FACULTAD DE INGENIERIA
Universidad de Buenos Aires

Teoría de la Programación

75.24

Informe Individual

Etheroll

1er cuat 2018

Nombre	**Padrón**
Savulsky, Sebastián Alejandro	93081

Índice

Introducción

Se presentará el funcionamiento de Etheroll[1], un casino descentralizado de Ethereum en donde se apuesta en línea usando Ether en la red de Ethereum.
Posee su propia Criptomoneda; Etheroll Coin.
Etheroll Coin es una criptomoneda que garantiza un juego 100% justo. Basado en el protocolo de Ethereum y contratos inteligentes de Ethereum.
El margen de la casa es de 1% y la idea detrás del proyecto (al margen del interés económico de sus creadores) es ofrecer un juego que, al ser transparente, le garantiza al jugador que los vicios de los casinos tradicionales no están presentes.

Uso de Solidity

Se hizo uso[2] de de los Smart-Contracts de Solidity sobre la red Ethereum para garantizar un juego de dados de probabilidad justa 50/50, y un bajo margen para la casa de 1%.

Al estar en la red pública de Ethereum, cualquier interesado puede ingresar a la página de Github del proyecto y verificar[3] cómo están programados los smart-contracts de la plataforma.

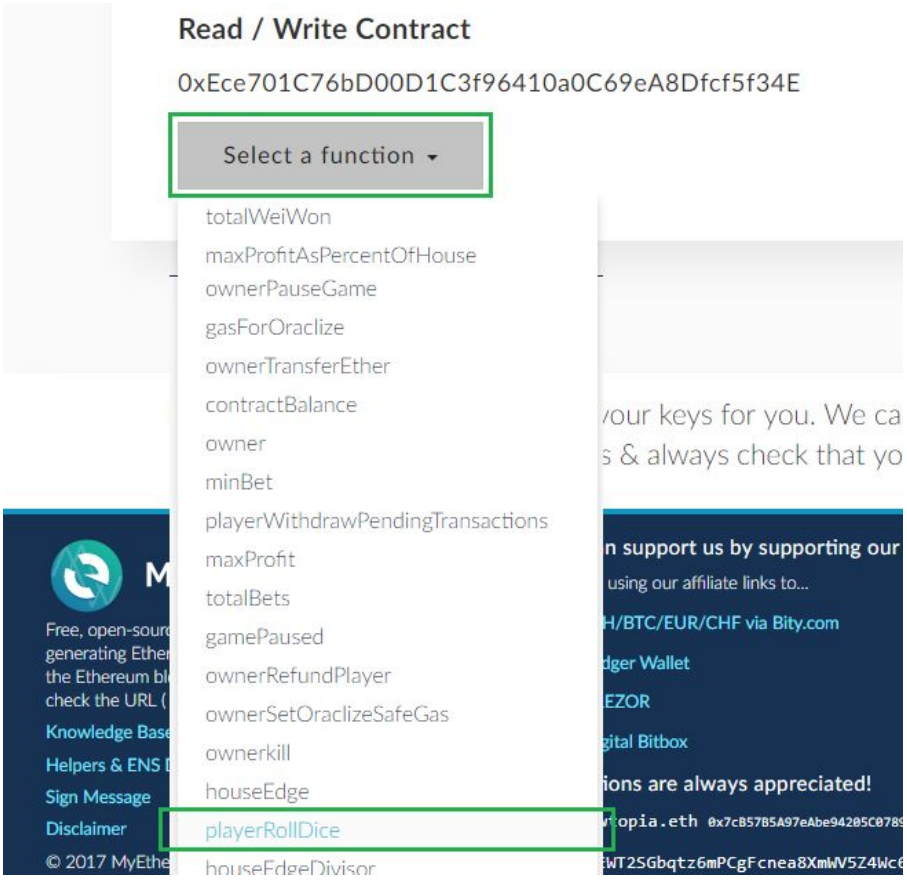
El Smart-Contract se encuentra publicado en la red Ethereum.
Etherscan es una de las plataformas por la que se pueden verificar los contratos y transacciones de la red:
https://etherscan.io/address/0x2e071D2966Aa7D8dECB1005885bA1977D6038A65#code

[1] https://etheroll.com/#/about
[2]https://steemit.com/steemit/@etheroll/hello-steem-i-am-the-founder-of-etheroll-an-ethereum-based-provably-fair-dice-game-with-50-50-odds-and-a-low-1-house-edge-this
[3] https://github.com/bokkypoobah/TokenTrader/wiki/DICE-%E2%80%90-Etheroll

Análisis del Smart-Contract de Etheroll

Probabilísticamente justo

Funciones del Smart-Contract de Etheroll



Como se puede apreciar en el Whitepaper de Etheroll[4], en la sección de Provably-fair (probabilísticamente justo), su generación de números aleatorios utiliza Oraclize.it (basado en cadena de bloques de código abierto) (un servicio de Oracle probabilísticamente justo) para recuperar un *entero* de forma segura desde fuera de la cadena de bloques. Este *entero* es suministrado por Random.org a través de TLSNotary. El contrato inteligente Etheroll luego realiza un cifrado sha3 () en el resultado devuelto por Random.org y la dirección IPFS de la prueba TLSNotary para alcanzar el resultado del final del dado. Actualmente, esta es la forma más segura para que Etheroll genere sus números aleatorios. Este método asegura a los posibles mineros atacantes y / o 3ras partes no pueden controlar el valor del resultado final de los dados.

[4] https://crowdfund.etheroll.com/etheroll-whitepaper.pdf

Al recibir una apuesta válida a través de la función playerRollDice (uint rollUnder), su SmartContract consulta Oraclize.it a través de una consulta parcialmente encriptada y anidada.
Al estar parcialmente encriptado, la consulta anidada asegura que la clave de la API que utiliza Etheroll para llamar a Random.org permanece segura, mientras que al exponer públicamente la solicitud y rango de números aleatorios, garantiza a los jugadores que el Smart-Contract es honesto.
Esto claro que se puede ver en el código.

El siguiente ejemplo de código en Solidity es el que usan para producir un número aleatorio razonablemente aceptable, limitado entre l y u inclusive (1, 100) y garantizado de tener una distribución uniforme a través del rango de valores:

```
finalResult = uint(sha3(r, p)) % 100 + 1;
```

En la misma sección explican que su contrato inteligente luego calcula el valor del entero **finalResult** vs el entero que fue enviado por el jugador (almacenado como **playerNumber**) a través de un mapeo a la dirección del jugador a través de lo siguiente:

```
mapping (bytes32 => uint) playerNumber;
function playerRollDice(uint rollUnder){
playerNumber[rngId] = rollUnder; }
```

Si **finalResult** es menor que **playerNumber** presentado por el jugador, el jugador gana. En este punto, el contrato inteligente calcula el pago requerido y paga las apuestas al instante, mientras se graban las propiedades de la apuesta en la cadena de bloques de Ethereum (como un evento), dejando un historial de las apuestas.