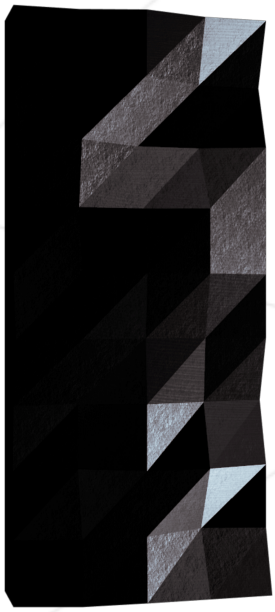

Bootcamp Ciberseguridad | 42 Madrid

ft_blockchain

Resumen: Criptografía y descentralización

Versión: 1

Índice general

Capítulo I

Introducción

El objetivo de este proyecto es crear una blockchain basada en una prueba de trabajo (`Proof of work`). Para ello, tendrás que implementar la lógica de la cadena de bloques, así como un servidor a través del cual se pueda interactuar con la misma.

Capítulo II

Prólogo

Una versión completamente electrónica del dinero en efectivo permitiría que los pagos en línea fuesen enviados directamente de un ente a otro sin tener que pasar por medio de una institución financiera. Firmas digitales proveen parte de la solución, pero los beneficios principales se pierden si existe un tercero confiable para prevenir el doble-gasto. Proponemos una solución al problema del doble gasto utilizando una red entre pares. La red coloca marcas de tiempo a las transacciones al crear un hash de las mismas en una cadena continua de pruebas de trabajo basadas en hashes, formando un registro que no puede ser cambiado sin volver a recrear la prueba de trabajo. La cadena más larga no solo sirve como la prueba de la secuencia de los eventos testificados, sino como prueba de que vino del gremio de poder de procesamiento de CPU más grande. Siempre que la mayoría del poder de procesamiento de CPU esté bajo el control de los nodos que no cooperan para atacar la red, estos generarán la cadena más larga y le llevarán la ventaja a los atacantes. La red en sí misma requiere una estructura mínima. Los mensajes son enviados bajo la base de mejor esfuerzo, y los nodos pueden irse y volver a unirse a la red como les parezca, aceptando la cadena de prueba de trabajo de lo que sucedió durante su ausencia.

Satoshi Nakamoto, 2012

`0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f`

Capítulo III

Instrucciones generales

Para este proyecto puedes utilizar cualquier lenguaje de programación. Puedes utilizar librerías criptográficas como `openssl` o `hashlib` para la generación de `hashes`, pero la estructura de la cadena de bloques debe ser implementada por ti. De la misma manera, un framework web como `NestJS` o `Flask` pueden ser utilizados para la implementación del servidor.

```
block =
{
    'index': 4,
    'timestamp': 1644045050.00042,
    'transactions': [
        {
            'sender': '4c6e7e2a9f2f7f7ff8e7d3d6c8b7c6e8e23a7',
            'recipient': 'b3c6e7e2a9f2f7f7ff8e7d3d6c8b7c6e8e23a7',
            'amount': 42,
        }
    ],
    'proof': 324984774000,
    'previous_hash':
        '084c799cd551dd1d8d5c5f9a5d593b2e931f5e36122ee5c793c1d08a19839cc0',
}
```

Ejemplo de un bloque. El hash del bloque anterior se ha generado mediante el algoritmo SHA-256.

Capítulo IV

Parte Obligatoria

El flujo de trabajo es añadir distintas transacciones al bloque actual y minar el bloque para que se añada la cadena.

El `algoritmo de la prueba de trabajo` debe ser simple, por ejemplo, encontrar el número que concatenado con la prueba de trabajo anterior, sea el resultado del hash SHA-256 termine en 4242. La cadena de bloques no será persistente, se almacenará en la memoria del servidor pero éste no estará conectado a ningún software específico de base de datos. A la hora de desarrollar la minería, se deben realizar tres cosas:

- Calcular la prueba de trabajo
- Recompensar a los mineros (una transacción)
- Creación del nuevo bloque y añadirlo a la cadena

Una vez creada la blockchain, se podrá interactuar con ella a través de diferentes peticiones HTTP:

POST `/transactions/new` : Envía una nueva transacción para añadir al próximo bloque.

GET `/mine` : Ejecuta la prueba de trabajo y crea un nuevo bloque.

GET `/chain` : Devuelve la información sobre la cadena de bloques (bloques, transacciones, etc).

Capítulo V

Parte Bonus

La evaluación de los bonus se hará `SI Y SOLO SI` la parte obligatoria es `PERFECTA`. De lo contrario, los bonus serán totalmente `IGNORADOS`.

Puedes mejorar tu proyecto con las siguientes características:

- Dificultad del algoritmo de PoW dinámica, ascendente en función del número de bloques minados o del tiempo transcurrido.
- Implementación de comunicación automatizada con otros nodos de la red mediante una red descentralizada y un algoritmo de consenso para verificar la cadena correcta.
- Implementación de Proof of Stake como forma alternativa de consenso (y mucho más ecológica que PoW).

Capítulo VI

Evaluación por pares

Este proyecto será corregido por tus compañeros. Entrega los archivos en el repositorio Git y asegúrate de que todo funciona como se espera.