高度h2

高度h1

可能2: 根据不同应用要求可选：

1. u违规操作，惩罚

2. 放烟雾是u合法策略

高度h0

可能2: u行为无效

可能1: 验证: ah == Hash(A +n) ，Storage更新{**user**:u, **action**: A}

可能1: u原来做了A这件事

可能2: 这个鬼真坐得住

观察者

用户u可能干了些什么，我们最早h1最迟h2就会知道真相

可能2: 验证: ah != Hash(B +n1)，不合法请求，忽略

执行行为A:

1. 本地生成并记住随机量 nonce = n

2. 计算ah = Hash(A + n)}

2.发送{**actionHash**: ah}

Storage写入{**user**:u,

**actionHash**: ah, **expose**:(h1,h2)}   
用户必须在[h1,h2]期间曝光自己实际行为

可能2: 什么也不做, 或发送不合法{**action**: B, **nonce**: n1}

可能1: 发送{**action**: A, **nonce**: n}

合约逻辑

用户u