主题：谈谈zkp大规模普及的障碍

主聊人/主要参与者:

- Dream, Cecilia, and 3H.

内容

- 协议：现状，特点
- 应用开发：开发者工具链
- 开发者教育：社区，教程
- 如何去普及，需求是什么

hhh

- 今年开始学习 zkp
- 对 folding 比较感兴趣
- 对这个话题挺感兴趣
- 为什么zkp 这几年发展的好
  - 可以脱离区块链
  - 可以把计算外包，比如 zkrollup
  - 因为有区块链才发展的这么好
- 当前的技术
  - 因为有扩容计算的需求
  - 资本的叙事
  - 带动底层infra 的发展
- 现在需要另外一个叙事来支撑 zkp 的发展
  - 如果layer2叙事不成立怎么办
- sui zklogin
  - 实际很简单
  - 通过zk验证会话秘钥
  - 用的 groth16
- 大部分的 zkp 应用都不复杂？？
- zkvm 的技术才比较复杂
- 做一些应用，目前的技术已经够用了
- 需要一些需求，促进底层的基础设置发展
- zkml没有看到可以发展起来的地方

Dream

- 在 scroll 做电路的开发
- 这几年一直在做 zkp 的东西
- 我们的工程实践来看，技术还没到成熟的阶段，还在向中期过渡的阶段
- 开发工具，技术栈，脚手架都不完备
- 山头林立，各个工具链都是独立的
  - circom
  - cairo
- kaccak 等一些密码库要自己写
- 开发成本高
- 对开发人员要求也比较高
- 面临的问题
  - 有些库没有
  - 不好用
  - 不通用，在其它生态
- 应用为什么轻量级
  - 亿的电路级别
    - prover 成本非常高
    - 对于底层协议，效率也没法支持
- 大规模普及 - 什么叫大规模普及呢，进入人们的生活才叫大规模普及 - 假设技术成熟了 - 参与的相关方有没有动力去做 - 比如提供存款证明，余额在 50万以上 - 银行是否有动力去做 - 就算提供了证明，验证方是谁呢 - 使馆会用来去验证吗，这样需要使用对应的设备 - 用户教育可能需要一个过程 hhh
- 赞同最后一点
- web2搜集信息都是通过立法过程去使用和保护数据
- 可能的场景
  - 可以提供证明，说我没去过某些地方
- web2用户出售自己的数据获得服务
- 两方面的改变
  - 商业模式
  - 思维模式
- 目前电路的语言特别多
  - 每个都学，每个都不精
  - 郭老师说过
    - 当做一个复杂的工程化的zk项目
    - 做出来之后就落伍了
    - 公司会死，但程序员会留下来，会更好
- 市场上有不同的电路，需要去中心化的 prover 生成 proof
  - 目前还不成熟
  - 希望可以及时生成 proof

- 审计问题

郭老师

- 谈到 zkp 应用的问题，好像回到了 2018 年的区块链

dream

- 3 年前都不可能做zkevm，但现在都上线了

郭老师

- 18 年，一个 vm 的速度只有 1hz

dream

- 后端 proof system 不同，每秒可以运行的指令是不同的

hhh

- 如果看前端
  - plonkish 是最好用的前端
  - polygon做了个 prl2，支持 plonkish
  - 感觉plonkish大一统
  - 虽然tool不同，但是都是从这个地方去转

dream

- 3h说的有一个中间件来做翻译
- 但看起来这样不是太容易，特别是跨平台的话
- 用语言开发，可能不太在乎后端的事情
- 做一些 DSL 还是可以的，但是这两类还是比较难以统一的

郭老师

- Jolt 说不定可以和 plonk 整合在一起
- 但 Jolt 是 sumcheck
- sumcheck 能力还是挺强的
- 开源社区也有战争，是个常态，一般分为两派
- 最终会收敛到两个主流的生态

dream

- 开发游戏，要看如何电路化
- 越是上层的业务，电路起来就更困难一些
- 工具链会越来越傻瓜，一定会实现大家可以直接用上层语言去写

郭老师

- 为什么risc0要用 risc-v
- risc-v 和 risc指令集没有任何关系
- risc不能给 risc-v vm带来任何好处
- nervos 用的 risc-v，可以用任何编程语言写，然后compile到 binary code
- 问题在于，安全角度来看，非常有问题，攻击面会非常多
- 用任何语言写电路，也是不太现实的
- 如果不一定用 risc0，那用什么 vm更靠谱吗
- zkevm 吗，还是新的 vm，或者说一定是需要是 vm 吗，还是说可以是一种不像vm的 vm，但是可以表达 computation trace
- 问题：在 rollup 之上，做一个 zkevm 兼容 evm 是否值得？prover cost 会有损失吗?