Distributed Randomness Beacon

邱飞旸
Anders Qiu

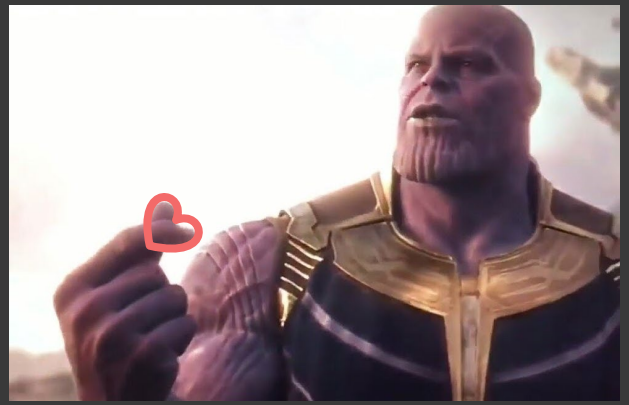
2018.12.01 北京

主要内容

- 什么情况下我们需要 Distributed Random Beacon (DRB)
- 随机性、随机数发生器以及他们和 DRB 的关系
- 几种构造方法
- DRB 与区块链的关系

什么情况下我们需要 DRB

- 已有的去中心化系统上获取不可预测的随机数
  - 区块链
- 无法假设中心机构足够可信的场景
  - 彩票开奖
  - 车牌摇号



随机序列的定义

Uniformity

1. 均匀性：该序列服从均匀分布。

Independence

2. 独立性：该序列的各个元素相互独立。

Unpredictability

3. 不可预测性：从任意片段序列不能预测该序列余下的部分。

密码学特有

随机数发生器 (1/2)

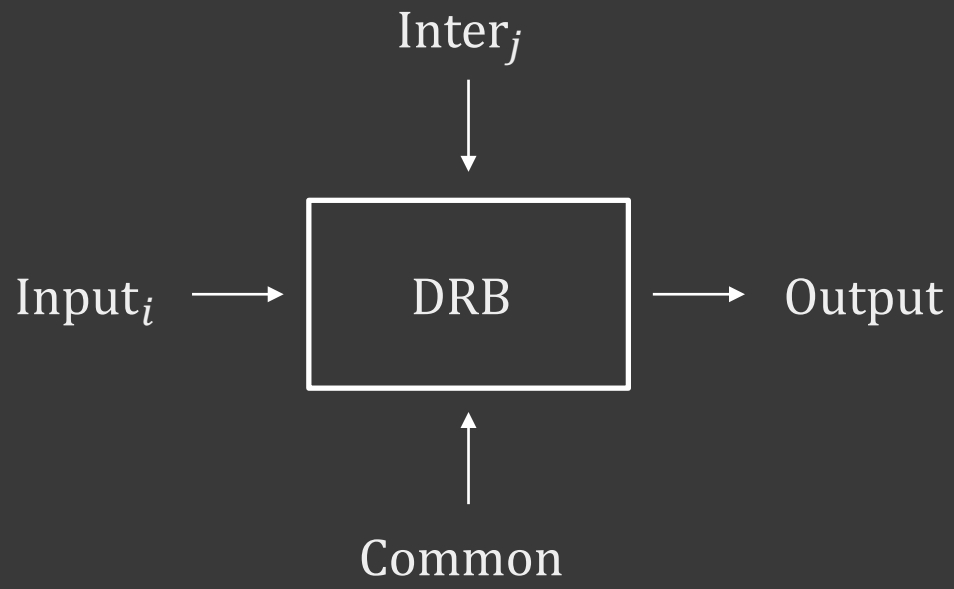
随机数发生器 (2/2)

- 多项式时间计算不可区分的伪随机数发生器是否存在?
  - 还不知道。目前评估是否密码学安全都是使用统计学测试。
- 伪随机性和不可预测性的关系?
  - 伪随机性等价于多项式时间不可预测性。

如何在区块链里获取随机数

- 为什么伪随机数发生器的不可预测性在区块链上不够?
  - 区块链上一切算法、算法的输入以及算法的输出都是透明的。另外种子的选择也是个问题。
- 真随机数发生器呢?
  - 去中心化非常困难。

一个抽象模型



v1.0

$$\xi = \xi_B \oplus \xi_H$$
$$\xi = (\xi_B + \xi_H) \mod 2$$

0：Blink 吃
1：Huai 吃

性质：
1. 所有输入与输出相互独立。
2. 只要有一个输入是均匀分布，结果就是均匀分布。

v2.0

我等 Blink 提交了我再出手，嘻嘻嘻。

$\text{sig}_{sk_B}(\xi_B) \longrightarrow$

$\text{sig}_{sk_H}(\xi_H) \longrightarrow$

$\xi_B \longrightarrow$

$\xi_H \longrightarrow$

$\text{sig}_{sk_B}(\xi_B)$

$\text{sig}_{sk_H}(\xi_H)$

$\longrightarrow \xi$

0：Blink 吃

1：Huai 吃

Commit的实现方法：

a) 签名

b) 在区块链的设定下可以只哈希。

v3.0a

如果不是我，我就不 reveal，嘻嘻嘻。

0：Blink 吃
1：Huai 吃
2：Pero 吃

$\mathrm{sig}_{sk_B}(\xi_B)$ + 1 BTC ⟶

$\mathrm{sig}_{sk_H}(\xi_H)$ + 1 BTC ⟶

$\mathrm{sig}_{sk_P}(\xi_P)$ + 1 BTC ⟶

ξ_B ⟶

ξ_H ⟶

ξ_P ⟶

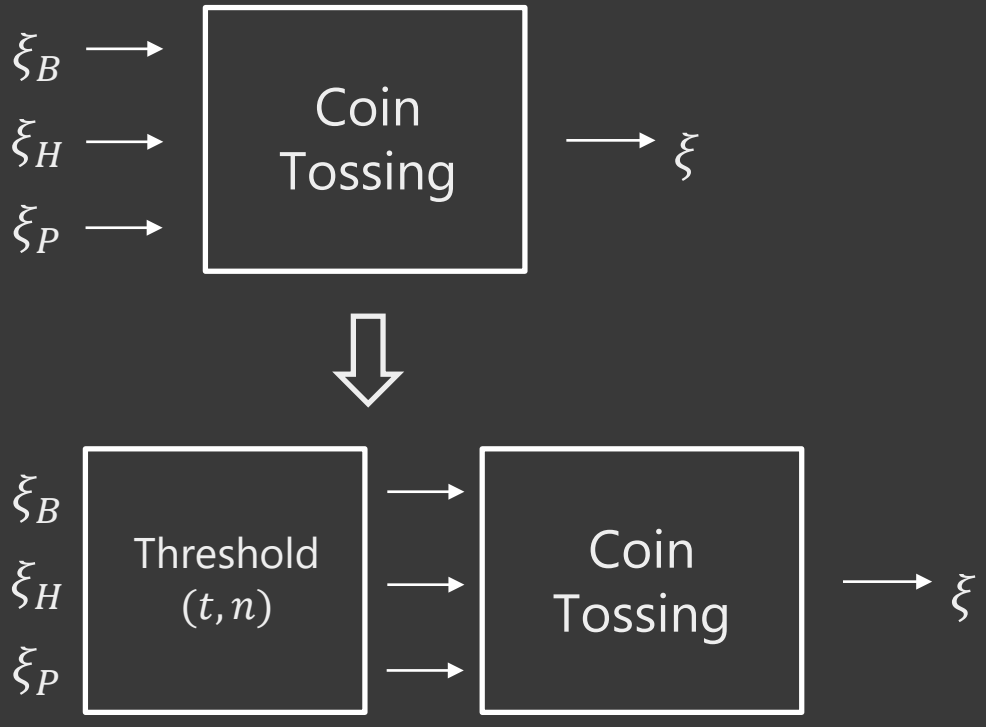
$\mathrm{sig}_{sk_J}(\xi_B)$

$\mathrm{sig}_{sk_D}(\xi_H)$

$\mathrm{sig}_{sk_T}(\xi_P)$

⟶ ξ

v3.0b



Threshold 机制实现方法

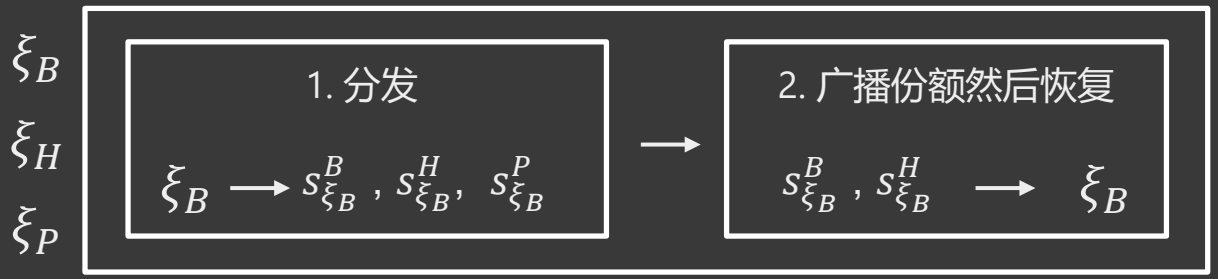
a) 取前t个输入
   - 不抗 Sybil 攻击

b) 无分发者的（（公开）可验证）秘密分享
   - 需要每一轮都进行
   - 许可环境下

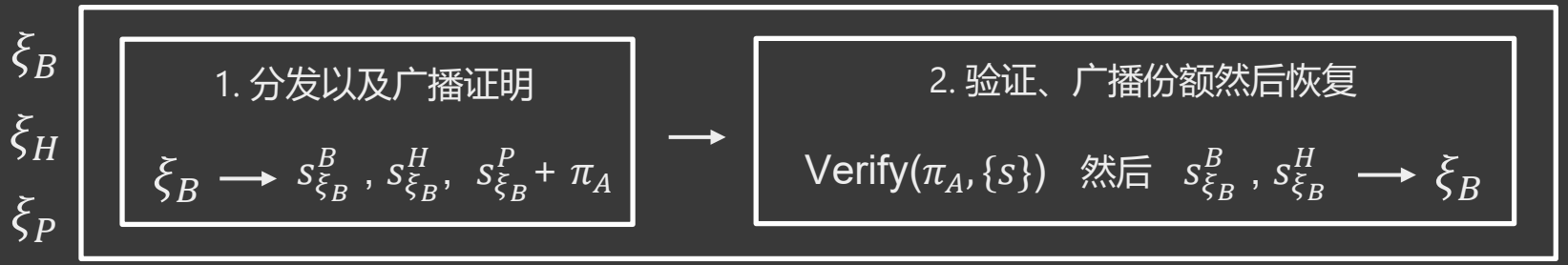
c) 分布式密钥生成 + 门限签名（利用了秘密分享的签名算法）
   - 需要许可环境下

v3.0b

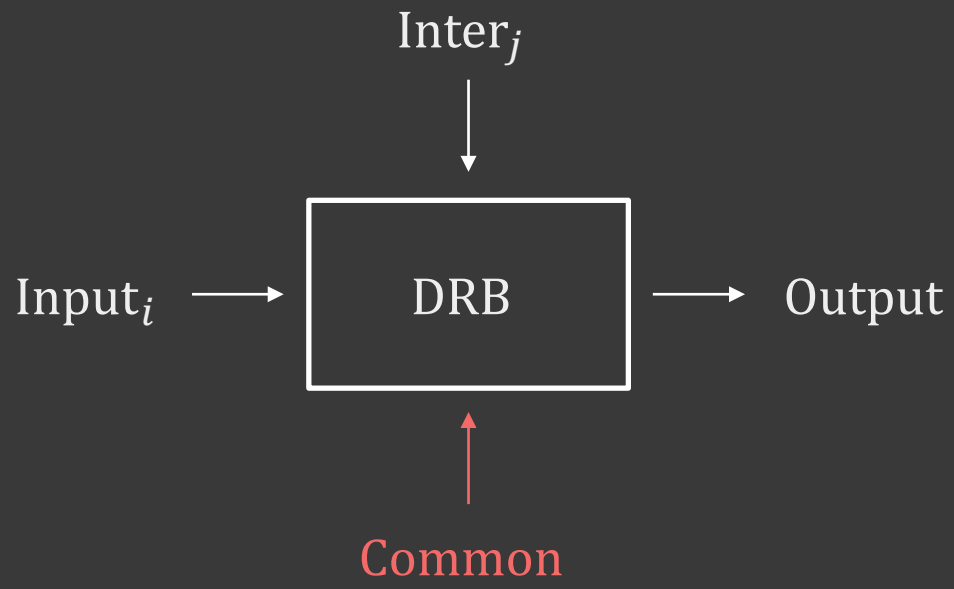
a) 无分发者的秘密分享 (Secret Sharing) (t, n)



b) 无分发者的公开可验证秘密分享 (Publicly Verifiable Secret Sharing) (t, n)



一个抽象模型

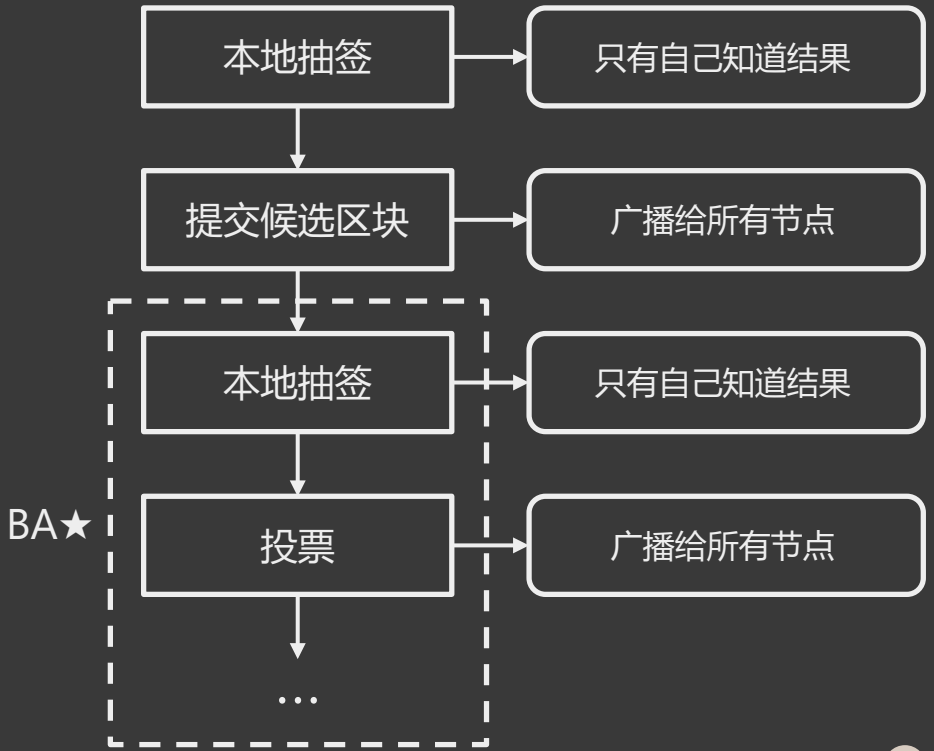


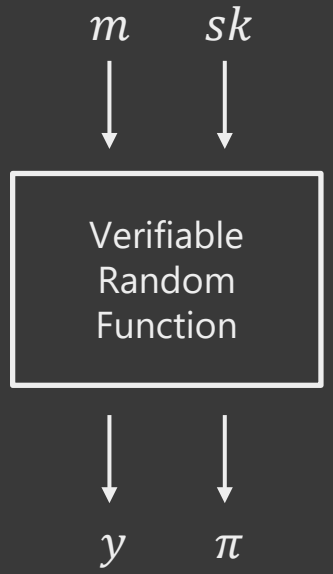
Verifiable Delay Function (VDF)

$$Setup(\lambda, T) \rightarrow pp$$
$$Eval(x, pp) \rightarrow (\mathrm{y}, \pi)$$
$$Verify(pp, x, y, \pi) \rightarrow \{accept, reject\}$$

实际应用

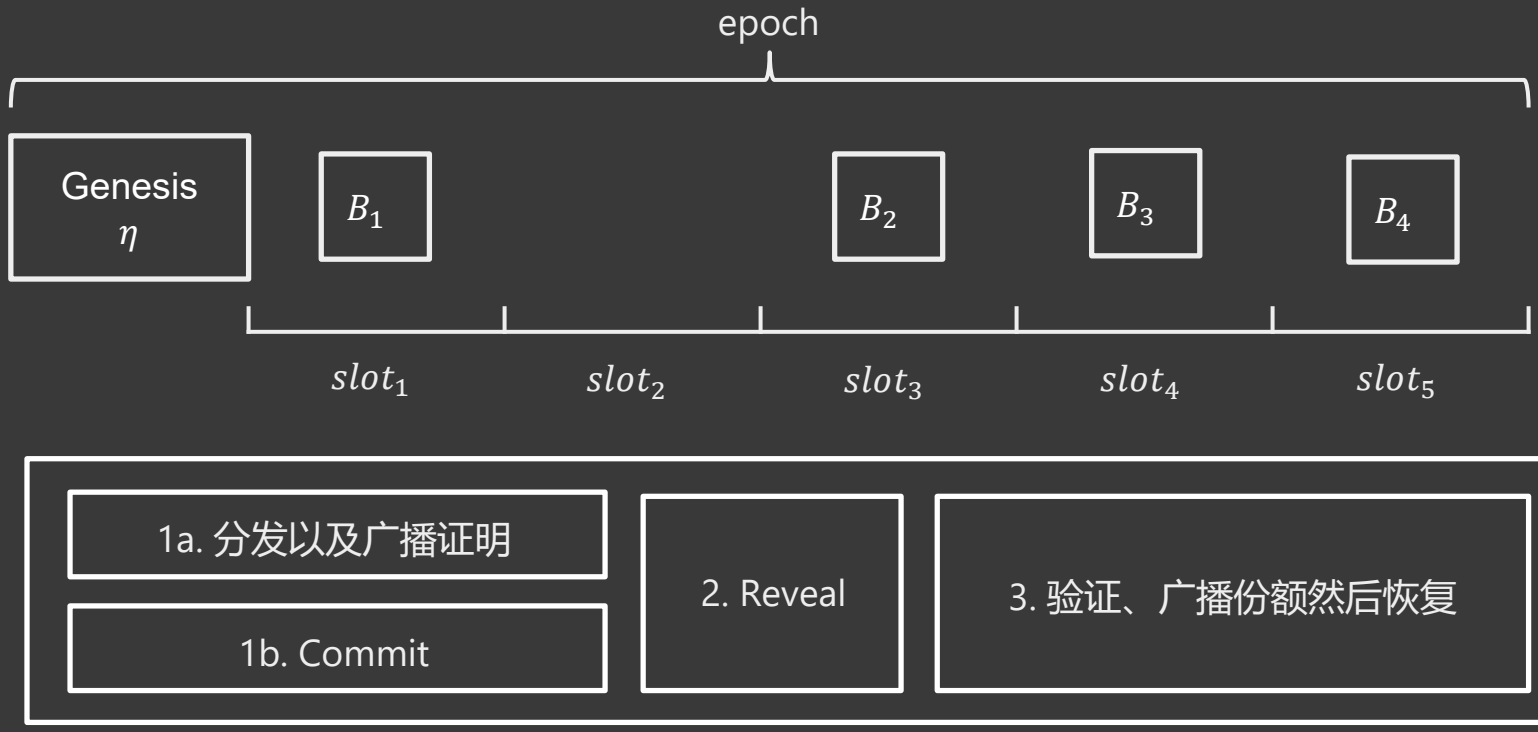
Algorand



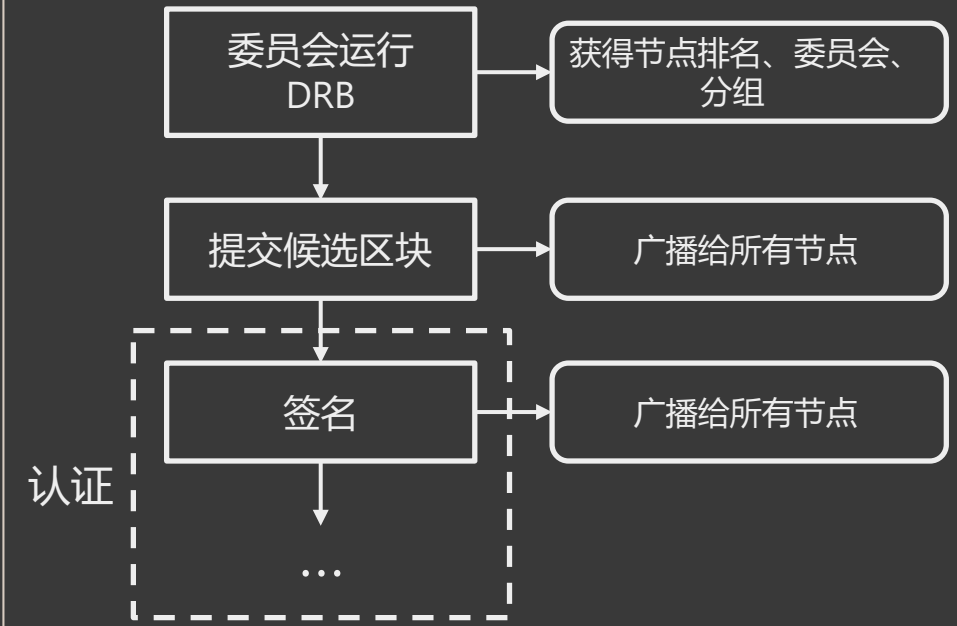


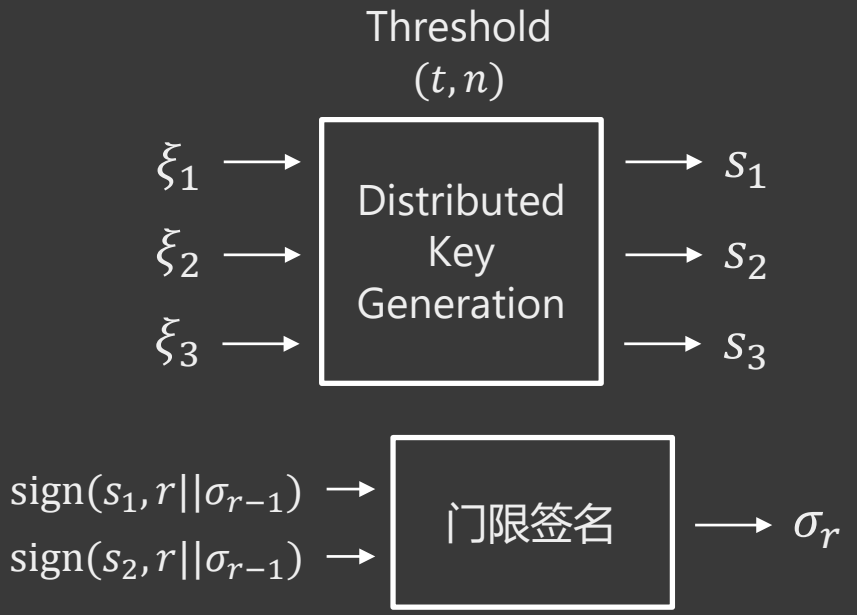
Verify (y, m, π)

Cardano


epoch
Genesis
η
B_1
B_2
B_3
B_4
$slot_1$
$slot_2$
$slot_3$
$slot_4$
$slot_5$
ξ_1
ξ_2
ξ_3
1a. 分发以及广播证明
1b. Commit
2. Reveal
3. 验证、广播份额然后恢复
η

DFINITY



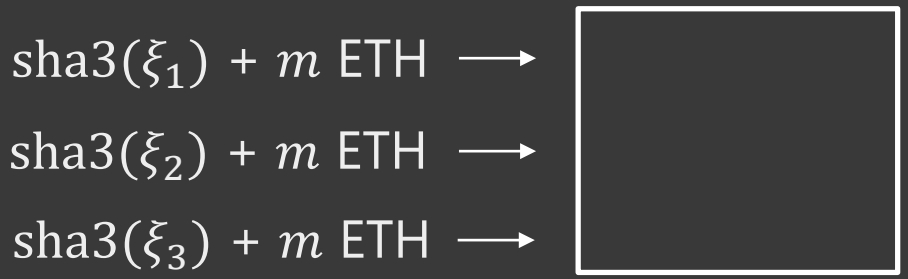


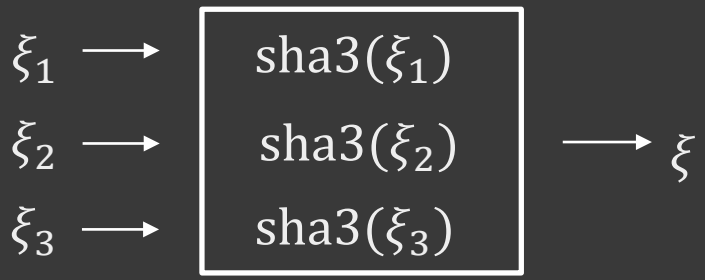
采用（基于 BLS 的）门限签名：

1. 一次购买，终生免费。
2. 确定性。

Randao

基于 Ethereum 智能合约





说明：

1. 同一地址的commit只接受第一次。
2. Commit数有最小要求。
3. 不reveal的地址会被没收押金，一旦不是全部reveal，返回失败。

最后一步：返还押金，给参与者支付奖励。

随机数与共识协议的关系

- Sybil Attack Resistance 的方法之一是不可预测地随机抽签。
  - PoW
  - PoS
- 区块链上的随机数安全依赖于共识协议。
  - Censorship Attack
  - Grinding Attack

“区块链上随机数的生成是需要 CONTEXT 的”

Question?

Email: i@priewienv.me

Blog: https://blog.priewienv.me