.

MODELO DEL SISTEMA DE TRANSACCIONES EN LA BLOCKCHAIN DE BITCOIN

Capdevila Gastón

e-mail: gaston.capdevila@mi.unc.edu.ar

Juri Martina

e-mail: martina.juri@mi.unc.edu.ar

Mugni Juan Mauricio

e-mail: mauricio.mugni@mi.unc.edu.ar

Seia Nicolas

e-mail: nicolas.seia@mi.unc.edu.ar

Viberti Tomas

e-mail: tomas.viberti@mi.unc.edu.ar

RESUMEN: *Realizamos la simulación de cómo las transacciones son enviadas a través de la blockchain, como se generan los bloques y como se envía el bloque a la cadena de bloques para confirmarse. Planteamos la simulación desde que la transacción sale, es decir entra a la red, como se une al bloque y como se conecta en la blockchain, analizando tiempos, demoras y cuantos bloques son agregados a la red. Como resultados obtuvimos que en la primer simulación, con una media de 3,5 transacciones por segundo, salían cierta cantidad de bloques y al aumentar la media del generador, en 7 transacciones por segundos, se generaron más cantidad de bloques, pero su tiempo de demora fue mucho mayor debido a la cantidad de transacciones que se acumulan en la mempool, esperando a ser aceptadas.*

PALABRAS CLAVE:

Blockchain, bloques, hash, transacción.

INTRODUCCIÓN

El comercio en Internet ha venido a depender exclusivamente de instituciones financieras las cuales sirven como terceros confiables para el procesamiento de pagos electrónicos. Mientras que el sistema funciona lo suficientemente bien para la mayoría de las transacciones, aún sufre de las debilidades inherentes del modelo basado en confianza. Transacciones completamente no revertibles no son realmente posibles, dado que las instituciones financieras no

.

pueden evitar mediar disputas. Con la posibilidad de revertir, la necesidad de confianza se expande. Pero no existe un mecanismo para hacer pagos por un canal de comunicación confiable. Lo que se necesita es un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiéndole a dos partes interesadas en realizar transacciones directamente sin la necesidad de un tercero. El mundo tal y como funciona actualmente necesita producir, gestionar y almacenar una enorme cantidad de información certificada en todo momento. Hasta ahora esta gestión es llevada a cabo por humanos, la propuesta de blockchain es que este trabajo sea realizado por los ordenadores. Blockchain es mucho más que una simple base de datos, es un sistema de almacenaje de información fuera del sistema convencional.

PRINCIPIOS BÁSICOS DE LA BLOCKCHAIN

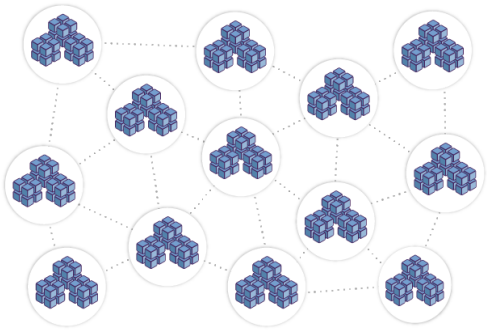
La blockchain es una tecnología diseñada para administrar un registro de datos online, caracterizada por ser transparente y prácticamente incorruptible.

A grandes rasgos, se puede pensar como un libro contable, donde solo se puede ingresar entradas nuevas y donde todas las existentes no se pueden modificar ni eliminar. Esas entradas se denominan transacciones y se agrupan en bloques que se van agregando al registro en forma de cadena secuencial, cada uno de ellos relacionado con el anterior.

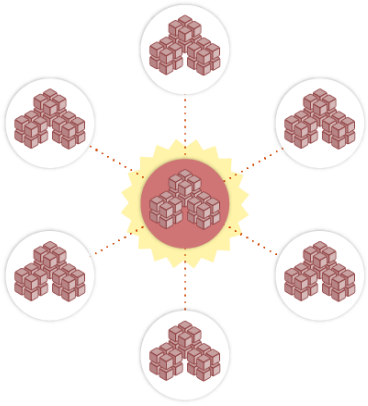
Se puede definir también como una estructura matemática para almacenar datos de una manera que es casi imposible de falsificar. Es una suerte de libro electrónico público que se puede compartir abiertamente entre usuarios dispares y que crea un registro inmutable de sus transacciones.

2.1 CARACTERÍSTICAS GENERALES

- El registro se replica permanentemente en un conjunto de computadoras que forman una red de pares. Cuando un usuario realiza una entrada a la blockchain, esa transacción se suma a otras para componer un bloque. Este bloque se agrega a la cadena y de forma casi automática se replica en todas esas computadoras conectadas. Así, se garantiza la seguridad de esa información ya que, por ejemplo, habría que “hackear” gran parte de la red y no solamente un servidor central para poder modificarla, borrarla o robarla.
- La blockchain, además de ser descentralizada , también está atravesada por métodos criptográficos que garantizan que nada pueda ser borrado o alterado sin que todos los usuarios puedan darse cuenta de ello.
- La blockchain opera sin intermediarios: no hace falta una persona, empresa o institución que legitime la información guardada en la cadena, ya que es segura por naturaleza.



Red distribuida



Red centralizada

.

3 TRANSACCIONES EN BITCOIN

Las transacciones en blockchain son, a grandes rasgos, envíos de criptomonedas entre usuarios. En un lenguaje más técnico, se definen como operaciones que se hacen para ir añadiendo información a la cadena de bloques. En general, el contenido de estas transacciones es muy variado y depende del tipo de red en el que se opera.

Específicamente una transacción con Bitcoin es simplemente una transferencia de valor entre dos wallets, la cual queda grabada en la blockchain.

La transacción tendrá 3 partes:

- Una entrada: Un registro de tu dirección.
- Una cantidad: Cantidad específica de BTC que se quiere transferir.
- Una salida: La clave pública de amigo o la dirección de su wallet.

Para poder enviar Bitcoin, se necesita tener acceso a las claves públicas y privadas que están asociadas a la cantidad específica de Bitcoin que quieres enviar. Una persona que tiene BTC, tiene dos tipos de claves:

- Una clave pública a la que se ha enviado BTC previamente.
- Una clave privada que permite que estos BTC puedan ser enviados a otros sitios.

3.1 CARACTERÍSTICAS DE LAS TRANSACCIONES DE BTC

- Son irreversibles.
- Se ejecutan bajo pseudónimos.
- Se realizan en escala global y son rápidas.
- Son seguras.

4 VERIFICACIÓN DE TRANSACCIÓN

4.1 MEMPOOL

Una mempool es básicamente un área de espera para las transacciones, donde esperan a que un minero las seleccione y las introduzca en un bloque.

4.2 PoW (PROOF OF WORK)

Cuando la transacción se agrega al bloque, el minero necesita encontrar una firma o hash antes de poder añadir el bloque a la blockchain.

Esto se consigue mediante el algoritmo de “Prueba de Trabajo” o PoW (Proof of Work), lo cual permite a los mineros encontrar una firma elegible para los bloques. Esto se consigue resolviendo una serie de operaciones matemáticas en equipos informáticos. Para ser resueltas, requieren un alto poder de cómputo, y eso recae en los gastos energéticos, los cuales son elevados. Este proceso se conoce como “Minado de criptomonedas”.

Los equipos informáticos varían mucho entre cada minero, ya que hay una amplia variedad de componentes con los que se pueden armar, pero los más importantes son las placas de video. Para este estudio, daremos por hecho que el equipo de minado está compuesto por 5 placas de video “RTX 3060”. Las cuales consumen 0.79$USD por día de minado (se entiende como día de minado a 24hs seguidas sin apagar en ningún momento el equipo).

4.3 ¿CUÁNTO PUEDE TARDAR UNA TRANSACCIÓN EN BTC?

Idealmente, una transacción debería ser confirmada en cuestión de minutos. Sin embargo, hay personas que deben esperar más tiempo para la confirmación y la recepción de fondos.

A veces las transacciones necesitan más tiempo para ser confirmadas a causa del tráfico en la red, dejando cientos de estas sin confirmar durante horas. Tarde o temprano, las transacciones se verifican. Hay opciones para que se garantice una verificación rápido, las cuales constan de pagar un fee (tarifa de transacción) más alto.

5 SIMULACIÓN

Para esta simulación trabajamos en eventos discretos utilizando el software “Extend”. Decidimos utilizar este

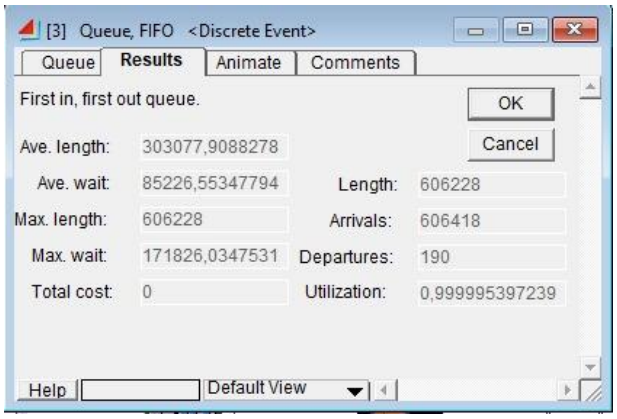
.

tipo de evento ya que sabíamos que se realizaban 3,5 transacciones por segundo de media, entonces podemos discretizar el tiempo entre llegada de cada transacción que es de 0.285 segundos. Esto es lo general pero se supone que en la blockchain de BTC puede soportar 7 transacciones por segundos. Estos son los dos escenarios que vamos a simular y ver qué tiempo transcurre y cuantas transacciones se acumulan en la mempool. El tiempo de simulación son 2880 minutos o 48hs, lo que serían 2 días.

6 RESULTADOS

6.1

Primero, realizamos la simulación con 3.5 transacciones por segundo.



Esto nos indica que en la cola mempool se juntaron en promedio 303 077, 9 transacciones.

Nosotros hemos realizado una modificación, la cual es que trabajamos con 1 sola transacción cuando en realidad se trabajan con 2500. Por ende en la actividad formar bloque se puso el tiempo que tardaron en juntarse 2500 transacciones. Esto nos lleva a que en la cola mempool solo se juntaron 121.3 transacciones de promedio. Como resultado de esta simulación obtuvimos que se obtienen 188 en las 48 horas simuladas, esto es 3.91 bloques cada una hora, lo que nos lleva a decir que se forma un bloque cada 15 minutos.

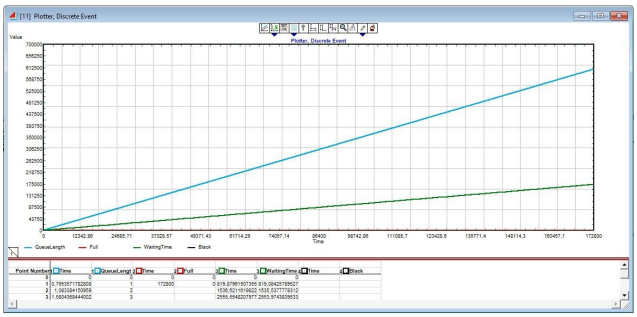
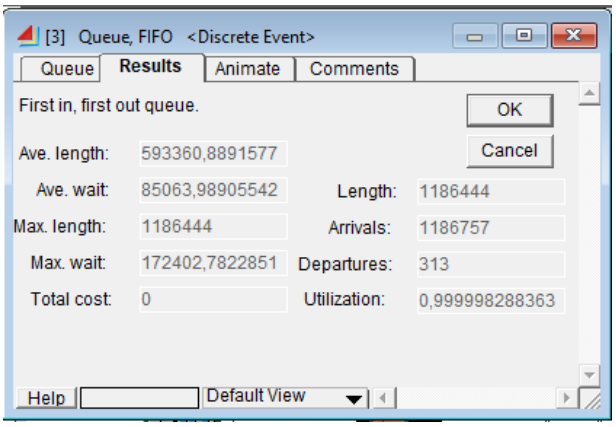


Gráfico 1.

6.2

Segundo, realizamos la simulación con 7 transacciones por segundo.



Esto nos indica que en la cola mempool se juntaron en promedio 593360.8 transacciones.

Pero recordando la modificación que se realizó vemos que en realidad se juntaron 237,4 transacciones en promedio.

Como resultado de esta simulación obtuvimos que se obtienen 309 en las 48 horas simuladas, esto es 6,43 bloques cada una hora, lo que nos lleva a decir que se forma un bloque cada 9.33 minutos.

.

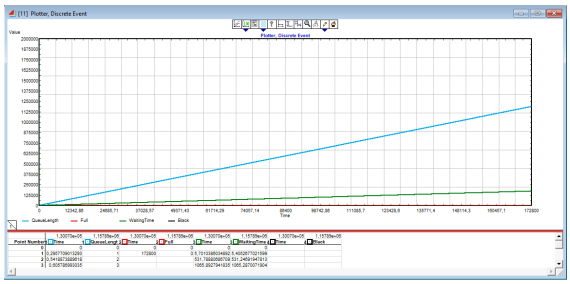


Gráfico 2.

[Los gráficos pueden verse con más claridad en el archivo .mox donde se realizó la simulación]

7 CONCLUSIÓN

Como conclusión a este trabajo podemos decir que en la realidad se realizan más de 3.5 transacciones por segundo, pero menos de 7.

Todo esto debido a que los datos reales de la blockchain dicen que se genera un bloque cada 10 minutos y en nuestra simulación (ambos escenarios) obtuvimos que con 3.5 transacciones por segundo se genera un bloque cada 15 minutos aproximadamente, pero con 7 transacciones por segundo se tarda 9,33 en generar un bloque, pero cabe resaltar que esto es un caso de estrés del modelo, debido a que se duplican las transacciones en espera en la mempool. Por el valor de varianza que utilizamos en nuestro modelo, los resultados obtenidos son correctos y se mantiene la media de 10 minutos por bloque.

Además, concluimos que en el segundo escenario (7 transacciones por segundo) donde se sometió a un gran estrés a la blockchain, la cantidad de transacciones en la mempool es muy grande, lo que indica que las transacciones de las personas tardaran más de lo normal en verificarse, por ende realizar una transacción tomará más tiempo. En comparación con el primer escenario, las transacciones demoradas incluso llegan a 2,5 veces más.

8 REFERENCIAS

[1] https://bfa.ar/blockchain/blockchain

[2]https://www.bbva.com/es/claves-para-entender-la-tecnologia-blockchain/

[3]https://www.youtube.com/watch?v=Yn8WGaO__ak

[4]https://es.beincrypto.com/aprende/guia-basica-como-funcionan-transacciones-bitcoin-btc/

[5]https://ticnegocios.camaravalencia.com/servicios/tendencias/blockchain-que-es-y-que-ventajas-tiene/#:~:text=eficiencia%20de%20Blockchain-,%C2%BFQu%C3%A9%20es%20el%20Blockchain%3F,registro%20inmutable%20de%20sus%20transacciones

Carpeta de drive:

https://drive.google.com/drive/folders/11MzOwsuDMgdj-Q3LdEowL_O213bnsMZF?usp=share_link