Diploma Programme
Programme du diplôme
Programa del Diploma

Informática
Estudio de caso: Una economía local impulsada por cadenas de bloques

Para usar en mayo de 2020, noviembre de 2020 y mayo de 2021

Instrucciones para los alumnos

- Para la prueba 3 de nivel superior se requiere el cuadernillo del estudio de caso.

8 páginas

Introducción

Santa Mónica es una ciudad como otras muchas del mundo. En las últimas décadas, la población ha disminuido y muchas empresas locales han cerrado. Cuando la gente de Santa Mónica gasta sus pesos en las tiendas de empresas multinacionales, el dinero sale de la ciudad.

Pablo, el alcalde, quiere revertir este proceso. Para ello, ha investigado varias ciudades que han creado su propia moneda local, y piensa que esta es una idea que podría aplicarse en Santa Mónica. Pablo averiguó que estas monedas locales funcionaban junto con la moneda nacional. Por ejemplo, una unidad de la moneda local sería igual a un peso. La moneda local tampoco tendría valor fuera del área local, por lo que no se podría cambiar por otras monedas, como el dólar estadounidense. Sin embargo, si se adopta en Santa Mónica, los ciudadanos podrían cambiar la nueva moneda local a pesos cuando lo deseen.

Las investigaciones de Pablo indicaron que establecer una moneda local produjo beneficios considerables a las ciudades. Las empresas locales lograron más clientes y pudieron ofrecer descuentos a quienes decidieran usar la nueva moneda local. Muchos trabajadores locales se dieron cuenta de los beneficios de usarla y decidieron aceptar el pago en moneda local de una parte de su salario. Sin embargo, muchas de estas monedas locales fallaron debido a los costos administrativos incurridos, tales como los de imprimir billetes, de combatir el fraude y de brindar servicios bancarios adicionales.

Una informática de Santa Mónica llamada Dolores sugirió una manera de solucionar estos problemas. Explicó que “una *criptomoneda* (*cryptocurrency*) basada en *cadenas de bloques* (*blockchain*) podría ayudar a Santa Mónica a evitar estos problemas porque no requiere ninguna administración centralizada. Las personas que no se conocen pueden realizar transacciones sin necesidad de una autoridad central, y así se eliminarían tales costos”. Pablo y Dolores decidieron que el próximo paso sería promover la idea de una nueva criptomoneda, llamada MONS, para Santa Mónica.

El proyecto MONS

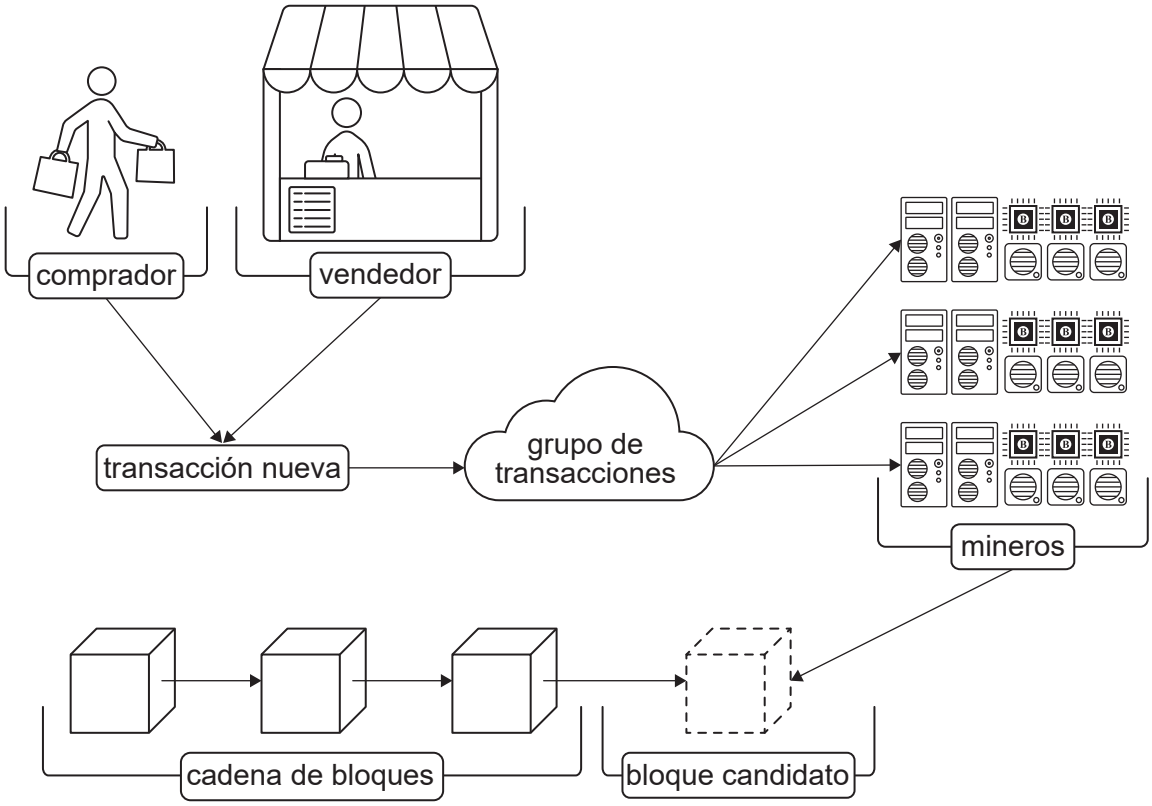
En un sistema bancario tradicional, un pago pasa por un proceso de compensación que puede demorar hasta diez días hábiles. En este período, el banco del pagador y el beneficiario se coordinan para validar la transacción, transferir el dinero y verificar que el pago se haya completado correctamente. MONS no tendría un banco central para hacer esto, por lo que habría que encontrar una alternativa.

Algunos desafíos de usar una criptomoneda son:

- cómo crear una transacción
- cómo verificar que la transacción sea precisa
- cómo registrar una transacción de tal manera que no pueda modificarse posteriormente.

Dolores le explicó a Pablo cómo se podrían crear y validar las transacciones MONS mediante los nodos de la red, en lugar de una autoridad central. Luego se pueden agregar en grupos llamados *bloques* (*blocks*), que son similares a las páginas de un *libro de contabilidad* (*ledger*) digital. “Después de validar una transacción, se puede agregar un nuevo bloque a la cadena de bloques”, dijo. “Todos lo pueden ver, pero no se puede cambiar”, añadió.

Figura 1: El recorrido de una transacción



Dolores explicó que “las criptomonedas modernas operan usando una red de igual a igual (P2P) para realizar y recibir pagos. El dispositivo de cada usuario de MONS es un nodo en la red y tiene una dirección que consta de 26 caracteres alfanuméricos. Cuando un usuario gasta la moneda, transfiere el valor de MONS desde su dirección a aquella de la cuenta de la persona a quien está pagando. Los detalles de esta transacción luego se transmiten a la red”.

“Los otros nodos de la red validan cada transacción de forma independiente mediante la ejecución de una gama de verificaciones. Una verificación utiliza la *firma digital* (*digital signature*) de la transacción para comprobar la identidad del remitente. Otra verificación garantiza que el comprador no haya gastado previamente el MONS que se está utilizando en esta transacción [conocido como el *problema de doble gasto* (*double-spend problem*)]”. Si la transacción es válida, el nodo lo envía a sus nodos vecinos, que también lo comprueban y lo envían. De esta manera, solo las transacciones válidas se propagan por la red y, lo que es esencial, no hay una autoridad única que determine la validez de la transacción. El conjunto de transacciones validadas se conoce como *grupo de transacciones* (*transaction pool*).

Aunque las transacciones del grupo de transacciones se validen, estas siguen sin confirmarse. En la red también hay nodos especializados llamados *mineros* (*miners*). Los mineros están a cargo de agrupar las transacciones no confirmadas del grupo con el fin de crear *bloques candidatos* (*candidate blocks*) que se agregarán a la cadena de bloques. La cadena de bloques tiene todas las transacciones confirmadas que se han efectuado en cualquier momento.

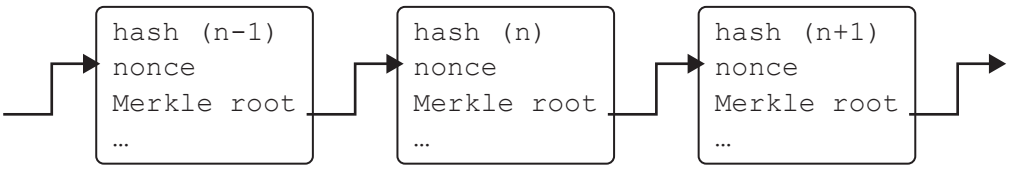
Los mineros calculan una *prueba de trabajo* (*proof of work*). Es necesario hacer esto para encontrar un *nonce* (número aleatorio utilizado una sola vez) con el fin de resolver un bloque y luego agregar el bloque candidato a la cadena de bloques. El incentivo para que los mineros realicen este trabajo es que recibirán una pequeña cantidad de MONS de la red y una tarifa de transacción nominal de los participantes de la venta. Dolores dijo que "la cantidad de tiempo necesaria para resolver un bloque no debe ser demasiado corta, pero tampoco excesivamente larga. Nuestra meta es que sean unos 10 minutos".

Para mejorar sus posibilidades de ser los primeros en resolver un bloque, los mineros pueden utilizar una gran cantidad de unidades de procesamiento gráfico (GPU). Dolores explicó que, "a medida que la moneda se use más ampliamente, habrá más mineros que intentarán resolver la prueba de trabajo, con lo cual se podrá resolver cada bloque más rápidamente. Sin embargo, una de las mejores cosas de la cadena de bloques es que podemos garantizar que el tiempo de solución seguirá siendo de 10 minutos, y se mantendrá este valor incluso si aumenta el número de mineros de MONS".

La estructura de la cadena de bloques

La cadena de bloques es una *estructura de datos autorreferencial* (*self-referential data structure*) en la que cada bloque tiene una referencia al bloque siguiente.

Figura 2: Una representación esquemática de la cadena de bloques



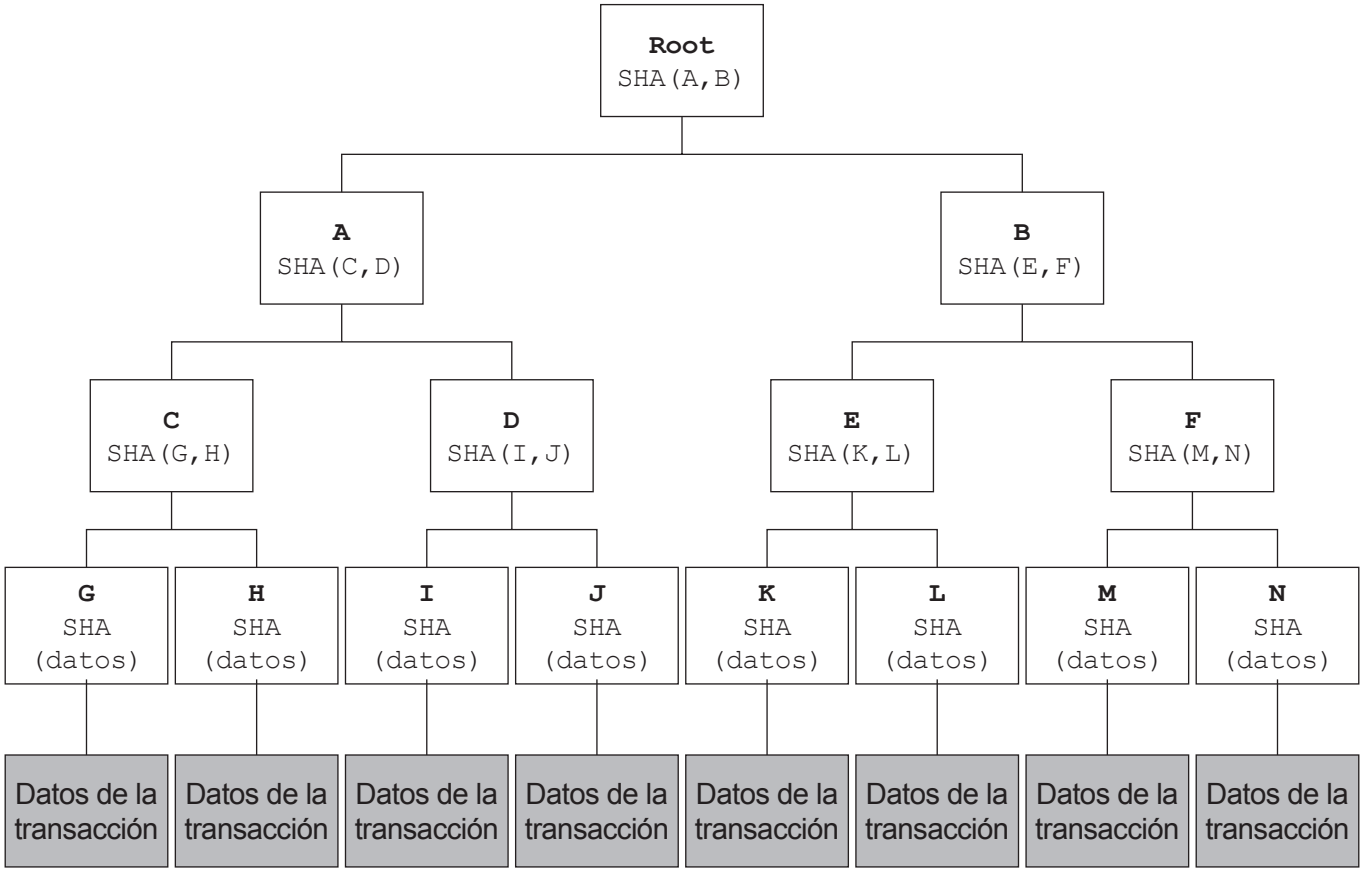
Un conjunto de metadatos llamado *encabezado de bloque* (*block header*) tiene información detallada de cada bloque.

Figura 3: Un ejemplo de un encabezado de bloque


```
"number_of_transactions":188
"height":5432
"block_reward":2
"timestamp":1391270636
"merkle_root":0e83db9efb10076982a……94574318e7e
"previous_block":5341
"difficulty":2548.2
"bits":172758700
"size":317202
"version":912
"nonce":196898444
"next_block":5433
```

80 La lista de transacciones de cada bloque se almacena en un *árbol de Merkle* (*Merkle tree*), cuya raíz se referencia en el encabezado de bloque. Un árbol de Merkle es un árbol binario en el que cada nodo principal contiene el *hash criptográfico* (*cryptographic hash*) de sus nodos secundarios, y cada nodo hoja tiene el *hash* criptográfico de su nodo de datos único. En la cadena de bloques de MONS, cada nodo de datos almacena los detalles de una transacción.

Figura 4: Un ejemplo de un árbol de Merkle



Véase al dorso

El uso de la criptografía en el proyecto de MONS

Dolores tenía mucho interés en enfatizar el papel de los algoritmos criptográficos en el proyecto de MONS propuesto. “La criptografía se utilizará en todo el sistema, en particular algoritmos de *hashing*, tales como *SHA256*”, explicó. “Las características esenciales de los buenos algoritmos de *hashing* son el *determinismo* (*determinism*), la *no invertibilidad* (*non-invertibility*) y la *resistencia a la colisión* (*collision resistance*)”.

Cuadro 1: Algunos ejemplos de entradas y salidas de SHA256

Entrada	Salida
`"a"`	`87428fc522803d31065e7bce3cf03fe4750 96631e5e07bbd7a0fde60c4cf25c7`
`"El veloz murciélago hindú comía feliz cardillo y kiwi"`	`c03905fcdab297513a620ec81ed46ca44dd b62d41cbbd83eb4a5a3592be26a67`
`"El veloz murciélago hindú comía feliz cardillo y kiwi."`	`b47cc0f104b62d4c7c30bcd68fd8e67613e 287dc4ad8c310ef10cbadea9c4382`
`[La Guía de Informática del IB en PDF]`	`370e5655ff2e4e63e307e09e560639c72abb b8b5066616a72a130e2eb0240b8s`

Dolores identificó las siguientes cuatro áreas clave del proyecto en las que los algoritmos criptográficos desempeñarán un papel importante.

La firma digital

La firma digital se basa en criptografía de clave asimétrica y *hashing* para garantizar tres criterios cruciales. Estos criterios son:

- Autenticación
- *No repudio* (*non-repudiation*)
- Integridad

Las firmas digitales se utilizan para validar las transacciones de MONS antes de que se agreguen al grupo de transacciones. Hay tres pasos en el proceso de validación:

- Generación de claves
- Creación de una firma
- Verificación de una firma

“El software de generación de claves, tal como *PuTTYgen*, con frecuencia utiliza una fuente física de *entropía* (*entropy*) para generar pares de claves”, afirmó.

La prueba de trabajo

Además, la prueba de trabajo requerirá que los mineros encuentren un *hash* con una característica particular, sobre el que podemos decidir. Algunas criptomonedas existentes especifican que el *hash* debe comenzar con cierta cantidad de ceros, por ejemplo.

La cadena de bloques

La cadena de bloques utiliza el *hashing* para garantizar que no puedan alterarse las transacciones del libro contable, aunque a la vez seguirán estando disponibles a todos los usuarios de la red.

El árbol de Merkle

El árbol de Merkle se conoce también como un árbol de *hash*. Este árbol permite que se determine la existencia de una transacción en un bloque de una forma mucho más eficiente que mantener las transacciones en una lista.

Promoción de MONS a los ciudadanos de Santa Mónica

Dolores ha convencido a Pablo de los beneficios de adoptar MONS como criptomoneda local, pero le preocupa que los ciudadanos de Santa Mónica se muestren reacios a cambiar del peso al MONS.

Pablo indica que existe una diferencia entre una moneda tradicional y MONS que deberá explicarse cuidadosamente: “En un sistema bancario tradicional, los usuarios confían en los bancos para mantener seguro el dinero de todos, pero con MONS, la totalidad de la cadena de bloques, desde la primera transacción, sería visible a todos los usuarios de MONS. Por lo tanto, es importante poder explicar a los ciudadanos cómo se garantizará que su dinero estará seguro”.

Dolores responde que “el saldo de MONS de un usuario no se almacena, sino que se calcula en tiempo real cuando se verifican todas las transacciones anteriores. De esta manera, mientras todas las transacciones anteriores sigan siendo precisas, su saldo actual también será el correcto. La cadena de bloques se basa en un *consenso distribuido* (*distributed consensus*) en todos los nodos de la red, por lo que en una red lo suficientemente grande es difícil lanzar un *ataque del 51%* (*51% attack*)”.

Pablo también tiene dudas acerca de algunas de las posibles consecuencias para los residentes de la falta de una autoridad central que administre MONS, así como otras desventajas potenciales de una criptomoneda.

Desafíos que se plantean

Hay varios desafíos relacionados con la adopción de MONS, entre ellos:

- comprender cómo se agregan los nuevos bloques al libro de contabilidad y cómo la prueba de trabajo evita que nodos maliciosos se apoderen de la red de MONS
- comprender cómo la arquitectura de MONS es escalable y cómo puede seguir siendo eficiente a medida que aumenta el número de usuarios
- comprender cómo se utilizan técnicas criptográficas en el proyecto de MONS
- explicar a los ciudadanos de Santa Mónica cómo se calcula su saldo de MONS a partir de datos de transacciones almacenados de forma segura en un libro contable de cadena de bloques con acceso público
- investigar cómo la naturaleza distribuida de una criptomoneda de cadena de bloques y el proceso de confirmación pueden tener desventajas para los ciudadanos de Santa Mónica.

No se requiere que los candidatos conozcan los detalles de cómo se implementa un algoritmo de *hashing* específico.

El análisis de los argumentos económicos a favor o en contra de las monedas locales y las criptomonedas está fuera del alcance de este estudio de caso.

Véase al dorso

Terminología adicional a la de la guía

Árbol de Merkle (*Merkle tree*)
Ataque del 51 % (*51% attack*)
Ataque de toma de poder (*takeover attack*)
Bloque (*block*)
Bloque candidato (*candidate block*)
Bloque de génesis (*genesis block*)
Cadena de bloques (*blockchain*)
Consenso distribuido (*distributed consensus*)
Criptomoneda (*cryptocurrency*)
Determinismo (*determinism*)
Encabezado de bloque (*block header*)
Entropía (*entropy*)
Estructura de datos autorreferencial (*self-referential data structure*)
Firma digital (*digital signature*)
Función unidireccional (*one-way function*)
Generación de pares de claves (*key pair generation*)
Grupo de transacciones (*transaction pool*)
Hash criptográfico (*cryptographic hash*)
Libro de contabilidad (*ledger*)
Minería (*mining*)
Minero (*miner*)
No invertibilidad (*non-invertibility*)
Nonce (número aleatorio utilizado una sola vez)
No repudio (*non-repudiation*)
Problema de doble gasto (*double-spend problem*)
Prueba de Merkle (*Merkle proof*)
Prueba de trabajo (*proof of work*)
PuTTYgen
Raíz de Merkle (*Merkle root*)
Resistencia a la colisión (*collision resistance*)
SHA256
Transacciones inmutables (*immutable transactions*)

Algunas empresas, productos o personas nombradas en este estudio de caso son ficticios y cualquier semejanza con entidades reales es solamente una coincidencia.