filecoin基础及开发网络实战

先河系统 CTO 杨尉

2019年3月16日

自上而下逐层分析，从抽象到具体

抓住本质分析，
理解设计者意图。

概念

核心通用语言理解

开发网络实战使用

filecoin 源码顶层架构分析

go-filecoin

rust-fil-proofs

网络层

协议层 / (REST&CMD)

内部 API 层

core 服务层

1 IPFS 基础
2 libp2p 基础

1 hello 协议
2 存储协议
3 检索协议
4 心跳协议
.....

1 REST
2 CMD

1 core api
2 porcelain api
3 plumbing api

1 Message pool
2 Chain store
3 Processor
4 Block service
5 Wallet
.....

自下而上反向总结，从具体到抽象

提纲

1 filecoin的是什么

2 filecoin的设计目的

3 filecoin与IPFS的关系

4 filecoin网络中的角色

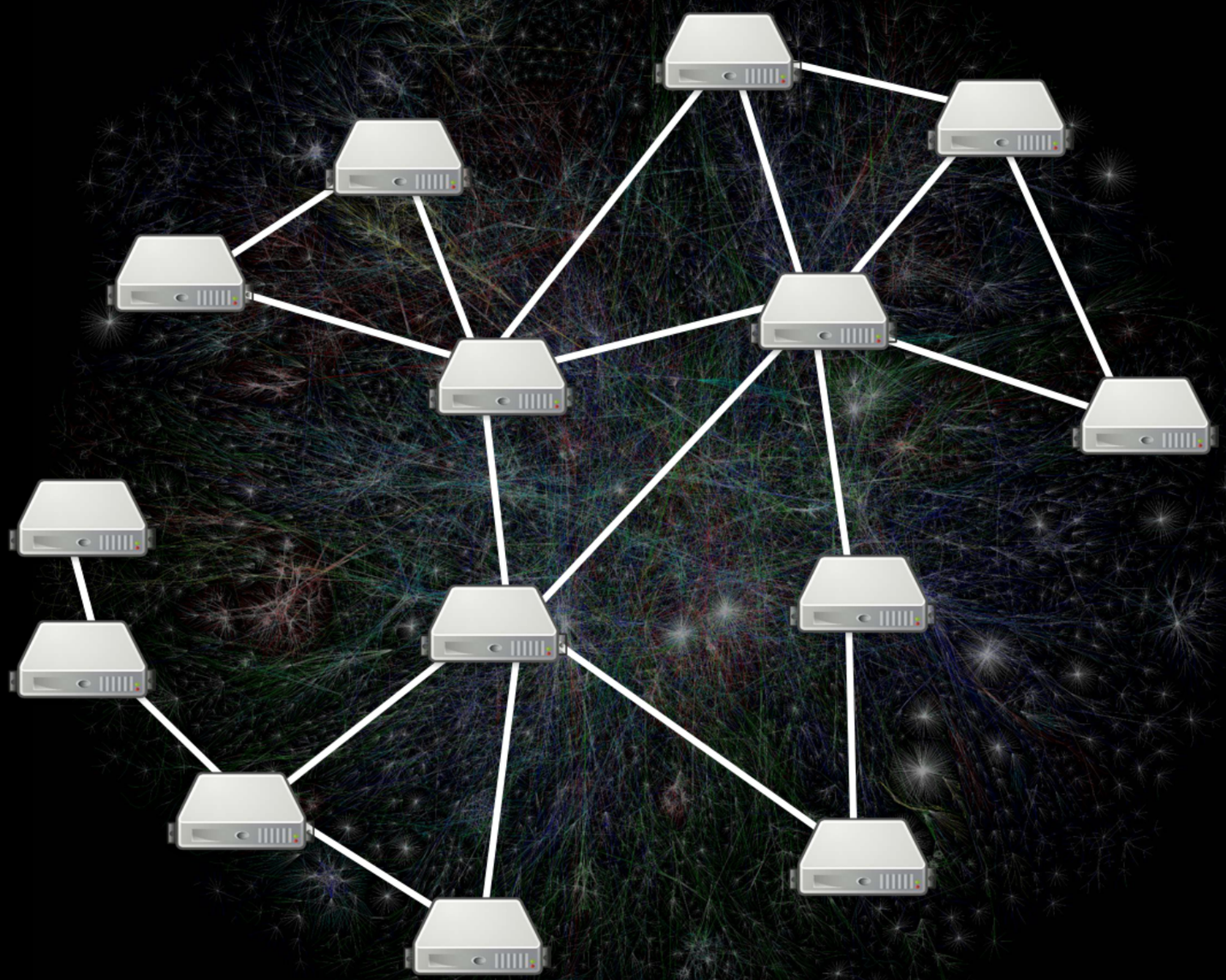
5 filecoin核心概念理解

6 filecoin开发网络实战

1 filecoin是什么

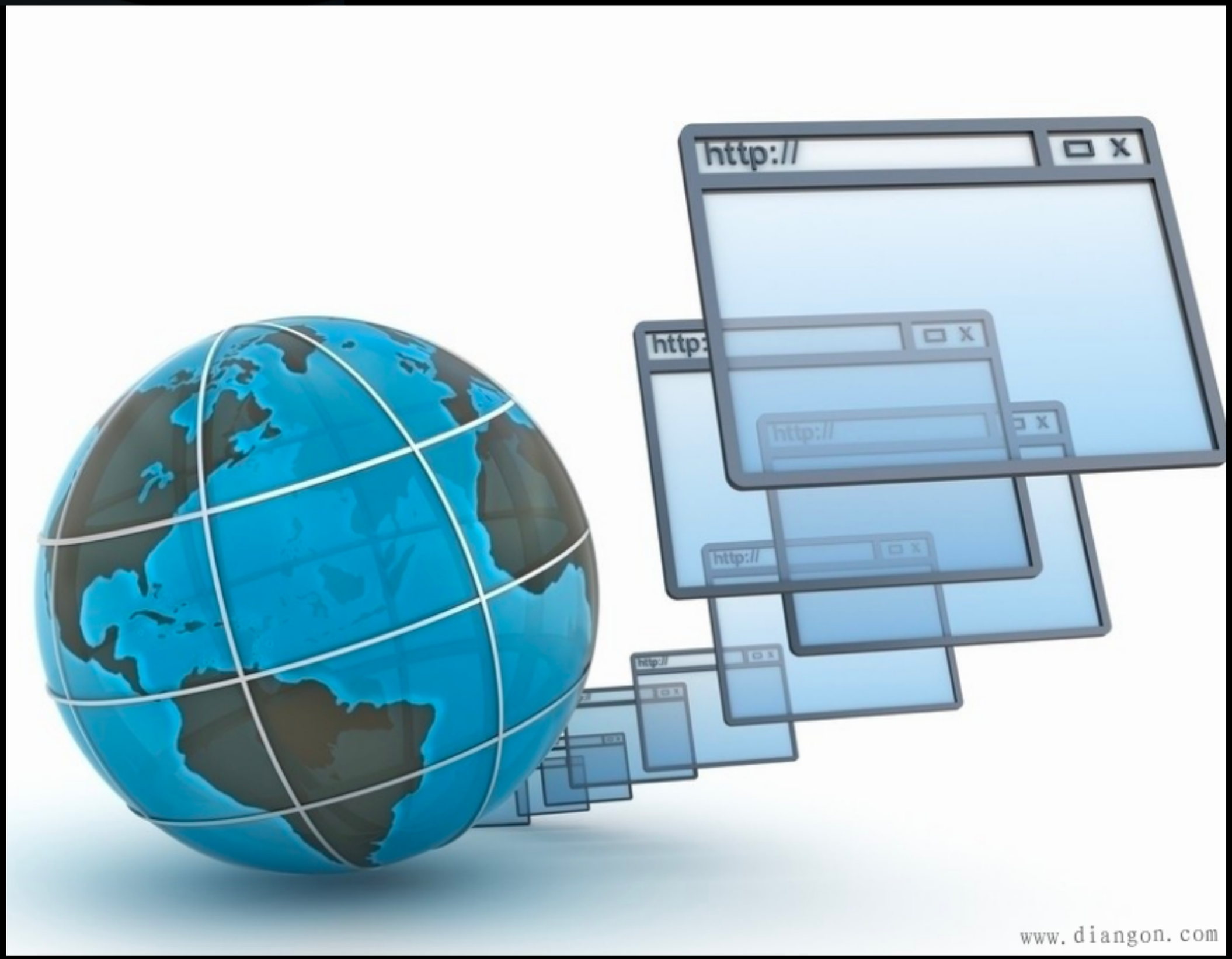
Filecoin

DSN



Filecoin 市场

Filecoin 协议



Filecoin

Toke
n

2 filecoin的设计目的

- 面向存储领域，以超高竞争力提供存储服务
  - 低成本
  - 高可靠
- 符合激励相容的设计
  - 各参与方的优势策略是提高filecoin网络服务质量
  - 参与方包括投资人、客户、矿工、开发人员
- 灵活的存储策略
  - 冗余
  - 检索速度
  - 成本

3 IPFS与filecoin的关系

类别	IPFS	Filecoin
功能	基于内容寻址的分布式存储基础设施	IPFS网络之上的激励层，提供一个云存储领域的自由交易市场
对标对象	HTTP	大型集中式孤岛存储提供商，如国外的aws、国内的aliyun等
存储权限	对有所有权的IPFS节点具备存储权限	1 除对有所有权的IPFS节点具备存储权限外 2 还可以通过支付的方式，在其供应商的节点之上具备存储权限
读取权限	ALL（只要知道内容cid）	ALL（只要知道内容cid）
架构设计	另行文章补充分析	原则上需要无缝对接到IPFS 1Filecoin将IPLD用于区块链数据结构 2 Filecoin节点使用libp2p建立彼此的安全连接 3 节点和Filecoin块传播之间的消息传递使用

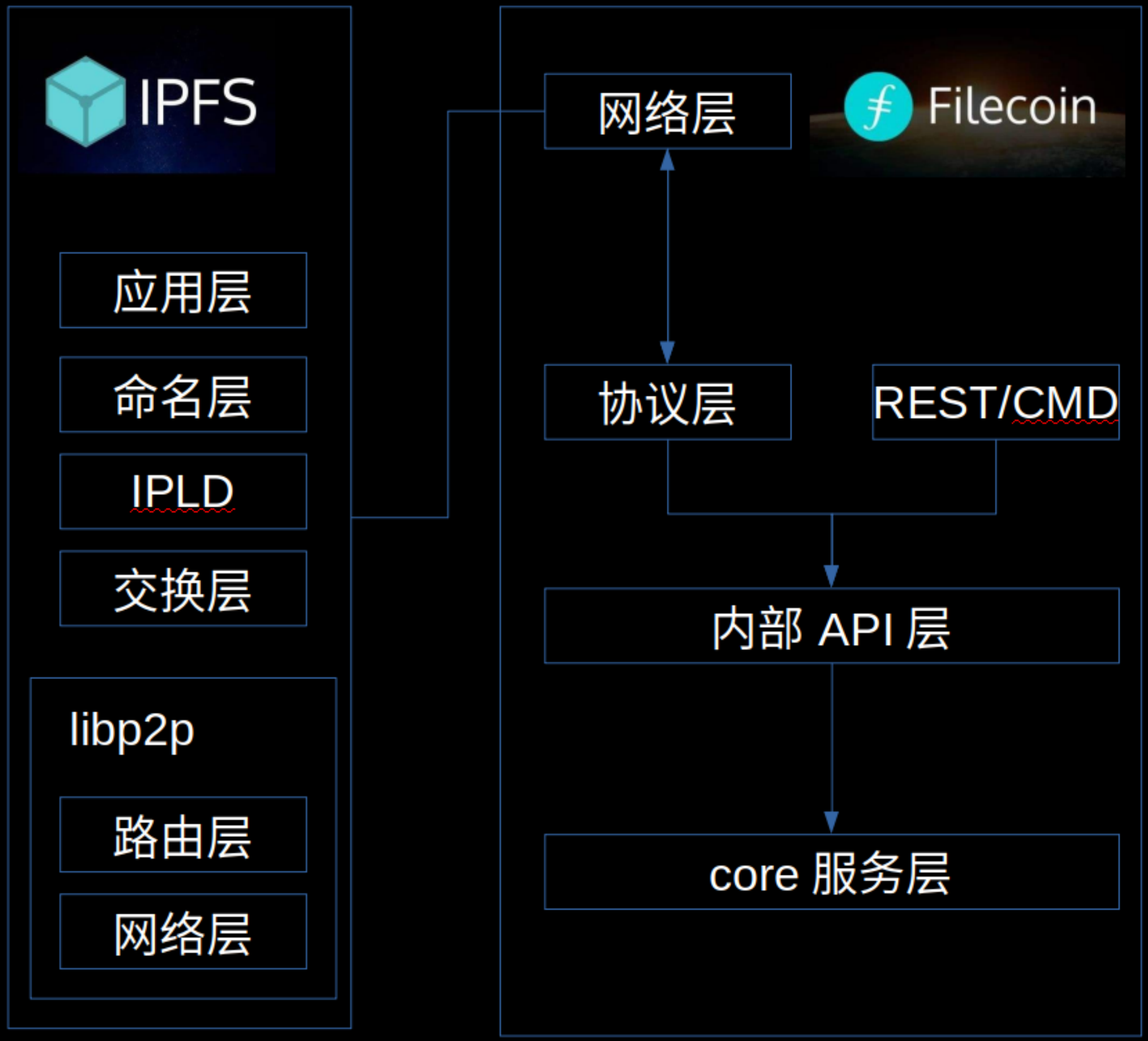
3.1 IPFS的竞争对手

特点	HTTP	IPFS
寻址方式	位置寻址 一维寻址，低效、脆弱	内容寻址 多维寻址，高效、稳定
效率	低效	高效
稳定性	脆弱	稳定
开放性	封闭、垄断	开放、共享

3.2 filecoin的竞争对手

特点	传统云存储提供商（大型集中式孤岛存储网络）	Filecoin
网络模式	集中式	DSN
加入门槛	高，从硬件底层基础设施、一直到软件、服务的提供，小企业很难插足	低、自由交易市场，Filecoin做好基础设施
宏观视野：闲置存储空间	高	低
价格	昂贵，垄断、可人为保持高水平	便宜，自由竞争市场
安全性	差，破坏隐私 1 云存储上可查看用户隐私，甚至密码明文存储 2 单个提供商的故障影响大	强 1 无中心，文件加密安全得到保障 2 单个云提供商的故障小

3.3 IPFS与filecoin技术架构层面的关系



4 filecoin网络中的角色

角色	说明	主要 影响因素
存储 矿工	存储矿工通过为客户存储数据来获得Filecoin； 获得区块奖励和交易费用的概率与矿工对Filecoin网络的存储量成正比需要存储：1 客户密封数据、2 区块数据	存储容量
检索 矿工	检索矿工的带宽和交易的出价/响应时间，将决定其在网络上检索交易的能力，数据来源：1 存储热门数据、 2 同时做存储矿工或者从其他存储矿工获取、 3 不限于从filecoin网络、可以从整个IPFS网络中获取	带宽
检索 客户	支付filecoin获取检索服务	
存储 客户	支付filecoin获取存储服务	

4.1 filecoin矿工的收益类比

收益来源	类比分析
提供存储服务	存储矿工类似于股份公司股东，有效存储类似于出资份额，收益来自两部分 1 工资（提供存储并收取服务费用） 2 按照出资比例分红（区块奖励就是按照有效存储占比来实现的）
提供检索服务	检索矿工是offchain的、全球分布的，不参与挖矿，收益来自 1 工资（提供检索并收取服务费用）

4.2 选择filecoin的理由

企业用户	1 技术先进性 2 数据安全 - 抵押机制、声誉系统 - 多供应商间修复 - 灵活的安全选择策略 3 价格低廉 - 闲散资源利用 - 全球性去重
个人用户	1 免费云时代的可能性？ - web 2.0网站的主要内容分发模型，网站所有者为基础设施服务付费，以免费向其用户提供数据，然后以其他方式通过内容获利 2 内容创作者，探索各种新的内容分发和经济模型

5 filecoin核心概念理解

- 从技术的角度来说说，filecoin包含如下两个维度。

- 1 分布式存储解决方案
  - 存储矿工
  - 检索矿工
  - 存储客户
  - 检索客户

- 2 区块链项目
  - filecoin公链
  - filecoin actors 智能合约

核心组件	目的
DSN	保障数据安全、包括故障容错、数据完整性、数据可恢复等
存储证明	证明矿工按照协议规范存储了客户指定的数据，数据有效性
可验证市场	对矿工与客户组成的交易市场进行了建模，保证交易的有效性
有效工作量证明 (预期共识)	出块的共识机制，很重要，做到激励兼容

5. 1 存储证明

5.2 共识机制

5.3 智能合约

5.4 交易市场

5.5 filecoin节点

5.1 存储证明

Proof-of-Storage包含复制证明(PoR)和时空证明(PoSt)，其作用主要有两点：

- 证明矿工做了有效存储
- 竞争区块打包出块，获取区块奖励

为什么使用存储证明

- 相对于PoW(Proof-of-Work)或者PoC
  - PoW耗能严重；PoC以空间换时间，同样存在耗能严重问题
  - 而filecoin网络的耗能必须远低于类似比特币的PoW，filecoin必须实现以更低的成对去应对商业竞争，同时提供相同级别的安全性，以及文件存储的效用
  - 存储证明需要做要与实体经济挂钩，减少无谓浪费
- 相对于PoS(Proof-of-Stake)
  - Proof-of-Storage在定向领域（分布式存储）以更简单方式，协调激励，并驱使矿工以有竞争力的价格提供真实的新存储，它促使矿工积极保证filecoin网络的效用

攻击类型	说明	阻止攻击原理
女巫攻击Sybil attack	作恶节点创造多个女巫身份，谎称存储了多个副本	每个节点的副本都是有签名的，想通过复制证明，就相当于真实做了有效存储
外包攻击 outsourcing attacks	作恶节点快速从其他节点获取内容，谎称他们存储了比他们实际存储更多的内容	针对外包攻击，从其他节点获取的整个过程，满足不了证明人随机挑战的要求，依然需要重新生成副本（重新seal需要时间），从而阻止外包攻击
生成攻击 generation	作恶节点宣称将要存储超过其实际容量的内容但并未存储内容，以此增加出	宣称无用，存储证明一定要确认密封动作并能应对随机挑战才能OK，如果重新密封就

复制证明与时空证明

- 复制证明本质上可以理解为一种零知识证明，既然是零知识证明，我们在后面需要理解filecoin复制证明的题目和答案

zk-SNARK zero knowledge Succinct Non-interactive ARgument of Knowledge

zero knowledge：零知识，即在证明的过程中不透露任何内情

succinct：简洁的，主要是指验证过程不涉及大量数据传输以及验证算法简单

non-interactive：无交互。

- 生成证明的方法在filecoin架构中称之为seal密封

密封过程是需要时间的，Seal过程串行加密的过程，无法并行操作，seal密

- 矿工的节点公钥、密封公钥、存储公钥、原始Data哈希、该矿工存储的副本根哈希

filecoin复制证明的题目和答案

- 隐含因素理解：
  - 特有节点的副本哈希是由哪些哈希组成（DAG），任意挑战者或者攻击者是不知情的
  - 挑战随机参数，通过CRH(防碰撞的哈希散列Collision-resistant hashing)生成哈希之后传递
  - 给证明者，作用是确定特定的叶子节点的哈希，比如让证明者自行计算离H(c))最近的叶子节点哈希。

- 复制证明的题目与答案
  - 挑战参数：副本哈希rt，挑战随机参数c -> H(c)
  - 证明者输入（题目）：
    - H(c)（每一次挑战都会变）

时空证明

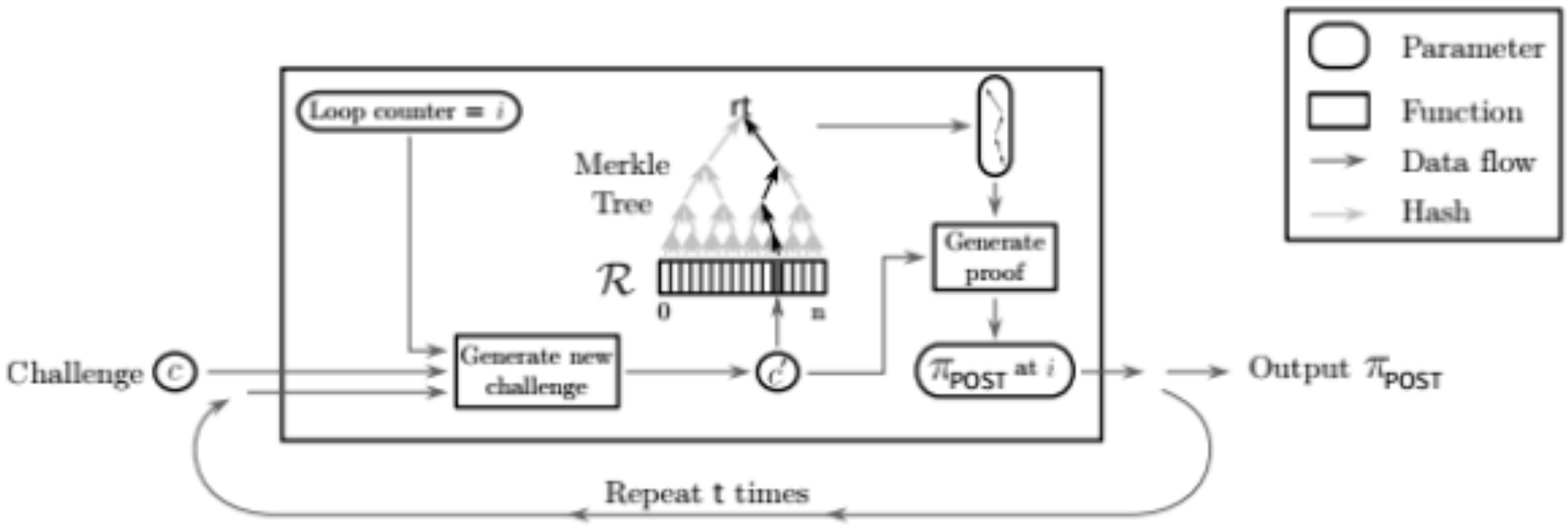


Figure 3: Illustration of the underlying mechanism of PoSt.Prove showing the iterative proof to demonstrate storage over time.

5.2 预期共识

power 属性	说明（filecoin基于有效存储来提高出块概率，赢得选举的概率与每个矿工分配的存储成比例）
公开	1 某一时刻，整个网络存储总量是公开的 2 单个矿工某一时刻，有效存储总量是公开的
可公开验证的	对于每个存储任务，矿工都需要生成”时空证明“，证明持续提供服务。通过读取区块链，任何人都可以验证矿工的power声明是否是正确的。
变化	在任意时间点，矿工都可以通过增加新增扇区和扇区补充的抵押来增加新的存储。这样矿工就能变更他们能提供的power。

$$\mathcal{H}\left(\langle t||\mathsf{rand}(t)\rangle_{\mathcal{M}_i}\right)/2^L \leq \frac{p_i^t}{\Sigma_j p_j^t}$$

EC Election

Storage Miner at epoch t

$\mathsf{ProveElect}(r, t, \mathcal{M}_i) \rightarrow \{\perp, \pi_i^t\}$

1. Compute $\mathcal{H}(\langle t||r\rangle_i)/2^L \leq \frac{p_i^t}{\Sigma_j p_j^t}$
   - on success, output $\pi_i^t = \langle t, r\rangle_i$
   - otherwise output $\perp$

Network node on receiving a block at epoch t

$\mathsf{VerifyElect}(\pi_t^i, t, \mathcal{M}_i) \rightarrow \{\perp|\top\}$

1. Check if π_i^t is a valid signature from user $\mathcal{M}_i$ on t and r
2. Check if p_i^t is the power from $\mathcal{M}_i$ at time t
3. Test if $\mathcal{M}_i$ is elected leader $\mathcal{H}(\pi_i^t)/2^L < \frac{p_i^t}{\Sigma_j p_j^t}$
   - on success, output $\top$
   - otherwise output $\perp$

Figure 13: Leader Election in the Expected Consensus protocol

选举方案属性	说明
公平	每个参与者每次选举只有一次试验，因为签名是确定性的，而且t和rand(t)是固定的。随机值rand(t)在时刻t之前是未知的
保密	有能力的攻击者不拥有Mi用来计算签名的秘钥
公开可验证	当选Leader i ∈ Lt 可以通过给出t，rand(t)，H(i)/2L，来说服一个有效的验证者。鉴于前面的观点（复制证明与时间证明），有能力的攻击者在不拥有获胜秘密秘

- 文件合约

5.3 filecoin actor

允许用户对他们提供的存储服务进行各种编程，从而形成一个多样化市场。

- 承包矿工：客户可以提前指定矿工提供服务而不参与市场
- 付款策略：客户可以为矿工设计不同的奖励策略，例如合约可以给矿工支付随着时间的推移越来高的费用
- 票务服务：合约可以允许矿工存放token和用于代表用户的存储/检索的支付
- 更复杂的操作：客户可以创建合约来运行数据更新

- 智能合约

用户可以将程序关联到其他系统（如以太坊)的交易上，他们不直接依赖存储的使用。

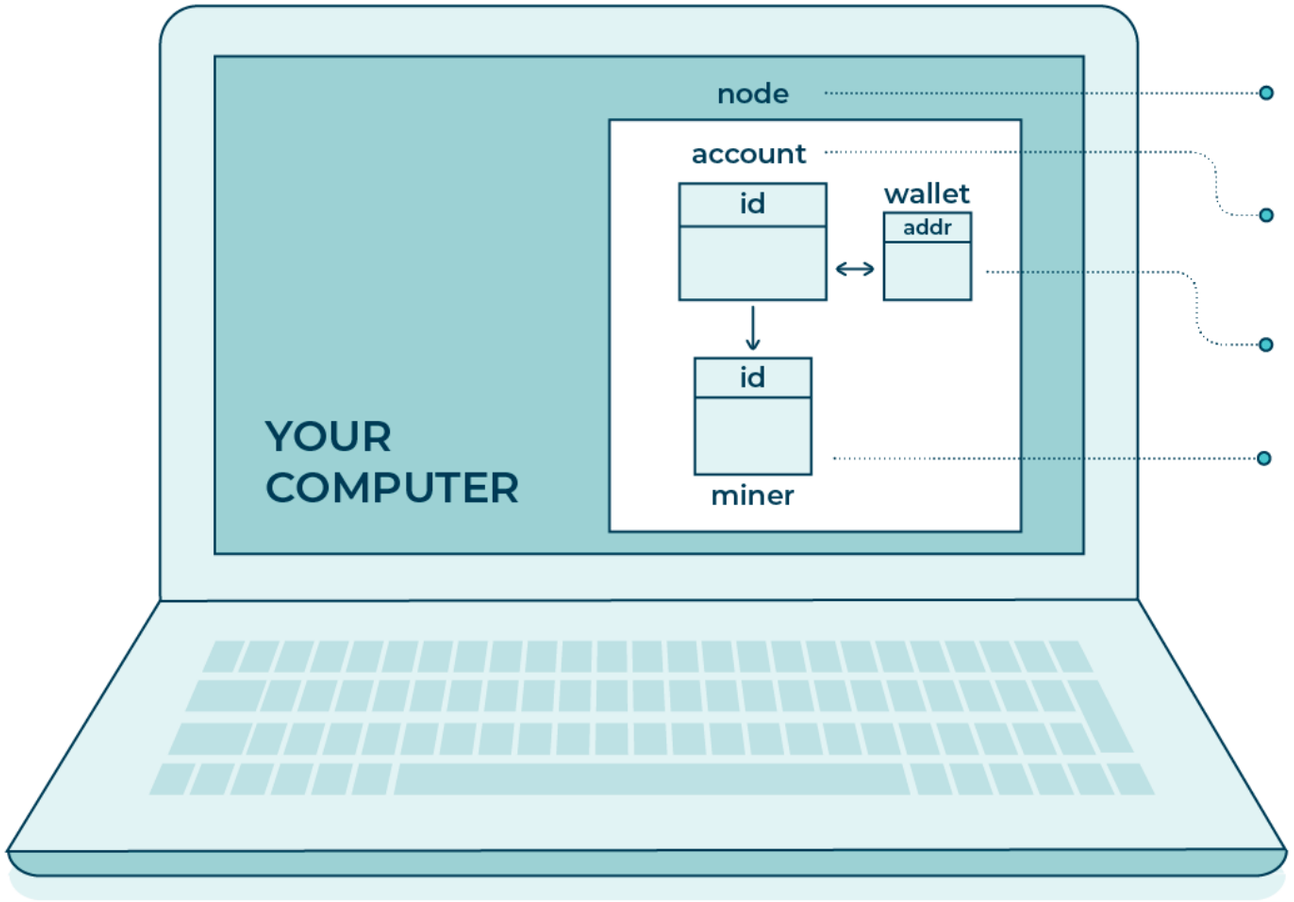
- 与其他系统的兼容

5.4 交易市场

- **存储市场**
  - 交易数据会上链，包含于区块之中。
  - 本质上也属于filecoin智能合约中的文件合约。
  - 20190214上线的开发网络已支持

- **检索市场**
  - 交易数据不会上链，属于offchain的方式。
  - 本质上也属于filecoin智能合约中的文件合约。

5.5 filecoin节点



- **node** (aka daemon aka process)
  (created by running `go-filecoin daemon`)
- nodes automatically create an **account**
- nodes automatically create a **wallet**
  (and defaults to using that wallet's address
  as the account id)
- **miner** (created by running `go-filecoin miner X Y create --from <account>`)

6 开发网络实战

- 3 filecoin开发网使用
  - 3.1 辅助资源
  - 3.2 使用
    - 3.2.1 接入filecoin开发网络
    - 3.2.2 获取Mock FIL用于测试
    - 3.2.3 矿工操作
      - 3.2.3.1 存储矿工
      - 3.2.3.2 检索矿工
      - 3.2.3.3 修复矿工
    - 3.2.4 客户操作
      - 3.2.4.1 存储客户
      - 3.2.4.2 检索客户
    - 3.2.5 filecoin合约
      - 3.2.5.1 文件合约
      - 3.2.5.2 智能合约
    - 3.2.6 单机运行多个filecoin节点
      - 3.2.6.1 修改资源目录和服务端口的方式
      - 3.2.6.2 容器部署方式

谢谢大家

- 欢迎大家关注
- 先河私有云公众号（右）

  - arsyun
- Wayne的简书链接及微信（右）
  - https://www.jianshu.com/u/01c1069071c7