存储分片

1. 技术背景

当前大多数区块链网络都是每个节点都要保存所有的历史数据，当节点数量超过一定量级时，会造成严重的资源浪费。且在数字化转型的大背景之下，可以让更多的数据流动起来，每个节点仅保存部分历史数据，并通过网络交互来获取需要的数据。本区块链平台存储基于 Kad 网络，分布式算法可以保证数据相对均匀的分布在区块链的各个节点上，同时新节点加入或者老节点宕机时数据可以做到自动调节局部数据的分布以达到新的平衡，保证数据的安全性。

1. 技术优势

本区块链平台每个节点的 p2p 模块都保存一对公私钥对，可以由用户导入或者节点自动生成，然后由该公钥生成节点 ID 作为网络中的唯一标识符。网络中的最新的 10000 个区块不进行分布式存储，可以提高查询效率以及应对区块数据回滚等情况。超过 10000 个块之后，每 1000 个块进行区块打包，并存储到网络中距离最近的 100 个节点上。（以上参数可以灵活配置）

本平台的存储分片技术，具备以下几点优势：

每个节点仅需要保存一部分数据，非常适合海量数据存储的场景，且可以随时增加机器实现动态扩容。

数据打包之后进行分布式存储，减少了数据的数量，避免数据过于碎片化增加网络负载。

每份数据存储 100 个节点时，在有一半节点宕机的极端情形下，数据丢失的概率仅为 1/2^100 ≈ 10^-30，因此数据可以做到安全存储。

前端定义了用户界面逻辑，前端会与智能合约中定义的应用逻辑进行交互。前端和区块链之间通过 JSON-RPC 通信。

Chain33 上的用户可以通过 MetaMask 或 WalletConnect 来管理自己的私钥和交易签名，当需要用户签署交易来登录平台或发送交易时，就会调用 MetaMask 或使用 WallectConnect 来签署。

为了节约区块链的存储成本，对于大文件（图片，音频，视频）采用分散的链外存储解决方案，如 IPFS。

通过 web3.js 库来查询和监听智能合约事件。可以监听特定的事件，并在每次事件被触发时指定一个回调，来实现前端和区块链智能合约间的事件交互。

智能合约完全兼容以太坊虚拟机（EVM），支持以太坊（或以太坊生态）链上的合约无缝移植。

支持使用以太坊生态的工具在 Chain33 上开发，比如可以通过 Hard-Hat,truffle，remix 等开发框架或工具更容易建立，部署和测试智能合约。