01游戏介绍

<https://dappdog.github.io/01game.html>

# 游戏介绍：

一轮游戏中存在两名玩家，玩家可选的操作包括 在 0 和 1 两个数字选择一个作为自己的策略，并选择或生成一个随机种子来掩盖自己的策略。玩家首先提交自己的策略和随机种子拼接后的哈希值（在我们的实现中使用 MD5 算法）。在两名玩家的哈希值均提交之后，两名玩家再提交自己选择的策略以及随机种子的原始值。系统会验证该两者拼接后的哈希值是否与之前提交的值一致，从而确定玩家没有作弊，并根据两名玩家的原始策略确定两者的胜负。

玩家的胜负规则如下：如果两名玩家选择的策略相同，则开启游戏的玩家获胜，否则加入游戏的玩家获胜。

注意在游戏开始时我们需要两名玩家分别提交 0.01 NAS 作为押金，押金的作用仅仅为保证游戏的顺利及公平进行：1. 保证玩家在限定时限内进行下一步操作（通过超时机制） 2. 保证玩家在第二阶段提交的策略和随机种子没有经过修改（通过检验哈希值）。如果上面两点没有得到满足，则押金将会转入对方玩家账号。

在其他的所有情况下，押金将会完整退回，仅收取合约运行所必须的少量 gas 费用。

# 游戏特色：

本游戏使用了基于经济激励的加密算法承诺方案，其中的随机种子可以保证玩家提交的随机数在对方提交之前无法被猜到。同时，玩家的最优策略是随机选择0 1并随机化种子。游戏为零和博弈，存在稳定的纳什均衡，先后手玩家的期望收益相同，都是50%的概率获胜。

使用哈希函数以及随机种子的原因：我们要保证游戏双方不能在结果确定之前知晓对方的策略，否则后手玩家存在必胜策略。通过添加随机种子并将计算其哈希值我们可以保证最终揭晓出来的策略是玩家最初选择的策略，否则由哈希函数难以产生碰撞的性质可知哈希值会发生变化。如果随机种子不存在，则我们可以通过枚举0 或1的策略值来计算其哈希值，从而哈希函数便失去了隐藏最初策略的效果。

长久以来，无需信任各种第三方的公平博弈是一个难题，我们通过哈希函数+随机种子的方式解决了这一难题。

# 游戏操作：

注意：在进行每一次操作之后，请稍等片刻已使得交易被成功写入区块链。