Filecoin入门基础概念总合

一、什么是Filecoin

官网：https://docs.filecoin.io/

https://filecoin.io/zh-cn/

技术白皮书：https://filecoin.io/filecoin.pdf

IPFS是一个去中心化存储网络，Filecoin是IPFS存储的激励层，Filecoin作为生态激励来保证 IPFS 节点的运行。

FIL 是 Filecoin 项目基于 Filecoin 公链发行的 Token，全称是：Filecoin ,符号是：FIL。

Filecoin项目主要组成部分

1、去中心化存储网络DSN

2、复制证明PoRep

3、构建两个可验证市场，即存储市场和检索市场

1. Filecoin测试网

测试网 官方文档 https://docs.lotu.sh/

Filecoin区块浏览器，查看链上消息和爆块消息等消息

区块浏览器 https://filscan.io/#/

2. Filecoin测试网怎么参与?

Filecoin测试网是公开开放的，任何人只要有硬件有软件基础都可以参与。

关于硬件：测试网第一阶段的时候，官网移除了1GB扇区的测试，目前仅支持32GB扇区，为了加速零知识证明，需要额外配置GPU，最低是N卡1060，内存最低128G，如此高的配置无疑阻挡了众多的矿机参与，市场上大多数矿机都处于不能挖矿状态，用家用电脑的愿望也会落空，但是我们不排除官方最后的优化方案会降低需求。

二、Filecoin实现方案

在接下来的几个月中，包括go-filecoin在内的几个（目前已经有四套lotus、go-filecoin、forest以及fuhon 其中Forest（由ChainSafe在Rust中实现）和fuhon（由Soramitsu在C ++中实现））实施方案，将能够在Filecoin测试网上进行互操作。而目前我们测试网都是基于lotus实现，官方为什么实现四套实施方案，主要基于安全考虑（考虑到项目的难度、进度和可控性，具有可在同一网络上互操作的多个软件实现，可以降低一个实现中的重大错误抬高头并破坏整个网络的风险。）

您可以在GitHub上的各个实现中跟踪每个实现的进度：

- go-filecoin（用Go编写）
- lotus（用Go语言编写）
- fuhon（用C ++编写）
- forest（用Rust编写）

说明：Filecoin协议尚未100%稳定和完成，因此测试网并非是稳定的网络。测试网的目的是让我们发现并且修复bug，测试网启动至今已经被多次攻击，比如内存溢出漏洞、空指针攻击等方式，官方也在根据线上的问题，快速修正问题。测试网网络已经多次被重置。

三、核心原理（共识机制）

Filecoin – Lotus存储证明了什么?

参考URL: https://www.lianyi.com/zixun/2201284

【协议学院】Filecoin 存储封印和证明初步解析

参考URL: https://www.jianshu.com/p/5a6febf1578b

共识机制是所有区块链项目的存在的基础和灵魂。

Faincoin创新的Filecoin 区块链共识机制，目前流行的区块链共识机制有POW、POS、DPOS等，而Filecoin将创新开发采用了一种混合共识机制——复制证明（PoRep）十 时空证明（PoSt）十 预期共识(Expected Consensus，EC)。

这种混合共识机制不浪费资源和能量，又解决实际应用问题，即共享存储空间，又与实体经济结合，是我们最能预见的第一个区块链＋实体经济的项目。

Filecoin协议将使用复制证明（Proof-of-Replication）和时空证明（Proof-of-Spacetime）来证明文件已经分配在记忆存储器里的它们自己的特定位置，并随着时间变化不断被存储。

官网FAQ描述：

我们对于以Hash为基础的工作量证明（Proof of Work) 所带来的能源浪费感到失望。比起工作量证明复制（Proof of Work)，复制证明（Proof-of-Replication）不仅耗能少，而且所需工作证明了矿工正在为网络提供宝贵的资源 - 即额外的存储容量。 此外，区块奖励可以激励矿工尽可能多地贡献存储容量，从而降低Filecoin网络上的储存成本。

1. 复制证明（Proof of Replication）

参考URL: https://blog.csdn.net/ipfs_newb/article/details/81318534

科普 | 如何理解Filecoin的复制证明和时空证明?

参考URL: https://www.jinse.com/blockchain/414056.html

【Filecoin源码仓库全解析】第七章：了解PoRep与PoSt并参与复制证明游戏

参考URL: https://blog.csdn.net/weixin_33725515/article/details/91388369?utm_medium=distribute.pc_relevant.none-task-blog-BlogCommendFromBaidu-6.nonecase&depth_1-utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromBaidu-6.nonecase

复制证明（PoRep）是一种新型的存储证明方案，它能够让存储矿工说服用户和其他矿工，数据已经被复制到了它的矿机上。这种方案能有效的阻止女巫攻击、外包攻击和生成攻击的存储作弊问题，以下是复制证明的简化步骤：

在Filecoin协议中，存储供应商要让他们的客户相信，客户所付费的数据已经被他们存储，**存储供应商通过生成“复制证明”（PoRep）和“时空证明”(PoST)给区块链网络或者客户来验证存储的真实性。**而我们说的复制证明和时空证明就是来实现这一验证功能的基础算法。

复制证明（PoRep），证明数据的一个单独的拷贝已经在一个特定的扇区内创建成功。复制证明由封印（Seal）操作完成，封印操作创建一份数据的拷贝，并产生相应的复制证明。 这是一种新型的存储证明方案，它能够让存储矿工说服用户和其他矿工，表明数据已经被复制到了它的矿机上。

复制证明也是一种交互式协议。当证明人P:（a）承诺存储某数据D的n个不同的副本（独立物理副本），然后（b）通过响应协议来说服验证者V，表明P确实已经存储了每个副本，这是复制证明的简化步骤。

复制证明必须能够防范以下三种常见的攻击方式：女巫攻击，外源攻击和生成攻击，他们的共同特点是攻击矿工实际存储的数据大小要比声称存储的数据小，这样攻击矿工就能获得本不该他获得的报酬。

- 女巫攻击（Sybil Attack）：
- 利用n个身份，承诺存储n份数据D，而实际上存储小于n份（比如1份），但是却提供了n份存储证明，攻击成功。
- 外部数据源攻击（Outsourcing Attack）：
- 当攻击者矿工收到检验者要求提供数据D的证明的时候，攻击者矿工从别的矿工那里生成证明，证明自己一直存储了数据D，而实际上没有存储，攻击成功。
- 生成攻击（Generation Attack）：
- 攻击者A可以使用某种方式生成数据D，当检验者验证的时候，攻击者A就可以重新生成数据D来完成存储证明，攻击成功。

PoRep本质是一个加密时间长，解密时间短且证明与验证过程高效的算法， 这个过程在学术圈，被称为可验证时延加密（Verifiable Time-Delay Encoding Function）。

Filecoin证明机制的角色和过程可以抽象成如下，挑战者、证明者、检验者。他们可以是矿工、用户或者任何网络内其他角色。涉及的定义包括如下：

- 证明者（prover）：一般只矿工。向系统提供证明了完成系统发起的挑战。
- 检验者（verifier）：向矿工发起挑战（challenge）一方，来检测是否矿工完成了数据存储任务。
- 数据（data）：用户向矿工提交的需要存储或者矿工已经存储的数据。
- 证明（proof）：矿工完成挑战（challenge）时候的回答。

验证者会按照一定的规则向矿工提起挑战，挑战是随机生成的，矿工不能提前获知。矿工作为证明者相应向检验者提交证明，证明的生成需要原始数据与随机挑战信息。证明生成后，证明者会交给验证者，并由验证者判定该证明是否有效，如果有效，则挑战成功。

PoRep的目标是确保矿工确实在自己的存储设备上存有某个数据的备份，PoSt的目标则是让存储矿工持续证明自己在约定时间内存储了该份数据。

“复制证明”挖矿分为Pre1、Pre2和commit 3个阶段。Pre1是对数据进行编码，Pre2是对编码后的结果计算哈希，commit则是对编码后的结果生成零知识证明，以备“时空证明”算法进行检验。

其中，Pre1是单线程工作，运算的时间长，Pre2是双线程，也即CPU会被用满。这些特性对CPU提出了较高的要求，需要用AMD的芯片，且要有SHA扩展、可以加速。带有SHA扩展的CPU可将Pre1的运算过程提速3-4倍。

2. 时空证明（PoSt）

Filecoin测试网12日凌晨上线，星际大陆带你回顾什么是时空证明

参考URL: https://baijiahao.baidu.com/s?id=1652695987787883881&wfr=spider&for=pc

Filecoin挖矿：什么是时空证明?

参考URL: https://baijiahao.baidu.com/s?id=1657844007685602759&wfr=spider&for=pc

我们如何证明数据在一段时间内都一直被存储？为了解决这个问题，filecoin介绍了新的证明，时空证明（proof-of-spacetime,post），时空证明提出了证明链的数据结构，证明链由挑战（challenge）和证明（proof）链接起来形成，在证明链的基础上添加上时间段，这样就得到了一段时间内的矿工存储数据的证明，这就是时空证明（Proof of Spacetime，PoSt），

PoST即Proof of Spacetime，时空证明，这一操作是为了证明存储节点在一定时间段内存储了相应文件，而PoST证明的生成涉及较大计算量，GPU的PoST计算速度要快于CPU，因此，引入GPU挖矿可以确保在规定时间内完成PoST证明。之所以要求矿工在一个区块周期内完成PoST计算则是为了增加攻击者的攻击成本，因为PoST的计算量较大。

这也就是官方所说的“GPU只是对CPU的一种补充”的意思。开发团队成员Why曾解释过：“如果能找到别的方法来实现快速计算，就不需要GPU。”

扣除部分代币。

仅当矿工在给定时期内因赢得大块奖励而赢得了选举票时，才在选举时空（“ElectionPoSt”）中运行SNARK 。每当矿工赢得选举票时，配置就使用GPU的功能来计算PoSt SNARK的输出结果，准确计算出每个纪元周期（约20秒）内的PoSt SNARK。PoSt所需的GPU功能在很大程度上取决于矿工在任何给定时期拥有多少张获胜选举票，这与他们在网络中的存储比例有关。

官方还建议使用较低延迟的网络连接来按时提交PoSt。如果矿工多次未能按时提交PoSt，则可能导致赢得较少的区块奖励，并增加被削减的风险。

总结： 通过（时空证明（Proofs-of-Spacetime）持续证明存储。

3. 零知识证明

零知识证明 - zkSNARK入门

参考URL: https://www.jianshu.com/p/828fef53cf13

Filecoin – Lotus存储证明了什么?

参考URL: https://www.lianyi.com/zixun/2201284

零知识证明，zkSNARK，zero-knowledge Succint Non-interactive ARguments of Knowledge的简称

零知识证明（Zero-Knowledge Proof）或零知识协议是一种基于概率的验证方法，包括两部分：宣称某一命题为真的证明者（prover）和确认该命题确实为真的验证者（verifier）。

零知识证明指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的，在密码学中非常有用。

顾名思义，零知识证明就是既能充分证明自己是某种权益的合法拥有者，又不把有关的信息泄漏出去，即给外界的 “知识” 为“零”。

“能够在不知道用户是谁，或者他们有多少钱的情况下判断‘一个用户是否有足够的钱发送给另一个用户’的问题，是零知识证明在区块链中的主要应用之一。”——Demiro Massessi

例如，当前网站将用户密码的哈希值存储在其 web 服务器中。为了验证客户端是否真的知道密码，大多数网站目前使用的方法是对客户端输入的密码进行哈希值计算，并将其与存储的结果进行比较。

零知识证明可以保护用户的帐号信息不被泄露。如果零知识证明可以实现，那么在客户的密码是未知的情况下，仍然可以在客户端登录进行身份验证。当服务器受到攻击时，用户的帐户仍然是安全的，因为客户的密码没有存储在 web 服务器中。

零知识证明在区块链中的应用

比特币和以太坊网络都使用公共地址来代替验证者和证明者的真实身份，使得交易部分匿名; 只有发送和接收地址，以及交易数量是公众知道的。但是，通过区块链上提供的各种信息，如交互记录等，可以发现地址的真实身份，存在隐私暴露的隐患。

最早使用零知识证明技巧的区块链叫做 Zcash，实际的作法叫做 Zk-Snarks，这是许多零知识证明的做法之一，也是最有名的一个。

Zk-Snarks 是 “零知识简洁无交互知识认证” 的简称，是一种在无需泄露数据本身情况下证明某些数据运算的一种零知识证明。

Zk-Snarks 技术缩减了证明所需的时间和验证它们所需的计算量。它能够证明有效交易的条件已经满足，而不需要透露交易所涉及的地址或交易量的任何关键信息。

Zcash 可以将交易纪录上的汇款者、收款者和金额都经过加密隐藏起来，因此矿工无从得知这些交易上的细节，但仍然可以验证交易。不过，目前多数使用者在 Zcash 上的交易，还是选择未经加密的作法，因为花费的成本比较高。

根据 Zk-Snarks 白皮书，Zk-Snarks 是第一个不依赖任何信任设置实现区块链验证的系统，而随着计算数据数量的增加，计算速度呈指数增长。它不依赖于公钥加密系统，而且更简单的假设使它在理论上更安全，因为它唯一的加密假设是哈希函数 (如 SHA2) 是不可预测的。零知识证明和 Zk-S(T|N)ARK 等技术的测试和采用需要时间。

4. 相关实现

Lotus/Filecoin项目由三部分组成：

1/ Lotus Blockchain部分 – 实现区块链相关逻辑（共识算法，P2P，区块管理，虚拟机等等）。注意的是，Lotus的区块链相关的数据存储在IPFS之上。go语言实现。

2/ RUST-FIL-PROOF部分 – 实现Sector的存储以及证明电路。也就是FPS（Filecoin Proving Subsystem）。Rust语言实现。

3/ Bellman部分 – 零知识证明(zk-SNARK)的证明系统，主要是基于BLS12_381椭圆曲线上，实现了Groth16的零知识证明系统。Lotus官方推荐采用Nvidia的2080ti显卡，也主要做这部分的性能加速。Rust语言实现。

Filecoin的存储封印（Sealing）和证明（PoRep & PoSt）是用rust语言编写，而且是单独成篇的，也就是说可以单独拿出来玩。

ilecoin复制游戏程序的源码可以到以下地址下载：

https://github.com/filecoin-project/replication-game

如果你不想下载源码，直接下载可执行代码的话，直接到这里：

https://github.com/filecoin-project/rust-fil-proofs/releases

四、官方FAQ

参考URL: https://filecoin.io/zh-cn/faqs/

IPFS和Filecoin之间有什么联系？

Filecoin和IPFS是互补协议，两者均由Protocol Labs创建。IPFS 允许网络中的参与者互相存储，索取和传输可验证的数据。 IPFS是开源的，可以被免费下载和使用，并且已经被大量的团队使用。运用IPFS，各个节点可存储它们认为重要的数据；没有简单的方法可以激励他人加入网络或存储特定数据。 为了解决这一关键问题，Filecoin的

储来获得付款和奖励。 简而言之：IPFS按内容寻址并使其移动； Filecoin就是缺失的激励机制。

Filecoin还使用了IPFS的许多性能。例如：

Filecoin将IPLD用于区块链数据结构

Filecoin节点使用libp2p保证安全连接

节点之间的消息传递和Filecoin块传播使用libp2p发布订阅

此外，Filecoin核心团队包括IPFS核心团队的成员。 IPFS和Filecoin之间的兼容将尽可能无缝对接。即使在Filecoin发布之后，我们仍然期望IPFS和Filecoin的开源社区们继续协作和提升两个项目的兼容性。

我什么时候应该选择使用Filecoin？何时应该选择IPFS？

首先，值得重复的是，Filecoin和IPFS相互补充，并且具有显着的交叉兼容性。 我们正努力地使自发的IPFS存储和付费Filecoin存储之间的转换更加简单。

使用IPFS，您可以通过直接提供硬件或从第三方购买存储来负责您自己的存储节点。在IPFS上，单独的节点可以存储他们认为重要的内容； 没有任何简单的方法来激励他人来保证储存你的数据在他们的系统里。Filecoin提供了缺少的激励机制。

如果您希望维护自己的存储节点，或者和外部协作来合作存储数据，IPFS将可能会是您的首选方案。如果您希望支付具有竞争力的价格并在特定的冗余和可用性下为您管理信息存储，Filecoin可能是您的首选方案。

总结，想要了解更多关于filecoin的知识请关注私信我，后续我也会出关于FIL挖矿的相关知识