Ensayo acerca del Block-Chain

Autor: Jairo Alejandro Castrillon Libreros

*Facultad de Ingenierías, Universidad Tecnológica de Pereira, Pereira, Colombia*

Correo-e: alejandro.castrillon@utp.edu.co

Block-Chain (“Cadena de Bloques”) son un tipo de estructura de datos donde la información se agrupa en contenedores (bloques) y a estos se le añade meta información haciendo referencia a otros bloques de la cadena anterior en una línea temporal (Técnica Criptográfica).

Debido a la implementación de la anterior técnica criptográfica la información de un bloque solo puede ser modificada alterando el contenido de todos los bloques posteriores lo que hace más difícil la corrupción de los mismos. Este nivel de seguridad permite aplicar el block-chain a entornos distribuidos tales como una base de datos pública no relacional o hasta un historial irrefutable de información. También gracias a este valor que tiene el block-chain se ha utilizado en la implementación de registro contable (ledger).

Es una estructura de datos integral, ya que es construida, alcanzada y fortalecida por los miembros que tienen acceso a dicha cadena y es especialmente adecuada para escenarios en los que se necesite almacenar de manera creciente datos ordenados en el tiempo, sin posibilidad de realizar modificación ni revisión y cuya confianza pretenda ser distribuida.

El concepto de Block-Chain fue aplicado por primera vez en el 2009 como parte de Bitcoin como manera de no permitir al usuario gastar dos veces un monto determinado.

Block-Chain se utiliza en los siguientes campos:

* **Criptomonedas:** Se utiliza como notario publico (registro de transacciones) no modificable de todo el sistema de transacciones.
* **Bases de datos de registro de nombres.**
* **Transacciones bancarias:** Como notario distribuido (dificulta el lavado de dinero)

**Clasificación:** Se da por el tipo de acceso a los datos y los permisos que tengan las cadenas de bloques y son las siguientes:

* **Acceso:**
* **Cadenas de bloques pública:** No tiene restricciones de lectura y escritura (guardar) transacciones, son de fácil acceso y salida, transparentes y construidas con precaución para la operación en un entorno confiable.
* **Cadenas de bloques privada:** Tiene restricción de acceso, solo para una lista de entidades predefinida.
* **Permisos:**
  + **Cadenas de bloques sin permiso:** No hay restricciones para que las entidades puedan procesar transacciones y crear bloques de información. Se necesitan tokens (incentivos) para estimular a las entidades a mantener la cadena. Un caso muy conocido de esto se da en Bitcoin que para obtener el nuevo bitcoin es necesario construir un bloque y las comisiones de las transacciones.
  + **Cadenas de bloques con permiso:** El procedimiento de transacciones solo está permitido e implementado para una lista de sujetos con identidades conocidas. Generalmente no se necesitan tokens nativos.

**Posibles combinaciones de acceso y permisos**

* **Cadenas de bloques publicas sin permisos:** Como no es posible la existencia de cadenas de bloques privadas sin permisos, a estas también se las llama simplemente cadenas de bloques sin permisos.
* **Cadenas de bloques privadas con permisos:** Esta combinación es posible por los siguientes factores:
  + **Leer las transacciones de bloques, quizás con algunas restricciones.**
  + **Proponer nuevas transacciones para la inclusión en la cadena de bloques.**
  + **Crear nuevos bloques de transacciones y añadirlo a la cadena de bloques.**

Las cadenas de bloques también pueden ser clasificadas según el modelo de estado en la base de datos:

* **Basada en el gusto de salidas de transacciones (Modelo UTXO):** En ellas cada transacción gasta salidas de transacciones anteriores y produce nuevas salidas que serán consumidas en transacciones posteriores. Este tipo de cadenas de bloques es ampliamente utilizado en Bitcoin.
  + **Ventajas:**
    - En la propia estructura de la cadena existe una prueba de que nunca se puede gastar dos veces ya que cada transacción prueba que la suma de sus entradas es más grande que la suma de las salidas.
    - Cada transacción puede ser procesada en paralelo porque son totalmente independientes y no hay conflictos en las salidas.

Sin embargo solo son utilizables para aplicaciones donde cada salida es propiedad de uno y solo un individuo como por ejemplo es el caso de las monedas digitales.

* **Basadas en mensajes:** En este caso la cadena de bloques representa un consenso sobre el orden de los mensajes y el estado es derivado de la forma determinista a partir de estos mensajes.

**Cadena Lateral (SideChain):** Son cadenas de bloques cuya función es validar los datos desde otras cadenas de bloques a la que se llama principal. Su utilidad principal es poder aportar nuevas funcionalidades, las cuales pueden estar en periodo de pruebas, apoyándose en la confianza ofrecida por la cadena de bloques principal. Este tipo de cadenas se puede conseguir de las siguientes maneras:

* **Vinculación federada:** Es la vinculación en la cual el consenso es alcanzado cuando cierto numero de partes están de acuerdo (confianza semicentralizada).
* **Vinculación SPV (Simplified Payment Verification):** Esencialmente una prueba SPV esta compuesta de una lista de cabeceras de bloque que demuestran prueba de trabajo y una prueba criptográfica de que una salida fue creada en uno de los bloques de la lista. Esto permite a los verificadores chequear que cantidad de trabajo ha sido realizada para la existencia de la salida.

1. CONCLUSIONES

Con el uso de cadenas de bloques se han resuelto dos problemas relacionados con el intercambio de activos sin una entidad certificadora de confianza, ya que:

1. Evita el doble gasto, es decir evita la falsificación y que una misma moneda sea utilizada dos veces.
2. Conseguir al descentralización de los pagos electrónicos, ya que con esto se garantiza un pago seguro.

REFERENCIAS

Las fuentes bibliográficas deben ser citadas a lo largo del texto, deberán aparecer entre corchetes y con números arábigos. Ejemplo: Como se menciona en [1], las políticas adoptadas por...

Las fuentes bibliográficas consultadas pero no citadas en el texto se colocarán al final de las referencias citadas y se numeran de la misma forma. La norma para escribir las referencias bibliográficas es como sigue:

Referencias de publicaciones periódicas:

1. [*https://es.wikipedia.org/wiki/Cadena\_de\_bloques*](https://es.wikipedia.org/wiki/Cadena_de_bloques)