

**Ingeniería Matemática e Inteligencia Artificial**

**Memoria Blockchain**

Práctica Final

Fundamentos de los Sistemas Operativos

Sergio Herreros Pérez

Daniel Sánchez Sánchez

**BlockChain.py**

* **Clase Bloque**:
  + Forma los cimientos de la cadena. Cada bloque tiene unas ciertas transacciones, las cuáles se formalizan una vez que el bloque se une a la cadena. Para “enganchar” los bloques entre sí, se le da un hash generado según su propia estructura, además de tener un valor de prueba para que cumpla con la dificultad elegida (que empiece con cierto número de ceros), y tiene el hash del bloque anterior en la cadena. Por último, tiene un índice y un registro de tiempo correspondiente a su creación.
  + Además, tiene tres métodos: calcular hash, el cual calcula el hash del bloque; toDict, el cual simplemente pasa el bloque a diccionario, y fromDict, que hace lo contrario.
* **Clase Blockchain**:
  + La cadena. Sirve para conectar los bloques y contiene la gran mayoría de métodos. Contiene una lista con los bloques añadidos, una lista con las transacciones aun no añadidas, su nivel de dificultad (explicado en la clase bloque) y el número de bloques añadidos. Además, para empezar, se añade un nuevo bloque.

Sus métodos son:

1. Primer bloque: Crea un nuevo bloque con hash previo igual al string 1 y lo integra, inicializándose con el hash que le corresponde
2. Nuevo bloque: Crea un nuevo bloque dado un hash previo cuyas transacciones son el pool de blockchain y lo devuelve
3. Nueva transacción: Crea una nueva transacción con un origen, una cantidad y un destino y la añade a pool.
4. Prueba trabajo: Calculará el hash del bloque añadiendo uno a la prueba hasta que cumpla la dificultad.
5. Prueba válida: Comprueba que un bloque tenga un hash correcto.
6. Integra bloque: Añade un bloque dado a la blockchain si el hash previo y su hash son correctos.
7. Check chain: Recorre la cadena desde el inicio y si algún bloque tiene un hash previo incorrecto, devuelve False. En caso contrario devolverá True.
8. toDict: Pasa la clase a diccionario (al igual que cada bloque de la blockchain).
9. fromDict: Crea la clase a partir de un diccionario creado por toDict.

El funcionamiento será el siguiente: se creará la blockchain cuando se inicialice el programa (con ello generándose el primer bloque). Se irán haciendo transacciones a medida que se hagan requests, y una vez que se mine un bloque (y no haya conflictos), se añadirán esas transacciones al nuevo bloque.

**Blockchain\_app.py**

En este fichero se incluye la funcionalidad de la aplicación de Blockchain. Utilizando Flask, creamos una app que se podrá ejecutar por cada nodo y permitirá la conexión con otros nodos, de manera que se cree una red peer-to-peer.

Aquí se creará una instancia de la clase Blockchain, y un set con los nodos de la red.

* **Nueva transacción:**
  + Asociamos la ruta “/transacciones/nueva” y el método POST a la funcion nueva\_transaccion().
  + Recibe un json con el contenido de la transacción, comprueba que al menos contiene origen destino y cantidad, y la incluye al pool de la Blockchain.
  + Devolvemos un string con formato json con la respuesta y el HTTP status code, que será 200 en caso de haberla incluido correctamente, o 400 si no contenía los campos necesarios.
* **Blockchain completa:**
  + Asociamos la ruta “/chain” y el método GET a la función blockchain\_completa().
  + Esta es una funcion para compartir la cadena con otros nodos, o poder ver la cadena en cualquier momento.
  + Devolvemos un string con formato json con la cadena y su longitud y el status 200 en caso de haberla incluido correctamente, o un mensaje de error y el status 500 en caso de haber habido algún fallo del lado del servidor. Esto nos ayuda mucho a la hora de debuggear la app.
* **Minar:**
  + Asociamos la ruta “/minar” y el método GET a la función minar().
  + En esta funcion, se sacan las transacciones no confirmadas de la pool y se crea un nuevo bloque para incluirlo en la cadena, calculando la prueba de trabajo correspondiente.
  + Pueden pasar varias cosas:
    - Si no había transacciones, devolvemos un mensaje y el status code 201
    - Si si que había, creamos un bloque con estas y comenzamos a trabajar en la prueba de trabajo. Una vez encontrado el nonce, procedemos a comprobar que no hay otra cadena de mayor longitud que la nuestra con la funcion resuelve\_conflictos().
    - Si somos la cadena mas larga, integramos el bloque en la cadena principal y quitamos del pool de transacciones las que acabamos de incluir. No la vaciamos del todo ya que en el tiempo que minamos el bloque (en bitcoin serian unos 10 mins) podrían llegar muchas nuevas transacciones a nuestra pool, y estas no habría que eliminarlas.

Si todo ha ido bien, recibimos un pago por minar creando una transacción a nosotros mismos, y devolvemos un json con el ultimo bloque minado, y el status code 200.

* + - En caso de conflicto, se actualizara nuestra cadena con la nueva mas larga, se desechara el bloque que acabamos de minar, y se devolvera un mensaje diciendo que ha habido un conflicto, y el status code 202.
    - Si ha habido algún problema integrando el bloque, se devolverá el status 203.
* **Regristrar nodos:**
  + Asociamos la ruta “/nodos/registrar” y el método POST a la función registrar\_nodos\_completo().
  + En esta funcion y en la siguiente se incluirá la funcionalidad de red peer-to-peer.
  + Primero comprobamos que nos ha llegado una lista con nuevos nodos, y en caso contrario devolvemos un 400.
  + Si tenemos la lista, comprobamos que cada nodo es un string con formato <http://ip:puerto>. Los que no lo sean, los quitamos y guardamos en un set.
  + Después, enviamos a cada nodo una copia de nuestra blockchain, y una copia de los nodos de la red, incluyéndonos a nosotros y excluyendo a dicho nodo. Los nodos a los que no es posible conectarse, los quitamos y guardamos en un set.
  + Finalmente añadimos a nuestra copia de nodos los nuevos nodos que se han podido conectar.
  + En caso de que todos los nodos se hayan conectado y estén bien formateados, devolvemos un mensaje satisfactorio y un 200.
  + En caso contrario, devolvemos un mensaje indicando que nodos han dado que tipo de fallo, y el código 201.
* **Actualizar blockchain:**
  + Asociamos la ruta “/nodos/registro\_simple”y el método POST a la función registrar\_nodo\_actualiza\_blockchain()
  + Esta funcion sirve para registrar a cada nodo desde la funcion mencionada anteriormente. Recibe la copia de la blockchain y los nodos de la red, actualizando su blockchain y los nodos para poder formar parte de la red.
  + Si falta o la blockchain o los nodos, se devuelve un 400
  + Si no, comprobamos que la blockchain recibida es válida, en cuyo caso simplemente actualizamos nuestra cadena, y si no lo es, devolvemos un mensaje avisando de que la blockchain es corrupta, con código 401.
* **Resolver conflictos:**
  + Esta función no va asociada a la app.
  + Simplemente se usa al minar para comprobar nodo por nodo si hay una cadena mas larga antes de incluir nuestro bloque recién minado.
  + Si no se encuentra ninguna cadena mas larga, devolvemos False, diciendo que no hay ningún conflicto.
  + En cambio, si ha habido conflicto, y existe una cadena valida mas larga, procedemos a reemplazar nuestra cadena con dicha cadena, y a quitar de nuestro pool de transacciones las que ya han sido incluidas en dicha cadena, para así no repetir transacciones y crear bloques no válidos. En este caso se devuelve True, indicando que si que ha habido un conflicto, y así desechar el bloque en la función de minar.