

≡ HOH 社区

存钱有奖系统

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

wechat: growfat mail:nextuser#163.com

汇报人：科学减肥



≡ HOH 社区

缘起

我总有一个2块钱中五百万的梦想

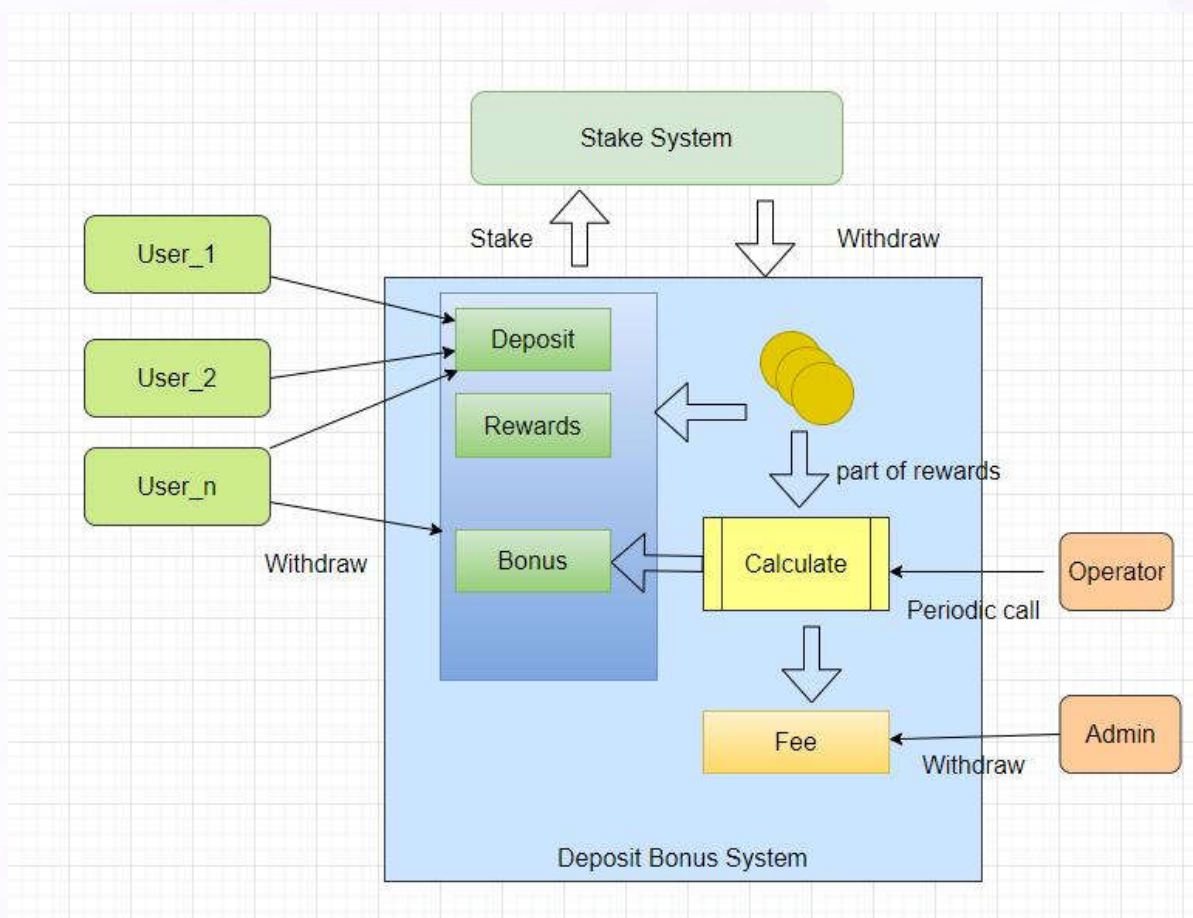
厌恶损失

以小博大

汇报人：科学减肥



多人存钱 少数人中奖



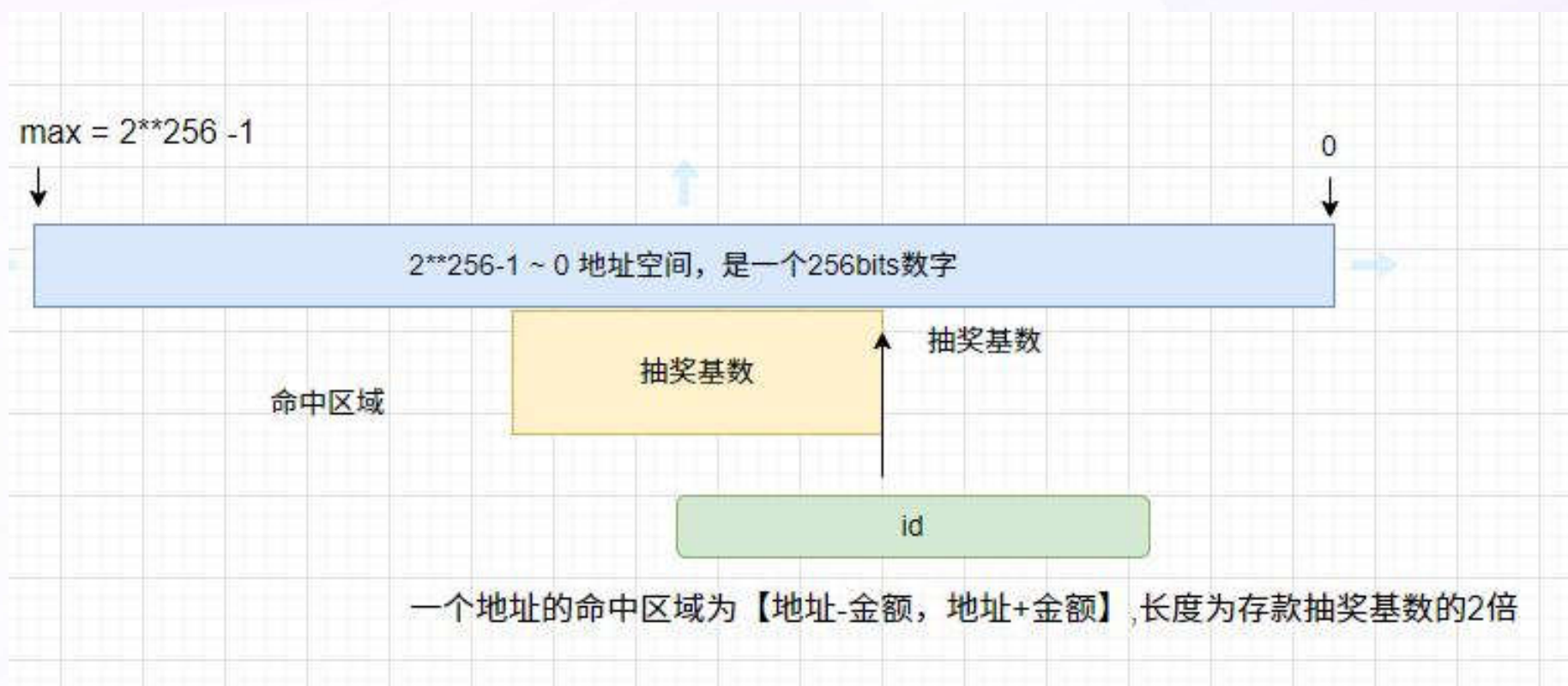
项目的优势

- 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服务
- 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



用户命中区域的说明

- 使用sha3_256 生成的id, 随机分布
 - id 目前使用用户的地址
 - 未来考虑系统另外生成一个256bit的id, 来规避攻击
- 虽然使用 $id + \text{存款基数}$, 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 = $(\text{存款利息} * \text{抽奖比例})$
 - 利息的 50% 用于抽奖

中奖区域说明

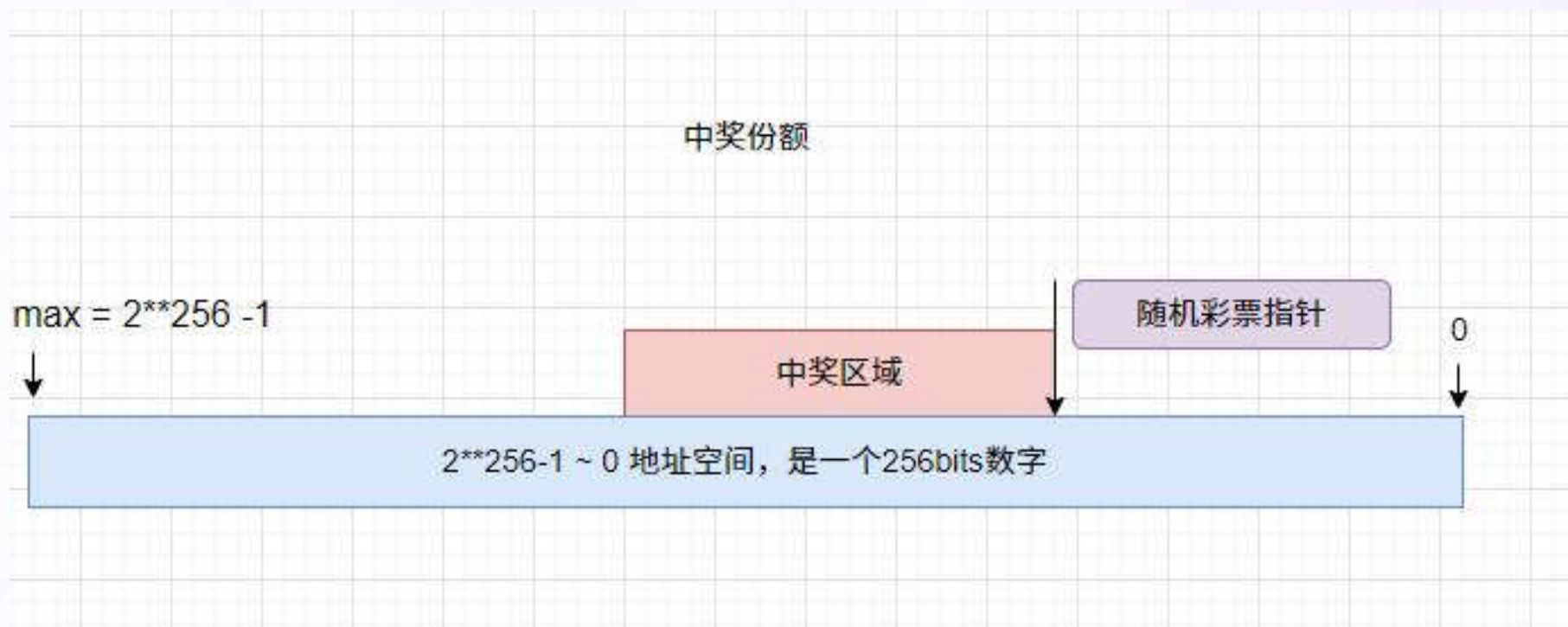
- 随机指针

- 根据一定随机算法，生成一个256bit hash值

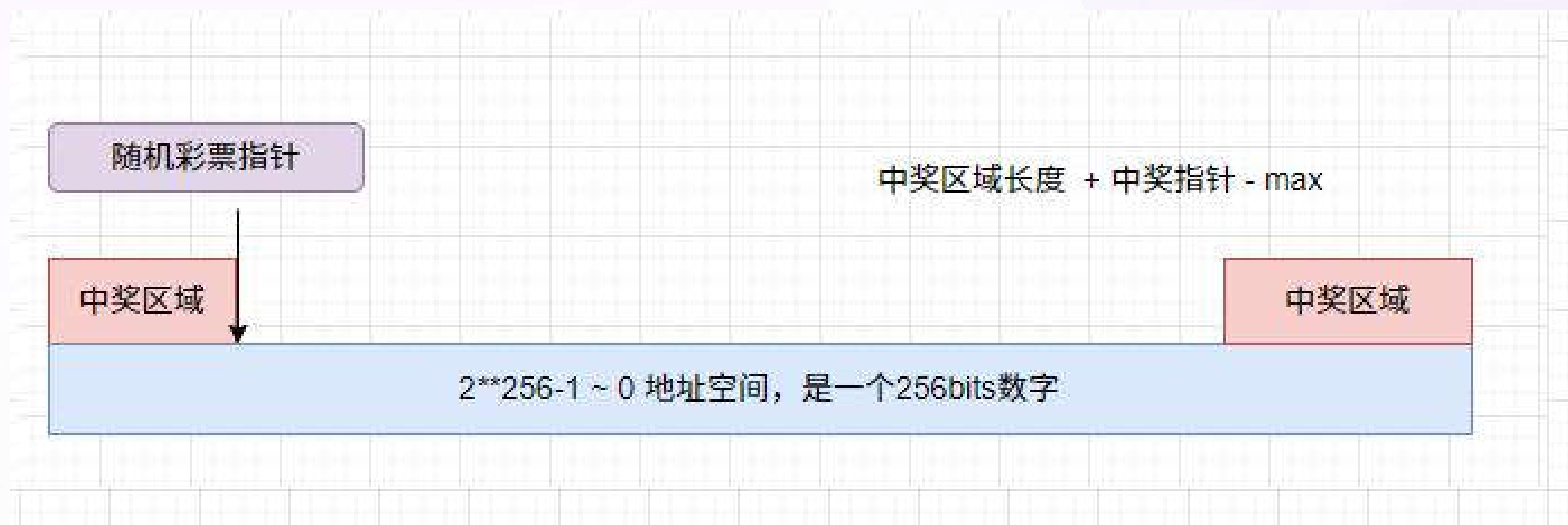
- 中奖区域长度

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

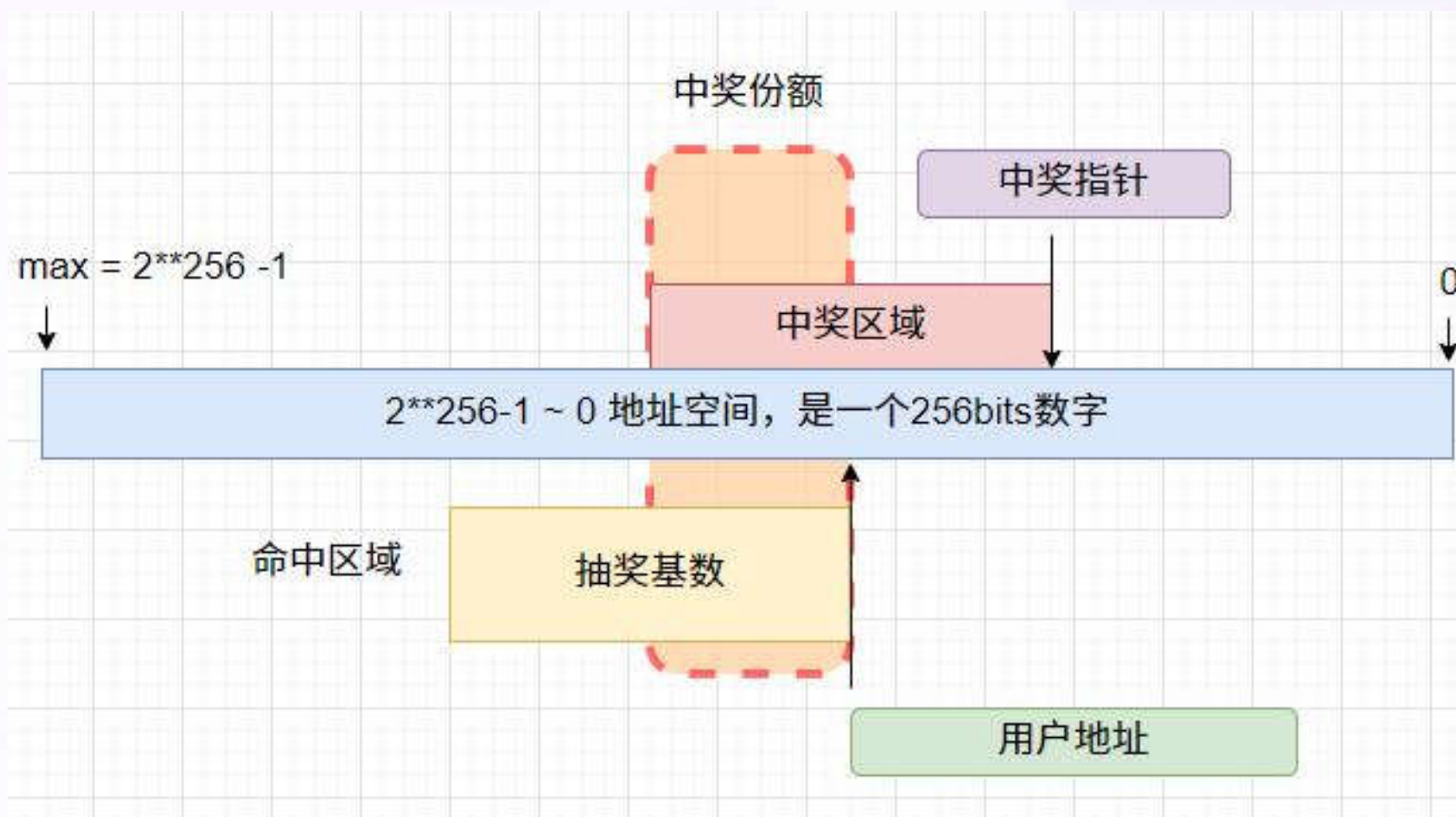
中奖区域----长度有中奖百分比决定



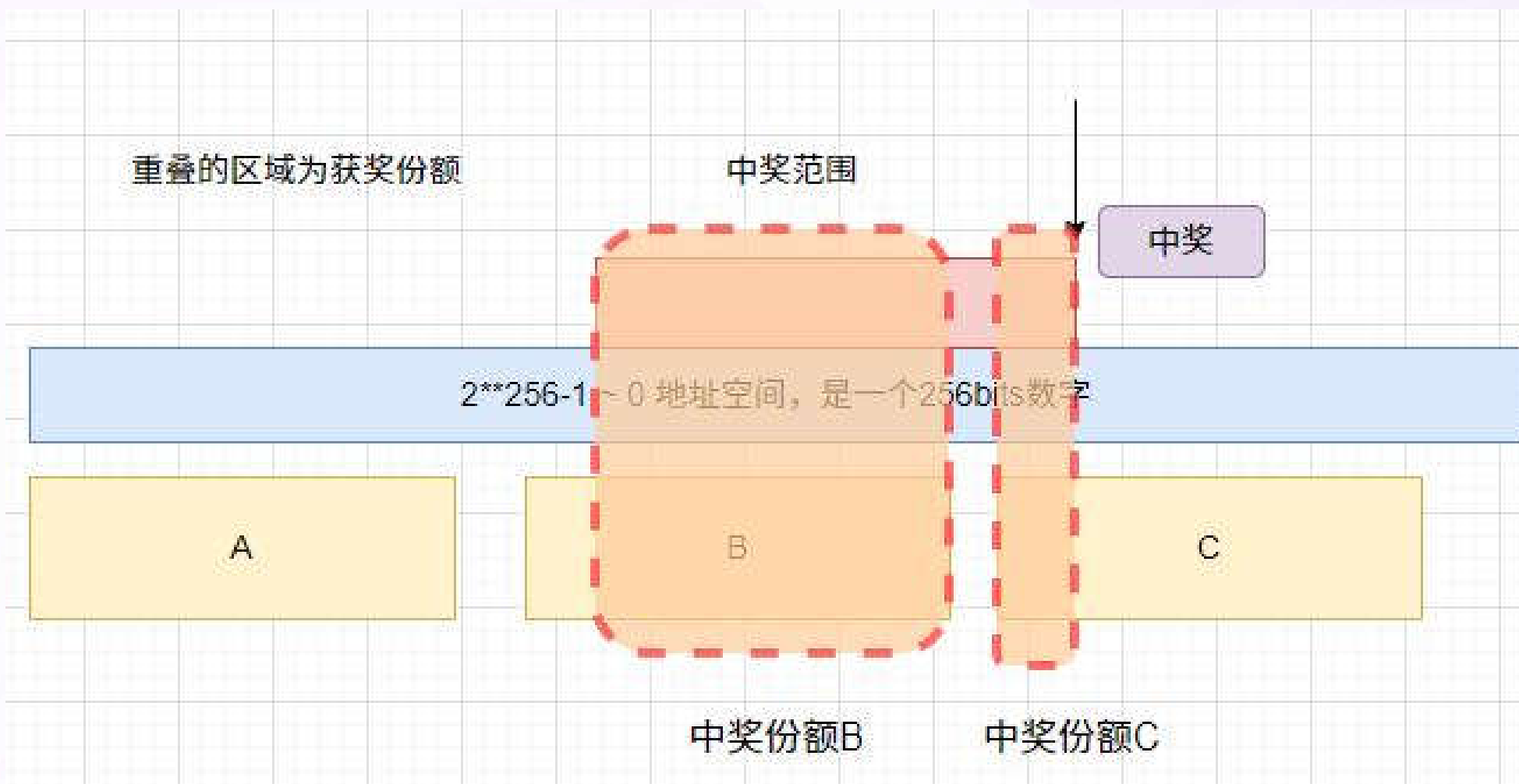
中奖区域--顶部



中奖命中区域-----重叠区域长度就是中奖份额



多人中奖分配

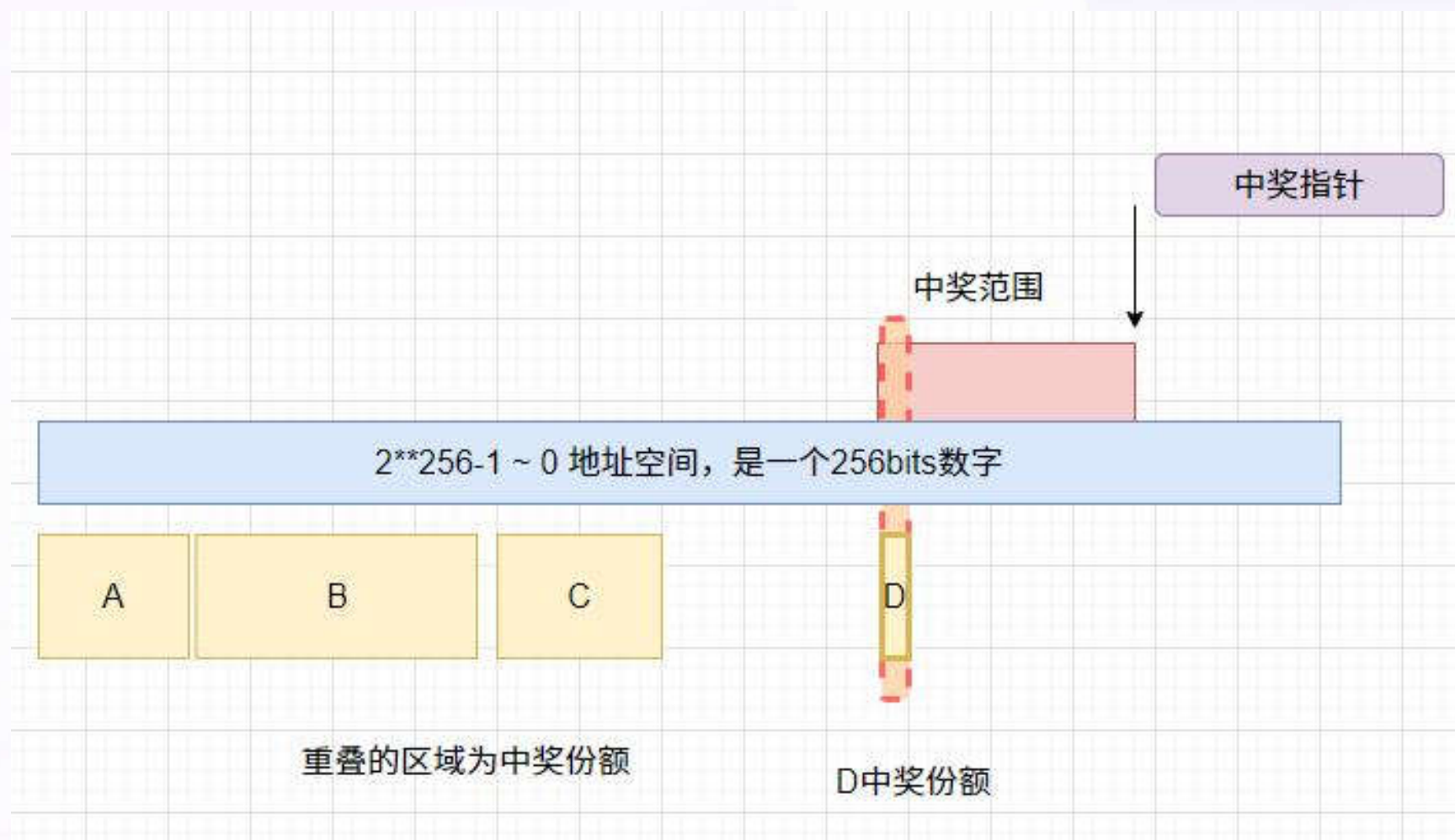


瓜分奖金

● B 奖金 = 总奖金 * B中奖份额/总中奖份额

● C 奖金 = 总奖金 * C中奖份额/总中奖份额

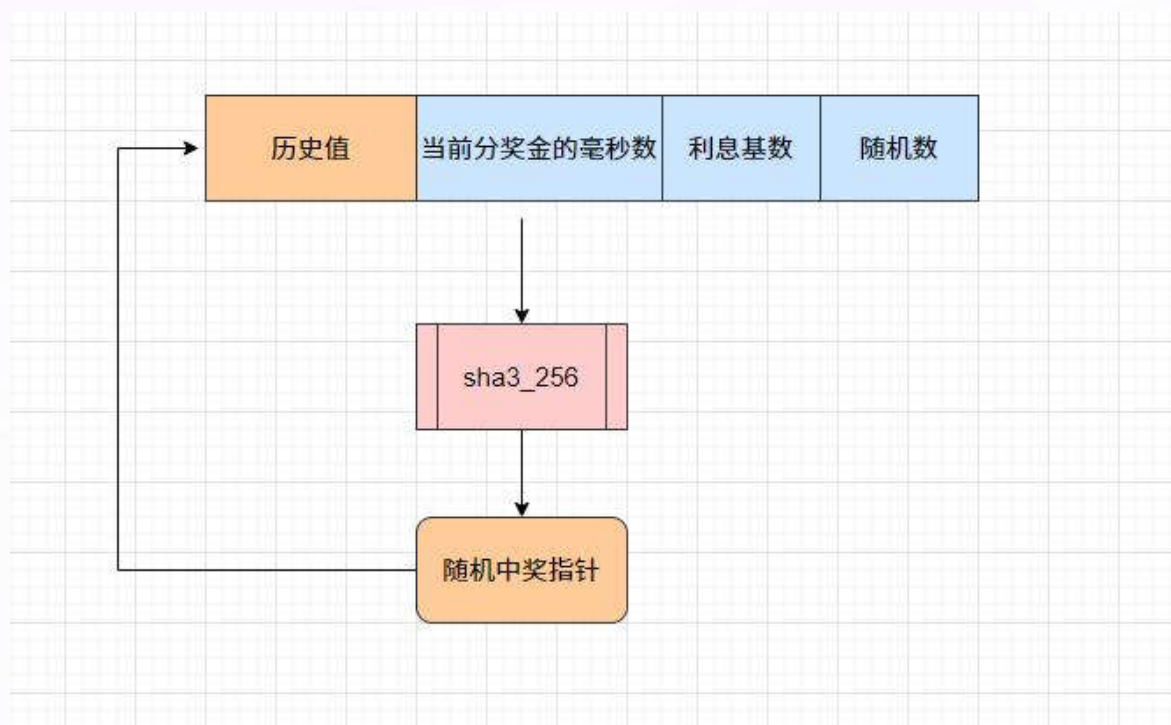
以小博大的可能



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

中奖指针-随机数设计



项目方的支出和收入

- 支出

- 定期开奖计算的gas费
 - 费用应该要能覆盖这笔开销

- 收入：

- 从总奖金按百分比扣除

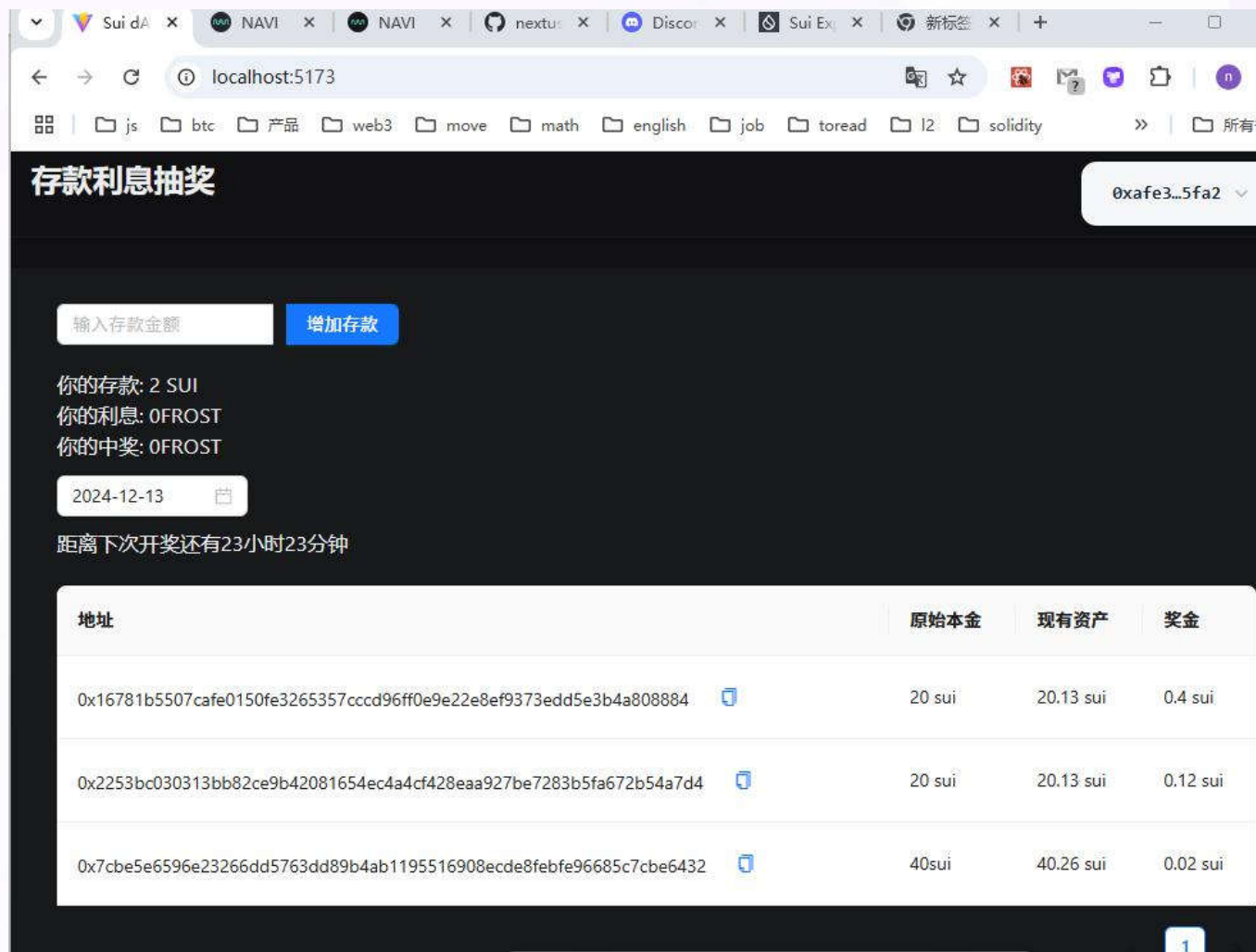
早期推广的考虑

- 项目方 donate 部分奖金
 - 用作构造演示数据
 - 有助于吸引用户存款

未来发展考虑

- 目前采用sui 系统的验证节点的质押
 - 优点
 - 稳定可靠
 - 接口稳定
- 未来
 - 考察其他高息质押平台
 - 作为质押平台的一个模块

UI



项目参与方

- 科学减肥 (wechat: growfat, tg: lose_weight)
 - 项目设计
 - 合约编写、测试
 - 构造测试数据
 - 联调界面
- goofy (wechat: MrHu9702)
 - 提供UI组件