调用智能合约接口
  public Receipt call(Transaction transaction);
  // 向智能合约发送交易
  public Receipt sendTransaction(Transaction transaction);
  // 注册事件回调
  public void registerEventHandler(EventCallback callback);
}
```

单个区块链上的资源可以通过合约地址或名称来定位和访问，在跨链和多个业务互通的复杂网络模型下则需要一个更高层的资源定位协议。为了让用户在复杂跨链分区下定位和访问区块链资源时无需关心资源位于哪个地域、机构或机房，也无需关心所在区块链的具体实现，只需提供资源地址和相关参数即可实现资源定位和访问，UBI 使用统一资源寻址协议，实现自动路由转发机制，为用户智能定位所需资源。



正如 2.2 “跨链系统架构”章节所介绍的跨链系统架构，WeCross 将跨链系统定义为跨链分区、业务链和业务链上的资源的组合，以上图中的支付分区为例：

- **跨链分区（Zone）**：管辖若干具有一定关联性的业务链，关联性可能包括业务模式、地域、领域等。图中的支付分区就是一个跨链分区。
- **业务链（Chain）：**业务链运行在某个跨链分区，而且仅属于一个跨链分区。图中的交易链、积分链和结算链都是支付分区中的业务链。
- **区块链资源（Resource）：**指业务链中的智能合约和资产等对象。如图中的资产资源是交易链的资源，结算资源是结算链的资源，账户资源是积分链的资源。

跨链分区、业务链和区块链资源都有唯一的标识，通过组合三种标识，可以唯一地定位到跨链系统中的任一资源的位置，这个寻址的标识称为跨链路径（iPath，Interchain Path），跨链路径定义为：

[跨链分区].[业务链].[区块链资源]

以图中的支付分区为例：

- 访问交易链的资产资源，跨链路径为：支付分区 . 交易链 . 资产资源
- 访问结算链的结算资源，跨链路径为：支付分区 . 结算链 . 结算资源
- 访问积分链的账户资源，跨链路径为：支付分区 . 积分链 . 账户资源

WeCross 设计实现 HTTP Restful 接口访问跨链路径，支持以 HTTP URL 的形式访问跨链系统中的资源，URL 格式为：

http://IP:Port/**[跨链分区]/[业务链]/[区块链资源]**/[资源方法]

以 FISCO BCOS 的智能合约为例，智能合约通过接口读写合约的数据比如 getData 为读接口， setData 为写接口，两者的参数都可以是合约内的变量名，在合约代码内实现读写流程；对智能合约的调用称为调用接口，分为 call 和 sendTransaction 两种，call 接口仅调用

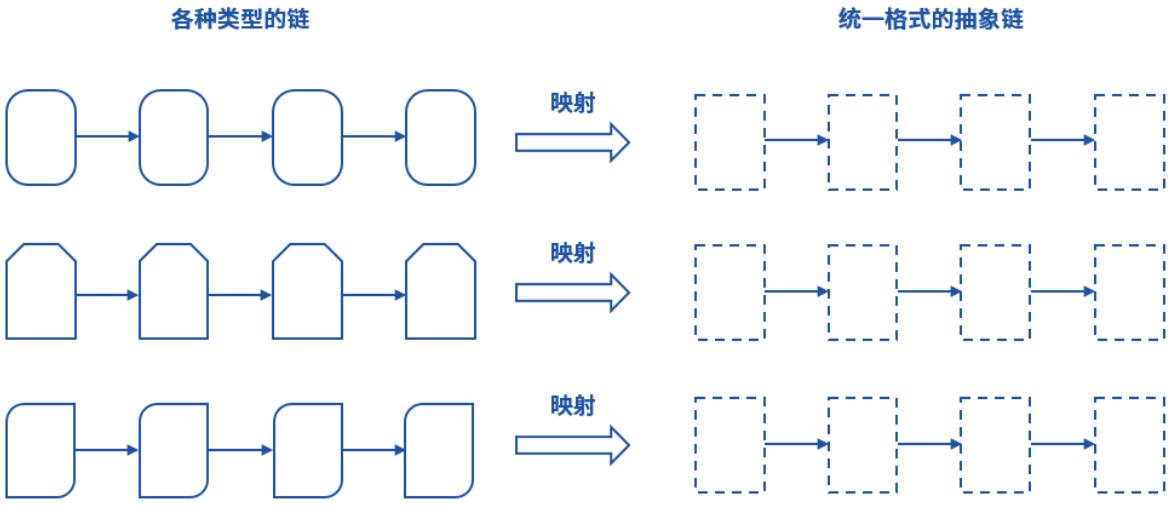
合约读接口以返回数据，不会改变链上状态，sendTransaction 会往链上发送交易并改变区块链状态；另外还有事件接口，供客户单接收智能合约的 event 事件。

以下用伪代码来描述资源的获取和调用流程：

```
// 根据配置初始化 Stub
Stub stub = context.getBean("fisco-bcos");
// 通过 iPath 获取智能合约资源
Resource myResource = stub.getResource("payment.fisco-bcos.HelloWeCross");

// 根据合约地址、方法名以及参数列表拼接调用交易
Transaction getTransaction = myResource.newTransaction();
getTransaction.setFrom("myAccount");
getTransaction.setMethod("get");
// 使用 call 方法，调用智能合约的 get 函数
Receipt myReceipt = myResource.call(getTransaction);

// 根据合约地址、方法名以及参数列表拼接调用交易
Transaction setTransaction = myResource.newTransaction();
setTransaction.setFrom("myAccount");
setTransaction.setMethod("set");
setTransaction.setArgs(new Object[]{"Hello WeCross!"});
// 使用 sendTransaction 方法，向链上发送交易，调用智能合约的 set 函数
Receipt myReceipt = myResource.sendTransaction(setTransaction);

// 解析返回值
Object[] results = myReceipt.decode();
```

3.1.2 抽象区块链结构

为了满足异构区块链之间的区块数据互信的需求，UBI 提出抽象区块的概念，由抽象区块组成的链称为“抽象链”。抽象区块里包含业界主流区块链共同的数据字段，用于验证区块链结构的正确性、查询区块链当前状态和验证区块链数据等。多个区块链之间，通过相互同步和获取抽象链的方式，来确认其它区块链的状态，验证预期交互数据的正确性。



以 FISCO BCOS 和 Hyperledger Fabric 为例，二者的区块结构中，区块高度、区块哈希、上一块哈希和状态数据哈希值字段的含义是相同的，不同的是用于验证的默克尔根字段。

	相同字段	差异字段
FISCO BCOS区块	区块高度 区块哈希 上一块哈希 状态数据哈希值	交易默克尔根 回执默克尔根 状态默克尔根
Hyperledger Fabric区块		

抽象区块的数据字段可以分为两类，一类是区块信息字段，包括区块高度、区块哈希值和上一块哈希，这些字段用于验证区块链的正确性；另一类是信息验证字段，包括交易默克尔根、回执默克尔根和状态默克尔根，分别用于验证该区块相关的交易、回执和状态数据的存在性和正确性，以证明某个交易是否属于当前区块、某个回执是否属于当前区块等。

3.2 异构链互联模型

区块链交互的核心是接口调用，尽管各家区块链平台的内部架构、网络模型和共识逻辑有很大差异，但这些区块链平台的对外接口存在共性，至少都有数据读写、调用智能合约和向智能合约发送交易等接口。以 FISCO BCOS 和 Hyperledger Fabric 为例， 其接口相似性对比如下：

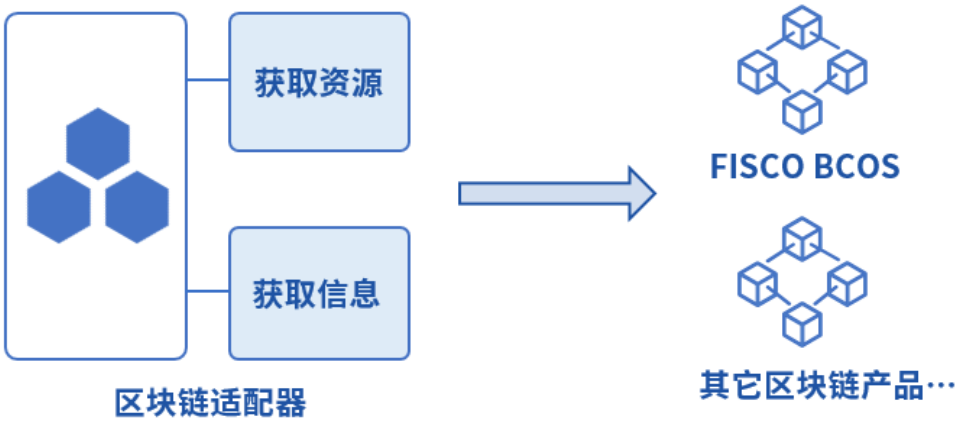
	相同接口	差异接口
FISCO BCOS	数据读写 调用智能合约接口 向智能合约发送交易	网络状态 共识信息
Hyperledger Fabric		

异构链互联模型（HIP）通过分析主流区块链平台交互方式的共性点，提炼一种通用的区块链接入范式与跨链交互模型，区块链平台之间进行少量适配对接，就可以实现异构链之间的跨链交互。

3.2.1 通用接入范式

HIP 定义一种通用的区块链接入范式，只需实现两个核心接口即可接入一条区块链，这两个接口分别是获取“资源”的接口和获取“信息”的接口。资源源自 3.1.1 “统一资源范式”章节中所述的统一资源定义，信息是区块和区块高度等区块链关键信息。基于这种通用范式，不同区块链平台可以各自提供一个区块链适配器（Stub）。区块链适配器可以基于原有区块链平台 SDK 进行封装，实现 HIP 的核心接口，而无需对原有区块链做渗透修改。任何区块

链只要遵循区块链接入模型，实现区块链适配器， 就可以接入 WeCross 平台。接入方式如 2.2“跨链系统架构”章节所述，由跨链路由加载区块链适配器，从而实现接入区块链平台。



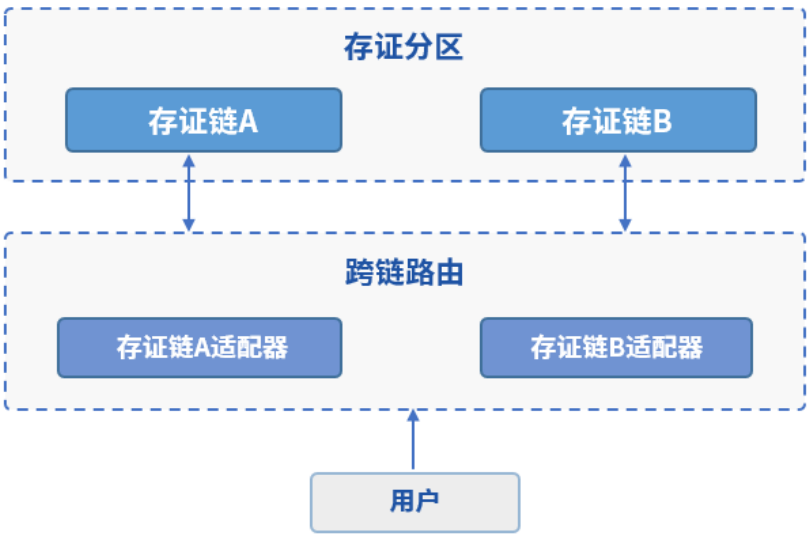
区块链适配器的接口声明如下（伪代码）：

```
public interface Stub {
  // 获取 Stub 类型
  public String getType();

  // 获取 Stub 管理的区块链的状态
  public ChainState getChainState();

  // 获取 Stub 管理的区块链的区块头信息
  public Header getHeader(int blockNumber);

  // 获取 Stub 管理的区块链上的资源
  public Resource getResource(Path path) throws Exception;
}
```

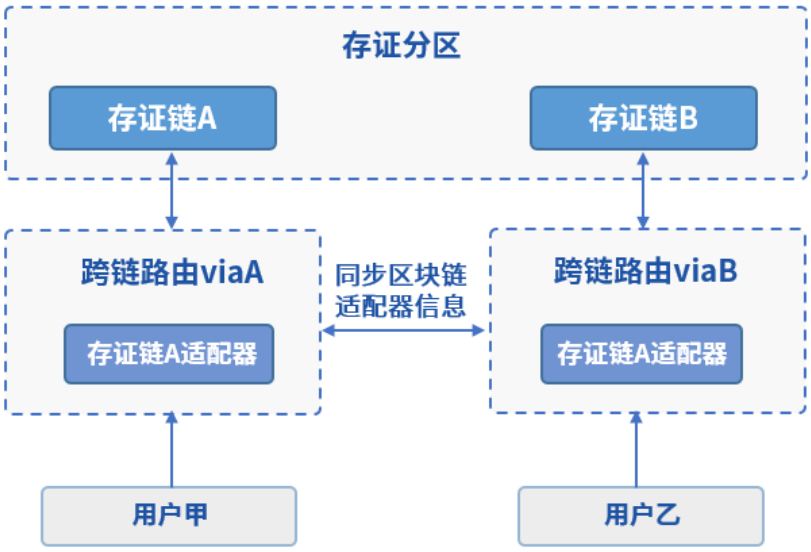
3.2.2 跨链交互模型

为适配多变的跨链业务场景，HIP 设计一套跨链交互模型，该模型可以支持单分区单路由、单分区多路由以及多分区多路由等多种场景。

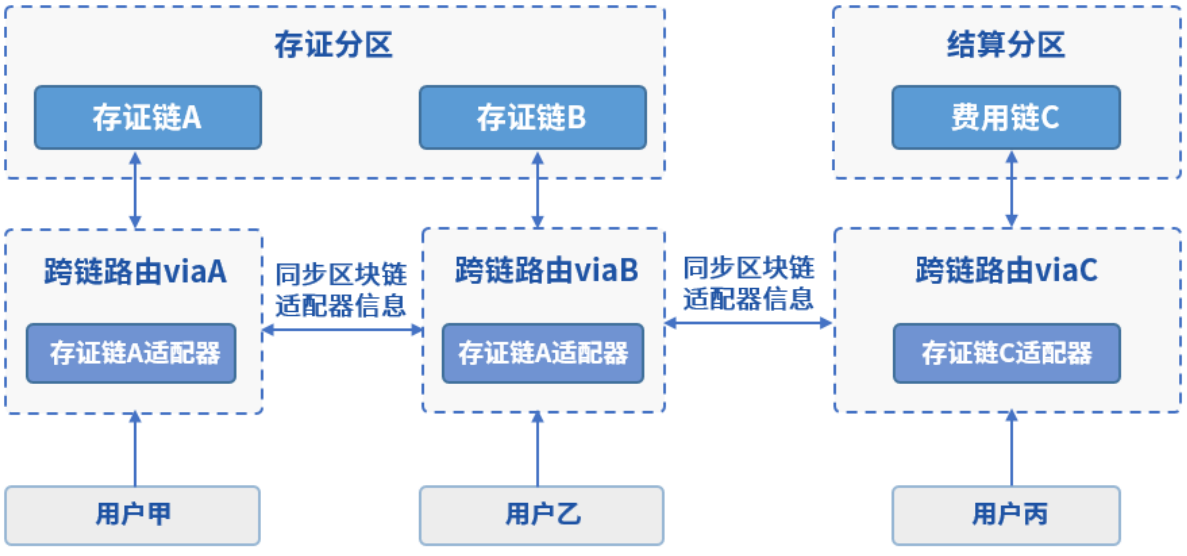
- **单分区单路由：**针对一个机构的用户需要同时访问多个区块链的场景，可以在机构内搭建一个跨链路由，并为其配置多个区块链适配器，连接到多个区块链。通过给多个区块链适配器配置不同的 iPath 前缀，用户可以通过跨链路由，任意寻址并访问网络中的资源。如图所示，用户 A 可以通过配置了两个不同区块链适配器的跨链路由，实现对两条链上资源的访问。



- **单分区多路由：**针对多个机构的多个用户想要交叉访问对方的区块链，可以部署多个跨链路由，并为其配置各自的区块链适配器。跨链路由之间通过 P2P 网络协议相连，跨链路由之间会自动同步交换各自的区块链适配器和资源信息。不同机构的用户可以通过调用本机构的跨链路由，由本机构的跨链路由转发至其它机构的跨链路由，访问相应资源并按路由返回。如图所示，用户甲可以通过跨链路由 viaA 和跨链路由 viaB 组成的路由网络，实现对两条存证管理链上资源的访问。



- **多分区多路由：**在更为复杂的业务场景中存在多种业务相互融合的需求，因此也就存在多个跨链分区互联访问的需求。面对这种需求，HIP 支持跨链路由动态增加与其他跨链路由的连接，通过权限控制保证跨链访问的安全可控，对原有业务不做任何渗透修改。如图所示，通过跨链路由将存证分区和结算分区相连，实现原有两个分区的用户能够访问对方分区的资源。



从以上三个场景可以看到，跨链路由是整个交互模型的核心模块，是连通多个区块链的桥梁。跨链路由作为独立的进程部署，一个跨链路由可以使用多个区块链适配器模块去连接多个区块链，多个跨链路由使用 P2P 网络互相连通。跨链路由内部采用分层设计的理念，自底向上分为四个层次：

- **基础层：**跨链路由底层最基础的部分，包括网络互联模块、区块链适配器模块和抽象链存储模块。网络互联模块负责跨链路由间的互联，区块链适配器模块负责连接具体的区块链节点，抽象链存储模块保存多个区块链的抽象区块头信息用于验证交易和回执。
- **交互层：**处理跨链路由的交互逻辑，包括资源同步、资源寻址以及跨链证明等模块。资源同步模块同步多个其它跨链路的资源配置信息，资源寻址模块帮助用户在跨链分区中按 iPath 寻址资源，跨链证明模块验证其它跨链路由返回的交易和回执数据。
- **事务层:** 处理和协调跨区块链的事务逻辑，包括两阶段事务模块和哈希时间锁定等机制。

跨链路由要在区块链之间建立连接，为了保证跨链路由间能维持高效、可靠和安全的网络连接，跨链路由设计如下网络机制：

- **网络准入：**跨链路由支持基于CA 认证机制的网络准入，支持任意多级的证书结构，保障信息保密性、认证性、完整性、不可抵赖性。所有通讯链路使用SSL 加密，加密算法可配置，保证数据传输的安全性。
- **TCP 长连接：**跨链路由之间维持长连接以保证双向通信，减少建立连接和断开连接的开销。跨链路由网络之间使用心跳包来保证可用性，在断连的时候自动重连。
- **状态同步：**跨链路由之间会自动同步各自区块链的区块高度、共识和网络等状态。
- **自适应路由：**跨链路由在P2P 网络中，会自动搜索和确认与另一个跨链路由的可行链路，并评估链路的响应速度、带宽和可用率，自动选取最佳的链路，当一个链路失效时，跨链路由会选取另一个可用的链路，保证跨链消息的可用性。

3.3 可信事务机制

正如第一章关于 Secure 的设计理念提到，基于共识机制和密码学技术，区块链建立了一套内部安全机制，但是在面对跨区块链调度时会突破区块链内部的安全边界，需要重新建立安全机制。以基于 PBFT 共识机制的区块链平台为例，参与共识的所有区块链节点不会直接同步来自其它节点的状态数据，而是先下载来自其它节点的区块，验证区块中的 PBFT 共识签名，然后执行区块中的所有交易，根据交易的执行结果来更新状态数据，保证所有需要上链的数据都经过签名的校验和执行的验证。然而，在跨链场景中，各自独立的区块链网络需要相互获取对方链上的数据，由于它们并没有参与对方区块链的共识流程，如何保证获得的数据可信是一个技术挑战点。

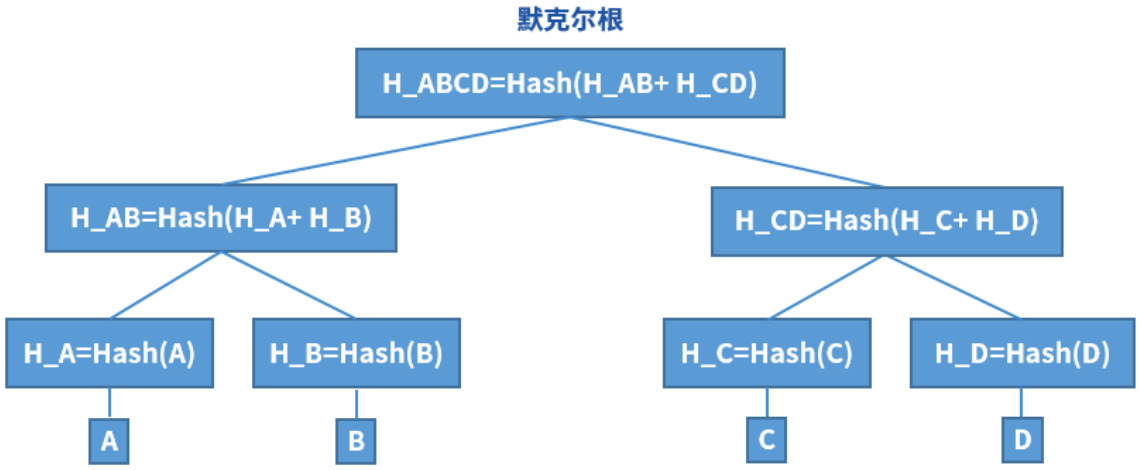
另一个技术挑战点是保证跨链交易中各自链上交易执行的事务性，例如跨链资产交易，让所有参与交易的区块链对资产的操作同时成功或者同时失败。传统的分布式事务如多个关系型数据库的事务中，多个数据库会选取一个共同可信的中心协调者，来协调多个数据库的事务操作。协调者向多个参与事务的数据库发送操作步骤，并监视和管理这些操作的执行状态，一旦出现异常，中心协调者会回滚整个事务，还原系统状态。然而，跨链场景中的多个区块链平台的地位是对等的，难以选出一个中心化的协调者，无法按照传统的方式实现分布式事务。

WeCross 可信事务机制（TTM）的目的是解决上述挑战，提出数据互信机制和跨链事务机制，分别解决数据可信问题和交易事务性的问题。

3.3.1 数据互信机制

假设两个用户甲和乙要在两条不同区块链上完成资产交换，那么必须要有一种机制来保证两个用户都真实拥有所宣称的资产，否则任何一方的用户都可以使用伪造的链上资产去兑换对方有效的链上资产。数据互信机制就是要解决这种跨链场景下的数据可信问题，它基于默克尔证明机制来实现，使得一方在不需要获取另一方区块链全量数据的情况下，仍然能够快速证明另一方区块链上特定数据的真实存在性。

参与跨链的双方通常没有条件和权限去存储另一方的全量区块链数据，要在不存储所有区块的情况下验证某个区块是否包含了特定的交易，需要借助一种特殊的数据结构——默克尔树。默克尔树的结构如下图所示，每个非叶子节点通过其子节点的哈希值来进行标注，树的根节点叫作默克尔根。



假设上图是区块 X 的默克尔树结构，如果要验证交易 D 是否在区块 X 中，无需获取整个区块 X，只需要提供交易 D，H_AB，H_C 以及默克尔根则可。具体过程如下：

- 根据交易 D 计算哈希，得到 H_D。
- 根据 H_C 和 H_D 计算哈希，得到 H_CD。
- 根据 H_AB 和 H_CD 计算哈希，得到 H_ABCD。
- 对比 H_ABCD 和默克尔根，如果相同，则证明区块 X 存在交易 D，否则说明不存在。

上述的验证过程称为默克尔证明，证明信息是指验证过程中用到的初始哈希值，即 H_AB 和 H_C。

默克尔证明是一种经典技术，用于证明交易存在于区块链的某个区块中，是实现轻客户端的关键技术。WeCross 采用默克尔证明做跨链互信技术的基本算法，在功能完备性和用户体验方面比传统轻客户端前进了一大步，主要表现在以下两方面：

- **多维度的默克尔证明：** WeCross 设计多维度的默克尔证明，不仅能够验证交易存在性，还能够验证交易执行结果的正确性，为跨链交易可信执行以及后续章节将讲述的事务机制提供完备的可信验证。交易存在性验证是指验证某一笔交易是否真实存在于某个区块，确保跨链交易中双方所声称的资产或数据是真实存在的。交易执行结果正确性验证是指验证跨链交易是否已在双方各自的区块链上正确执行，保证跨链交易执行结果的正确性。其中交易存在性验证需要用到交易默克尔根，交易执行结果正确性验证需要用到回执默克尔根。

- **对用户完全透明：** 上述提到的多维度默克尔证明，在 WeCross 中对用户完全透明，用户访问跨链资源与访问链内资源体验一致。跨链路由组件的交互层包含一个跨链证明模块，该模块负责实现默克尔证明机制。用户发送跨链交易请求，跨链路由根据路由寻址找到相应资源所在业务链，跨链路由会向业务链发送交易，并且获得相关默克尔证明，证明数据连同请求结果一并返回用户侧的跨链路由，由用户侧的跨链路由进行默克尔证明数据的验证。总体流程可见 2.3“可信交互流程”章节中的时序图，数据可信验证的全流程由跨链路由组件执行，用户无需关心实现细节。

借助默克尔证明机制，WeCross 能够有效地验证跨链交易的真实性和跨链交易执行结果的真实性，为跨链交易的可信执行提供了基础。同时，复杂的证明过程由跨链路由自动实现，对用户完全透明。

3.3.2 跨链事务机制

同样以跨链资产交换为例，通过数据互信机制保证资产和交易的真实有效，对整个交易流程而言仍有不足。假设在一条链上成功完成了资产转移，但是另一条链上并未成功执行资产转移，就会导致某一方损失资产，使跨链资产交换失败。数据互信机制虽然保证了跨链交易的可信性，但是为了跨链资产交换完全正确执行，还需要保证跨链交易的事务性。跨链事务机制保证多个区块链上的操作要么全部执行完毕，要么全部执行失败。传统分布式系统的事务技术有很多，例如两阶段提交和三阶段提交等，它们能够实现不同级别的分布式一致性，

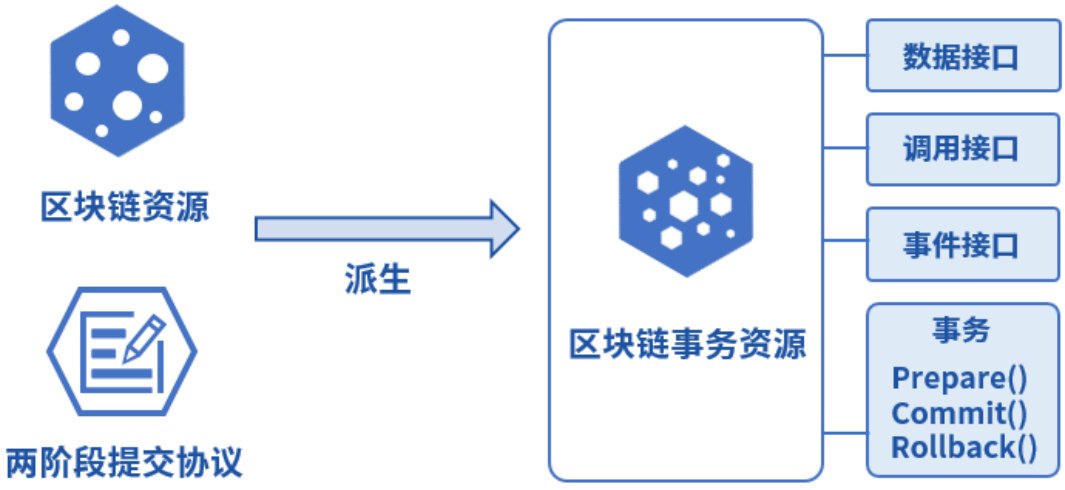
各有优缺点。区块链早期以数字资产交换为主要运用，基于区块链架构的特殊性，也有区块链升级版的事务技术，包括哈希锁定、分布式私钥控制等，这些技术主要用于保证跨链资产交换场景的事务性。TTM 的目标是不但能满足跨链数字资产的交换，还要支持更多复杂跨链场景，所以会逐步集成支持现有主流的事务技术，包括两阶段提交协议、哈希时间锁定合约等。

◆ 两阶段提交协议

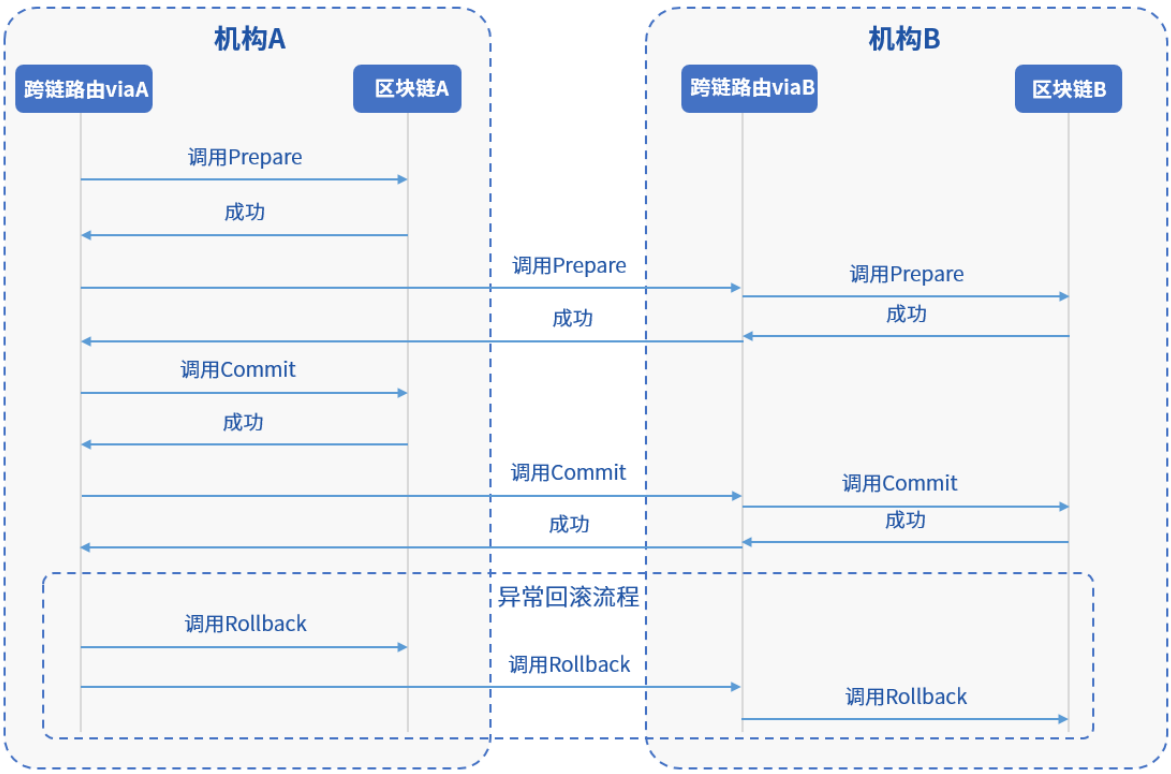
两阶段提交协议是一个原子性的提交协议，旨在保证分布式系统处理事务时的一致性。两阶段提交协议具备可靠性强、通用性强、实现简单等优势，大部分业务诸如跨链转账、跨链协同等，都可以使用两阶段提交协议来实现。

两阶段提交协议将事务的提交过程分成两个阶段来处理，分别是投票阶段和提交阶段。为了让整个事务能够正常运行，两阶段提交协议涉及三个接口，分别是准备（Prepare）、提交（Commit）和回滚（Rollback）。

在 3.1.1“统一资源范式”章节中介绍了统一的资源范式，为资源定义了数据获取、调用和事件通知的三个核心接口。结合两阶段提交协议，WeCross 为需要保证跨链事务性的资源增加三个事务接口，如下图所示。



在 3.2.2“跨链交互模型”章节中阐述了跨链路由的功能设计，其中事务层负责实现跨链事务机制。跨链路由会担任两阶段提交协议中的协调者角色，协调整个事务的运行。在准备阶段，跨链路由会向全体参与事务的资源发起准备请求，在所有资源完成准备后，再向全体资源发送提交请求。准备或提交两个阶段中，如果任一资源返回失败，跨链路由会向全体参与事务的资源发起回滚请求，放弃本次事务，恢复最初状态。跨链路由协调的事务机制整体流程如下图所示。



两阶段提交协议具有诸多优势，传统数据库和分布式系统大量使用两阶段提交协议实现事务机制，因此跨链事务机制也首选两阶段提交协议。

传统的两阶段提交协议非常依赖可靠的协调者，如果有恶意或异常的协调者拦截或阻拦部分事务请求，就会导致事务流程的中断，如果担任协调者的跨链路由因为系统或网络的原因失效，就会导致单点问题从而使事务无法继续。

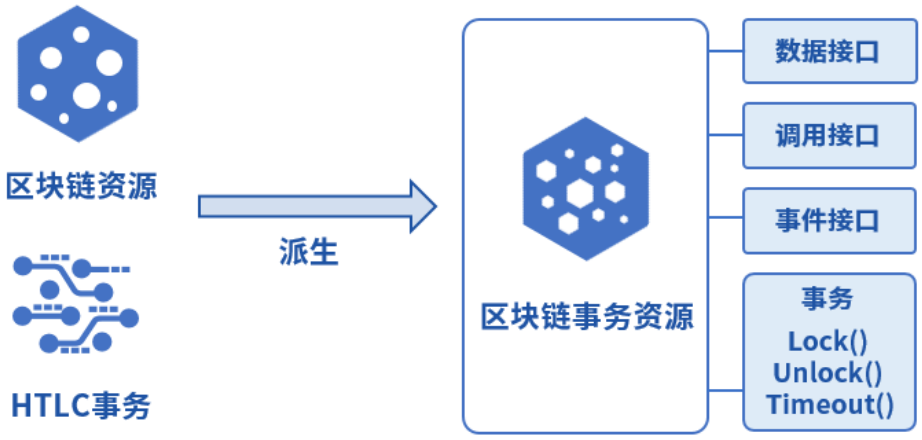
为了避免上述问题，TTM 支持用户在多个业务区块链之外可选地搭建一个专门用于协调事务的区块链，称为治理链。各个机构中参与事务的跨链路由通过配置区块链适配器连接

治理链，在处理两阶段事务的过程中，事务的状态都记录在治理链上，这样恶意的协调者就无法轻易地篡改两阶段事务的状态。当负责协调事务的跨链路由因为系统或网络原因出现异常时，其它跨链路由可以从治理链得到事务状态，继续处理事务，规避单点的问题，详细的实现参见 3.4.1 “权限事务管理”。

◆ 哈希时间锁定合约

哈希时间锁定合约（HTLC，Hashed Time Lock Contract）是一项进行区块链网络之间资产交换的技术。在资产交换过程中，为了保证各个区块链的资产安全，资产转移要么全部完成，要么全部没有完成，不存在任何中间状态。哈希时间锁定合约基于哈希算法和超时机制，对比两阶段提交，HTLC 并不依赖可信的协调者，特别适合区块链资产交换的场景。

基于统一资源范式，哈希时间锁定合约为区块链资源新增三个接口，分别是锁定（Lock）、解锁（Unlock）和超时（Timeout）接口。只要正确实现这三个接口，WeCross 跨链路由就可以协调该区块链资源，参与到任意基于哈希时间锁定合约的事务中。

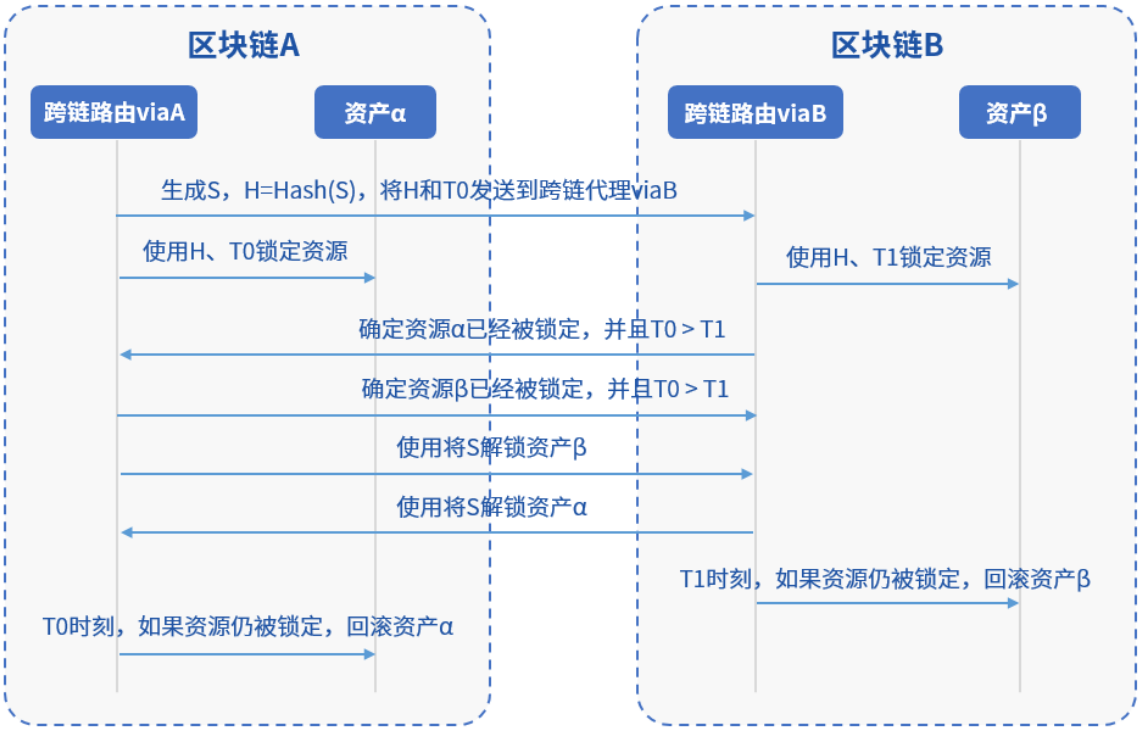


哈希时间锁定合约的处理流程基于哈希算法和超时机制，假设有两个区块链 A 和 B，试图交换位于链 A 的资产 α 和位于链 B 的资产 β，则整个哈希时间锁定的流程如下：

- A 首先选取一个秘密随机数 S，使用特定的哈希算法计算出 S 的哈希值 H，之后 A 将 H 发给 B，同时 A 和 B 协商两个时间点 T0 和 T1，确保 T0 >T1。

- A 基于 H 和 T0 创建资产锁定智能合约 LockContractA，该智能合约会锁定资产 α，其可以使用 S 来解锁并将资产 α 转移给 B，如果在 T0 前仍未解锁，则会自动撤销锁定，且不会发生任何资产转移。
- B 基于 H 和 T1 创建资产锁定智能合约 LockContractB，该智能合约会锁定资产 β，其可以使用 S 来解锁并将资产 β 转移给 A，如果在 T1 前仍未解锁，则会自动撤销锁定，且不会发生任何资产转移。
- A 使用秘密随机数 S，调用 B 上的智能合约 LockContractB，将资产 β 转移给 A。
- 经过上述步骤，B 获得了秘密随机数 S，B 使用 S 调用 A 上的智能合约 LockContractA，将资产 α 转移给 B，资产交换完成。
- 如果 A 或 B 任意一方超时未执行操作，则在 T1 时间点后，B 资产会撤销锁定，T0 时间点后，A 资产会撤销锁定，还原初始状态。

T0 和 T1 用于避免 A 或 B 单方延误交易，所以这其中的交易包 α 和交易包 β 都需要设定时间限制，超出这个时间限制后，相关资产立即撤销锁定，原路返回。整体操作时序流程如下图所示。

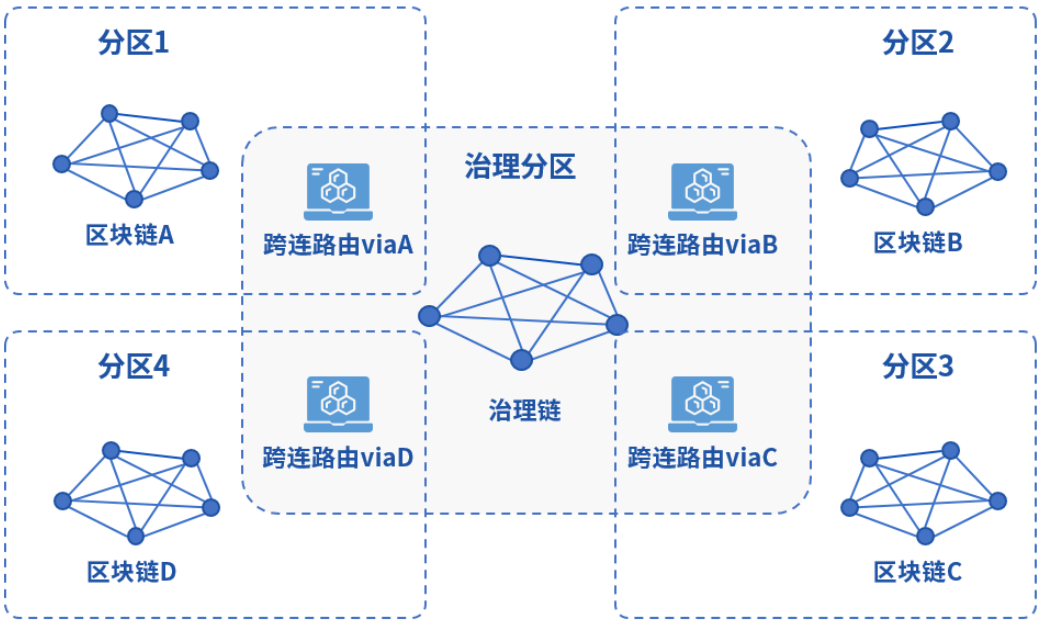


两阶段提交协议和哈希时间锁定合约各有特点。两阶段提交可以用于满足一般的事务处理请求，但是需要依赖可信协调者，为了引入多中心可信协调者，可能需要额外的治理链来配合实现。哈希时间锁定合约不依赖可信协调者，契合区块链资产交换的场景，但对于资产交换以外的场景，其流程较为复杂和冗长，没有两阶段提交通用和有效。

3.4 多边跨域治理

目前，区块链面临的扩展性瓶颈愈发明显，现有的一些技术手段例如多通道、多群组以及多链架构等仅仅解决区块链容量的平行扩展问题，但仍缺乏可信的准入、监管和治理机制，使得跨链应用限制在参与方都可信的场景。

多边跨域治理（MIG）是一套完整的区块链多边治理方案，支持多个区块链按照其业务需求，以不同的网络拓扑来组建跨链分区，并由多个机构共同维护治理链，实现多个区块链安全可信地执行事务。MIG 通过协商和投票的形式进行机构准入和区块链治理，并支持即时有效的监管仲裁。



治理链上部署多种跨链治理相关的智能合约，包括权限管理合约、事务管理合约、业务链监管合约、业务链准入合约和机构准入合约等，这些合约分别聚焦于权限、事务、监管和准入等功能。治理链由业务方和监管方等相关机构共同搭建，各个机构可以通过在各自的跨链路由中配置区块链适配器以接入治理链。

3.4.1 权限事务管理

区块链上的资源可能涉及个人资产、身份数据和商业机密等多种敏感信息，需要可靠的权限管理和授权机制来保障区块链资源的信息安全。通过在治理链上部署权限管理智能合约，能够将跨链操作的权限控制细化到分区、机构、区块链甚至是资源的具体接口。接入治理链的跨链路由将实时同步和执行来自权限管理合约的权限策略，控制和记录跨链操作的资源访问，实时保障跨链业务的信息安全。权限管理合约的逻辑表示例如下：

标识号（用户或机构）	资源路径	权限信息
用户甲	payment.evidence.asset 指向支付分区中证据链的资产资源	允许访问数据读接口
用户乙	payment.evidence.* 指向支付分区中证据链的所有资源	允许访问数据读接口 允许访问数据写接口
机构丙	payment.* 指向支付分区中所有链的所有资源	允许访问调用接口 允许访问交易接口

- **标识号：**区块链用户或机构的标识号，作为表的主键，记录该权限条目相关的用户或机构标识。
- **资源路径：**该权限条目涉及的资源路径，即 iPath，路径支持使用通配符。
- **权限信息：**控制该权限允许访问的资源接口，参见 3.1.1“统一资源范式”章节定义的资源接口列表，资源中任一个接口都可以配置独立的权限。

除了权限的控制，跨链的事务操作也通过治理链调度。治理链部署了事务管理合约，用于记录事务从生成到结束的完整生命周期。事务管理合约的逻辑表示例如下：

事务标识号*	步骤序号*	步骤操作	步骤状态
0x100	1	调用区块链A的资源α的Prepare接口	已完成
0x100	2	调用区块链B的资源β的Prepare接口	进行中
0x101	1	调用区块链A的资源γ的Commit接口	进行中

- **事务标识号：**事务的唯一标识号，每创建一个新事务时生成。
- **步骤序号：**一个事务需要多个步骤执行，步骤序号为某个事务已经执行的步骤的序号。
- **步骤操作：**该步骤需要执行的操作。
- **步骤状态：**步骤的当前状态。

事务管理合约将事务的步骤记录在治理链上，需要经过所有治理节点的共识。如有攻击者试图攻击某个事务，恶意篡改或丢弃事务步骤，意味着攻击者要攻击由多个不同机构共同维护的治理链并且篡改链上数据，成本极高。当网络或系统发生故障，导致当前负责协调事务的跨链路由无法工作时，其他跨链路由可以通过事务管理合约中已记录的事务步骤，继续事务的执行，从而避免单点问题，达到容灾的效果。

3.4.2 监管准入管理

治理链可以选择性地记录多个跨链分区间部分或所有的跨链操作，供监管机构进行穿透式监管。监管机构可以选择部署一个接入治理链的跨链路由，或是直接运行一个治理链的区块链节点从而获取监管数据。监管数据格式如下：

监管字段	说明
跨链发起方标识	发起跨链的用户标识
跨链发起方机构标识	发起跨链的用户所属的机构标识
跨链操作资源路径	跨链操作的资源的iPath
跨链操作资源接口	跨链操作调用的资源接口，数据接口、调用接口或是事件接口，例如sendTransaction
跨链操作参数	跨链操作的参数
跨链操作结果	跨链操作的结果
其它	其它字段

治理链上的监管数据以加密方式存储，只能由监管方解密读取。跨链分区中任何恶意跨链操作，都会被记录在治理链，供监管方实施事前拦截、事中监控以及事后追责。

治理链上的业务链准入合约和机构准入合约为参与跨链的业务和机构提供准入控制，支持基于 CA 认证机制来识别业务链和机构的身份。机构准入合约可以配置一个或多个管理员，合约中保存的准入信息可以动态地增删改查。当跨链分区中出现恶意行为时，管理员可以在治理链上发起投票表决，惩罚或踢出作恶的机构。

治理链的数量不局限于一个，在复杂的网络拓扑中，多个跨链分区可以组建各自的治理链，多个治理链之间允许组建更高层级的治理链，从而形成多级的治理架构，每一级治理链都能直接管理其接入的多个治理链，使得搭建大规模、跨地域、海量数据和可治理的广域区块链网络成为可能。

3.5 平台优势

3.5.1 开源开放

WeCross 遵循微众银行“把源码丢出去，把信任建起来”的开源共建理念，所有源代码全部开源，与社区共同维护 WeCross 的迭代升级，利用蓬勃发展的社区力量，更好、更高效地开发和引入新功能。

WeCross 秉承开放的态度，支持市面上多种主流的开源区块链，如 FISCO BCOS 和 Hyperledger Fabric 等。WeCross 已经通过开源共建的方式，和多个区块链平台和应用逐步对接，也欢迎社区积极参与贡献，让更多区块链平台能够接入 WeCross 生态。

◆ FISCO BCOS 支持

FISCO BCOS 支持群组架构、分布式存储，并行计算模型和预编译合约等特性，包含 PBFT 和 Raft 共识算法，在网络和存储层面上做了严格的安全控制，引入了节点准入机制、CA 黑名单和权限控制三种机制，支持默克尔树验证交易的存在性。

针对 FISCO BCOS 的特点，WeCross 做出如下适配：

- FISCO BCOS 的区块链结构转换为 WeCross 的抽象链结构，其抽象链的实现中，包含 FISCO BCOS 的块高、块 Hash 和多个默克尔根字段，支持区块链结构的校验和交易、回执和状态数据的校验。
- FISCO BCOS 的智能合约被抽象为 WeCross 资源，支持智能合约局部变量的读写和智能合约接口的调用。
- WeCross 跨链路由可以直接连接到 FISCO BCOS 节点，支持加密协议和 CA 认证。

◆ Hyperledger Fabric 支持

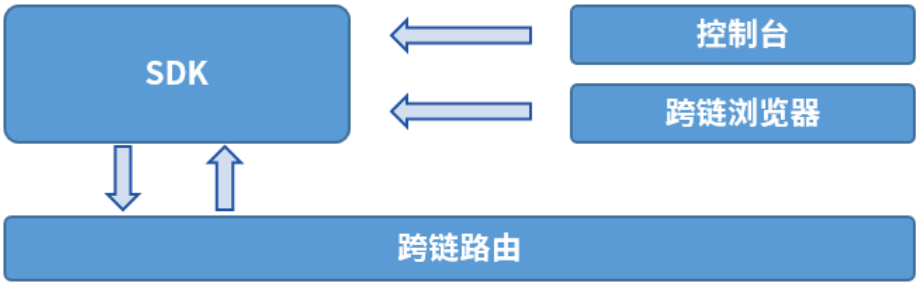
Hyperledger Fabric 是一个模块化架构的分布式账本平台，提供高度的机密性、弹性、灵活性和可扩展性。它旨在支持不同组件的可插拔实现，并且可以容纳生态系统中存在的高度复杂应用。Hyperledger Fabric 支持用通用编程语言（如 Java，Go 和 Node.js）编写智能合约。

针对 Hyperledger Fabric 的特点，WeCross 做出如下适配：

- Hyperledger Fabric 的区块链结构转换为 WeCross 的抽象链结构，抽象链的抽象区块中，包含 Hyperledger Fabric 的块高、块 hash 和 data_hash 字段，支持区块链结构的校验和状态数据存在性的校验。
- Hyperledger Fabric 的 Chaincode 被抽象为 WeCross 资源，支持数据和交易接口。
- WeCross 跨链路由可以直接连接到 Hyperledger Fabric 的 Endorser 或 Orderer，发起请求。

3.5.2 开发友好

WeCross 将逐步实现多语言版本的 SDK 工具，包括 Java SDK、Python SDK 等，用户只需根据自身跨链应用程序的要求选择相应语言的 SDK，使用 SDK 提供的 API 接口，就能实现对跨链资源的操作，进行跨链应用的开发。



WeCross 为用户提供交互式控制台，帮助用户即使不写代码也能完成跨链逻辑的验证。例如，当跨链应用中需要通过合约对链上状态进行更新时，各个链都有独立的相关合约来实现各自的更新逻辑，用户可以通过控制台快速地实现对某条链的合约访问，从而完成对各个链的跨链合约的功能校验。

WeCross 提供跨链浏览器，它对 SDK 的接口和功能进行再封装，支持图形化的数据输出。跨链浏览器旨在更形象地为用户展示多条链的状态，实现链的统一管理。同时提供相关指引性操作，帮助用户快速理解 WeCross 的开发逻辑，轻松发起跨链操作。

3.5.3 安全可信

WeCross 通过多种机制来保证跨链系统的安全性：

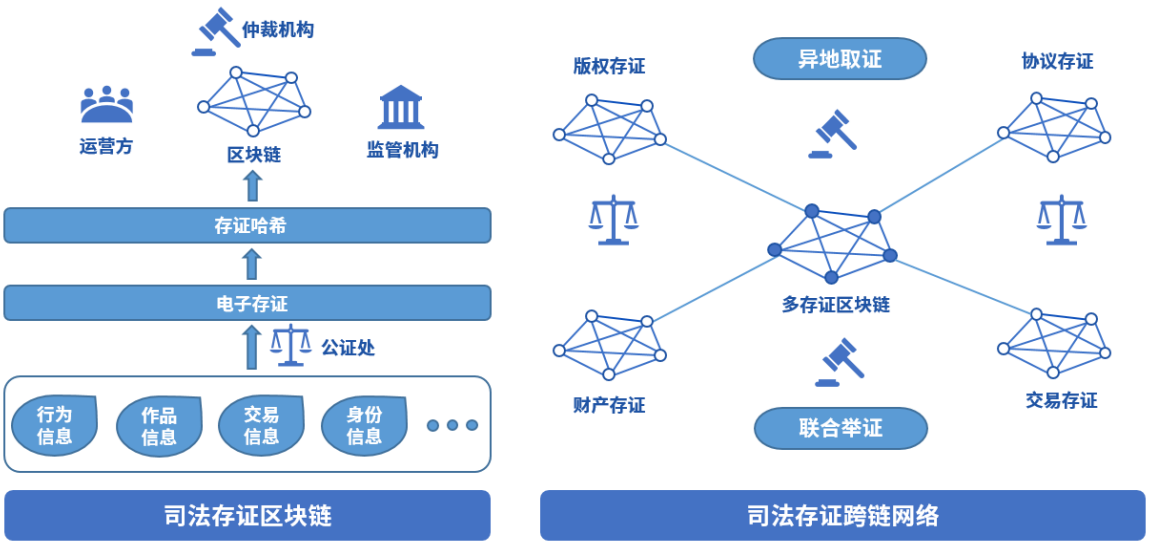
- **加密：**无论是网络中传输的跨链消息、磁盘上存储的跨链配置与区块链信息、链上暂存的事务状态，都将进行加密且支持配置加密算法和加密等级，保护数据不被恶意获取。
- **准入：**参与跨链的任何区块链的资源信息，都需要配置访问权限，权限的配置精确到资源和用户粒度。接入跨链分区的用户、机构和节点使用基于 CA 的认证准入机制。
- **隔离：**跨链交互所需要传输的数据遵循最小化原则，只传输跨链相关的必要数据，不会额外传输任何其它敏感数据。多个区块链之间没有直接连接，跨链路由严格控制各个跨链交互过程，防止数据未经授权地泄露，保证数据隔离。
- **追溯：**所有的跨链事务操作，其输入输出和完整的执行记录都会在跨链路由或治理链链上存储，一旦事务异常或是遇到恶意操作，可以回滚并还原现场，追溯整个事务的过程，检查事务的失败原因。
- **互信：**所有经由跨链路由传输的交易和回执，都需要默克尔证明并由双方的跨链路由验证，这使得跨链路由无法擅自伪造和篡改区块链的数据，保证跨链交互的互信互通。

第四章 WeCross 应用前景

4.1 司法跨域仲裁

随着数字经济高速发展，司法证据正逐步进入电子化时代。2017 年 9 月，微众银行区块链团队与第三方存证公司合作，推出区块链司法存证与仲裁平台，开创将仲裁、法院等机构作为链上节点的先河，并于 2018 年 2 月，联合仲裁机构基于该平台出具业内首份裁决书，标志着区块链应用在司法领域的真正落地并完成价值验证；2018 年 6 月，杭州互联网法院开始探求区块链在司法场景中的运用，进一步确立了区块链存证电子证据的合法性；2018 年 9 月，北京互联网法院推出电子证据平台“天平链”，加速推动在网络空间治理的法治化进程。由于区块链司法应用能够极大缩减仲裁流程，仲裁机构得以快速完成证据核实，快速解决纠纷。

随着区块链应用在司法存证领域的普及，不同司法存证链之间连通的需求愈发强烈。但区块链的信任模型使得不同的司法存证链上的证据无法互通互信，当司法仲裁需要异地取证或是联合举证时，需要引入一个中心化的可信机构来进行协调，影响了区块链的实用价值。

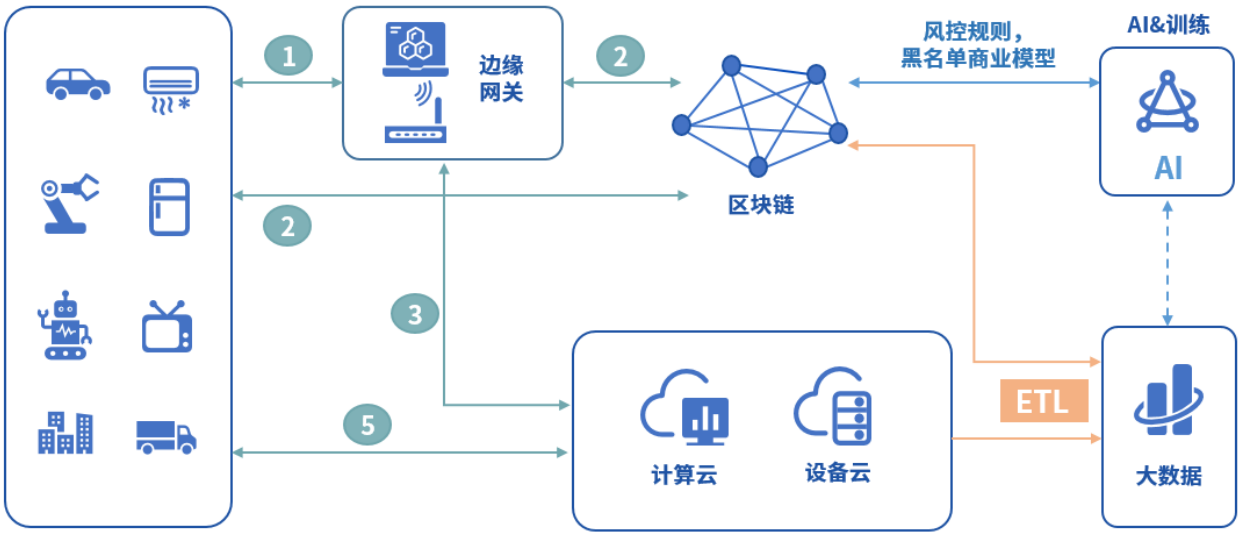


WeCross 跨链技术可以将各家存证链的证据统一抽象成证据资源，在不同的司法存证链之间可信地传输证据。WeCross 可以搭建一个拥有多类型存证的存证链网络，在面向重大问题和重大纠纷时，多中心地帮助各个链交互完备、可信和具备法律效力的证据材料，帮助仲裁机构完成裁决。

4.2 物联网跨平台联动

随着智能穿戴、智能家居、无人机及以人脸识别等人工智能设备的普及，智能设备的类别越来越多，人机交互的频次也越来越高，物联网数据的类型和结构呈现多样化和复杂化的趋势。在 5G 时代，实现万物互联之后，数据和场景的复杂度更是呈几何倍数增长。区块链技术为物联网设备提供信任机制，保证所有权、交易等记录的可信性、可靠性及透明性，同时还可为用户隐私提供保障机制，从而有效解决物联网发展面临的大数据管理、信任、安全和隐私等问题，推进物联网向更加灵活化、智能化的形态演进。

目前物联网行业的区块链项目，有的旨在解决物联网碎片化严重、物联网产品没有标准化等痛点，有的则探索区块链在智能城市、基础设施、智能电网、供应链以及运输等领域的应用。然而，它们都面临着相同的困境。物联网设备硬件模块的选择和组合非常多样，对区块链平台的支持能力不尽相同，一旦硬件部署完成后难以更新，单一的区块链平台在连通多样化的物联网设备时必然会遇到瓶颈，无法全面满足所有物联网设备在多样化场景中的需求。

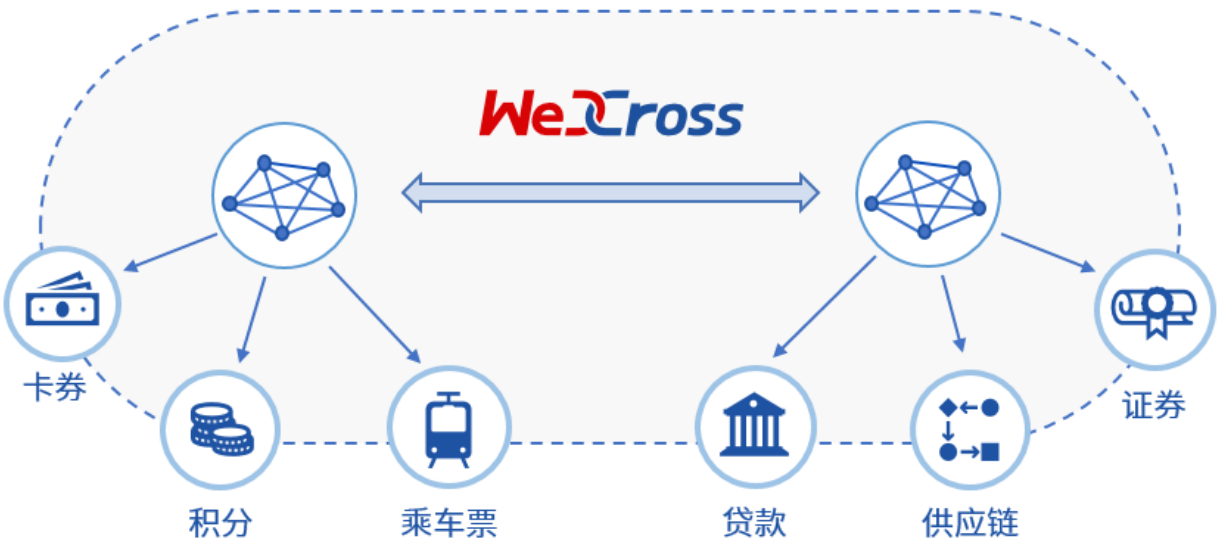


WeCross 跨链技术支持物联网设备跨链平行扩展，可用于构建高效、安全的分布式物联网网络，以及部署海量设备网络中运行的数据密集型应用；WeCross 跨链技术可以安全可信地融合连通多个物联网设备的区块链，在功能和安全上满足多样的场景需求。

4.3 数字资产交换

区块链天然具有金融属性，有望为金融业带来更多创新。支付清算方面，在基于区块链技术的架构下，市场多个参与者维护的多个账本或区块链融合连通并实时交互，短短几分钟内就能完成现在两三天才能完成的支付、对账、清算任务，降低了跨行跨境交易的复杂性和成本；同时，区块链技术能够确保交易记录透明安全，方便监管部门追踪链上交易，快速定位高风险交易流向。数字票据和供应链金融方面，区块链技术可以有效解决中小企业融资难问题。目前的供应链金融很难惠及产业链上游的中小企业，因为他们跟核心企业往往没有直接贸易往来，金融机构难以评估其信用资质。基于区块链技术，可以建立一种联盟多链网络，涵盖核心企业、上下游供应商、金融机构等，核心企业发放应收账款凭证给其供应商，票据数字化上链后可在供应商之间跨链流转，每一级供应商可凭数字票据实现对应额度的融资。

伴随着区块链在金融领域落地应用的飞速增长，多元化的数字资产场景和区块链应用带来了区块链资产相互隔离的问题，不同数字资产业务彼此搭建的区块链上的数字资产无法安全可信地实现互通，区块链上存在的数字资产价值越来越大，跨链的需求愈发迫切。

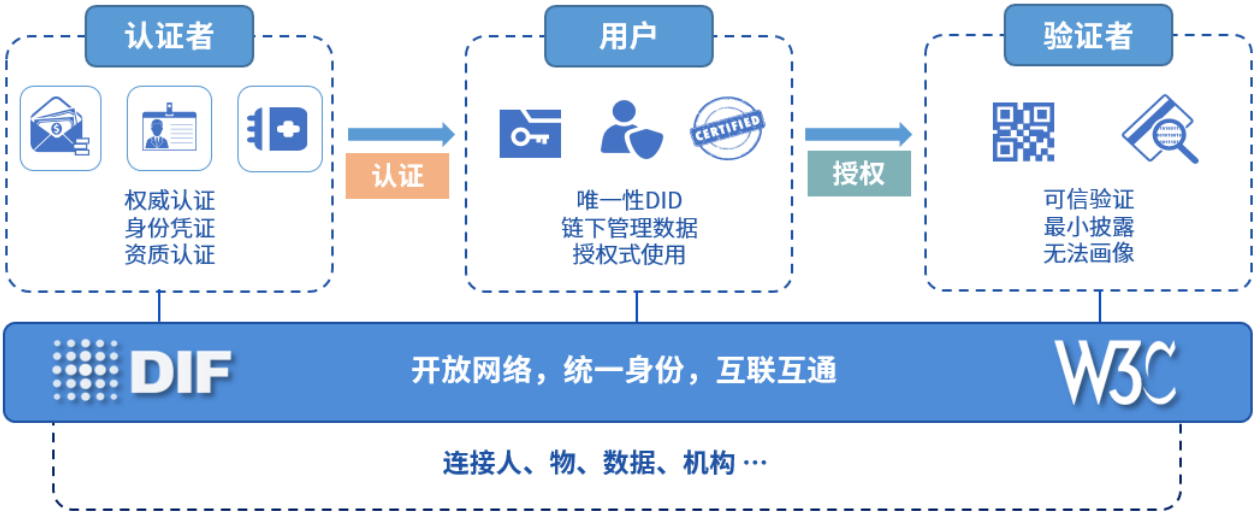


WeCross 支持以多种网络拓扑模型搭建数字资产的跨链分区。在交易逻辑上，两阶段事务模型和 HTLC 事务模型将实现数字资产的去中心、去信任和不可篡改的转移。在安全防护上，加密和准入机制将保障数字资产转移的安全与可信。通过以上技术优势，WeCross 将助力过去纸质形态的资产凭证全面数字化，让资产和信用层层深入传递到产业链末端，促进数字经济的发展。

4.4 个体数据跨域授权

随着 WeIdentity、Hyperledger Indy 等遵循 DID 协议的区块链身份认证系统出现，多个国家和地区开展了多中心化身份认证的实践与落地，多中心化身份认证目前市场需求巨大，加之政策鼓励支持，行业方兴未艾，处于高速发展的黄金时期。2019 年 2 月 27 日，微众银行区块链团队与澳门政府设立的澳门科学技术发展基金签署合作协议，在智慧城市、民生服务、政务管理、人才培训等方面开展合作。双方合作的首个项目基于“WeIdentity”的实体身份标识及可信数据交换解决方案展开，这是区块链在粤港澳大湾区应用落地的重要一步。

身份认证正向跨地域的方向发展，不同地域、业务和基于不同区块链平台的身份认证产品之间尚不能互认的现状造成信息的鸿沟，导致身份和资质等数据仍然局限在小范围的地域和业务内，无法互通。

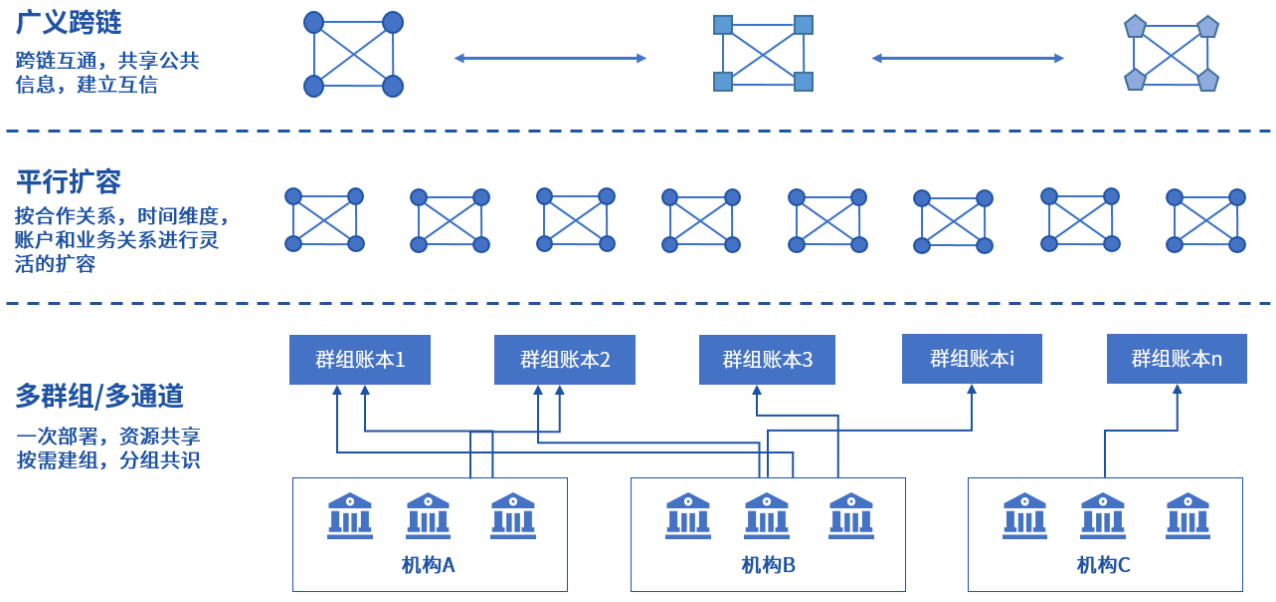


WeCross 可以将多个不同架构、行业和地域的多中心化身份认证平台联结起来，帮助多中心化身份认证更好地解决数据孤岛、数据滥用和数据黑产的问题，在推进数据资源开放共享与信息流通，促进跨行业、跨领域、跨地域大数据应用，形成良性互动的产业发展格局上，发挥更大的作用。

第五章 展望

区块链作为一种前瞻性的新兴技术倍受关注，在全球范围内掀起一股新的科技浪潮。随着区块链产业应用加速推进，区块链逐渐从金融行业向非金融行业渗透扩散，在司法存证、物联网、智能制造、身份管理等多个领域大显身手，催生了多样化的技术解决方案。未来，区块链应用要从单一走向多元，必然面临更复杂的场景、更多的参与方、更突出的数据孤岛困境，实现互联互通需求意义重大。

WeCross 针对区块链行业的现状与问题，提出 4S 跨链设计理念，设计一种通用、高效、安全和可扩展的区块链跨链协作平台，实现主流区块链平台之间的互通、互认、互联、互信以及互访。WeCross 对区块链体系和跨链网络架构进行高度抽象，降低用户部署和使用区块链的成本，提出四大核心技术，分别解决跨链场景中关键的区块链抽象、异构链互联、可信事务和多边跨域治理的问题。WeCross 不仅面向数字资产交换、司法仲裁和物联网等具体的应用场景，还将会作为未来分布式商业区块链互联的基础架构，促进跨行业、机构、地域的跨区块链价值交换和商业合作，实现高效、通用和安全的区块链跨链协作机制。



可以预见，区块链的多链架构将经历从多群组、多通道到平行扩容，最终演化到基于 WeCross 的广义跨链架构，融合连通不论同构还是异构的大量区块链平台。WeCross 将帮

助区块链技术在业务的多样性、网络的拓扑结构上做出新的突破，形成分层次纵深跨链协作，以此推动区块链与新兴科技产业和传统产业的结合，打造“区块链 +”的新型商业模式。

同时，我们把 WeCross 定位为一种链和链之间的“共同语言”，秉承“求同存异”、“携手共建”的精神，在技术和应用层面，都力求和行业建立开放、广泛的合作。WeCross 的方案和代码完全开源，持续更新，欢迎更多人以开源社区贡献、平台对接、应用实践等方式参与进来。越多人参与到跨链研究和应用中，共建的跨链方案就越具备可行性、可用性以及可持续性，这样的“网络规模效益”不仅体现在链内，更可以跨越场景、地域、人群，容纳更大的价值。

展望未来，微众银行区块链团队将一如既往，不忘初心，重点关注跨链技术发展现状和趋势，提高运用和管理跨链技术能力，使跨链技术助力建设网络强国、发展数字经济、助力经济社会发展等方面发挥更大作用。

技术路线

目前，已完成 WeCross-v1.0.0-rc1 版本的开发与发布。WeCross 在 2020 年度的技术路线如下：

- **Q1—WeCross 跨链基础架构：**完成 WeCross 四大核心技术 UBI、HIP、TTM 以及 MIG 的开发，并发布 WeCross-v1.0.0 正式版。
- **Q2—WeCross 跨链解决方案：**基于 WeCross，完成身份跨链、物联网跨链、司法存证跨链、以及数字资产跨链的应用示例开发。
- **Q3—WeCross 跨链管理平台：**完成 WeCross 跨链管理平台包括控制台和跨链浏览器的开发，实现部署、运维以及迁移的一体化、可视化管理。
- **Q4--WeCross 公共跨链服务平台：**基于 WeCross，搭建公共跨链服务平台，帮助用户快速搭建跨链服务，为用户屏蔽复杂运维操作。

WeBank 微众银行 | WeCross

微众银行区块链公众号

官网：https://fintech.webank.com/wecross

邮箱：wecross@webank.com

GitHub：https://github.com/WeBankFinTech/WeCross