WeCross跨链协作入门教程 | Meetup回顾+演讲PPT下载

原创 莫楠 微众银行区块链 4月4日

来自专辑

跨链协作开源平台WeCross

公众号对话框回复【0331】获取演讲PPT

3月31日，我们联合FISCO BCOS开源社区首次尝试线上Meetup，微众银行区块链高级架构师莫楠精心准备了一场零基础入门跨链的分享，透过“哪些领域需要跨链协作”、“我们为什么这么设计WeCross”、“WeCross怎么快速用起来”三个开发者极其关心的问题，以通俗理论配套实操演示，助力快速掌握跨链技术。

直播间讨论非常热闹，小伙伴们对跨链技术的热忱颇让我们感动。我们继续秉持开源开放的心态，分享演讲PPT供大家继续研究。直播过程的精彩内容和大家提出的典型问题，我们在本文进行精心整理，欢迎分享给更多人一起学习。

0.1. 四大应用场景启迪跨链灵感

可用于司法存证跨域仲裁

联盟链多中心和不可篡改的特性，天然吻合存证场景，甚至可以把区块链本身视为一个天然的存证平台，因而区块链存证应用非常广泛，全国各地的存证链多如牛毛。

各地存证链在地域上、业务上是分离的。各城市司法机构的案件和证据，常规情况下没有交集，彼此数据无法互通互信，当面临一些需要异地取证、联合举证或是联合仲裁的案件审判时，不仅需要耗费大量人力和时间在多地进行数据验证和比对，还需要引入一个中心化的可信机构来进行协调。若是涉及的存证链使用的底层框架不同，那要进行异地取证或是联合举证，可就更加困难了。

WeCross针对这类司法存证场景提供了有效解决方案，可以帮助司法机构一键从不同地区的多条链中同时取证，并且保证证据的可信和完备。

可用于数字资产可信交换

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。

WeCross的两阶段事务模型和HTLC事务模型支持数字资产的可信转移，加密和准入机制保障数字资产转移的安全。

可用于个体数据跨域授权

微众银行区块链在个人授权和认证方面，开源了分布式身份解决方案WeIdentify，可承载实体对象（人或者物）的现实身份与链上身份的可信映射、以及实现实体对象之间安全的访问授权与数据交换。方案在澳门政府的智慧城市建设中成功应用，为澳门电子政务服务提供技术支持。

随着WeIdentify方案的普及推广，未来其他城市也将部署相应的身份链，且在身份认证领域，Hyperledger Indy也做了一些实践，不同链间存在跨地域、跨技术框架的数据互通需求。这时，WeCross也能发挥作用。

可用于物联网跨平台联动

物联网并非一个新概念了。2005年，随着传感器、小型数码设备等产品的发展，以及一些RFID的应用，大众对物联网已经有一定认知。

随着时代的发展，物联网的概念也在不断发生变化，严格意义上来说，其实是一个不断往旧瓶装新酒的过程。最初，物联网和RFID绑定在一起。IPv6出现后，物联网和IPv6庞大的地址空间相结合，做一些设备的标识。大数据火了起来以后，物联网又能跟大数据结合，做到数据互联、人与人或物与物的互联。当前，物联网又可以和区块链结合。

为什么会有这种情况呢？因为物联网本身是一个很大很广的概念，从定义上可以看到，基本上，人与物、物与物之间的联动都是物联网，包括一些智能家居自动驾驶，都是物联网具体的应用。

物联网跟区块链有什么结合点呢？当下，物联网设备越来越多，拿一个家庭来说，可能会有摄像头、门铃传感器等设备，它采集的是用户的隐私数据，这些隐私数据需要授权和保护。物联网与区块链联动，可以将数据上链，对数据进行认证和授权。

物联网的特点是小而多。拿我家举例，WiFi的智能开关特别多，可能有20~30个，类似这样数量级别的物联网设备，用一条区块链去承载的话，压力很大。我们可以根据不同场景、不同设备分成多条区块链后进行互联，并通过跨链的交互，来满足物联网设备多样融合的需求。

应用场景小结

上述几个场景示例可以总结出一些结论：

现有的区块链是分散在不同地域、不同行业、不同领域的，分散的区块链之间，本身有互联互通需求，需要使用跨链。

一条区块链承载的容量有限，特别是联盟链，往往受制于类似PBFT或者Raft的共识机制，无法承载海量数据，需进行一些平行扩展、横向扩展，将数据分散到多条区块链上，然后

在多条区块链上做数据交互。跨链可以满足同构区块链平行扩展后的可信数据交换需求。

0.2.

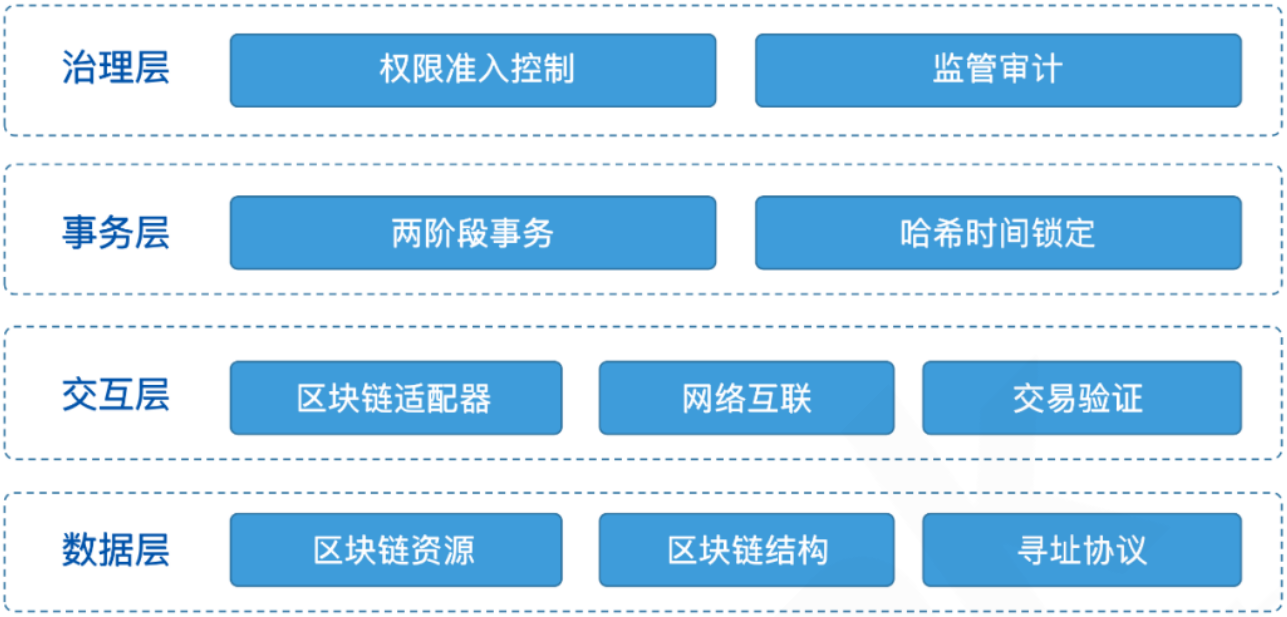
4S原则应对跨链挑战

WeCross设计理念

WeCross的设计理念主要体现四个方面，要做高性能、安全可信、可横向扩展和方便好用的跨链平台，归结起来就是我们提出的“4S”原则了。

WeCross体系抽象

基于上述原则，我们对跨链体系和架构的理解分为四个层次（如下图）。



数据层：我们把区块链上的一些信息和数据抽象为区块链资源。区块链资源可以指代智能合约资产或者是数据库信道这样的数据。对于区块链结构，我们抽象为一种通用区块数据结构；链上信息和数据要寻址的话，则抽象出一种叫做寻址协议的概念。

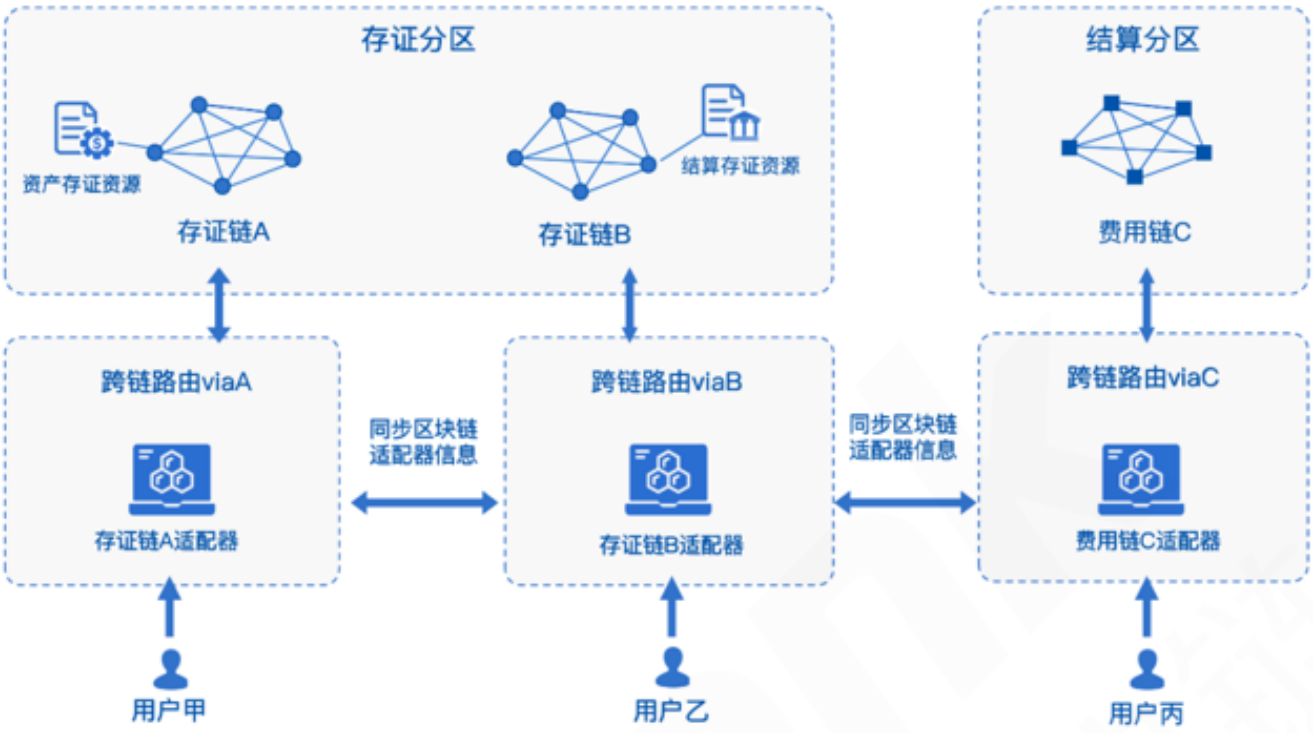
交互层：交互层由区块链适配器、网络互联以及交易验证所组成。区块链适配器用于适配不同区块链，而网络互联则方便不同区块链之间交互数据以及进行互联。交易验证保证我们在不同链上的数据是可信且不被篡改的。

事务层：事务层是基于数据结构和交互的抽象层，实现跨链事务效果。它保证两个区块链之间关联的交易要么同时发生，要么同时结束，不可能出现一个成功或者一个失败的情况。对于事务的实现，WeCross支持业界主流的两种事务实现方式：两阶段事务、哈希时间锁定。未来，我们还将依据场景需求设计更多事务机制。

治理层：作为更高的管理层级，治理层对区块链准入权限等作控制，支持区块链的监管审计。

WeCross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。

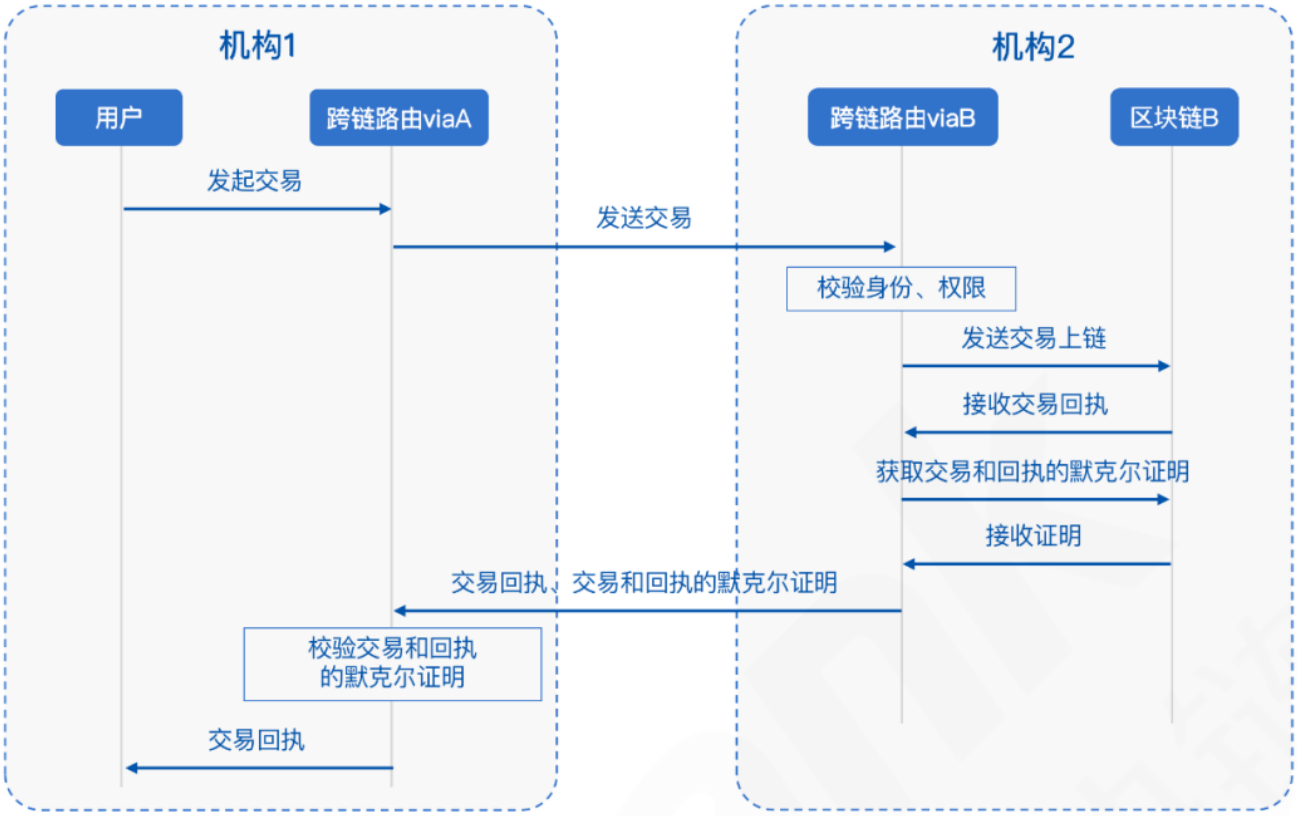


上图所示就是典型的跨链架构，共有三条区块链：存证链A、存证链B和费用链C，而用户甲、乙、丙则是三个区块链系统的用户，他们各自部署一个区块链。在WeCross系统架构中，每个独立的跨链路由连接各自对应的区块链，例如，跨链路由A连接区块链A，跨链路由B连接区块链B，以此类推。

通过P2P链接、网路连接，跨链路由之间可同步区块链上的智能合约与资源信息。我们可以看到，区块链B上有一个结算存证资源，这其实就是抽象出的一个智能合约概念。当用户调用区块链B上的资源时，A会将该用户的请求发送到跨链路由A，再由跨链路由A把请求转发到跨路由B。通过存证链B的适配器，跨链路由B将请求转化成区块链B的交易发送到区块链B，最终完成这个操作。

WeCross可信交互流程

在介绍WeCross的可信交互流程之前，先将刚才的架构分别放置在两个机构中。



当用户将交易发送到跨链路由A后，跨链路由A会将交易通过P2P网络发送给跨链路由B，收到交易后，跨链路由B会对交易做身份和权限的校验，并且把交易转化为区块链B的交易发送上链并接受交易回执。

除此之外，跨链路由B还会从区块链B处获取交易和回执的默克尔证明，以此证明交易确实存在于区块链B。完成这些之后，跨链路由B会将交易回执和交易回执的默克尔证明返回给跨链路由A，再由跨链路由A校验之后返回给用户。

整个交易流程确保了来自区块链B的数据不被篡改与伪造。

WeCross核心技术

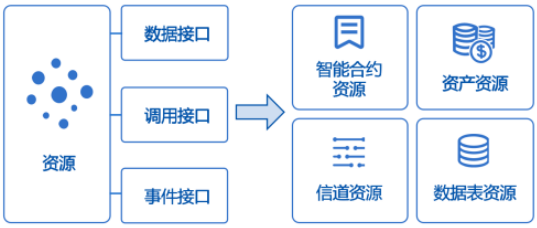
为了实现跨链交互的高效可用、安全可信和便捷治理，WeCross 基于区块链体系的抽象、跨链系统的架构和可信交互流程的顶层设计，提炼四个技术点，以实现跨链的核心功能，它们分别是通用区块链接口、异构链互联协议、可信事务机制与多边跨域治理。

首先说说**通用区块链接口**。

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，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。

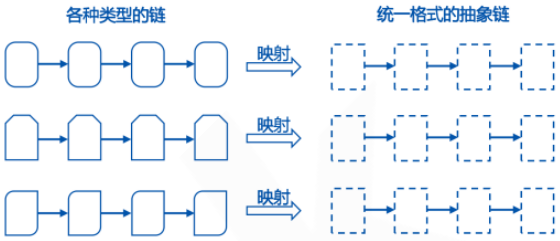
统一资源范式

通用区块链接口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注特定的区块链底层架构。



抽象区块结构

通用区块链接口提出抽象区块的概念，由抽象区块组成的链称为“抽象链”，用于验证区块链结构的正确性和查询区块链当前状态。



我们可以将通用区块链接口理解为不同区块链之间沟通的通用语言，例如，我们与外国人沟通，中文与英文本身不互通，但如果其中一方会说对方的语言，就可以沟通协作了。

为了方便区块链之间的“交流”，我们设计了“统一资源范式”的概念，即提出了一种包括数据接口、调用接口和事件接口的资源概念。在常见的区块链应用中，用户使用区块链首先不外乎就是从区块链上找到某个特定资源，这个特定资源可以是智能合约、用户的资产等，然后对这个资源进行调用操作。

如果我们将资源的数据接口和调用接口都抽象了，那用户就可以通过“统一资源”的概念去调用。比如，通过FISCO BCOS 的Solidity去调用Hyperledger Fabric chaincode。因为两者本质上都是对合约和方法的调用，传入的参数和返回值具备一致性，因此，我们可以用资源对两者做统一抽象与调用。

最终，当用户使用WeCross调用某个区块链接口或资源时，他不需要关心具体的区块链底层架构，只需用WeCross的资源接口，开发一次区块链逻辑，就可适配不同区块链。

这里的另一个概念是抽象区块结构。除了资源和智能合约，区块也是区块链中很重要的概念，虽然市面上区块链、联盟链的架构和结构都不一样，比如FISCO BCOS是用RLP编码，Hyperledger Fabric则是用Protocol Buffer编码，但这些区块链也具有共同的特性。例如，所有的区块链里都有区块高度、区块哈希等。

我们将区块链平台的字段统一提取出来，组成统一格式的“抽象链”概念。通过这个统一格式的抽象链，我们可以验证不同区块链的区块数据结构、区块是否合法、当前区块高度等

信息，还可以提取用于验证的Merkle证明数据。

第二项核心技术是**异构链互联协议**。

解决了区块链资源接口的抽象与区块链结构的抽象后，就要想办法让不同区块链之间进行交互。WeCross的方式是组建一个P2P网络，通过这个网络传输、中转区块链间的交易和数据等信息，为了实现这个效果，我们使用了通用接入范式与跨链交互模型两项技术。

通用接入范式可理解为通用区块链接口的一种具体实现。

WeCross本身就是一个插件化架构，不同区块链可通过插件接入到WeCross中，通过一系列抽象接口适配具体区块链。比如，WeCross在支持FISCO BCOS时，设计有一个FISCO BCOS插件，第三方用户包括WeCross使用者，可按照规范和指南开发类似的插件来支持不同的区块链。

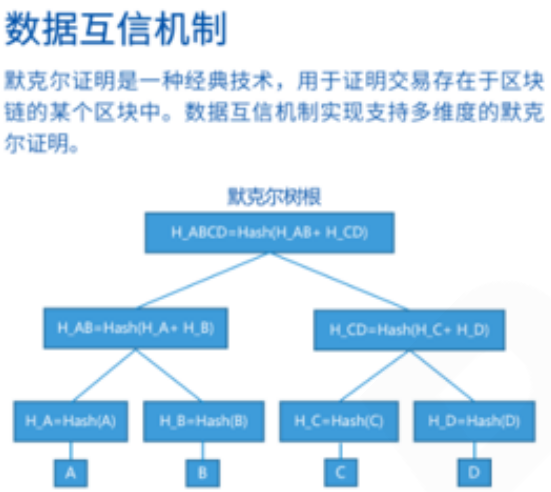
关键的一点是，WeCross对任何联盟链、区块链的适配都是非侵入式的，也就是说，WeCross不对原有区块链做任何渗透修改，就可以适配和接入。

完成适配和接入后，我们需要引入一种跨链交互模型，这也是前面提到的WeCross主体架构。它的核心思路是跨链路由间组成一个P2P网络交互链上信息，这样就能做到把不同区块链连接在一起。

多个区块链之间光是能通信或是能交互，是无法满足真实的业务需求的。

以网购举例，买东西通常都是一手交钱一手交货。交钱和交货其实是两个动作，在区块链世界里，交钱可能发生在资金的区块链上，交货可能发生在物流的物品链上，而交钱相当于在资金链上发生了一笔交易，交货则是在物品链上发生了另外一笔交易。

这两条交易必须是原子事务，即这两个动作必须同时成功或者同时失败，否则就可能出现钱交了，货没到手，或钱没交，货却到手的情况。针对这种场景，WeCross提供了**可信事务机制**。



可信事务机制基于两项基础技术，数据互信机制与跨链事务机制。

数据互信机制依赖默克尔证明技术，这是一种经典技术，现在FISCO BCOS和很多联盟链平台都支持。它本身是树状数据结构，对内部数据进行树状和逻辑关系证明。它能达到两个区块链之间无法互相伪造或篡改的效果。

跨链事务机制就是保证两个区块链上关联交易操作的原子性和事务性。

WeCross支持两种跨链事务机制实现。一种是两阶段事务机制，它是大家所熟悉的比如Mysql这样的数据库做分布式事务的首选，优势是通用性好，能适用于任何场景。另一种是哈希时间锁定，各位如果对闪电网络或者雷电网络这样的工业项目有所了解，就会很熟悉哈希时间锁定，它是一种专门用于数字资产间的事务机制，基于抵押模式实现，尤其适合数字资产交换。

这两种事务机制WeCross都支持，大家可以根据PPT里的简单时序图，了解实现的效果是让两个区块链上关联的交易同时发生、同时失败，理解到这个就可以了。

多边跨域治理所面向的场景不仅局限于两个区块链之间。

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。

业务方和监管方等相关机构可以共同搭建治理链，基于治理链聚焦权限、事务、监管和准入等功能。

虽然WeCross支持多个区块链间的交互，但随着区块链数量增长，区块链间两两互联的连接数量也会成倍增长。

多边跨域治理提出治理链的概念，一方面可中转多个区块链之间的跨链消息，另一方面提供了一些权限控制、事务管理以及监管准入的功能，监管机构可以通过治理链来介入和监管各个链间的交互。

WeCross核心优势

首先，WeCross是**开源开放**的，遵循微众银行“把源码丢出去，把信任建起来”的理念，所有源代码全部开源。基于透明的技术和理念，所有参与者都能检阅我们的代码，理解其实现，杜绝恶意作恶的情况。

WeCross对**开发友好**。实现了多语言版本SDK，并提供交互式控制台。即便不会写代码，用户也可通过控制台进行跨链逻辑操作和验证。浏览器也在WeCross的计划中，未来用户可通过浏览器，点击鼠标就可轻松管理多个区块链。

跨链和区块链底层在**安全可信**上，保持同样的高要求，WeCross为安全可信做的措施包

括：

- **加密**：WeCross所有跨链信息的交互都是加密的。
- **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。
- **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。

基于FISCO BCOS的实操演示

WeCross的代码已经正式开源，大家可以在代码仓库下载最新代码，查看技术文档。

github代码仓库：
https://github.com/WeBankFinTech/WeCross

gitee高速镜像：
https://gitee.com/WeBank/WeCross

环境需求

条目	要求	备注
CPU	2核或以上	
内存	2G或以上	
磁盘	20G或以上的空闲容量	
网络	10M或以上的网络带宽	
操作系统	Linux Kernel 2.6或以上	Ubuntu16.04或Centos7.3以上
运行环境	Java 1.8或以上	

WeCross对环境的需求如表所示，总体而言，对服务器环境、磁盘和网络的要求均不高。

操作系统目前支持Linux Kernel 2.6或以上，我们建议的操作系统最好是Ubuntu16.04或Centos7.3以上。WeCross基于Java开发，要求Java的运行环境。

支持的区块链底层框架

依赖项	版本	备注
FISCO BCOS	2.3及以上版本	需要FISCO BCOS的Merkle特性
Hyperledger Fabric	1.4版本	当前暂不支持2.0及更新版本

通过开源共建的方式，WeCross会逐步对接更多的区块链平台和应用，欢迎社区积极参与贡献。

组件构成

组件	说明	备注
WeCross	WeCross跨链路由	JAVA开发
WeCross-Java-SDK	WeCross Java版本的SDK	JAVA开发
WeCross-Console	WeCross命令行控制台	JAVA开发

实操演示如何快速支持多个区块链

此部分以FISCO BCOS为例，演示【搭建FISCO BCOS区块链→→启动区块链→→使用控制台，在区块链上部署合约→→拉取WeCross项目→→构建WeCross→→搭建WeCross→→WeCross Stub创建→→Stub连接和证书配置→→P2P与RPC配置→→查看WeCross日志→→发送交易】的操作流程。

相关解析已在演讲PPT中增补注释，步骤涉及较多代码，为方便学习，请直接下载演讲PPT查看。

演讲PPT下载：关注本公众号，对话框回复【**0331**】获取

直播互动精选

小伙伴讨论热情高涨，因篇幅有限，这里仅选取部分高频问题进行分享。我们建设有不打烊的【**微众银行区块链交流群**】，欢迎大家入群和我们深度交流。

入群方式：本公众号对话框回复【**小助手**】

Q：这个项目的目标区块链只能是联盟链吗?

A：是的，目前不支持公链。

Q：跨链操作涉及的链回滚问题是如何解决的?

A：如果在跨链事务中，某个区块链的交易发生了回滚，WeCross会按照跨链事务的机制对整个事务中的其它区块链进行回滚处理，具体的回滚方式与事务机制有关，两阶段事务中是向其它区块链发送rollback交易，HTLC事务中是让其它区块链超时。

Q：WeCross的账户系统和底层原生链的账户系统是什么关系?

A：WeCross的账户用于向区块链发送交易，与原生链的账户是等同的。

Q：WeCross更像是高安全可信的跨链网关吗？实现同构和异构链之间的链交互，WeCross属于中继跨链还是侧链?

A：可以这么理解，WeCross兼具中继链与侧链的模式。

Q：WeCross怎么多链锁定?

A：通过事务机制，向多个区块链发送lock交易。

Q：跨链系统的安全性是怎么设计的？如果受到攻击在跨链的时候，会影响其他区块链吗？

A：WeCross的跨链事务在两个区块链间发生，不涉及其它未参与事务的区块链，当任一个区块链出现异常时，仅影响与该链正在进行事务操作的区块链。

Q：跨链路由，在新链加入的时候或者旧链退出的时候，怎么更新跨链路由？这之间有同步机制？

A：跨链路由间有定时的自动状态同步和更新机制。

Q：WeCross异构链A机构怎么保证B机构不恶意篡改A合约上某人的资产呢？

A：WeCross跨链路由间有权限控制。

附：互动获奖名单

鱼翔浅底、S47734033、刘希诚、磐石、Thea

* 名称为微吼直播间昵称

长按二维码关注

微众银行区块链

白皮书下载 | 订阅干货 | 进群交流 | 合作联系