Desarrollo Blockchain Ethereum con Solidity

Módulo 6 - Introducción a Oráculos

Introducción a Oráculos

Limitaciones en la tecnología

- Basado en la tecnología distribuida de la plataforma, siempre que se ejecute la misma operación con los mismos datos se va a dar el mismo resultado.
- Esto se debe a que si no, sería imposible validar si la ejecución de un contrato es correcta.
- ¿Qué pasaría si se consultara una fuente externa, por ejemplo, la cotización del Ether?
  - Si se consulta supongamos un martes, una API convencional devuelve el valor de la fecha a ese momento.
  - Si se valida la transacción el miércoles, la API va a devolver una cotización distinta ya que siempre responde al momento en que se llama.
  - Además la API puede caerse, o puede ser hackeada, y sucedería el mismo problema.
- Por este motivo tampoco existen los números aleatorios en la plataform.

¿Cómo hacemos entonces para lidiar con estos problemas?

Generación aleatoria

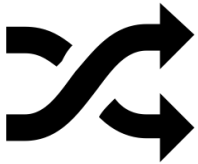
En Solidity, en Ethereum en realidad, dada la distribución real de la red, la no centralización y las inherentes condiciones por ser una Blockchain **NO existe** una manera real de **generar un número aleatorio.** No obstante, existen múltiples maneras de simular esta tarea.

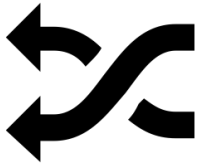
De momento, utilizaremos variables del bloque, el momento actual, entre otras, para generar un número pseudo-aleatorio.

```
function miFuncionRandom() private view returns (uint) {
    return uint(keccak256(block.difficulty, now, apostadores));
}
```

Generación aleatoria

Keccak256 nos es provisto por la simple utilización de Solidity, y nos permite generar un hash en base a los valores pasados por parámetro, los cuales para el caso de ejemplo, son la dificultad actual del bloque, el momento actual y un array de direcciones al que llamamos apostadores.



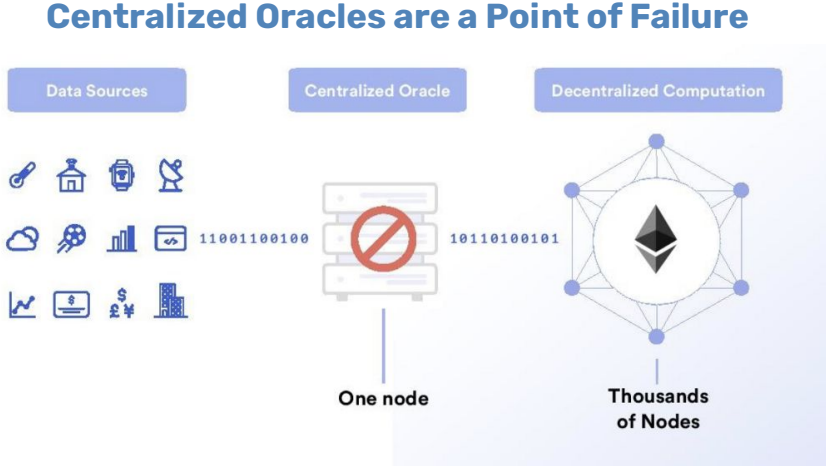


Oráculos

- Un oráculo en el entorno de blockchain es una entidad que conecta una plataforma de cadena de bloques con fuentes externas de datos que viven fuera de la misma.
- Los oráculos se encargan de tomar la información de las fuentes externas y brindarla a los contratos dentro de la blockchain.
- Sin embargo, los oráculos también tienen limitaciones...

Problemas con los oráculos

- Si la fuente de datos externa es centralizada, estamos consumiendo información centralizada en un entorno descentralizado.
- No es bueno que sea el oráculo el que tenga todo el poder de decisión sobre nuestro contrato, ya que a pesar de no tener malas intenciones puede ser atacado.



Fuente: https://docs.chain.link/

¡Muchas gracias!

¡Sigamos trabajando!