Justin Drake的ZK观点

以太坊创始人：V神

解读V神2024年香港Web3峰会提倡使用ASIC进行ZK硬件加速！

原创 Bill & Max Max说说 2024-04-10 13:12

新加坡 36人听过

2024 香港 Web3 嘉年华期间，以太坊联合创始人 Vitalik Buterin 在由DRK Lab主办的 "Web3 学者峰会 2024" 上发表主旨演讲《Reaching the Limits of Protocol Design》。

演讲的主要重点总结如下：

*1. 现在，zk-SNARK 验证一个普通以太坊区块所需的时间约为 **20 分钟**。现在的目标就是 zk-SNARK 需要**实时证明**，目标是当一个区块被创建时，在下一个区块被创建之前，你就能得到该区块的证明，可能在5秒之内。*

2. zk-SNARKs 不仅可以实现隐私性，还有可扩展性，但是隐私计算很多事情又是zk-SNARKs 无法完成的，需要用到 MPC（多方计算）和 FHE（同态加密），与此同时，MPC 和 FHE 的成本非常高，在区块链领域无法大规模普及，只有 zk-SNARKs 是可以的。

*3. 需要大量并行计算和优化聚合证明，在硬件成本和电费相同的情况下，ASIC 的哈希值基本上是 GPU 的 100 倍，使用 zk-SNARK ASIC 来做证明计算，**能从20分钟缩短到5秒。***

4. 提高安全性，减少出错的几率，协议所依赖的实际技术可以是非常强大、非常值得信赖的，人们可以尽可能地依赖它。

在这次峰会上，V神重提 ASIC，这是罕见的，我们都知道V神在以太坊早期是一直反对 ASIC 的，甚至说当 ASIC 算力超过全网算力的某个比例就会改变算法，但是现在却大谈 ASIC 的好处，主要原因就是 ZK 证明的生成太慢了！

V神其实之前在很多公开场合力推 zk-SNARKs，认为是非常有潜力的发展方向：

接下来以太坊的算力模式要改变！

现在以太坊算力工具是显卡；接下来要把显卡改变成 Zk芯片！

zk芯片技术可以做到什么？

现在以太坊用显卡的算力时间是20分钟，

改成zk芯片算力之后，5秒钟就够了！

视频网址：https://www.bilibili.com/video/BV1tM4m197Fy/?spm_id_from=333.337.search-card.all.click&vd_source=4706dd4f6cf2578759c99439a27fc04c