PEER TO PEER BASADO BLOCKCHAIN

Cristhian Enriquez – Nicolas Zapata – Juan Diego Cobo y Ricardo Páez Yepes
Universidad Autónoma Del Occidente
Ingeniería Informática
Servicios Telematicos
Docente: Oscar Mondragón

Resumen - Las criptomonedas han protagonizado una de las mayores revoluciones tecnológicas de los últimos años. La pionera y más famosa de ellas es el Bitcoin, aunque existen cientos de ellas. Cada una con distintas características, diferentes objetivos y diversas tecnologías detrás que las hacen funcionar. Una de las más importantes son las redes peer-to-peer.

La mayoría de ellas están basadas en la blockchain, una cadena de bloques unidos entre sí gracias a métodos criptográficos. Este concepto está en auge por su aplicación, no solo en criptomonedas, sino en innumerables campos, gracias a que garantiza que los datos en los bloques no han sido modificados. Si un atacante quiere modificar un solo bit, deberá también generar todos los bloques que le siguen.

A todo esto, se le suma el uso de una red descentralizada o peer-to-peer. Para hacer más fácil la explicación, nos centraremos en el Bitcoin. Cada nodo posee una copia del blockchain, que se va sincronizando con los bloques que van apareciendo (block mining) y que son validados y transmitidos por los nodos conectados.

Abstract - Cryptocurrencies have starred in one of the greatest technological revolutions of recent years. The pioneer and most famous of them is Bitcoin, although there are hundreds of them. Each one with different characteristics, different objectives and different technologies behind them that make them work. One of the most important are peer-to-peer networks.

Most of them are based on the blockchain, a chain of blocks linked together thanks to cryptographic methods. This concept is on the rise due to its application, not only in cryptocurrencies, but in innumerable fields, thanks to the fact that it guarantees that the data in the blocks has not been modified. If an attacker wants to modify a single bit, he must also generate all the blocks that follow.

Added to all this is the use of a decentralized or peer-to-peer network. To make the explanation easier, we will focus on Bitcoin. Each node has a copy of the blockchain, which is synchronized with the blocks that appear (block mining) and which are validated and transmitted by the connected nodes.

I. INTRODUCCION

Este documento relatara como es el funcionamiento de las redes peer to peer en base a blockchain, acorde al tema se demostrará los funcionamientos, las debilidades y amenazas que este afronta hasta llegar al punto de los beneficios que este da a las personas que realizan dichas redes en los diferentes sistemas.
En informática, la definición, también conocida como red peer-to-peer, es una red descentralizada que comprende un grupo de dispositivos (usuarios) conectados entre sí para compartir y almacenar información entre sí. Cada nodo o dispositivo actúa como un servidor individual.
En tecnología blockchain generalmente se refiere al intercambio de activos virtuales o criptomonedas a través de una red distribuid. En una red P2P de este tipo, los compradores y vendedores implementan transacciones sin necesidad de intermediarios.
Las conexiones a Internet P2P pueden ser ideales para diversas tareas, pero se hicieron frecuentes a mediados de la década de 1990, cuando se creó el primer programa para compartir archivos. Algunas de las plataformas de uso compartido de archivos que se utilizan regularmente incluyen Gnutella y Napster.

II. DISTRIBUIDO VS DESCENTRALIZADO

A pesar de que la arquitectura P2P es, de forma inherente, distribuida, resulta importante señalar que existen diversos grados de descentralización. Así, no todas las redes P2P son descentralizadas.
De hecho, muchas dependen de una autoridad central que guía la actividad de la red, lo que hace que sean, en cierta medida, sistemas centralizados. Por ejemplo, algunos sistemas de compartición de archivos P2P permiten a los usuarios buscar y descargar archivos de otros pares, pero son incapaces de participar en otros procesos, como por ejemplo, la gestión de consultas de búsqueda (search queries).

Además, el grado de centralización de las redes pequeñas, controladas por una base de usuarios limitada y con objetivos compartidos, puede considerarse mayor, a pesar de carecer de una infraestructura de red centralizada.

A. Funcionamiento P2P

Una red de pares es administrada esencialmente por una gran cantidad de usuarios que están conectados entre sí a través de una red distribuida. Por lo general, las redes P2P no asumen un modelo central ni tienen un administrador. Cada usuario tiene una copia de los archivos, actuando tanto como servidor como cliente.
Por lo tanto, cada usuario puede cargar archivos en otras computadoras y descargar archivos en ellas. Este es el principal atributo que hace que las conexiones de Internet P2P se destaquen de otras redes cliente-servidor convencionales.
En las redes cliente-servidor convencionales, los pares descargan archivos y documentos desde un servidor centralizado.
- Redes híbridas P2P:
Las computadoras híbridas de igual a igual reúnen algunos aspectos de la red de pares con el modelo tradicional de cliente-servidor. En comparación con los modelos estructurados y no estructurados, las computadoras híbridas tienden a ofrecer un rendimiento general mejorado. Esto se debe a que combina las ventajas de las plataformas estructuradas y no estructuradas para brindar y lograr niveles significativos de competencia y descentralización al mismo tiempo.
- Redes P2P Estructuradas:
Adyacentemente, un sistema estructurado punto a punto ofrece una arquitectura organizada que permite a los pares buscar archivos en la red de manera eficiente, incluso cuando el contenido no está ampliamente disponible. La mayoría de las veces, esto se logra mediante la optimización de la función hash que mejora las búsquedas en la base de datos.
Aunque estas computadoras ofrecen más eficiencia en sus operaciones, tienden a requerir mayores costos de mantenimiento y configuración al tiempo que brindan niveles de centralización más altos. Aparte de eso, los sistemas estructurados son menos productivos cuando se enfrentan a tasas más altas de abandono.
- Redes P2P no estructuradas:
Como sugiere el nombre, un modelo P2P no estructurado no opera en ninguna organización específica. Los usuarios se comunican aleatoriamente entre sí sin seguir ningún procedimiento establecido.
Esta acción tiende a inundar el sistema con solicitudes, especialmente si una pequeña cantidad de discos duros ofrece la respuesta deseada.

B. Papel P2P en Blockchain

En las etapas iniciales de la criptomoneda líder, Bitcoin, tron Nakamoto la describió como un sistema de Cash electrónico P2P. Utilizando la tecnología blockchain, Bitcoin puede transferirse de una persona a otra a través de una red P2P.
Un servicio peer-to-peer (P2P) es una plataforma descentralizada en la que dos personas interactúan directamente entre sí, sin la intermediación de un tercero. El papel de la tecnología Blockchain es actuar como un libro mayor distribuido. La arquitectura peer-to-peer de blockchain permite que todas las criptomonedas se transfieran en todo el mundo, sin la necesidad de intermediarios o servidores centrales.
Por lo tanto, no hay operaciones de mantenimiento de registros o de procesamiento bancario en la red de Bitcoin. Alternativamente, el software blockchain P2P actúa como un libro mayor virtual que registra abiertamente todas las actividades de Bitcoin. El disco duro de cada usuario tiene una copia de la cadena de bloques y la verifica con el disco duro de sus pares para garantizar que la información sea precisa. En caso de cualquier inexactitud o actividad maliciosa, la red rechaza rápidamente la transacción.

C. Ejemplos P2P basado en Blockchain

En los últimos años, varias empresas como Uber, Air bnb y Lyft han tenido éxito utilizando sistemas de intercambio entre pares. A cambio, la economía compartida continúa siendo testigo de un aumento drástico en popularidad. En la actualidad, Investopedia predice que los proveedores de servicios peer-to-peer impulsarán gran parte de la economía compartida, y los analistas proyectan un tamaño de mercado de alrededor de 330 mil millones de dólares estadounidenses antes de 2025.
Dado que el servicio depende de la conexión a Internet, siguen surgiendo nuevos proveedores de servicios de Internet. Archivos electrónicos de Imagen (Opcional)

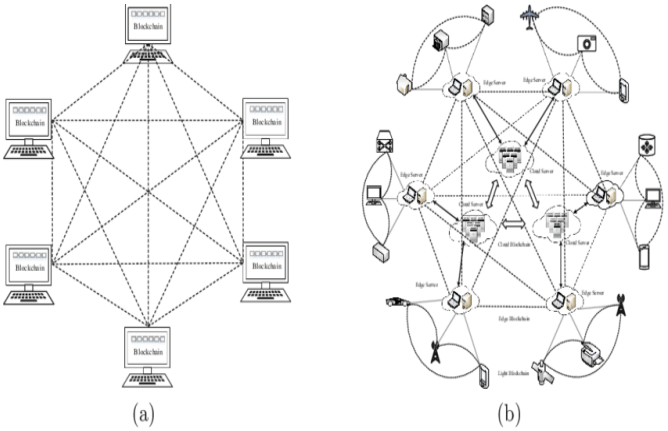


Fig. a. Muestra una red peer to peer común y corriente entre diferentes maquinas. Fig. b. Ilustra una red peer to peer basado en blockchain con sus diferentes conectividades con variedad de dispositivos con un fin en comun

D. Papel de los sistemas informáticos en las redes P2P

Como ya sabrá, P2P significa peer-to-peer. Y en el software P2P, los sistemas informáticos se consideran pares y están interconectados entre sí a través de Internet.

En un software P2P, la música, los juegos y los documentos se pueden compartir directamente entre sistemas informáticos sin necesidad de un servidor central. En otras palabras, cada dispositivo informático en la red de igual a igual se convierte en un servidor de archivos independiente mientras mantiene su estado de cliente.

1) Ventajas de la arquitectura P2P en blockchain

Los muchos beneficios asociados con el modelo peer-to-peer utilizado en blockchain son infinitos. Según la experiencia del usuario, los beneficios más significativos son que las redes punto a punto ofrecen una seguridad superior a los sistemas cliente-servidor convencionales.

A diferencia de otras redes, las redes peer-to-peer asociadas a la tecnología blockchain son prácticamente inmunes a los ataques de Denegación de Servicio (DoS). Además, dado que la mayoría de los discos duros de los clientes deben establecer un consenso entre sí antes de implementar una transacción, es casi imposible alterar el archivo original.

Además de la seguridad, la arquitectura de cadena de bloques de usuario a usuario también hace que los usuarios sean inmunes a la censura por parte de un órgano de gobierno central. A diferencia de las cuentas bancarias ordinarias, los bancos o los gobiernos no pueden drenar ni congelar las billeteras de moneda virtual.

2) Limitaciones de las redes P2P en Blockchain

El uso de redes peer-to-peer en blockchain también viene con una buena cantidad de limitaciones. Teniendo en cuenta que la norma es que los registros distribuidos se actualicen en cada computadora en lugar de un servidor central, se necesita una potencia de CPU masiva para implementar transacciones en una red de cadena de bloques.

Si bien ofrece mayor seguridad, la eficiencia reducida es una de las principales limitaciones de esta tecnología. Otro obstáculo que nos gustaría aclarar son los eventos de bifurcación dura. Aunque la cadena de bloques y las criptomonedas son seguras, no son 100 % seguras.

Esto significa que están sujetos a piratería y otros ataques que pueden modificarlos. En términos más simples, el evento de bifurcación dura significa que cualquiera puede duplicar el archivo principal, modificarlo de acuerdo con sus especificaciones y crear una nueva cadena de red paralela.

III. ROL DEL P2P EN BLOCKCHAIN

En las primeras etapas de Bitcoin, Satoshi Nakamoto lo definió como un “Sistema de cash (Dinero en efectivo) electrónico peer to peer”. Bitcoin se creó como una forma digital de dinero. Se puede transferir de un usuario a otro a través de una red P2P, que gestiona un libro mayor distribuido llamado blockchain.

En este contexto, la arquitectura P2P que es inherente a la tecnología blockchain es lo que permite que Bitcoin y otras criptomonedas se transfieran a todo el mundo, sin la necesidad de intermediarios ni ningún servidor central. Además, cualquiera puede configurar un nodo de Bitcoin si desea participar en el proceso de verificación y validación de bloques.

Por lo tanto, no hay bancos que procesen o registren transacciones en la red Bitcoin. En cambio, la blockchain actúa como un libro de contabilidad digital que registra públicamente toda la actividad. Básicamente, cada nodo contiene una copia de la blockchain y la compara con otros nodos para garantizar que los datos sean precisos. La red rechaza rápidamente cualquier actividad maliciosa o inexactitud.

En el contexto de las blockchains de criptomonedas, los nodos pueden asumir una variedad de roles diferentes. Los nodos completos, por ejemplo, son los que proporcionan seguridad a la red al verificar las transacciones con las reglas de consenso del sistema.

Cada nodo completo mantiene una copia completa y actualizada de la blockchain, lo que les permite participar en el trabajo colectivo de verificar el verdadero estado del libro mayor distribuido. Sin embargo, vale la pena señalar que no todos los nodos de validación completos son mineros.

IV. VULNERABILIDADES

Como hemos mencionado al principio, un Eclipse Attack, o Ataque Eclipse, busca desconectar a la víctima del flujo de datos válido de la red. Esto con el fin de que la víctima reciba datos manipulados por parte del atacante. Suena bastante aterrador desde un punto de vista de seguridad, y ciertamente lo es. Pero te preguntarás ¿Por qué es posible realizar un ataque de este tipo? ¿Se pueden evitar de alguna manera?

Pues bien, en primer lugar, este tipo de ataques son posibles debido a la estructura y las limitaciones del protocolo de comunicación peer-to-peer que use una blockchain. Más específicamente se debe a la limitación en la cantidad de conexiones y selección segura de los nodos. Por ejemplo, en la red Bitcoin el límite de conexiones de salida (las que puedes establecer con otros nodos remotos) es de 8 conexiones. Esto significa que cada nodo de Bitcoin es capaz de mantener conexiones bidireccionales con 8 nodos a la vez. El ciclo se repite en cada nodo, porque este comportamiento es parte del protocolo descrito en Bitcoin Core.

V. ALTERNATIVAS

De las posibles alternativas que se encontraron para hacer nuestro proyecto son:

- el lenguaje Java

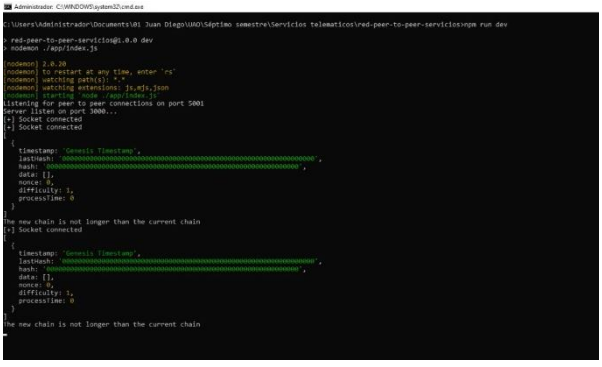
Con este lenguaje es necesario tener un servidor y un cliente corriendo todo el tiempo al igual que es importante el constante envio de informacion al servidor por medio de java sockets ya que este permite enviar mensajes a multiples pares y al mismo tiempo aceptar multiples clientes todo esto simultaneamente puede hacer el envio y recepcion de informacion para que las cadenas se mantengan funcionando y el sistema no se detenga, en caso de que haya algun problema se debe implementar un sistema de recuperacion del servidor

-Se puede realizar en el lenguaje Go, c++, python, php, java entre otros

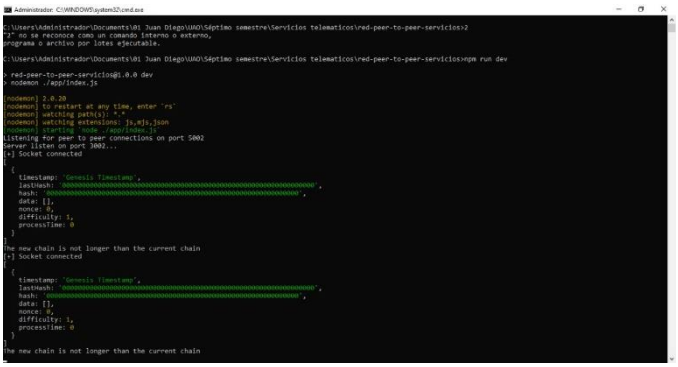
VI. DEFINICION DE LA PROBLEMATICA

En este documento relataremos la problemática o necesidad que solucionaremos con el proyecto.
La problemática o necesidad que se evidencio es que en cierta zona existe una falencia o apertura a posible exposición de datos de empresas y comunidades donde la información que estos almacenan es delicada.
El objetivo del proyecto es realizar una comunicación mas eficaz y asertiva entre los diferentes miembros de las organizaciones, esto permitiendo una transmisión y recepción de archivos con los incidentes de desastres naturales de manera rápida y simultánea.

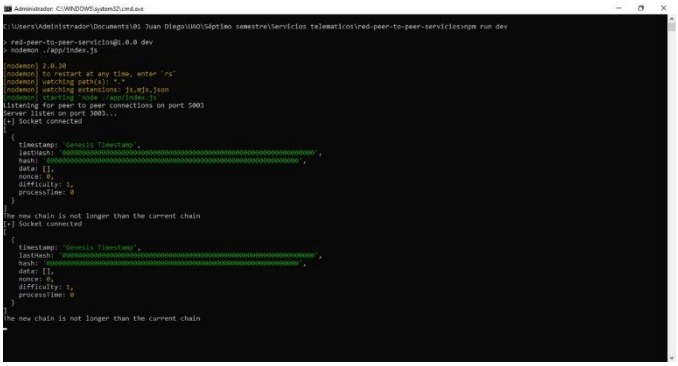
VII. EVIDENCIAS DE LA SOLUCIÓN:

1. 

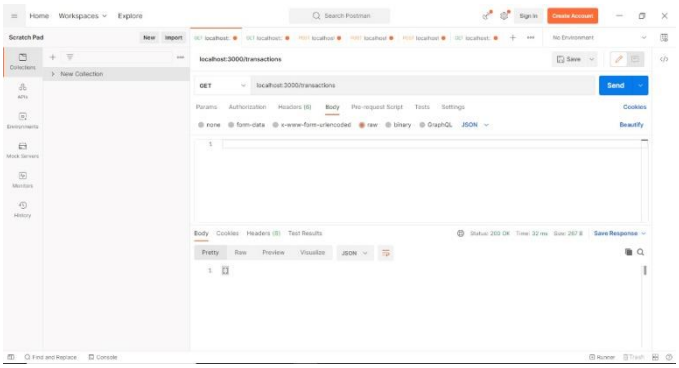
Conexión 1er Nodo o Nodo padre

2. 

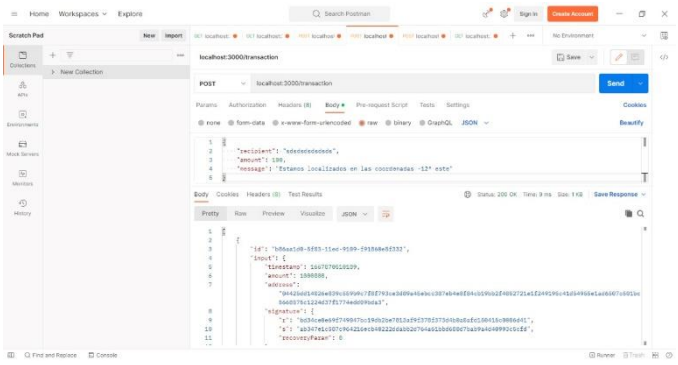
Conexión 2do Nodo

3. 

Conexión 3er Nodo

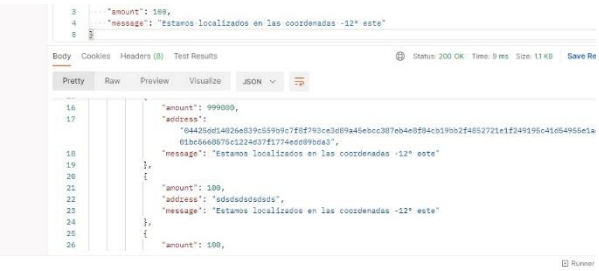
4. 

Estado inicial de las transacciones

5. 

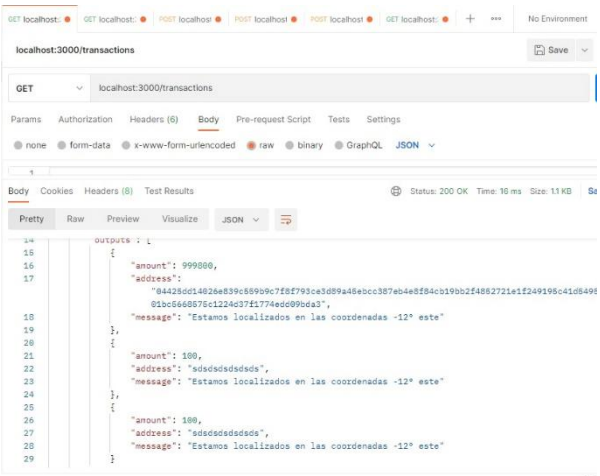
Envío de una transacción especificando dinero y mensaje

6.



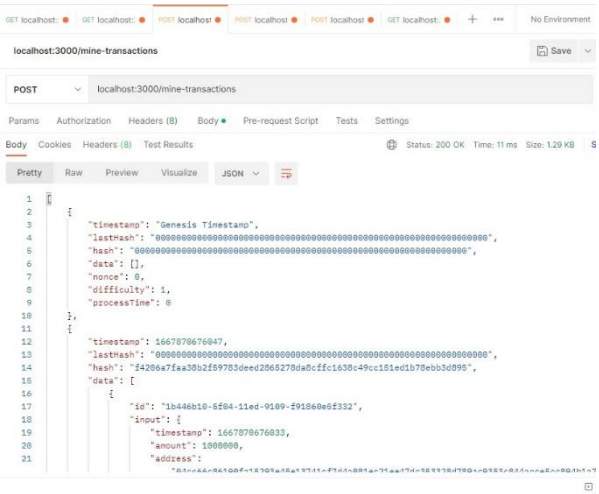
Se envía una segunda transacción y se observa como el valor de la wallet 1 va disminuyendo. Podemos asumir que el valor de la wallet 1 corresponde con la del estado gubernamental, informando su posición para brindar ayudas y un monto con el cual las organizaciones que tengan wallet con la blockchain podrán utilizar para suplirse de insumos

7.



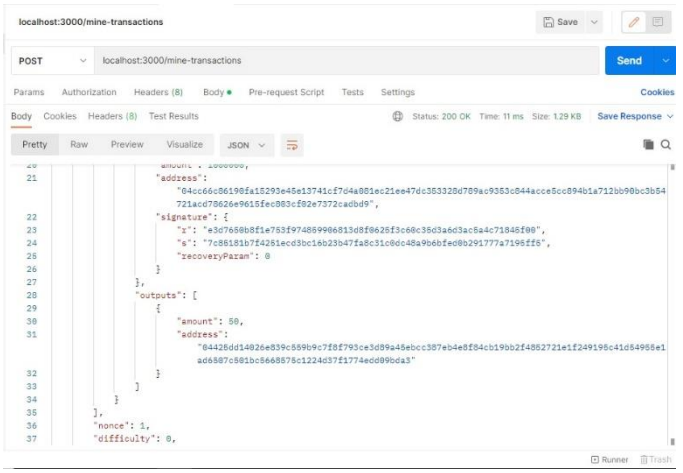
Listado de transacciones válidas que aún no han sido añadidas a la blockchain en forma de bloque.

8.



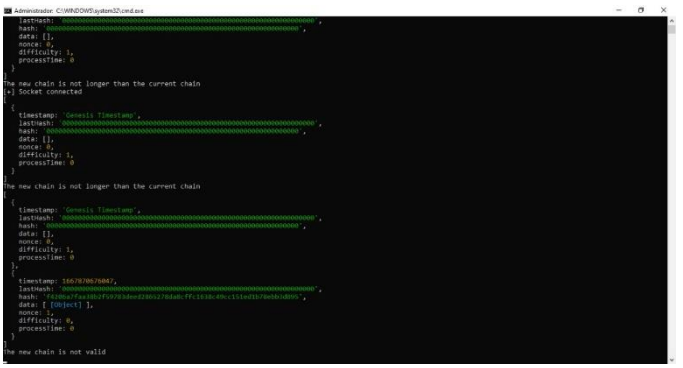
Minado de bloque y observación de cómo se genera un nuevo Hash cuando se agrega el bloque y también como este nuevo bloque esta concatenado a un Hash inicial

9.



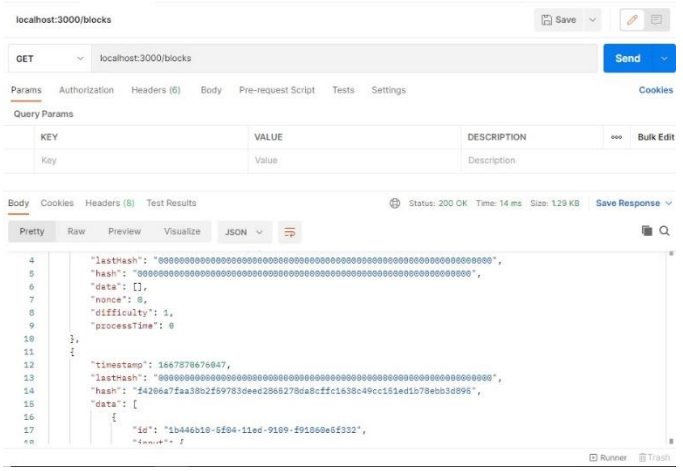
Implementando el minado propio de criptomonedas, establecimos una recompensa de 50 cuando se logra minar un bloque

10.



Evidencia de cómo se van observando los nuevos bloques dentro de la blockchain.

11.



Finalmente se obtienen los bloques para verificar que efectivamente se van agregando.

VIII. CONSECUENCIAS DE ESTE TIPO DE ATAQUE

Las consecuencias de los Eclipse Attack o Ataque Eclipse son variadas y entre ellas podemos mencionar:

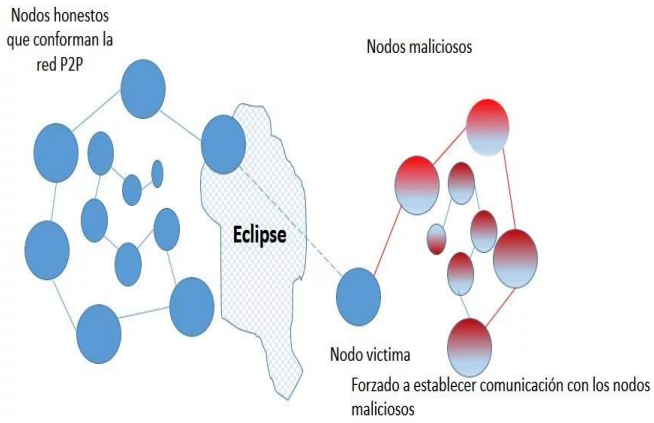
- Explotar las conexiones para controlar la red:
Una vez que un un actor malicioso ha tomado cierto control de la red, nada le detiene para seguir aumentando dicho control. De hecho, con cada nuevo nodo bajo su control, aumentar su presencia en la red se vuelve cada vez más sencillo. Una vez que tiene el manejo de los nodos puede manipular a su antojo las confirmaciones de bloques e incluso sabotear las conexiones de la red y rastrearlas.

- **Realizar ingeniería de carrera de bloques:**
Este es un tipo de ataque altamente especializado que puede realizarse en redes que usan el Protocolo de Prueba de Trabajo (PoW). Este tipo de ataque fue señalado en 2015 por los investigadores Ethan Heilman, Alison Kendler, Aviv Zohar, y Sharon Goldberg, en su trabajo "Eclipse Attack on Bitcoin's Peer-to-Peer Network".
La explicación del ataque es que si dos mineros descubren un bloque simultáneamente; un atacante podría usar un ataque de eclipse para que los mineros eclipsados desperdicien el esfuerzo minero en bloques huérfanos. Eso le daría al atacante la capacidad de minar sus propios bloques. Al final, el atacante se asegura de que su bloque sea procesado por la red bajo su control y recibe la recompensa.

- **Ataques a protocolos de segunda capa:**
Otra consecuencia de este tipo de ataques es el de realizar ataques a los protocolos de segunda capa. Es decir, hacer vulnerable a protocolos como Lightning Network, OmniLayer o RSK en Bitcoin. O Incluso a creaciones derivadas de smart contracts como todas las que se ejecutan sobre Ethereum, EOS o TRON.
Esto sería posible porque un Eclipse Attack engañaría a su víctima para que vea un estado irreal de la red. Por ejemplo, un canal de pago de Lightning se mostraría como abierto para la víctima, mientras que el atacante ha cerrado el canal llevándose consigo los fondos.

- **Dar origen a nuevos y más peligrosos vectores de Ataques:**
El Ataque Eclipse es también el origen de un tipo de ataque más peligros y de mayor alcance, el Ataque Erebus. Este ataque, es capaz de ejecutar un Ataque Eclipse a gran escala sobre la red, teniendo como resultado la partición de la misma. Como resultado, quien realice un Ataque Erebus es capaz de partir la red y manejarla a su antojo, pudiendo incluso hacer una Denegación de Servicios (DoS), realizar un Ataque de 51% o crear un hard fork de la blockchain.

A. Imagen



IX. PREVENIR ESTE TIPO DE ATAQUE

Este ataque es conocido desde hace mucho tiempo, de hecho, se conocen desde la misma creación de las primeras redes peer-to-peer. Por ejemplo, el protocolo Kademlia era susceptible a este tipo de ataques. Sin embargo, este protocolo implementó una serie de medidas para evitarlos. Algunas de estas medidas se siguen implementando hoy en día con algunas mejoras. Entre etsas medidas podemos mencionar:

a) Sistema de identificación de pares

Este sistema busca que los pares de la red tenga un ID único e irrepetible. Esto es una forma de crear un árbol de ID que permite saber quién es quién en la red. En blockchain esto es posible gracias al uso de la criptografía asimétrica. Sin embargo, esta medida es insuficiente puesto que es posible ejecutar varios nodos que usen una misma IP. Así por ejemplo, un atacante puede crear varios nodos controlarlos y seguir aplicando su ataque a la red.

b) Proceso de selección de pares

Otro punto importante para evitar ataques eclipse es tener un proceso confiable de selección de pares para la red. Por ejemplo, en Ethereum este proceso usa un protocolo basado en Kademlia. Esto le permite a Ethereum que cada elemento sea asociado con una clave y se almacena sólo en aquellos pares cuyo ID de nodo está "cerca" de su clave asociada. Esta "cercanía" se define como la distancia binaria de Hamming entre la clave y la ID del nodo.

c) Controlar las conexiones entrantes y salientes

Otra medida de control aplicada en blockchain para controlar los Eclipse Attack es controlar las conexiones entrantes y salientes. Para ello se establecen límites de comunicación con los nodos de la red de forma que en caso de un ataque a un nodo éste no pueda afectar a buena parte de la red. Así se evita que el área de acción

de un nodo sea muy grande y el atacante deba controlar varios nodos para realizar un ataque con éxito. Adicionalmente la medida se va fortaleciendo con la descentralización y ampliación de la red.
Escriba con mayúscula sólo los primeros términos del título del documento, salvo los nombres propios y símbolos del elemento. Si usted esta corto de espacio, puede omitir los títulos del documento. Sin embargo, los títulos del documento son útiles a sus lectores y se recomiendan fuertemente.

X. Eclipse Attack vs Sybil Attack, diferencias entre estos ataques

Un Eclipse Attack o Ataque Eclipse tiene lugar cuando la mayoría (si no todos) de sus pares son maliciosos y básicamente evitan que esté bien conectado a la red para obtener información sobre las transacciones que tienen lugar en la misma. Esto resulta útil cuando un atacante quiere manipular una transacción para hacerle creer que la misma se ha ejecutado con éxito, cuando realmente ha sido manipulado.
Para resumir, un Ataque Eclipse está dirigido a una sola parte; mientras que un Ataque Sybil está dirigido a toda la red.

A. Evitar ser víctima de estos ataques

La mejor manera de protegerse de este tipo de ataques es tener en cuenta una serie de recomendaciones. Entre estas podemos destacar:

- Asegúrese de usar un sistema de pago y wallets con buena reputación. De ser posible, trate de instalar un nodo propio y úselo para verificar sus transacciones. De esta forma no solo contribuirá a asegurar la red, sino que creará una medida de seguridad para protegerse de este tipo de ataques.
- Evite en cualquier caso aceptar pagos 0-conf o sin confirmaciones. Recuerde que, en este estado, las transacciones pueden ser manipuladas de muchas maneras y el ataque eclipse es una de ellas.
- Si tiene un nodo propio asegúrese de blindar el mismo. La forma más sencilla es limitar el número de conexiones entrantes, un firewall que evite estas conexiones es una buena forma de empezar.
- Asimismo, también puede revisar de forma periódica las conexiones de su nodo o wallet y crear una lista de nodos confiables para que los uses en todo momento. Esto le evitará amargas sorpresas en caso de que su nodo esté conectado a un nodo malicioso que libere este tipo de ataques hacia usted o cualquier otro usuario de la red.
- Mantenga actualizados sus wallets y nodos. Los desarrolladores son conscientes de los ataques eclipse y siempre buscan manera de fortalecer los protocolos de conexión. Una actualización en este sentido puede proporcionarles una mejor defensa contra este tipo de ataques.

IX. CONCLUSIÓN

La arquitectura peer-to-peer se puede desarrollar y usar de muchas maneras diferentes, y es el núcleo de las blockchain que hacen posibles las criptomonedas. Al distribuir los libros de transacciones en grandes redes de nodos, la arquitectura P2P ofrece seguridad, descentralización y resistencia a la censura.
Además de su utilidad en la tecnología blockchain, los sistemas P2P también pueden servir a otras aplicaciones informáticas distribuidas, que van desde redes de intercambio de archivos hasta plataformas de trading de energía. Tambien cabe resaltar que no podemos negar que la arquitectura P2P está aquí con nosotros. Después de todo, es compatible con una de las tecnologías más destacadas de nuestro tiempo, la tecnología blockchain.
Aunque la arquitectura P2P puede potenciar muchas otras tecnologías, como las plataformas de comercio de energía y las redes de intercambio de archivos, actualmente se está utilizando para ofrecer soluciones de cadena de bloques y criptomonedas.
Las redes P2P ofrecen una mejor descentralización, libertad, seguridad e inmutabilidad cuando se combinan con la tecnología blockchain.

Reconocimiento
Este trabajo debemos de darle merito ya que para nosotros como estudiante y futuros ingenieros fue muy satisfactorio el poder investigar y averiguar sobre este mundo que hoy en día está dando un gran impacto a la sociedad y el mundo, podríamos reconsiderarlo como la revolución/evolución de la tecnología.
A su vez agradecerle al docente no por solo sus clases sino también por la oportunidad de mostrarnos los diferentes temas que propuso para las clases y así como para nosotros este tema fue muy bueno, pensaríamos que los demás serán así de increíbles

REFERENCIAS

[1] https://www.cryptopolitan.com/es/peer-to-peer-en-blockchain-como-funciona/#What_is_Peer-to-Peer_P2P
[2] https://academy.bit2me.com/que-es-ataque-eclipse-eclipse-attack/
[3] Architecture for Blockchain Applications (Xiwei Xu, Ingo Weber, Mark Staples) (z-lib.org).pdf
[4] https://es.cointelegraph.com/news/peer-to-peer-internet-has-lofty-goal-to-bring-true-decentralization
[9] Python
https://skolo-online.medium.com/develop-a-peer-to-peer-blockchain-in-python-f7c9bdbefcda
[10] Java
https://cylab.be/blog/26/a-simple-java-implementation-of-blockchain?accept-cookies=1
https://gitlab.cylab.be/cylab/simple-blockchain
https://github.com/csaguil/p2p-blockchain
[11] c++ ➔ https://github.com/tko22/simple-blockchain
[12] Go➔ https://mycoralhealth.medium.com/code-your-own-blockchain-in-less-than-200-lines-of-go-e296282bcffc

[13]PHP ➔ https://github.com/akondas/php-blockchain