Jogo de par ou ímpar em contrato

Executando o programa

Você precisa instalar o truffle com `npm -g install truffle`. Feito isso rode o ganache do jeito que quiser e poderá então rodar os testes com `truffle test`.

Considerações sobre o código

Eu fiz algumas mudanças na library do `SimpleCommit.sol`. Apenas mudanças de variáveis para funcionar para o propósito desse jogo e validações.

O código do `EvenOddGame.sol` tem várias validações. Uma delas é que apenas os dois endereços colocados no deploy podem interagir com o contrato.

Na hora de gerar o hash do valor escolhido enviar para o contrato o javascript me deu muitos problemas. Não consegui achar nenhuma maneira de gerar um hash, dentro do javascript, de um valor de 32 bytes em hexadecimal que o valor do seu hash com nonce fosse igual ao gerado pela função de hash Sha256 do Solidity. Tentei adicionar o padding na função, mudar o encoding, sem sucesso. Contornei esse problema fazendo uma função pura auxiliar dentro do contrato. Tive o cuidado para pensar que talvez a chamada dessa função pudesse ser registrada na blockchain de alguma forma, mas funções puras não fazem transactions, então se eu rodar apenas essa função, só o nó da rede diretamente conectado deveria ser capaz de ver os valores que foram enviados como parâmetros de função. Não tenho certeza ser funcionaria se os participantes tivessem acesso ao mesmo nó, mas em condições normais eles geralmente não tem, então acho que é uma solução ok. Encontrei essa informação aqui: https://ethereum.stackexchange.com/questions/57046/pure-function-execution-flow?rq=1

O arquivo `1_tests.js` descreve um jogo funcionando. Há o deploy do contrato, jogadores escolhem par ou ímpar. Em seguida enviam o commit dos seus valores escolhidos e revelam seus valores. O contrato recebe um valor de `startTime` e `endTime` durante o deploy no arquivo `1_initial_migration.js`. Esses valores são usados para aplicar a punição do jogador: se ele não revelar seu commit nesse intervalo de tempo, ele perde sua aposta para o outro jogador. Se nenhum dos dois revelar, o dinheiro fica para sempre no contrato. Se as duas partes revelarem, verifica se a soma dos números é par ou ímpar e o valor é retornado para quem apostou corretamente.