第二周周报

汪子龙

本周我试图深入了解 Filecoin 的 PoRep 算法，翻阅各种资料和官方文档，总结了一下算法的思路。但网络上可供学习的资料太少，所以对这些核心算法的了解非常有限，对算法的具体实现依旧没搞清楚。

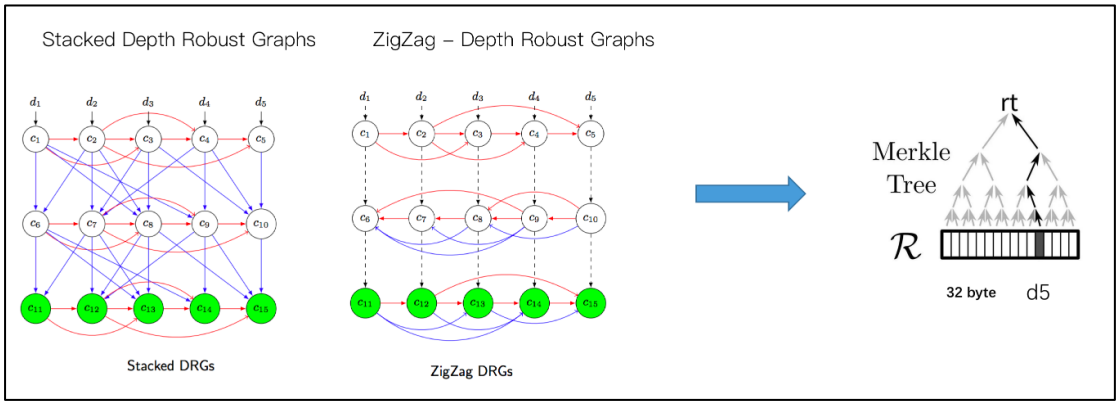
本周最大的感受就是：一周下来感觉都在做无用功。在这个全新的领域，我还在四处摸索。由于相关资料太少，一直没能找到一个很好的研究方向。希望我能尽快跟着专业的研究团队，尝试做一下具体的项目，深入了解学习相关的知识，不要再浪费时间盲目学习。

Filecoin 的 PoRep 算法需要抵御三种区中心化系统常见攻击：

类型	简介
女巫攻击	多份数据使用同一物理存储
外包攻击	谎报他人的数据是自己的
生成攻击	临时生成检验数据

算法本质是可验证时延加密函数(VDF)，具有加密时间长、验证时间短的特点。使用这种方法，计算的时候很慢，但验证的时候很快，需要在一个给定的时间拿出结果，所以不容易伪造。

Filecoin 使用的 VDF 是 StackedDRG 和 ZigZagDRG。如下图所示，原始数据首先依次分成一个个小数据，每个小数据 32 个字节。这些小数据之间按照 DRG 建立连接关系。按照每个小数据的依赖关系，通过 VDE 函数，计算出下一层的所有小数据。



整个 PoRep 的计算过程分为若干层，数据解码过程中，每一层之间互不依赖，即可并行执行，相对于串行编码要更为快速。这样就实现了 PoRep 的本质：编码快，而解码和验证证明快的效果，从而防范各种攻击。