**Informe de Laboratorio PTI –**

**Blockchain**

Sergio Mazzariol

## Acerca de Blockchain

Una cadena de bloques o cadena articulada, conocida en inglés como blockchain, es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se les añade metainformaciones relativas a otro bloque de la cadena anterior en una línea temporal, de manera que gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores.

Esta propiedad permite su aplicación en entorno distribuido de manera que la estructura de datos blockchain puede ejercer de base de datos pública no relacional que contenga un histórico irrefutable de información.

En la práctica ha permitido, gracias a la criptografía asimétrica y las funciones de resumen o hash, la implementación de un registro contable (ledger) distribuido que permite soportar y garantizar la seguridad de dinero digital.

Siguiendo un protocolo apropiado para todas las operaciones efectuadas sobre la blockchain, es posible alcanzar un consenso sobre la integridad de sus datos por parte de todos los participantes de la red sin necesidad de recurrir a una entidad de confianza que centralice la información. Por ello se considera una tecnología en la que la "verdad" (estado confiable del sistema) es construida, alcanzada y fortalecida por los propios miembros; incluso en un entorno en el que exista una minoría de nodos en la red con comportamiento malicioso (nodos sybil) dado que, en teoría, para comprometer los datos, un atacante requeriría de una mayor potencia de cómputo y presencia en la red que el resultante de la suma de todos los restantes nodos combinados.

Por las razones anteriores, la tecnología blockchain es especialmente adecuada para escenarios en los que se requiera almacenar de forma creciente datos ordenados en el tiempo, sin posibilidad de modificación ni revisión y cuya confianza pretenda ser distribuida en lugar de residir en una entidad certificadora. Este enfoque tiene diferentes aspectos:

* Almacenamiento de datos: se logra mediante la replicación de la información de la cadena de bloques
* Transmisión de datos: se logra mediante redes de pares.
* Confirmación de datos: se logra mediante un proceso de consenso entre los nodos participantes. El tipo de algoritmo más utilizado es el de prueba de trabajo en el que hay un proceso abierto competitivo y transparente de validación de las nuevas entradas llamada minería.

Para nuestra practica realizaremos la programación de nuestra cadena de bloques en python3.6.

Para compilar un codigo en python utilizaremos el comando

python blockchain.py -p 5000

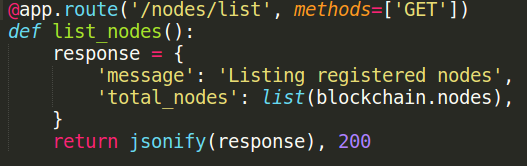
Primero optenemos el codigo del repositorio gitlab, luego procedemos a crear un script, en el cual se generan varias transacciones en dos nodos y luego estos proceden a sincronizarse, de esta forma podemos ver como los datos pasan de un nodo a otro hasta estar iguales.

Tenemos que realizar algo similar que con la practica de GoLang, ejecutar una función al acceder a una URL.

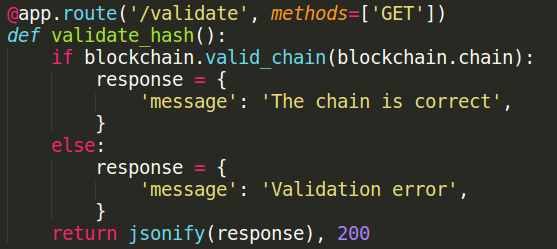
Para este caso generaremos una nueva función que será litar todos los nodos de la red registrados, para realizar el redireccionamiento hacemos

@app.route('/nodes/list', methods=['GET'])

luego solicitamos a nuestra cadena de bloque los nodos y que los imprima en formato Json con la librería jsonify.



La siguiente función generada es la de validar cadena, esto revisa que no se haya realizado ninguna modificación en la cadena.



Y por último manipular la cadena de nodos, cambiar un valor para asi poder comprobar si nuestra cadena se ha modificado, con la función validate.

## 

## Otras opciones posibles

Para realizar la programación de blockchain se puede realizar en casi cualquier lenguaje, pero hoy en día hay un lenguaje especializado para esto y se llama Solidity, esta especialmente diseñado para realizar esta tarea.

## Aspectos positivos y negativos

Tiene un gran campo de uso, por lo que lo convierte en una gran tecnología, permite realizar muchas tareas sin intermediarios, lo que permite hacer transacciones más seguras, también tiene un amplio uso en otras áreas que no son solo dinero, hoy en día se esta utilizando la red etherum para este último caso.

El gran uso de energía por la cantidad de cálculos que se necesitan a medida que la cadena va creciendo, esto es un gran problema que esta afectando hasta a ciudades completas.