Paradigm: Permanent Storage Layer for Limitless Scalability

Liu-Cheng Xu

Abstract

Paradigm 基于 Substrate 框架在 Polkadot 生态内构建了一个永久存储网络，支持 IPFS 等多种存储层协议，通过将文件哈希值记录在区块链网络并将文件存储在分布式网络中，为新的存储计算范式应用生态提供底层存储服务，实现对区块链的无限扩展。

Contents

1 引言

1.1 动机

1. 去中心化存储。
2. 存储计算范式。

从 Bitcoin 到 Ethereum, 再到今天的各种公链 Polkadot, Near, Solana 等，基于区块链的计算能力已经得到了长足的发展，但是基于区块链的分布式存储技术尚未得到广泛应用，仍然处于早期阶段。

基于区块链的分布式存储天然具有不可篡改和数据追踪特性, 数据没有单点故障的风险。

1.2 文章组织

2 相关工作

2.1 Filecoin

Filecoin 旨在作为一个经济激励层解决去中心化 **P2P** 网络 **IPFS** 所面临的存储激励与效率问题 [1]。**Filecoin** 采用了基于零知识证明的复杂密码学技术证明矿工真实存储了用户数据, 用户可以随时挑战数据证明保证网络正确存储了文件。

由于生成零知识证明对硬件的计算能力要求非常高，成为 **Filecoin** 的矿工具有很高的门槛。为了抵御各种攻击，**Filecoin** 对存储的文件都需要经过"密封"才能被正确存储，受到算法限制，封装 **32G** 文件需要接近两个小时, 文件存储的实际成本很高。存储矿工为了尽可能地最大化挖矿收益，不可避免地在网络中存储了大量的垃圾数据，如何在网络中存储有意义的文件仍然是一个难题。

2.2 Crust

Crust 是一个基于波卡生态的分布式存储网络, 愿景是构建一个注重数据隐私和主权的分布式云生态系统 [2]。不同于 **Filecoin** 的复杂密码学方案，对于如何保证矿工持续地正确存储了用户文件这个问题，**Crust** 采用了硬件层面的解决方案 **TEE (Trusted Execution Environment)** 。每个存储节点必须要先通过 **TEE** 进行注册，**TEE** 模块定期检查并汇报本地文件的存储情况。

相比于 **Filecoin, Crust** 的矿工硬件门槛较低，但是仍需要绑定能够支持 **TEE** 功能的特定硬件, 受上游硬件厂商的影响较大。

2.3 Arweave

Arweave 是一个致力于提供数据永久存储的去中心化存储网络 [3]，采用 **PoW** 加 **PoA** 的新型机制激励节点尽可能地存储更多文件以获得更高的出块概率。基于现代计算机存储的硬件成本每年下降 **30%**，并且这一趋势可预见性地将维持数百年，**Arweave** 通过预收未来存储费用来实现一次性付费，永久存储文件的特性。

2.4 Polkadot

Polkadot 是一个将多个专注特定领域的功能型区块链在同一个网络框架中实现互联互通的下一代区块链协议 [4]。**Polkadot** 基于首个区块链开发框架 **Substrate** 实现，其提供的无分叉升级可以让区块链网络实现快速更新迭代，链上治理极大地简化了区块链协议升级的复杂度。

Polkadot 提供的共享安全机制，让特定领域的功能型区块链可专注于其业务逻辑而不用关心共识安全, **Paradigm** 希望以平行链的方式接入到 **Polkadot** 网络，将平行链节点间的共识安全交由中继链负责，自身主要负责平行链存储节点间的激励证明机制。

2.5 Everpay

3 系统设计

3.1 经济系统

3.1.1 永久存储成本

$$P_{GBH} = \frac{HDD_{price}}{HDD_{capacity} * HDD_{mtbf}} \tag{1}$$

其中

- P_{GBH} =: 1GB 数据在 HDD 硬盘上存储一小时的价格
- HDD_{price}: 当前市场购买一个 HDD 硬盘的最低价格
- $HDD_{capacity}$: 硬盘容量
- HDD_{mtbf}: 硬盘损坏的平均时间

3.1.2 存储交易手续费

$$TX_{permacost} = TX_{data\_size} * Sum \tag{2}$$
$$TX_{bandwidthcost} = TX_{data\_size} * C_{network\_per\_byte} \tag{3}$$
$$TX_{reward} = TX_{permacost} * C_{fee} + TX_{bandwidthcost} \tag{4}$$
$$TX_{total} = TX_{permacost} + TX_{reward} \tag{5}$$

其中

- $TX_{permacost}$ 在网络中永久存储该笔交易的总成本
- TX_{data_size} 交易的数据大小 (以 GB 为单位).
- $TX_{bandwidthcost}$ 传输数据的带宽成本
- TX_{reward} 打包交易的即时奖励, 会立即打给矿工
- TX_{total} 用户支付网络的总费用

3.1.3 节点抵押

每个用户都可以通过抵押一定的系统代币成为节点，节点负责打包区块并向全网提供数据存储服务。

节点抵押用于维护网络稳定，当节点持续因为没有 **recall block** 而导致漏块则进行相应的惩罚，允许节点间歇性部分漏块，但是不允许持续大面积漏块，考虑是否能够采用概率估算节点的实际存储覆盖率。节点抵押量同时决定节点能够持续打包数据交易的大小。

3.1.4 节点奖励

预收费用大部分进入资金池, 按需发放。TODO

3.1.5 多币种支付

用户可以通过 aUSD 等稳定币支付手续费。

3.2 共识机制

3.2.1 PoA

PoA, Proof of Access 是 Arweave 首先提出通过在 PoW 共识中融合一个随机的历史回忆块, 用以激励矿工在进行算力竞争的同时尽量多地存储文件。矿工能够挖出新块的概率除了与矿工算力占全网算力相关，同时与其存储了新块所关联的回忆块概率相关。为了最大化挖矿收益，矿工除了要增加自身的挖矿算力，同时还要尽量提高自身的存储能力。

$$P(\text{win})_{\mathbf{poa}} = P(\text{has recall block}) * P(\text{finds hash first}) \tag{6}$$

3.2.2 PPoA

Paradigm 基于 PoS 共识，节点的出块顺序将采用 Aura 或者 Babe 共识算法，同时融合 Proof of Access 的一个变种: PPoA, Pure Proof of Access, 节点挖出新块的概率仅与本地是否存储有新块所关联的回忆块。

$$P(\text{win})_{\mathbf{ppoa}} = P(\text{has recall block}) \tag{7}$$

3.3 新区块产生步骤

如何产生新区块:

1. 收集 recall block 元数据
2. 收集交易
3. 生成 Block Data Segment(BDS)
4. 打包区块并广播 BlockShadow

4 路线图

1. 实现 PoS 版的 Arweave，打造面向 DAPP 的永久存储网络
2. 依托波卡跨链生态，构建存储计算范式生态，打破区块链边界实现无限扩展
3. 支持除 IPFS 外更高性能的存储层，实现面向通用数据存储的永久存储网络

5 总结

5.1 未来工作

- 文件分享
- 文件删除
- 文件隐私
- 内容审查
- 存储计算范式生态

References

[1] Protocol Labs, Filecoin: A Decentralized Storage Network, https://filecoin.io/filecoin.pdf.

[2] https://crust.network/

[3] Sam Williams, Viktor Diordiiev, Lev Berman, India Raybould, Ivan Uemlianin. Arweave: A Protocol for Economically Sustainable Information Permanence.

[4] Gavid wood. Polkadot: Vision for A Heterogeneous Multi-chain Framework. https://polkadot.network/PolkaDotPaper.pdf

A 附录

A.1 回忆块

$$BH_{recall} = BHL[B_{indep\_hash} \mod B_{height}]$$

recall block 的块高为当前块哈希对当前块高取模，那么 recall block 的范围为 $[0, Height)$

A.2 FAQ

与 Filecoin,Storj 等项目的区别?

Paradigm 在路线图的第一阶段并不是致力于成为一个通用型存储平台，而是关注为新的存储计算范式 DAPP 提供一个中间件，提高区块链的可扩展性。

与 Arweave 的区别?