

Blockchain Research

于皓翔 PB23000055

2025 年 3 月 23 日

第一章 介绍

1.1 区块链原理

区块链是一种分布式账本技术 (DLT, Distributed Ledger Technology), 其核心目标是确保所有交易记录的安全性、透明性和不可篡改性。它的基本单位是区块 (block), 多个区块按照时间顺序链接形成区块链 (blockchain)。区块链的核心原理主要围绕去中心化、分布式账本、共识机制、加密技术展开。

1.2 IPFS

IPFS (InterPlanetary File System, 星际文件系统) 是一种去中心化的、分布式的文件存储和共享协议。它的目标是取代传统的 HTTP 协议, 使互联网更高效、持久, 并降低存储成本。IPFS 采用内容寻址 (Content Addressing)、去中心化存储和 P2P 传输

1.3 分布式文件系统

分布式文件系统 (DFS) 是一种将文件存储在多个物理或逻辑上分布的服务器上的系统, 允许用户像访问本地文件一样访问远程存储的数据。DFS 旨在提高数据的可用性、可靠性、扩展性和容错性, 广泛应用于大规模数据

存储、云计算和分布式计算环境。

1.4 结合的技术路线

区块链的优点在于它能够保证数据的安全性，无法被篡改，但对资源的消耗较大，将文件都存储在区块链上带来的消耗是很难接受的；分布式文件系统能够适用于大规模的数据存储，更适合与网络相结合的场景，但相对来说更容易受到攻击。

为了解决这个问题，我们可以将区块链和分布式文件系统通过 IPFS 结合起来，做一个混合式文件系统，具体的构想是区块链存储 IPFS 得到的文件的哈希值，文件本身由分布式文件系统进行存储。这样从系统重取出文件时，通过重新求文件的哈希值并和区块链上存储的哈希值进行比对，就能够发现文件是否被篡改。这样保证了安全性，同时也能够大规模存储。

第二章 参考文献

1. <https://assets.pubpub.org/d8wct41f/31611263538139.pdf>
2. <https://www.zhihu.com/question/434202066/answer/3361354532>
3. https://en.wikipedia.org/wiki/InterPlanetary_File_System
4. <https://github.com/sjqzhang/go-fastdfs>