Algoritmos y Estructuras de Datos - DC - UBA

Primer cuatrimestre de 2025

Trabajo práctico 1: Especificación de TADs

Normativa

Límite de entrega: Domingo 20 de Abril a las 23:59hs.

Normas de entrega: Subir el pdf a la tarea del campus.

Introducción[1]

A continuación presentamos un breve resumen de los aspectos más relevantes de una criptomoneda: qué es, cómo se hace un pago y cómo se garantiza la seguridad para evitar fraudes.

Todo lo sólido se desvanece en el aire: ¿Qué es una criptomoneda?

Una *criptomoneda* (o cripto) es una divisa o sistema monetario, es decir: es un medio de intercambio, una estandarización del dinero para la compra-venta de bienes (ej.: comprar en el supermercado) y servicios (ej.: pagar la peluquería o el estacionamiento). Es como el peso, el dólar o el yuán.

En los últimos años se viene experimentando una digitalización completa de la economía. Las transacciones (compra-venta de bienes y servicios) se realizan masivamente a través de transferencias y billeteras virtuales. El uso del dinero físico -el papel dinero y las monedas-, está siendo reemplazado por estas modalidades digitalizadas. No obstante las transacciones se realizan en divisas soberanas, o sea cada peso que gastamos está respaldado por el Estado (el Banco Central es el encargado de emitir ese peso) y tiene potencialmente su contraparte física (billete o moneda). Una cripto tiene las siguientes características:

- Es completamente digital: desde su creación hasta su uso, no tiene contraparte física.
- No está respaldado por una entidad centralizada soberana sino que depende exclusivamente del mercado para definir su valor y del consenso de una mayoría de participantes del sistema monetario, es decir: de las computadoras conectadas a la red para definir su veracidad.
- Su uso no está mediado por instituciones bancarias.

Show me the money: ¿Cómo funciona una criptomoneda?

Una transacción tiene un comprador que es quien adquiere el bien, un vendedor y un monto (expresado en la cripto) asociado al valor del bien. En la transacción el monto se traspasa del comprador al vendedor. Desde el punto de vista de la cripto se produce un traspaso de la propiedad de ese monto induciendo una cadena de dueños validados criptográficamente.

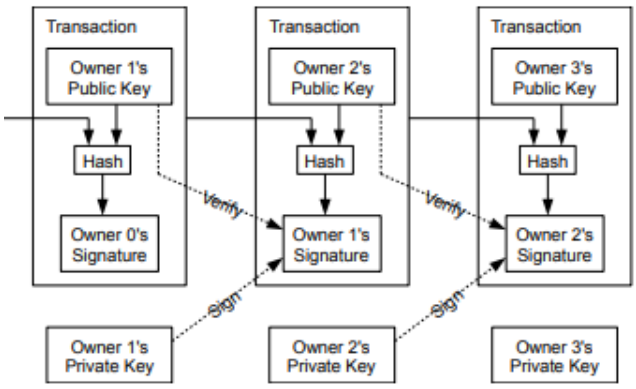

Figura 1: Cadena de traspasos de propiedad de una cantidad de cripto.

[1]Esta introducción está basada en el artículo Bitcoin: A Peer-to-Peer Electronic Cash System (`https://bitcoin.org/bitcoin.pdf`)

Para registrar una transacción se utiliza un *sistema criptográfico de clave pública*[2], cada usuario tiene un par de claves (pública/privada). En cada transacción el dueño actual (comprador) encripta un *hash*[3] (asociado a la transacción anterior) con la clave pública del futuro dueño (vendedor) y firma al final con su clave privada. De este modo se garantiza que la cadena de propiedad sea correcta: 1) que el emisor del pago es el dueño actual y 2) que el único que podrá disponer del dinero será el nuevo dueño porque es el único capaz de desencriptar la información (Fig. 1).

La verificación de la propiedad de un monto de cripto es muy simple: el dueño actual muestra que al desencriptar (con su clave privada) el último bloque, el hash que obtiene es el mismo que el que se obtiene al calcular el hash de la anteúltima transacción.

***Blockchain*: ¿Lo qué?**

Para entender el funcionamiento global de una cripto hay que pensar en una red de computadoras que cooperan entre sí. Las transacciones se van propagando en esta red y se van registrando. Para evitar fraudes, el punto crucial es poder garantizar que la mayoría de los participantes (o nodos) de la red estén de acuerdo en el orden en que se produjeron las transacciones y en que una misma cantidad de cripto no se utilice dos (o más) veces para hacer compras por el mismo dueño a la vez, lo que se conoce como "gasto duplicado".

La técnica de *Blockchain*[4] permite resolver de forma eficiente el problema de que varios nodos se pongan de acuerdo[5] sobre el orden temporal y la integridad de las transacciones.

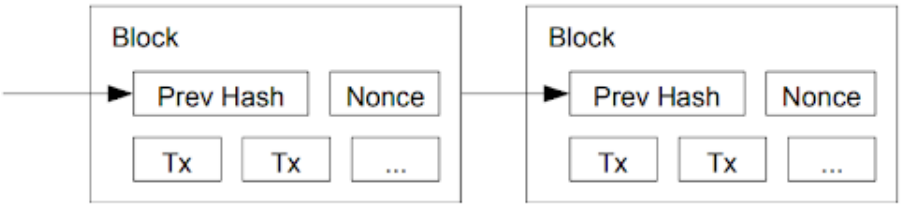

Figura 2: Encadenamiento de los bloques.

Blockchain es eso: una cadena de bloques (Fig. 2). La secuencia de los bloques preserva la secuencia temporal de las transacciones. En cada momento a nivel global hay un único bloque activo que es donde se alojan las transacciones válidas que ocurrieron desde que se cerró el bloque anterior.

Ahora viene la parte importante: todos los nodos trabajan para producir un número que se llama "Nonce". Ese número tiene la característica de que si calculamos un hash del bloque activo, ese hash va a tener una cierta propiedad (en el caso de Bitcoin es que el hash empiece con una cierta cantidad de 0's). Lograr encontrar ese número requiere mucho poder de cómputo por parte de todos los nodos de la red. Cuando un nodo encuentra un Nonce que verifica la propiedad, se cierra el bloque activo y se abre un nuevo bloque.

La seguridad de una cripto se basa en el hecho de que encontrar el Nonce es muy costoso computacionalmente y que un atacante que quiera hacer un fraude, por ejemplo hacer todos los gastos duplicados que pueda, requeriría al menos el mismo poder de cómputo que toda la red en su conjunto, para producir una cadena de bloques "válida" más larga que la actual.

Encontrar el Nonce por parte de los nodos es lo que se conoce coloquialmente como "minar una cripto", esta metáfora hace referencia a los mineros que buscaban oro cuando el medio de intercambio en la economía estaba basado en ese patrón. Cada vez que un nodo encuentra el Nonce del bloque activo se le da una recompensa como si encontrara una pepita de oro, en ese momento se crea una nueva fracción de la cripto y ese es el modo en el que se "crea" la moneda. Este mecanismo es equivalente a cuando el Banco Central imprime un billete. Este procedimiento tiene un límite (para evitar la inflación) que se conoce como "límite de emisión", por ejemplo en el caso de Bitcoin es de 21 millones de unidades.

Para compensar el gasto energético de la red, las transacciones pagan comisiones.

***Pros y contras*: ¿Qué puede salir mal, *cryptobro*?**

Es indiscutible el impacto en la economía que tienen las criptomonedas. Todo indica que los Estados, las entidades bancarias, financieras, y crediticias van a tener que adoptarlas y regularlas de algún modo. Permiten realizar transacciones a nivel mundial de forma anónima y sin intermediarios. La contracara es que no hay ningún amparo legal. Es decir, hay cosas que pueden fallar (y es importante conocerlas):

- Hackeos: si bien Blockchain es una infraestructura segura, nada impide que haya robos de claves privadas, esto equivale al robo de una (o muchas) billetera(s).

[2] `https://en.wikipedia.org/wiki/Public-key_cryptography`
[3] `https://en.wikipedia.org/wiki/Hash_function`
[4] `https://en.wikipedia.org/wiki/Blockchain`
[5] `https://en.wikipedia.org/wiki/Consensus_(computer_science)`

- Financiamiento de actividades ilícitas: una cripto posibilita transacciones asociadas a actos ilícitos (compra-venta de armas, trata de personas, narcotráfico, lavado de dinero, juego ilegal, evasión impositiva, etc., etc.,). Más allá de los aspectos éticamente reprobables, esta característica debilita legalmente a una cripto y en consecuencia la vuelve proclive a perder su valor.
- Extrema volatilidad: ante las incertidumbres de los mercados financieros, las cripto tienden a perder un valor mucho mayor que el de otros activos.
- Esquema de estafa *pump-and-dump*[6]: alguien con algún poder de compra genera un movimiento artificial en el mercado y con eso hace subir o bajar momentáneamente y de manera artificial el valor de la moneda. En entornos controlados, como los mercados financieros (la bolsa), esto está penado severamente.

Enunciado

Proponemos la creación de la única cripto completamente libre de controles criptográficos: la **$Berretacoin**.

Nuestra cripto tiene usuarios que identificamos con un número entero positivo. Cada transacción involucra a dos usuarios: 1) un comprador que es quien adquiere el bien (o servicio) pagando con la cripto, y 2) un vendedor que es quien recibe el pago. Además, una transacción tiene un monto asociado que también es un número entero positivo y un identificador dentro del bloque (un entero no negativo). Es decir que una transacción es una tupla de enteros: `id_transaccion, id_comprador, id_vendedor, monto`.

Las transacciones se agrupan en bloques como en Blockchain. Cada bloque contiene a lo sumo 50 transacciones cuyos identificadores están ordenados dentro del bloque. La primera transacción de cada bloque "crea" una nueva unidad de $Berretacoin hasta alcanzar el límite de emisión, que está fijado en 3000 unidades. A estas transacciones especiales las denominamos "transacciones de creación", y tienen la característica de que el comprador tiene identificador 0 y el vendedor es algún usuario arbitrario siempre distinto. Aclaración: a partir del bloque 3000 no hay más "transacciones de creación".

A su vez, cada bloque tiene un identificador que es un entero no negativo. Los bloques se encadenan de forma secuencial de acuerdo al identificador.

Consignas

Se pide especificar el `TAD $Berretacoin` con las siguientes operaciones:

- **agregarBloque**: agrega un nuevo bloque a la cadena de bloques.
- **maximosTenedores**: devuelve una lista que contiene al o los usuarios que tienen la mayor cantidad de $Berretacoin.
- **montoMedio**: devuelve el monto promedio de todas las transacciones sin considerar las "transacciones de creación".
- **cotizacionAPesos**: dada una lista de cotizaciones (números enteros positivos, que está en correspondencia biyectiva con la cantidad de bloques) que indica a cuántos pesos equivale un $Berretacoin, se pide devolver otra lista de la misma longitud que indique la cantidad de total de pesos que representa la $Berretacoin en cada momento.

Observaciones importantes:

- El TAD debe estar completo, hay que agregar todo lo que corresponda (ej. la operación de creación).
- En todo momento hay que garantizar que nadie gaste más de lo que tiene.
- En una transacción los ids del comprador y del vendedor son distintos.
- **No hay que modelar ningún aspecto criptográfico** (ni el Nonce, ni los hashes ni las claves).

[6] `https://en.wikipedia.org/wiki/Pump_and_dump`