Middleware.web3

Sanchuan

2022-12-7

要解决什么人的什么问题?

- 1. 区块链项目方
- 2. 对链上用户的管理难，对相同项目在多链上管理较难的问题。

痛点1：链上用户管理难

- 一个NFT项目方，只需要部署一个合约，或者加一个静态前端。
- 如果要管理增量用户，白名单，会员，或者奖励社区积极成员。
- 需要动态的在链上批准。
- 如果想要设置服务器去审批权限，就需要构建一系列的工程，
  - 包括 用户管理面板、用户授权API，链端数据监控

解决

- 可以做成一套标准的中间件，连接 NFT的链下授权到链上验签。

痛点2：多链项目互相联动难

- 一个项目方，想要吸收多条链上的用户群体，扩大自己项目的知名度和影响力，常常会在多条链上部署同一种资产（Token或者NFT）
- 而如果要把多条链上分散的用户耦合起来，扩大项目的流动性。
- 就需要一套监控方案（A链锁定，B链新发行）
- 需要 部署 A链的实时监控，owner授权，B链结果监控。以及整体环节的后台管理面板。
- 对小型项目方更不安全。

解决

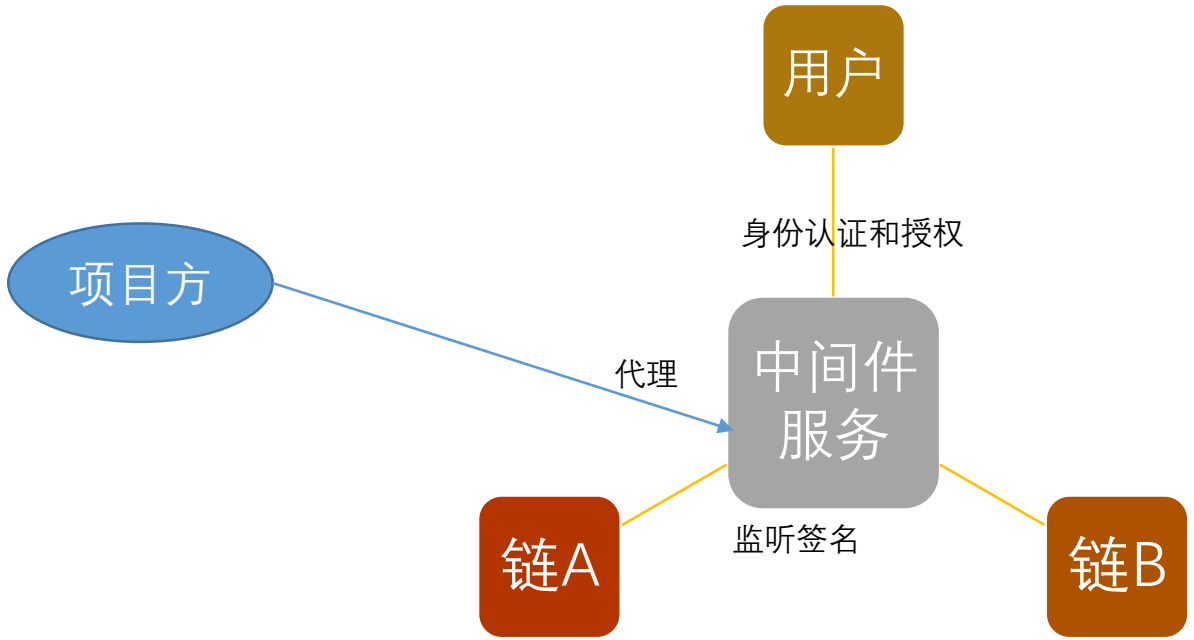
- 可以做成一套标准的中间件，连接 不同链上的资产。

整体方案：

- 针对以上的需求分析，项目方在进行项目管理时。

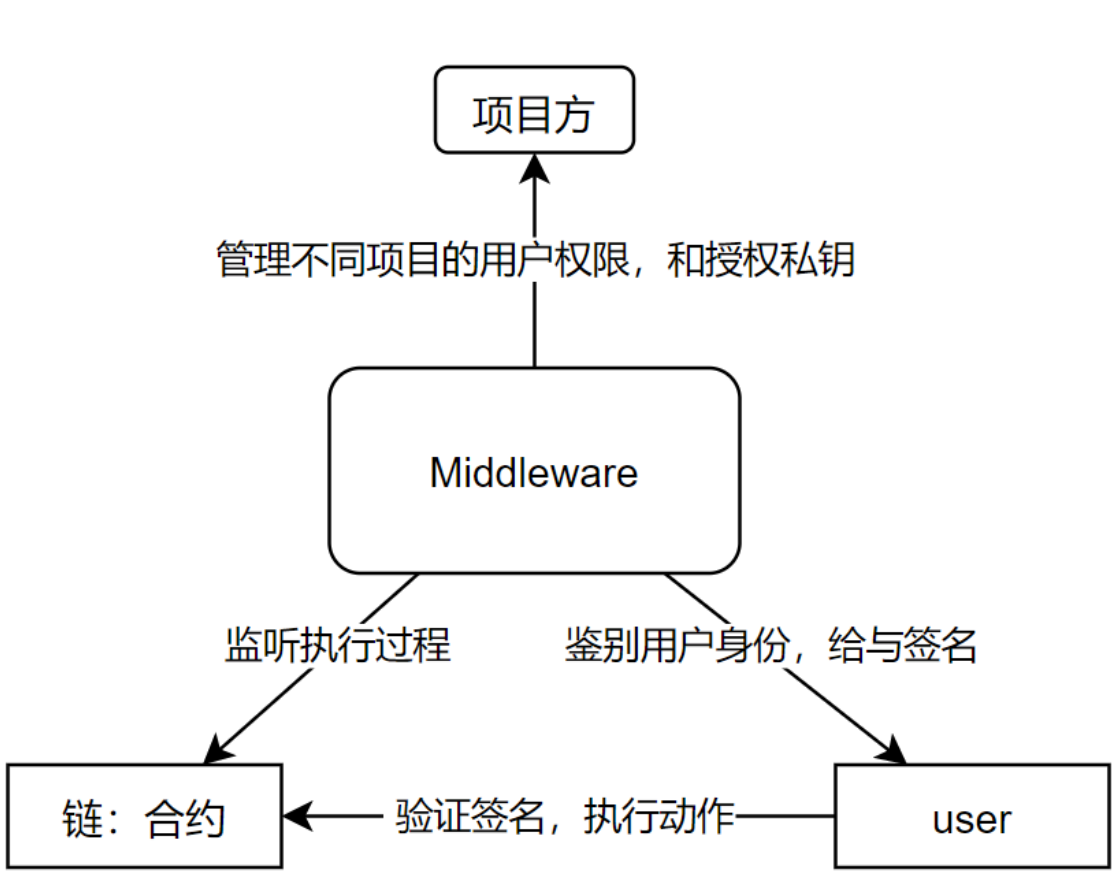
  针对链上用户的权限，需要一套中间件服务来动态维护。

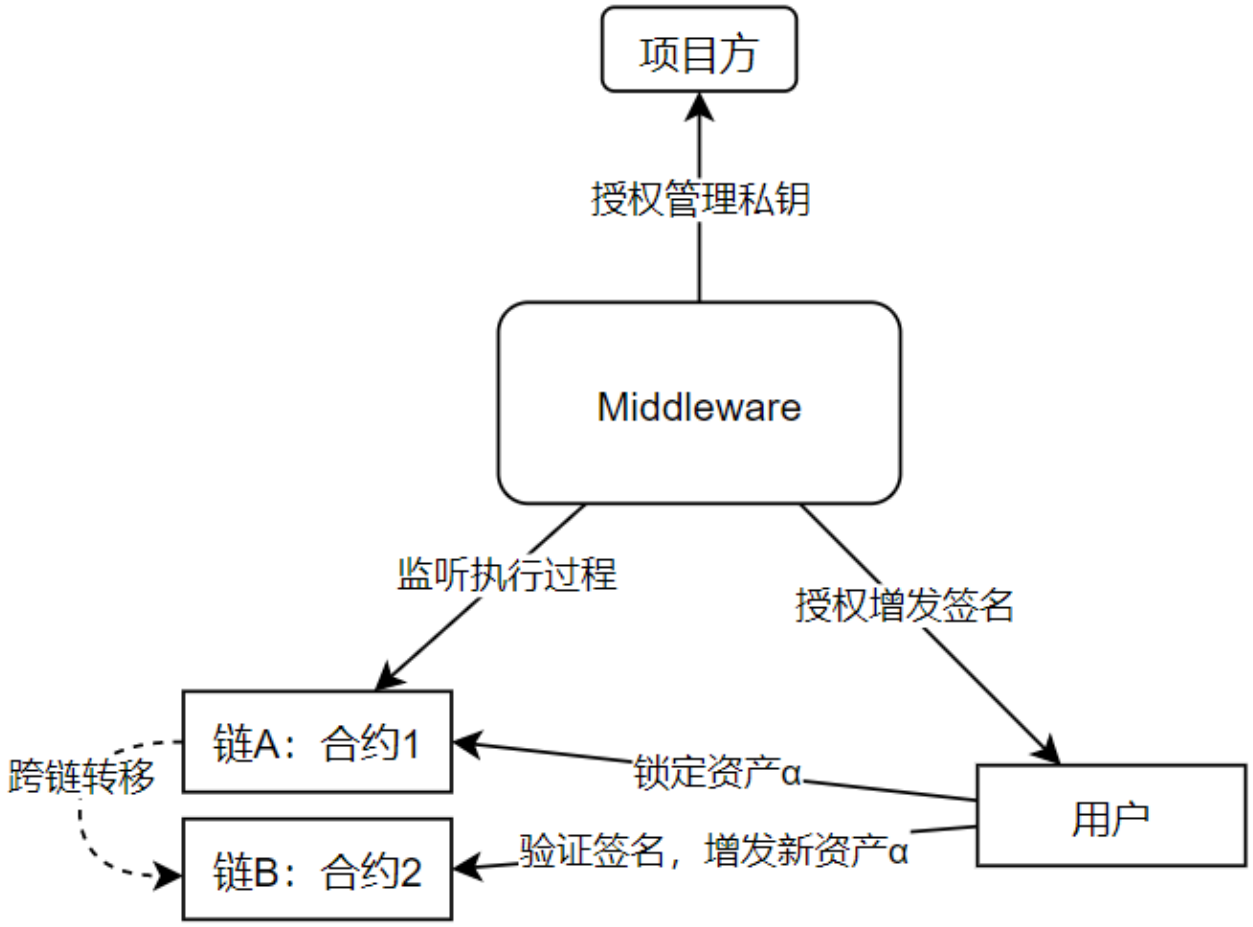
  针对多链上的资产跨转，需要一套中间件服务来实时管理。



这些中间件 作为项目方的代理，围绕一个项目的 链与用户，进行管理。这就是我们的标准化中间件服务。

实现方案


项目方
管理不同项目的用户权限，和授权私钥
Middleware
监听执行过程
鉴别用户身份，给与签名
链：合约
验证签名，执行动作
user


项目方
授权管理私钥
Middleware
监听执行过程
授权增发签名
链A：合约1
跨链转移
锁定资产α
用户
链B：合约2
验证签名，增发新资产α

网站

- **项目方**
- - 钱包登录
- - 用户管理
- 用户 权限 申请状态
- - 项目管理
- 添加项目 链信息

- 监听事件

- 授权秘钥
- - 兼容项目方官网
- API调用，跨站请求处理

- **用户**
- - 登录
- - 添加项目
- - 查看权限（白名单，首发）状态

- - 白名单 请求（钱包）
- - 选择项目 跨链操作

- **区块链**
- - 根据ABI生成 可监听列表
- - 监听链上的事件(subgraph)
- - 监听用户状态(subgraph)
- - 监听跨链流程进展

CrossEngine：微服务跨链互联的解决方案

针对NFT项目方和艺术家，实现同一个NFT项目的多链部署、NFT跨链转账、多链用户管理的后端数据引擎。

- 创作者友好：为多链，跨链，用户管理提供一个轻量的低成本方案；
- 价值认可：实现每一个NFT在所有链上都独一无二；
- 用户增长：让用户能把低成本链上的资产等价的跨到高认可度的链上；
- 成本降低：以通用的服务来降低成本，用规模管理来提高安全性；

微服务跨链方案的意义：

对项目方：

把一个项目以极低的成本部署到多条链生态中，
覆盖了多个社群，用户基数变大，需求潜力增多。

对用户：

多链的项目用户能自由选择车道，
让自己的资产在在低手续费链上流通，在高认可度链上保值。

对公链：

新公链能快速获得其他链的优质资产，
老公链能借助其他链充当潮汐车道，降低拥堵。

安全性：

替代现有的跨链总线方案，
每个项目的微服务容器作为中间件，相当于拥有一条跨链专线
使漏洞或黑客袭击问题隔离在一个沙箱中，避免造成整体风险。

需求：监控A链锁定合约的执行状态，以及B链铸造合约的执行状态
方法：用TheGraph监控并索引某个时间的历史数据

具体功能：

```
//添加事件,用以添加某个合约的事件
fun addEventOfContractAtChain(event, contract, chain) return event
//查询事件历史
fun findAllEvents(address, event,contract,chain) return event[]
// 查询某个交易的状态
fun getTxStatus(txIdx)
```

一个在多条链上部署的项目具有什么特点？

1. 团队实力强。
2. 项目规模大，用户多
3.

创建合约

钱包登录

选择NFT的类型参数模板

盲盒， mint价格，总量，其他

选择白名单管理方式

白名单折扣率 （ ）%

- Merkle树一次性白名单
- 动态添加白名单

是否跨链（）

选择目标区块链(多选)

- ☐ ETH
- ☐ BSC
- ☐ Solana
- ☐ Fantom
- ☐ Moonbeam

部署合约

跳转到合约监控面板

用户NFT跨链流程（从BSC链的x合约，跨链到ETH链的y合约）

1. 用户在BSC链的X合约中有一枚NFT
2. 调用FreezeCross函数冻结该NFT，并发出event
   该event 包含 { NFT ID，目标链ID，目标链接收地址 }
3. 微服务中的TheGraph监听到这个事件，去区块链上核对，记录到数据库
4. 微服务对Event内容生成一条 sign（event）作为凭证
5. 用户在网站上获得凭证，
6. 用户再以目标钱包调用ETH链的y合约unfreezeCross()
7. 函数首先验证微服务的签名是否有效，最后铸造跨链过来的这枚NFT，
8. 用户获得了一枚ETH上的NFT