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，系统会计算出这两者的拼接的哈希值。在两名玩家的哈希值均确定之后，两名玩家提交自己的随机种子的原始值。系统会据此计算出各玩家的策略，并且该计算出的策略是确定与玩家最初提交的策略相同的，这一点是由哈希函数的性质来保证。

玩家的收益计算如下：如果两者选择的策略相同，则开启游戏的玩家获得0.1 NAS，否则加入游戏的玩家获得 0.1 NAS.

# 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01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。

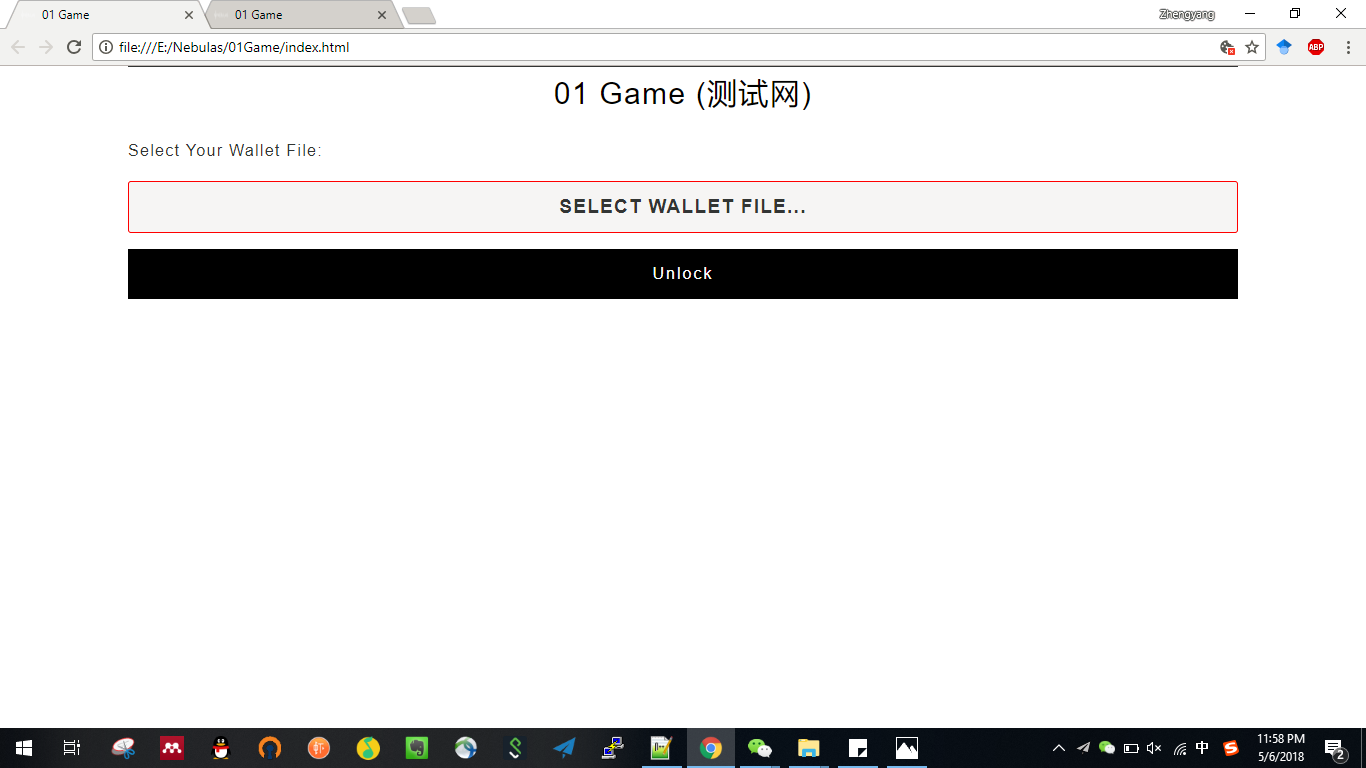
长久以来，无需信任各种第三方的公平博弈是一个难题，我们通过哈希函数+随机种子的方式解决了这一难题。

# 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。

游戏进行操作的截图如下所示：

玩家 A 首先进入游戏，会看到登录的界面：



玩家 A 登录钱包之后，如果当前没有游戏进行，会被要求选择自己的策略和确定随机种子以开启新游戏：



此时玩家 A已经选定了策略以及随机种子：



在玩家 A 提交了策略和随机种子的哈希值之后会看到等待另一玩家的界面：

在玩家B 同样登录了自己的钱包之后，会自动加入到已有的游戏之中：

玩家B选定了策略和随机种子之后：



在两名玩家均确定策略且提交过随机种子哈希值之后，会被要求提交随机种子原始值：



在两名玩家均提交过随机种子原始值之后，系统会自动判定游戏结果，并将相应的 NAS 进行转移（注意两名玩家的 balance 变化）：