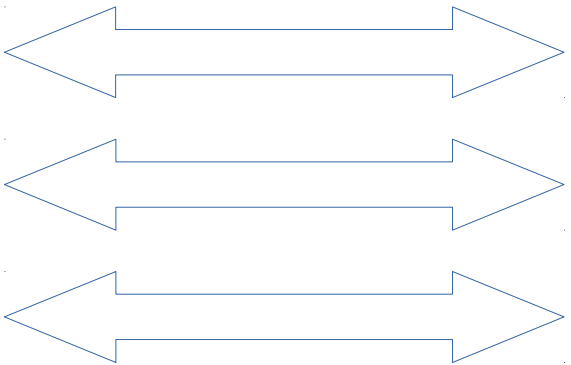
AlphaWallet

2017.7.20, 杭州

https://awallet.io

区块链的三宝

- 佛三宝
  - 佛宝
  - 法宝
  - 僧宝



- 区块链的三宝
  - 公链
  - 协议
  - 社区

区块链哪里掉了链子

- 公链
  - 扩展性：每秒交易数和区块链文件大小
  - 保密：合约数据的隐私和合约内容的隐私
  - 安全：防止合约退出和意外结果
  - 可靠：防止交易 stale

区块链哪里掉了链子

- 协议
  - 提供隐私的协议（看我的 paper[1]）
  - 减少交易成本的协议（ERC875）
  - 跨链资产交换协议（如 Timed Hash Contracts）
  - 提供即时性的协议（如 Payment Channel）

今天我们重点讲这个

1. https://github.com/alpha-wallet/ethereum-attestation/releases

区块链哪里掉了链子

- 社区
  - 资产投资和投机行为（价值发现）
  - 资产使用者（游戏用户，区块链订酒店用户）
  - 厂商（资产发行方）
  - 虚拟平台（无中心执行如 ctrip 这样的中介职能）

协议是什么

- 传统非区块链方案

手机

- UI 层
- BO 层 (业务逻辑)
- SO 层（存储逻辑）

服务器

- 区块链完成相应任务

手机

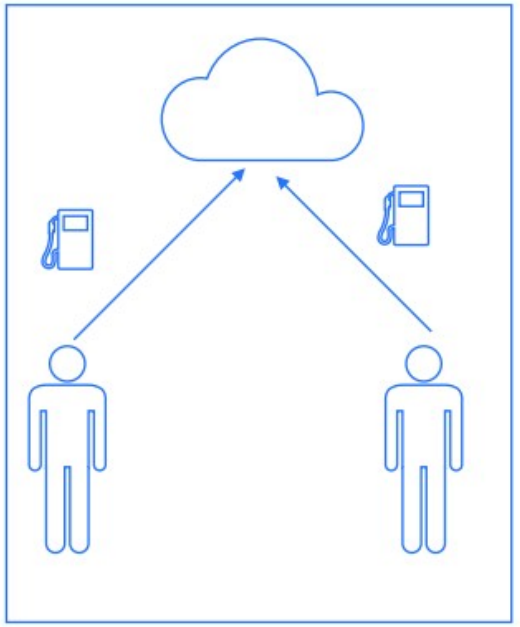
- UI 层
- 协议（业务逻辑）
- 区块链（业务逻辑的验证部分）

区块链

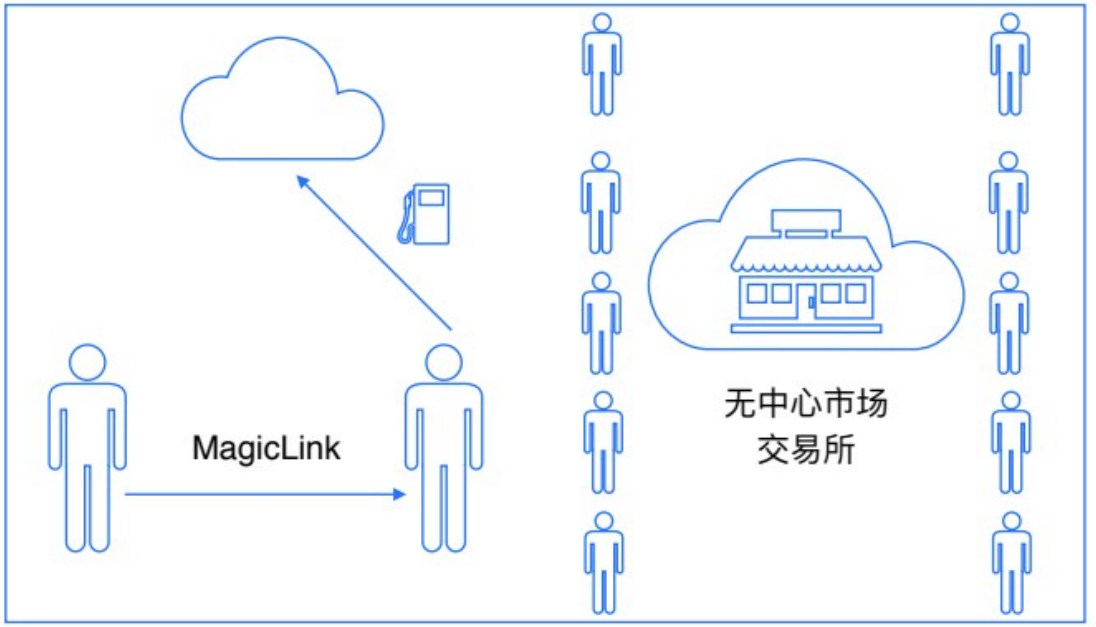
最简单的协议 :ERC 875

AlphaWallet

能实现什么样的先进功能?



ERC721



ERC875

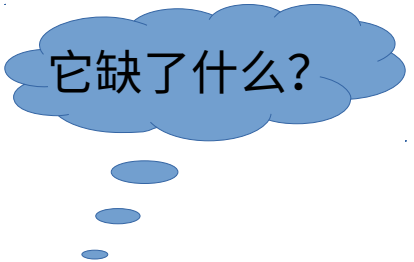
复杂一点的协议：公平随机数

- Alice
  - 生成 x 和 $h\ (x)$
  - 学习 $h\ (y)$
  - 打开 x
  - 计算 $x + y \bmod 6$

- Bob
  - 生成 y 和 $h\ (y)$
  - 学习 $h\ (x)$
  - 打开 y
  - 计算 $x + y \bmod 6$

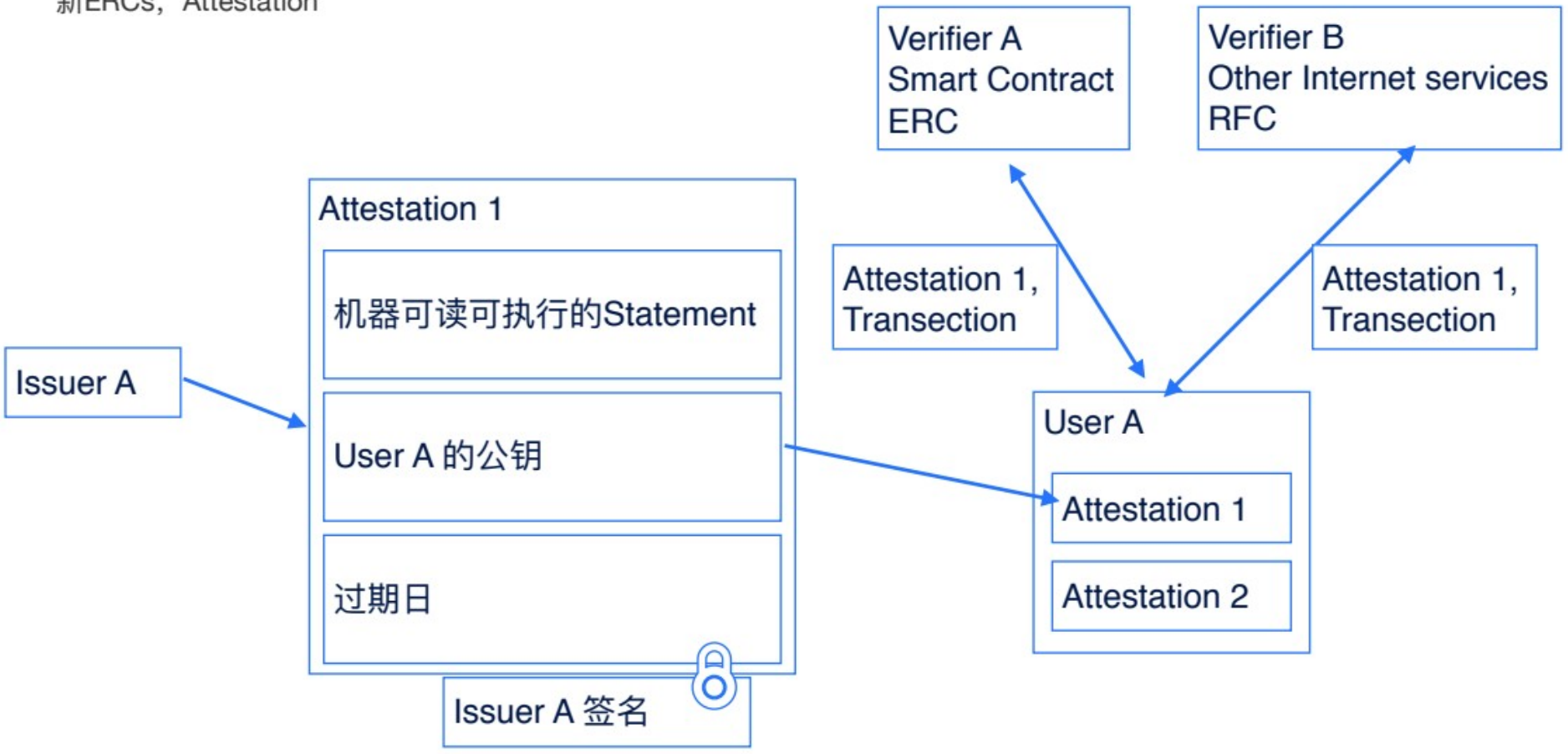
身份验证协议

- 考虑这个非区块链传统 attestation

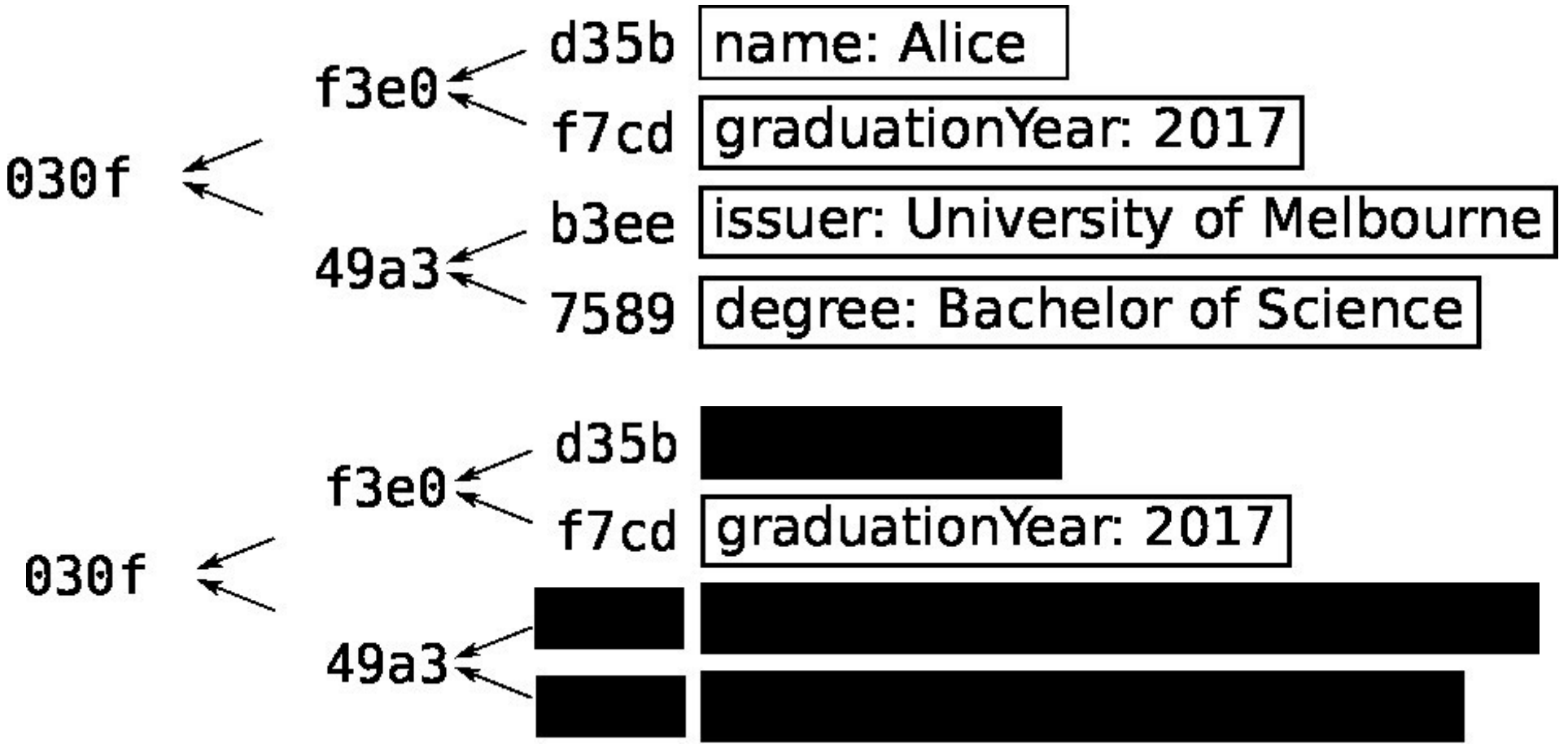


AlphaWallet

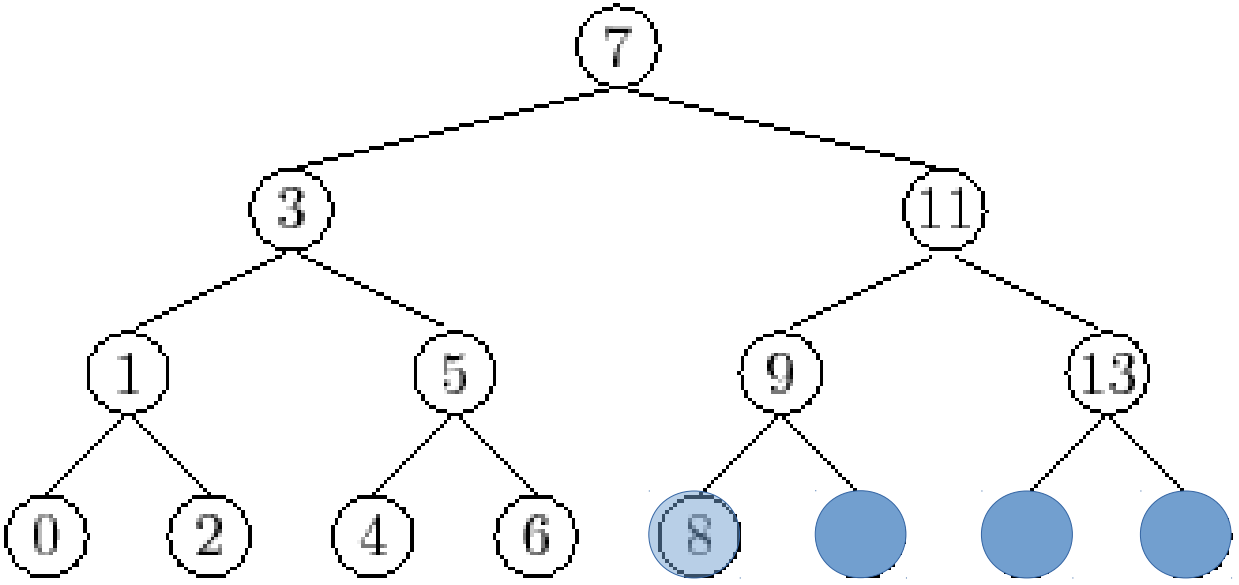
新ERCs，Attestation



实际 attestation 协议中用到的样子




捕鱼达人
千炮HR
70
9342
70
x1
20



鱼	鱼	鱼	鱼	鱼
戏	戏	戏	戏	戏
莲	莲	莲	莲	。
叶	叶	叶	叶	。
东	西	南	北	。

联系方式

没有微信，使用论坛可以方便索引文字内容、整理问题以及搜索引擎收录，欢迎提问交流，一起探讨更多话题

https://community.awallet.io