作者：黎连文@哈希数字

V1.0.0 Date:2019/07/05

区块链技术总结

|  |  |
| --- | --- |
| 类别 | 内容 |
| 关键词 | 区块链技术总结 |
| 摘 要 | 总结目前区块链出现的技术 |

**修订历史**

|  |  |  |
| --- | --- | --- |
| 版本 | 日期 | 原因 |
| V1.0.0 | 2019/07/05 | 创建文档 |
|  |  |  |

目 录

[1. Sms的使用 1](#_Toc8723610)

# 石墨烯

## Bitsahres

## Steem

## GXB

## YOYOW

## SEER

## CYBEX

## EOS

# Oracle

## ONT

## AE

## ChainLink

## OracleChain

## Qtum

# 隐私交易

## DASH

混币

## XMR

环签名

## Zcash

零知识证明

## Grin

MimbleWimble协议

# 去中心化存储

## FileCoin

FileCoin是IPFS的代币，IPFS是一个面向全球的、点对点的分布式存储文件系统，目标是为了取代目前传统的互联网协议HTTP。它将所有具有相同文件系统的计算设备连接在一起。原理**是用基于内容的地址取代基于域名的地址**。也就是用户寻找的不是某个地址而是存储在某个地方的内容，不需要验证内容的哈希，通过这样可以让网页的速度更快、更安全。

Filecoin 为存储和分发都做了设计。它的存储矿工用于存储场景，而检索矿工用于分发场景，但 Filecoin 更关注在存储上。

就 Filecoin 目前公布的资料，不论是白皮书还是代码，都没有提到和服务质量相关的想法。整个团队还在忙于基础建设工作，但不排除未来 Filecoin 会做 QoS 相关设计的可能性。

Filecoin 是直接一步到位完全去中心且完全开源的。

Filecoin 支持 PoRep（复制证明）和 PoSt（时空证明）。复制证明是指实际产生一次网络复制后所取得的证明；时空证明是一个文件占据了一定的空间，保存了一定的时间所产生的证明。Filecoin 是这两个证明的算法的提出者，在 Filecoin 的白皮书里，这两个证明算法的过程占据了 70% 以上的篇幅。

## SiaCoin

能够使一群互不信任的和互不了解的计算机节点联合起来成为一种有统一运行逻辑和程序的云存储平台。

优点：

数据共享迅速便捷，加密社区很稳定

缺点：

速度较慢，必须锁定资金才能使用网络设备数据

## Lambda

## Storj

功能与中心化的dropbox。Onedrive类似。Storj激励用户分享自己的剩余空间和流量以获得区块奖励，因为其充分利用用户资源，成本极低，并且数据采用冗余和端对端加密存储，更佳安全可靠。

Storj 是专注做存储场景的，它所有的设计都是为存储考虑的。

Storj 在白皮书和官方发布的文章中，也讨论过一些核心存储指标，比如耐用性（Durability）的测算，可以看出 Storj 对 QoS 有一定程度的关注。

Storj 目前除了 Token 是基于以太坊 ERC20 发行的去中心货币以外，存储的调度索引系统仍是中心化设置，目前不确定 Storj 后续是否会更加去中心化。

Storj 仅使用 ERC20 的 Token 来标识其存储节点的贡献，而平台本身没有区块链的支持。因此其客户端（Client/User）与存储节点（Storage Node/Miner）之间的交易是通过中心化的服务节点（Satellite）来完成。因此严格的说，Storj 并不是一个公链项目，是基于以太坊上一个应用。Filecoin 和 PPIO 则都拥有自己的链，并且不仅实现了价值在链上的流通，而且交易和证明也在链上完成，是真正意义上的基于区块链的存储和分发平台。

优点：

私钥加密，网络信息安全性高。

缺点：

网络倾向去中心化，而不是按照使用量数据量分配。

## Maidsafe

优点：

集存储，访问和交换数据为一体的互联网。

缺点：

很难被用户理解，而且开发速度太慢。

## Genaro

## PPIO

PPIO 和 Filecoin 一样，同时兼顾存储和分发，但更重点关注的是分发场景。PPIO 很快会在应用层增加流媒体输出能力，支持主流的点播和直播方案。

PPIO 是最注重服务质量的，PPIO 的所有设计也都是围绕 QoS 进行的。

PPIO 则选择逐步实现去中心化并逐步开源。

PPIO 也使用了 PoRep 和 PoSt 这两种更为严谨的算法。另外 PPIO 还自创了 PoD（下载证明）， 主要用于对多点下载数据的证明，这种算法对流媒体传输比较友好。PPIO 在白皮书中还提过一种 LPoC（轻量级容量证明算法），来做存储节点的冷启动。不过后来官方已经决定取消 LPoC了，原因是因为 LPoC 并不产生有价值的服务，而是像 BurstCoin 一样，在对硬盘资源做无畏地消耗，这点不符合做 PPIO 项目的初衷。

## Cryptyk

## 参考链接

【五种区块链存储项目对比，谁会更胜一筹？】<https://www.jianshu.com/p/2129872a2136>

【去中心化存储项目终极指南 | Filecoin, Storj 和 PPIO 项目技术对比（上）】<https://blog.csdn.net/PPIO_Official/article/details/88953281>

【去中心化存储项目终极指南 | Filecoin, Storj 和 PPIO 项目技术对比（下）】<https://www.cnblogs.com/elninowang/p/10695316.html>

# DAG

## ByteCoin

CryptoNote技术

## IOTA

## NANO

# 跨链

## 公证人

## 侧链

## 中继

## 哈希锁定

# 隐私计算

## ARPA

## Trias

## iExec

# 扩容方案

## Lay0

### BDN分发

### 组播锁定组

### QUIC UDP协议

## Lay1

### DAG

### 分片

## Lay2

### 侧链

### 子链

### 状态通道