

储蓄有奖系统

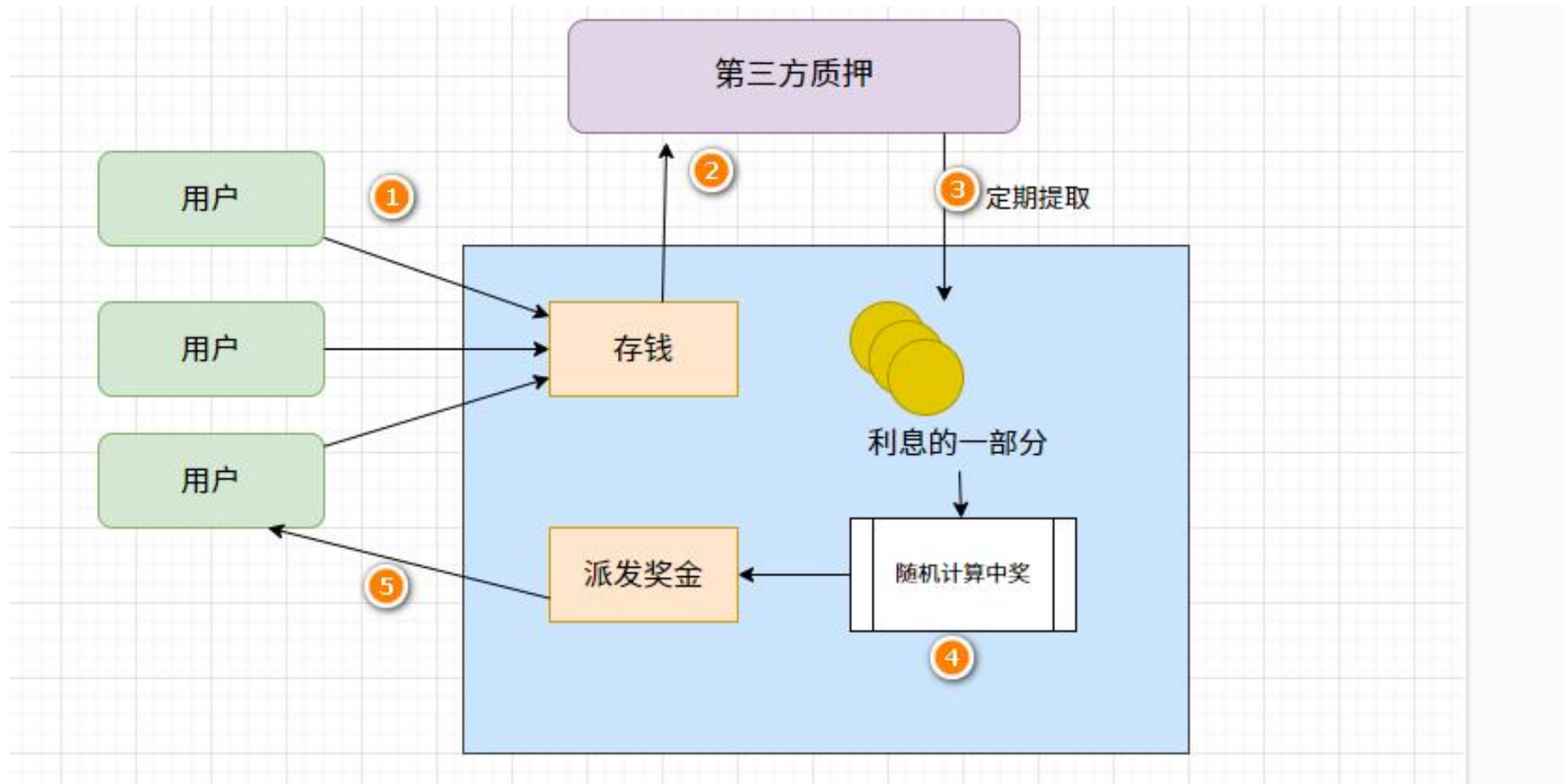
<https://github.com/nextuser/deposit-bonus>

wechat: growfat tg:low_weight mail:nextuser#163.com

缘起

- 我总有一个2块钱中五百万的梦想
 - 厌恶损失
 - 以小博大

多人存钱 一人中奖



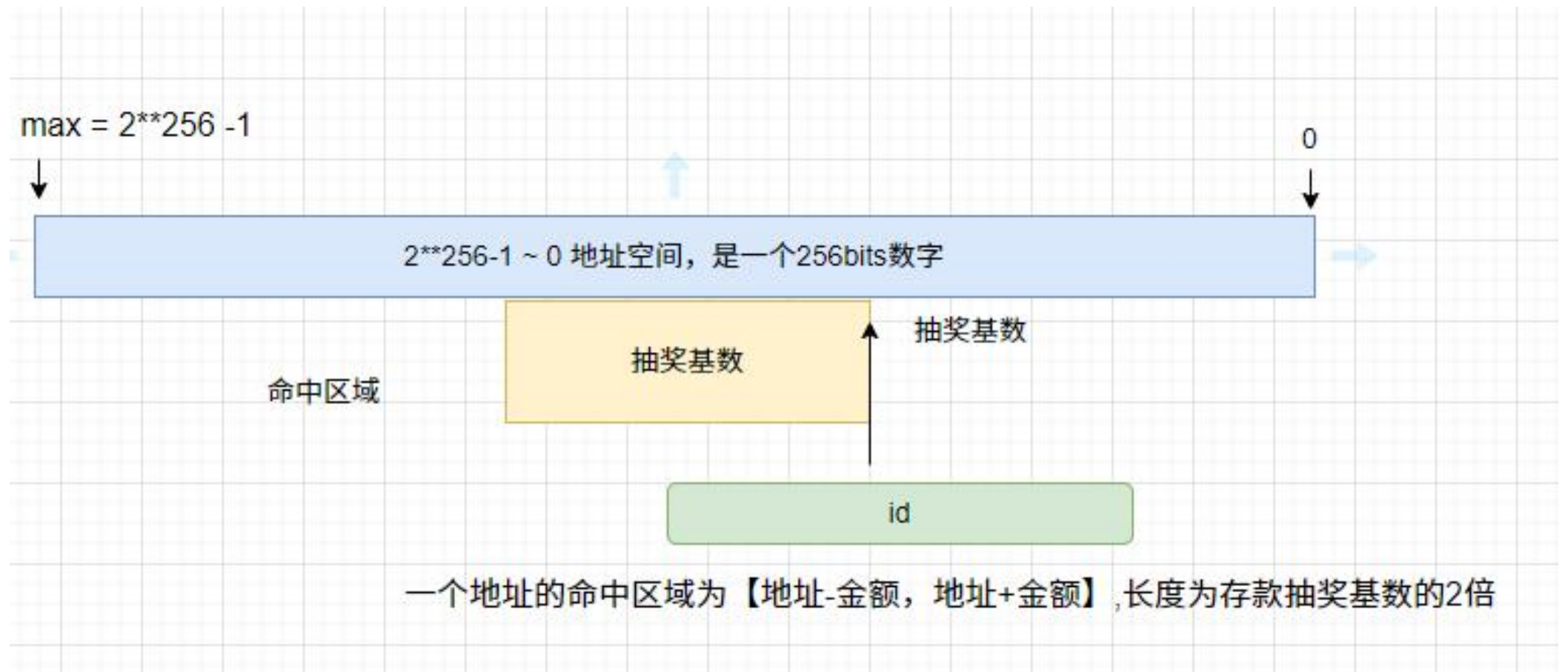
项目的优势

- 保本
 - 存钱还是有利息
- 中奖吸引人存钱
 - 存钱的人越多，奖金越多
 - 极少的钱，也可能中奖
 - 还可能中大奖
 - 更多的钱，更大的中奖比率

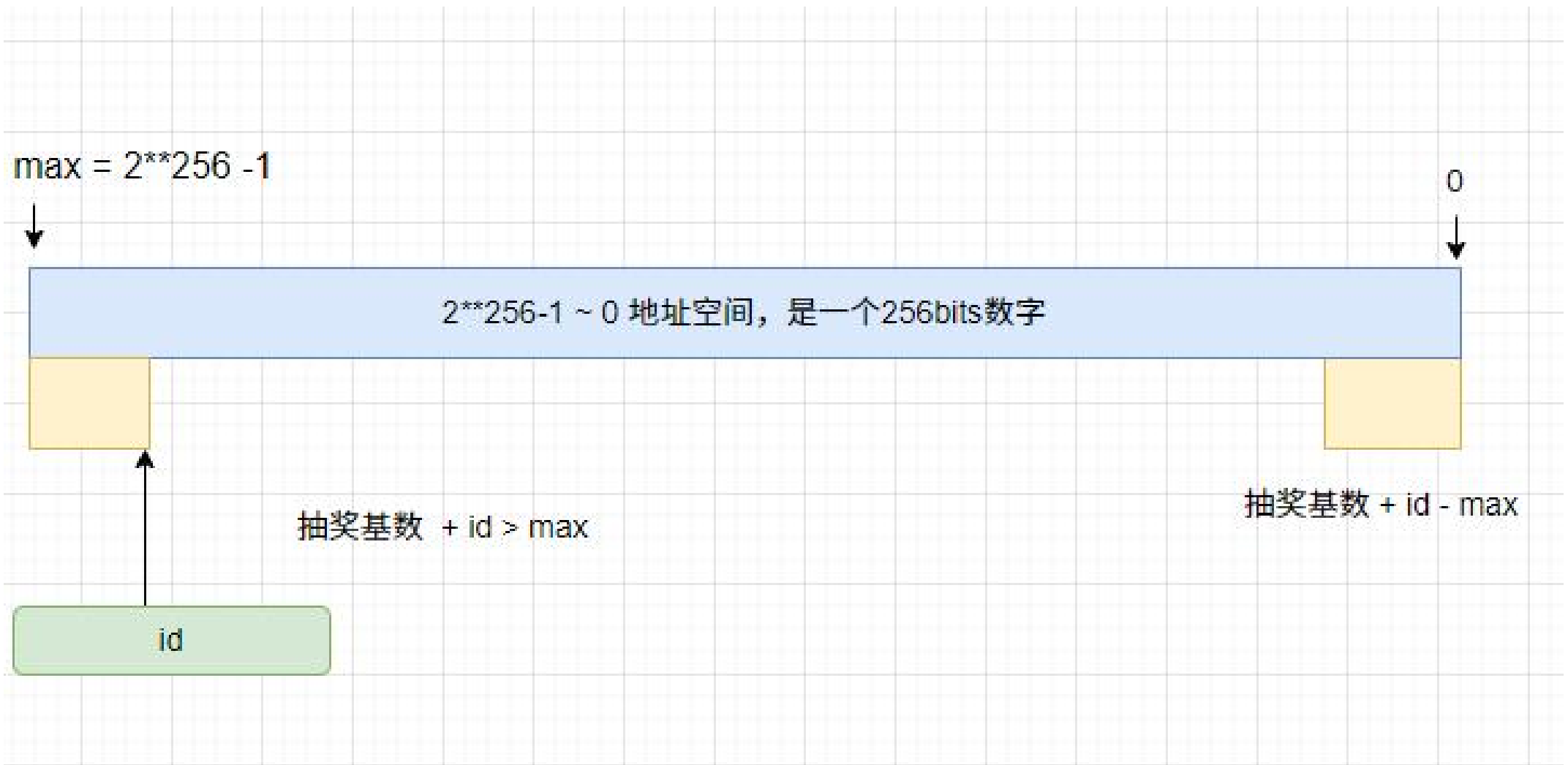
项目对SUI生态系统的意义

- 鼓励储蓄
 - 有利于SUI的币值稳定
- 给其他系统提供流动性
 - 未来可以考虑自己提供质押
- 激励散户存款
 - 以小博大
 - 极少的钱也可能命中大奖
 - 刚好中奖区域只有你一个用户
 - 拉新
 - 存钱的人越多，你中奖时奖金越多

每个地址有一个命中区域，



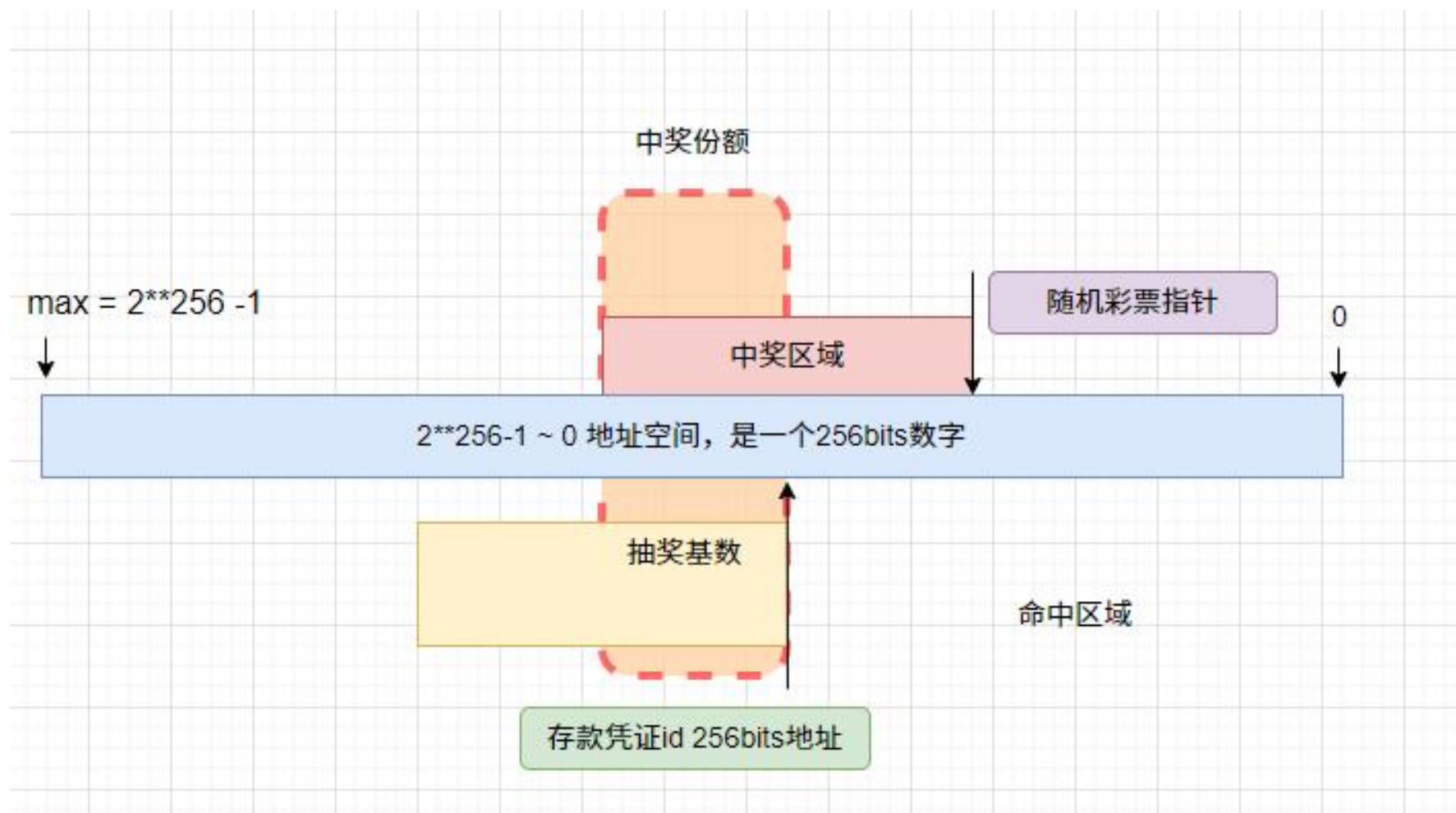
id值过大



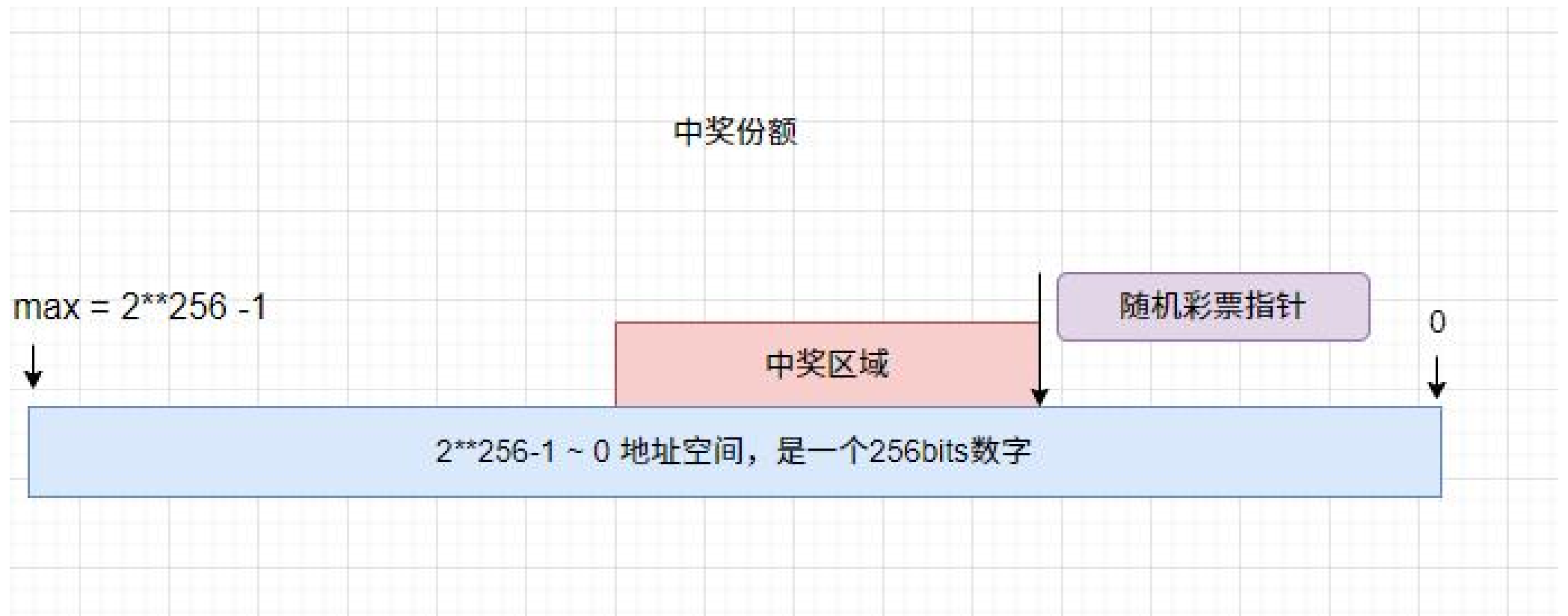
命中区域的说明

- 使用keccak256 生成的id, 随机分布
 - id 考虑使用用户的地址
 - id考虑在用户存款的时候生成一个256 id
 - 避免用户在外面构造多种地址攻击??
- 虽然使用 id + 存款基数, 但是因为顶端和低端设计, 每个点的命中概率应该是一致的。
- 抽奖基数 正比于 (利率 * 抽奖比例)
 - 每个用户可以选择 10%~100% 利率用于抽奖

中奖命中区域



中奖区域



中奖区域说明

- 随机指针

- 根据一定算法，一个256bit hash值

- 中奖区域长度

- 根据中奖比率计算出来的一个长度 (中奖区域长度 = $\max * \text{中奖比率}$)

中奖区域--顶部

中奖份额

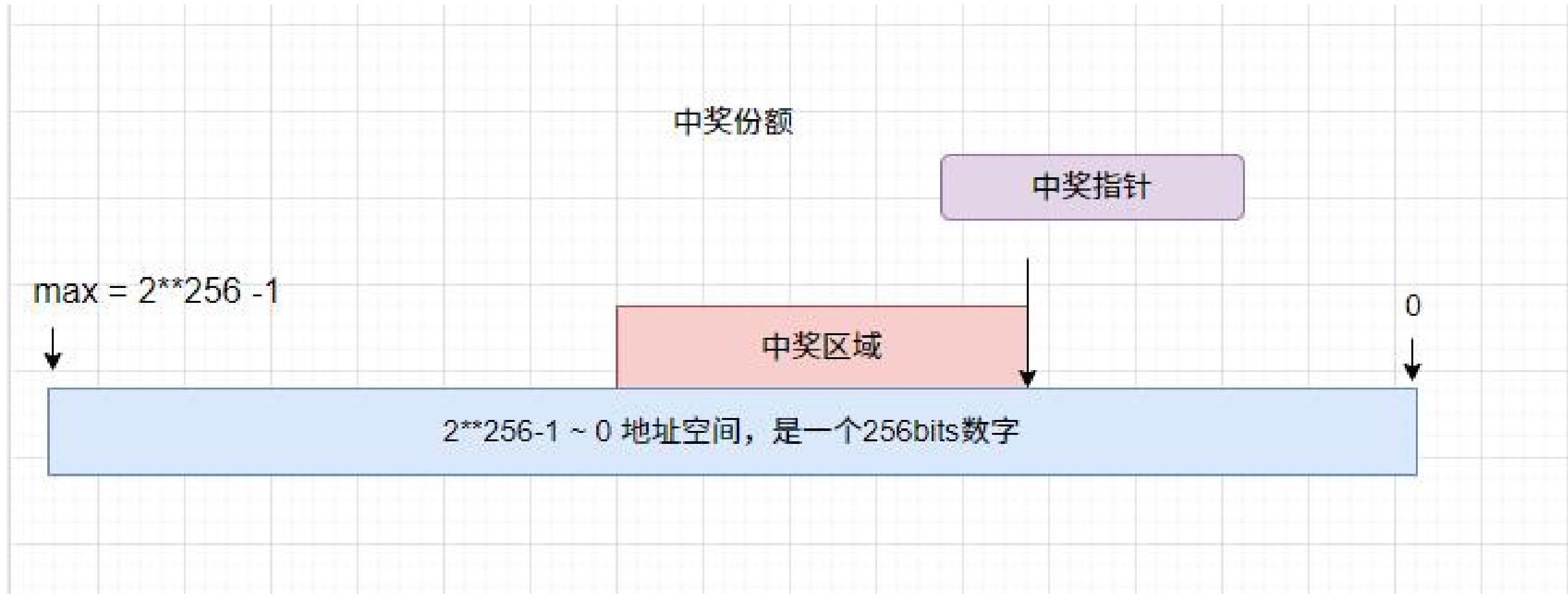
中奖指针

$\max = 2^{256} - 1$

0

中奖区域

$2^{256}-1 \sim 0$ 地址空间, 是一个256bits数字

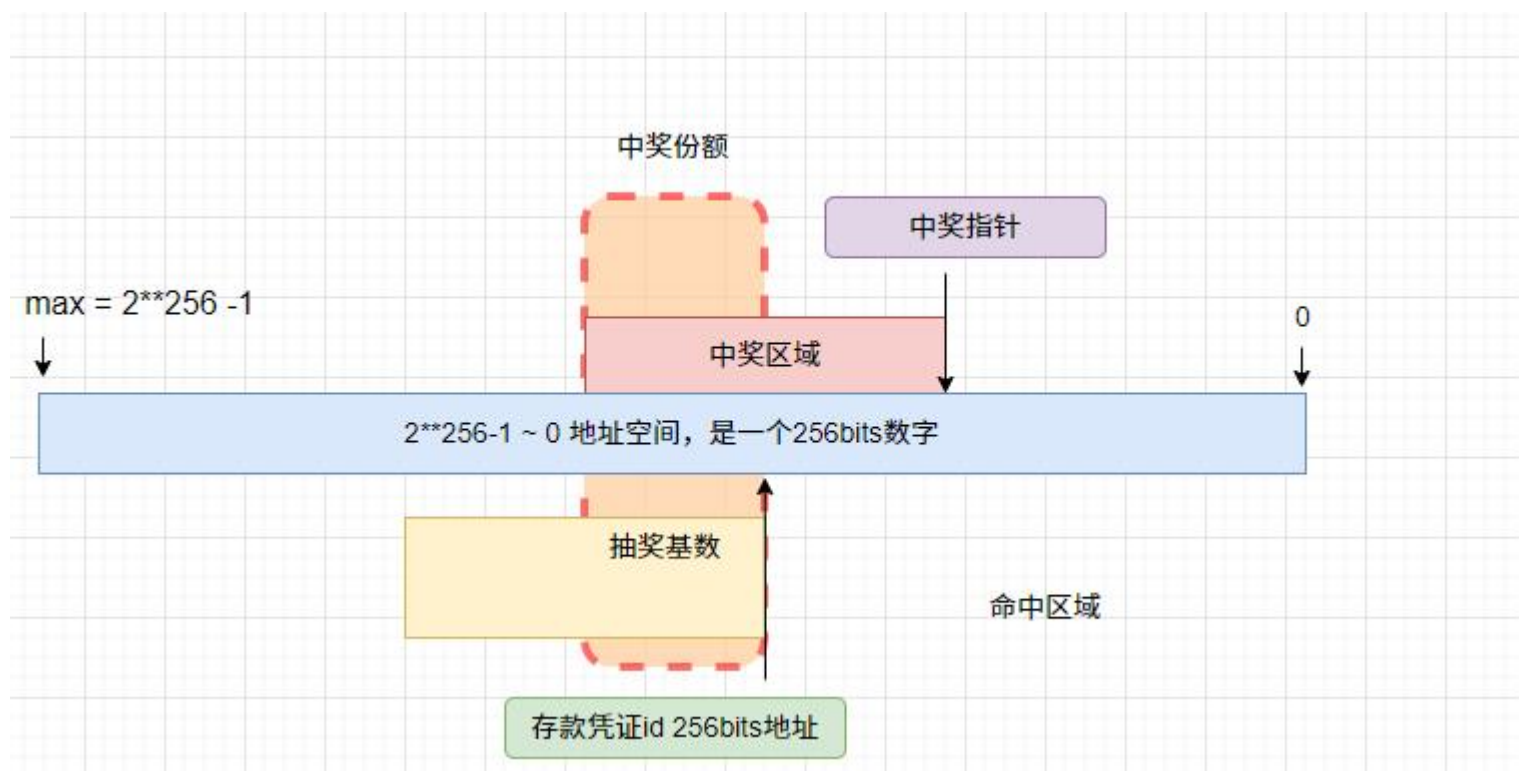


中奖区域, 底部 中奖指针 < 中奖区域长度

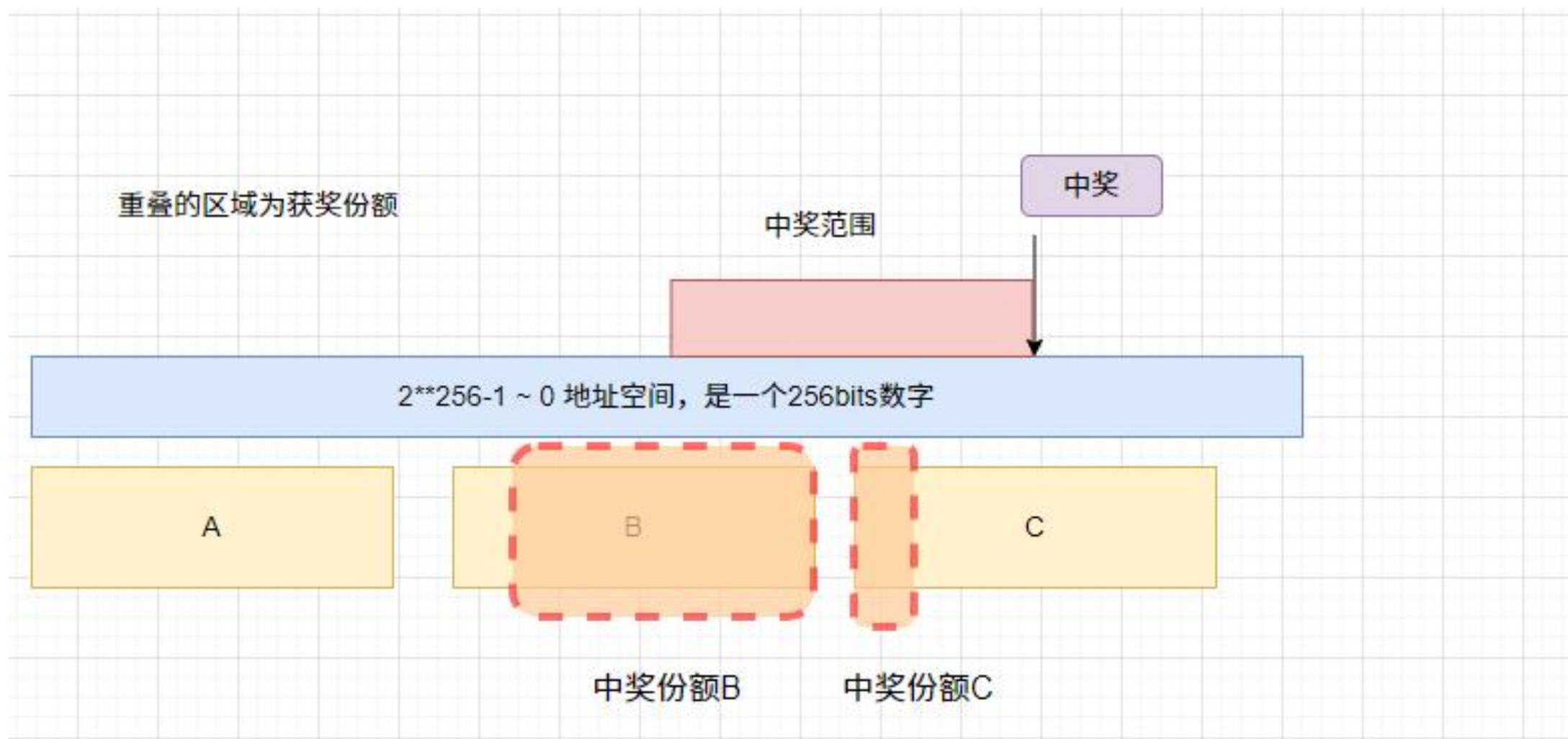


中奖判定

- 中奖份额
 - 用户的命中区域 和中奖区域重叠的长度



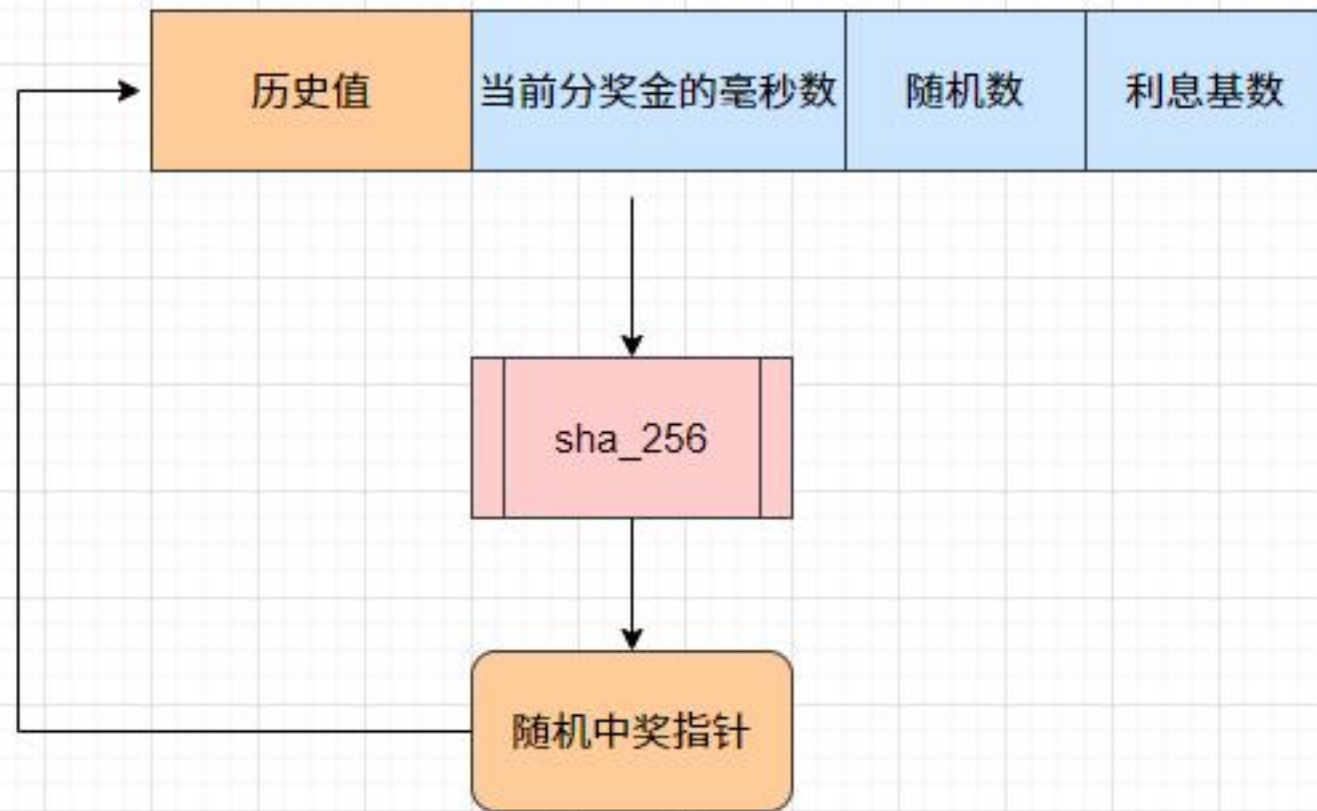
多人中奖分配



算法特点总结

- 即使极少的钱，也可能命中，得大奖
- hash算法命中范围分布比较均匀
- 更多的钱更容易命中
- 多个用户命中，命中的重叠的区域，往往花钱多的，更容易重叠区域大。
- 不损失本金

随机数设计



中奖区域比率设计

- 初始采用低费率
- 可以变更
- 最大费率限制不超过奖金的2.7%

项目方的支出和收入

- 支出

- 每日提交到stake的gas值
 - 从费用扣除。
- 抽奖计算的开销
 - 从总奖金扣除

- 收入：

- 抽奖总奖金的抽水比率

UI考虑

- 存钱
- 兑奖
- 中奖宣传
 - 当前总存款
 - 奖金
 - 奖金池总数
 - 参与人数
 - 往期中奖
 - 中奖地址
 - 中奖金额
 - 开奖区域
 - 存款金额
 - 抽奖比例