Mooda: 一个基于比特币可持续验证的数据可用层

简介

随着区块链技术的持续发展，各种各样的区块链喷涌而出，但随着参与的人越来越多，像比特币、以太坊这样的知名区块链上交易和数据日益增多，导致了网络拥堵，推高了交易的成本，这使得它们不得不提高每个区块的大小和区块的处理速度，来容纳更多的数据以满足发展需要。

比特币通过隔离见证（SegWit）将每个区块的大小从 1MB 提升到了 4MB，每个区块可以多处理两千笔交易，提高了比特币处理交易的速度，然后通过了主根（Taproot）升级优化了交易的大小，同时允许批量签名，使得交易更快，交易费用更低，进一步增强了比特币处理交易的效率也降低了比特币的使用成本。

新的升级带了新的发展，比特币的隔离见证和主根升级，提高了比特币区块的大小和处理复杂事务的能力，从而带来新的生态序数协议和铭文。铭文的快速发展，重新将比特币的区块给占满了，最大一个铭文可以独自占满整个区块，将比特币区块大小不够的问题再次暴露出来。但是区块大小并不能无限制扩展，更大的区块大小意味着需要更好的设备和更高的网络质量，这样可能会导致部分人放弃部署比特币节点，从而降低比特币去中心化的能力。

Mooda 是一个基于比特币的持续可验证的数据可用层，致力于在不牺牲安全性的情况下，提高比特币的存储效率，降低存储成本。通过将验证信息上链，线下验证节点确认的方式，向用户表明存储于可用层中的数据的可用性。

KZG 多项式承诺是由 Kate，Zaverucha 和 Goldberg 发表的多项式承诺方案。通常被称为卡特多项式承诺方案。在多项式承诺方案中，证明方计算一个多项式承诺（commitment）将这个承诺发送给验证方，证明方无法篡改当前计算的多项式，只能对当前的多项式提供有效的证明，验证方可以验证这个证明是否正确。

Mooda 实现

Mooda 是一个基于比特币的持续验证的数据可用层的实现方案，可以在不牺牲安全性的情况下提供更多的存储空间，能有效地降低使用比特币区块存储的成本。

Mooda 将数据的承诺放在比特币链上，同时周期性的向链上提交证明，链下通过索引器验证数据证明的正确性。

通过将数据承诺放在链上，可以公开的展示数据存放的地方以及方便后续验证时确认验证

数据的范围，

下面具体讲述如何实现：

服务端

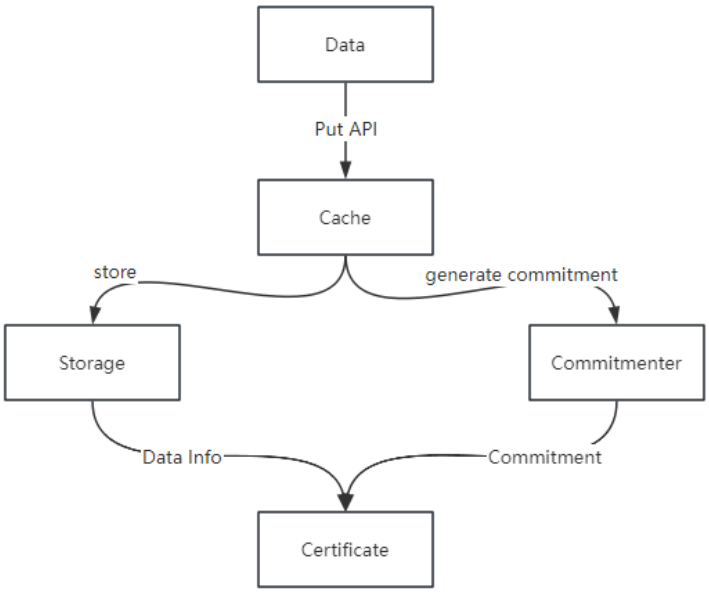
作为 Mooda 的服务端，会向用户提供上传，下载等服务，同时也会在后端提交数据承诺，以及周期性的提交周期信息和证明信息。

用户通过上传接口上传自己的数据，存储层会现将数据缓存然后根据数据，并根据文件内容生成一个哈希值，用以确保数据的唯一性和完整性，存储层将返回以下结构给用户用于后续的下载。

字段	类型	含义
id	字符串	数据 Hash
Size	整数	数据大小

上传响应

上传的数据会被分割成多个切片，通过就删码或者进行多个备份技术进行数据冗余，最大限度的保证数据的可用性。



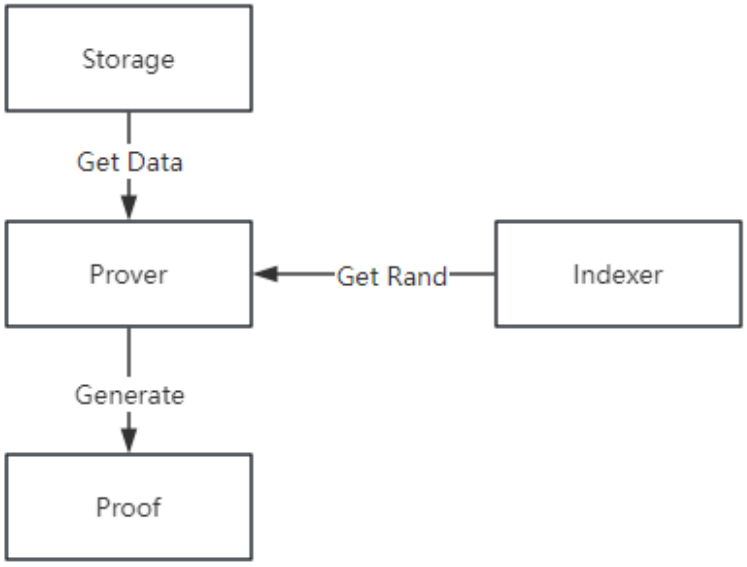
上传流程

周期与证明生成

为了实现可持续的验证，存储在每个周期高度都要对对应的数据生成可用性证明，用以证明当前周期内数据的可用性，当前周期如果有多个证明需要提交，则按照数据存储的先后顺序聚合这些证明，减少上链的消耗。

字段	类型	含义
Epoch	整数	周期
Proof	字符串	证明

证明生成器(Prover)在每个周期时，检查有哪些数据需要提交证明，再从 indexer 获取上次证明和本次周期的 hash 值，生成本个周期的证明。



证明流程

为了保证存储持续的存储了数据，每次提交的证明需要与上一次的证明以及时间相关，从而保证存储无法提前生成证明，而没有实际存储数据。

索引与验证生成

索引器检索比特币每个区块的内容，将符合要求的验证信息存储到本地，验证者在每个周期内验证信息信息的正确信性，判断存储中数据是否可用。

验证信息包括

1. 数据的承诺
2. 数据的证明
3. 随机数

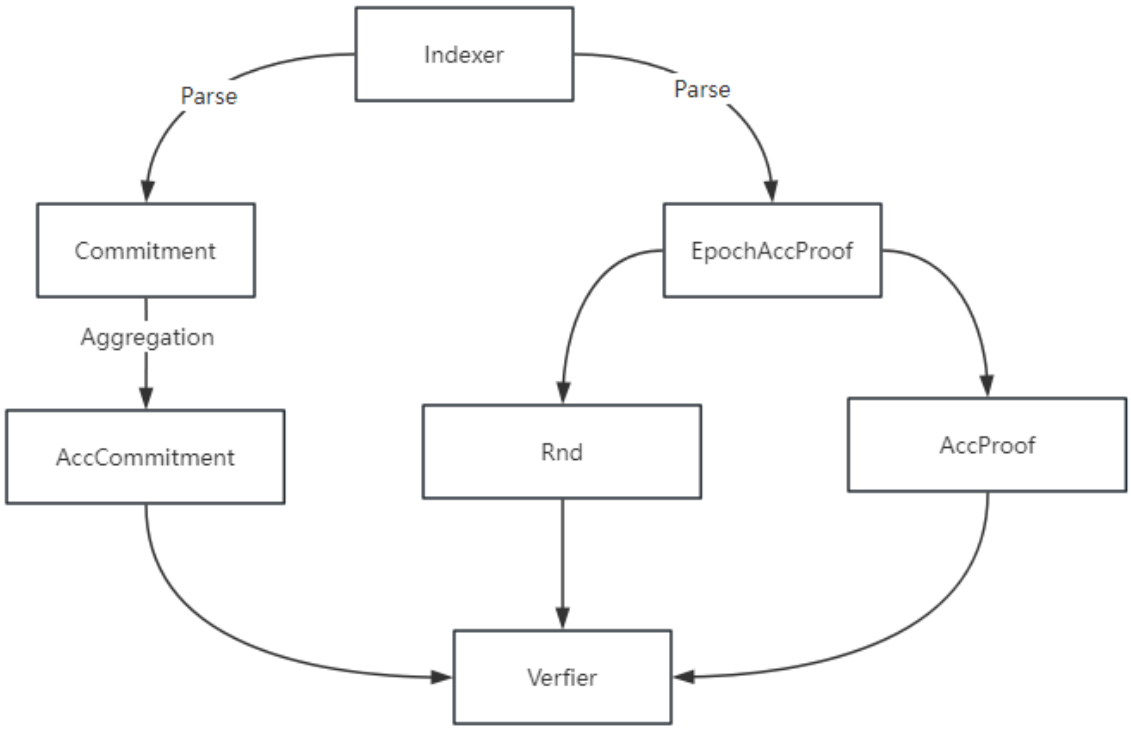
数据承诺是将本周期内所有有效数据的承诺，验证者通过筛选本周期内的有效数据承诺，通过先后顺序将承诺聚合成一个承诺

数据证明是存储证明端提交的本个周期内所有有效数据的证明

随机数是上次与数据证明与上链后的交易值的哈希

同时为了保证验证信息的准确性设计了以下规则

1. 证明的所有者为第一次发出证明的地址，不会因为转移而改变，避免将错误证明发给其他所有者的情况。
2. 证明的所有者需要与凭证中的签名相匹配，避免发生恶意提交错误证明的情况。
3. 所有者在同一个周期高度发送多个证明，以 收到的第一个为有效的证明。



索引验证流程

链上交互

Mooda 系统中目前所有的上链信息都采取以铭文的方式铭刻到链上，因为现有的铭文技术经受了时间的检验完全能够作为验证信息的存储方式，同时现有的成熟技术能够方便快捷并且安全的将验证数据存放到链上。

为此设计了一整套规则 BRC-985 协议，来规范 Mooda 中是用的凭证铭文和周期证明铭文