

Misión 2

Lección 2:

Escalabilidad y desempeño

Escalabilidad y desempeño

Tiempo de ejecución: 3 horas

Materiales

- PC con conexión a internet.

Planteamiento de la sesión:

La sección aborda los desafíos críticos de escalabilidad y consumo de recursos en el contexto del desarrollo y la adopción de tecnologías blockchain. En primer lugar, se destacan los retos inherentes a la escalabilidad, como el crecimiento del tamaño de la cadena de bloques con el aumento de las transacciones, la dificultad para gestionar grandes volúmenes de transacciones en blockchains públicas, y las limitaciones impuestas por los algoritmos de consenso, como Prueba de Trabajo (PoW) o Prueba de Participación (PoS), en la capacidad de la red para manejar un gran número de transacciones simultáneas.

Por otro lado, se abordan los desafíos relacionados con el consumo de recursos computacionales, entre ellos, el elevado consumo energético asociado a algoritmos de consenso como PoW, los costosos requisitos de hardware necesarios para la validación de transacciones y la minería de bloques, y la posible latencia de red que puede afectar la eficiencia del proceso de consenso y la experiencia del usuario.

Para enfrentar estos desafíos, se proponen diversas estrategias, tales como la optimización de protocolos de consenso hacia alternativas más eficientes y escalables, la implementación de soluciones de capa 2 para aumentar la capacidad de procesamiento de transacciones, la búsqueda de algoritmos de consenso más eficientes en términos de consumo energético y la exploración de técnicas de compresión de datos para mejorar la eficiencia en el almacenamiento y transmisión de información en la cadena de bloques. Estas medidas tienen como objetivo mitigar los desafíos mencionados y promover un desarrollo sostenible y eficiente en el ámbito de las tecnologías blockchain.

Desarrollo de sesión

Una parte central de esta lección se centrará en capacitar a los estudiantes para identificar amenazas potenciales en entornos blockchain. Se analizarán casos de estudio reales y escenarios de ataques comunes para que los participantes puedan reconocer los riesgos y vulnerabilidades que enfrentan los sistemas blockchain en la actualidad. La escalabilidad y el consumo de recursos computacionales son desafíos fundamentales en el desarrollo y la adopción de tecnologías blockchain. A medida que la popularidad de la blockchain continúa creciendo, es esencial abordar estos desafíos para garantizar su viabilidad en aplicaciones de alto rendimiento y su sostenibilidad a largo plazo.

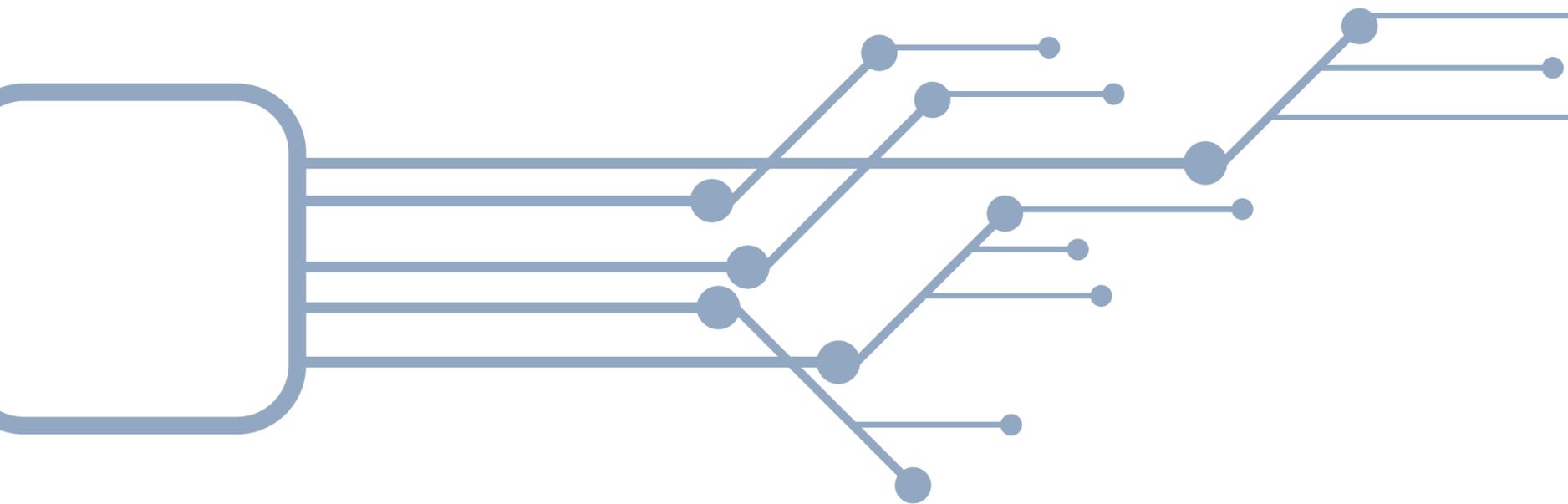


En primer lugar, la escalabilidad en blockchain se refiere a su capacidad para manejar un crecimiento en el número de transacciones sin comprometer la eficiencia y la velocidad del sistema. A medida que la cadena de bloques crece en tamaño con más transacciones, pueden surgir problemas de rendimiento, como congestión de red y retrasos en la confirmación de transacciones. Además, los algoritmos de consenso utilizados, como Prueba de Trabajo (PoW) o Prueba de Participación (PoS), pueden limitar la capacidad de la red para escalar horizontalmente y procesar un gran número de transacciones simultáneas.

Por otro lado, el consumo de recursos computacionales en blockchain es significativo, especialmente en términos de energía, poder de cómputo y hardware necesario para mantener y operar la red. Algoritmos de consenso como PoW requieren una cantidad considerable de energía para validar y confirmar transacciones, lo que ha generado preocupaciones ambientales y económicas. Además, los requisitos de hardware para la validación de transacciones y la minería de bloques pueden ser costosos y limitar la participación en la red.

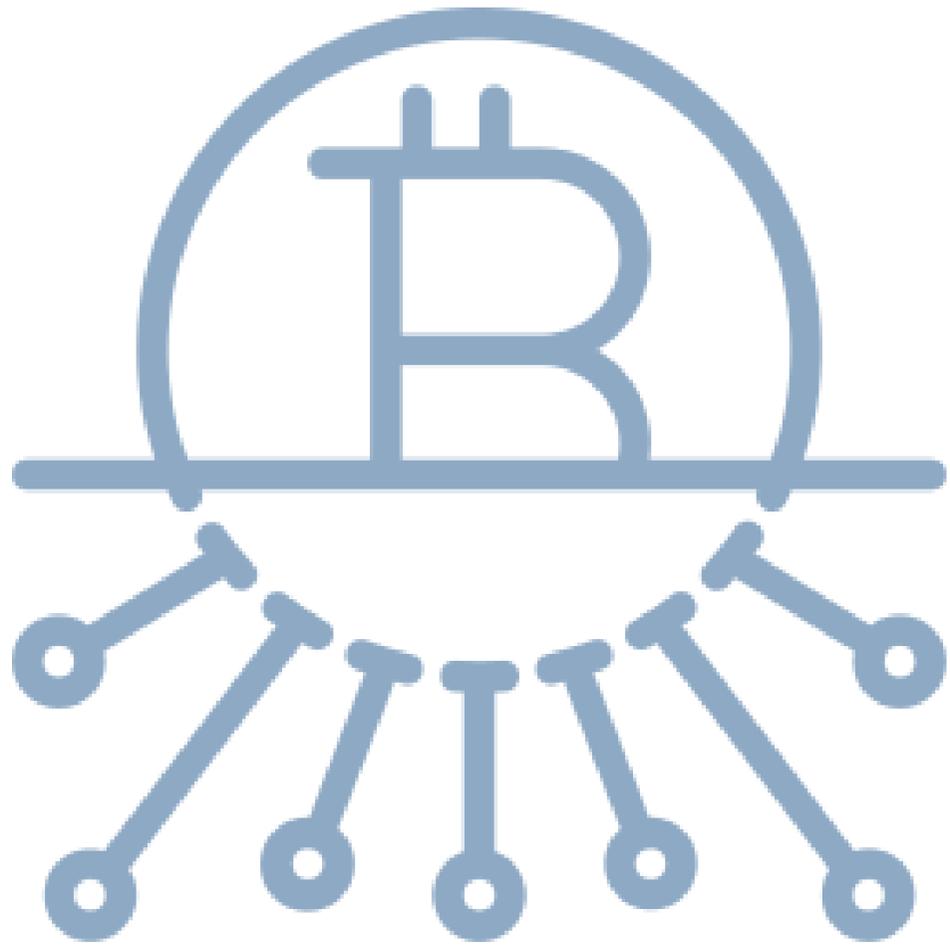


Para abordar estos desafíos, existen diversas estrategias. Por ejemplo, la optimización de protocolos de consenso hacia alternativas más eficientes y escalables, como PoS o PoA, puede reducir el consumo de recursos computacionales. La implementación de soluciones de capa 2, como canales de pago o sidechains, también puede aumentar la capacidad de procesamiento de transacciones sin afectar la cadena de bloques principal. Además, es crucial investigar y desarrollar algoritmos de consenso más eficientes en términos de consumo energético y explorar fuentes de energía renovable para alimentar la minería de criptomonedas. Finalmente, la utilización de técnicas de compresión de datos puede reducir el tamaño de la cadena de bloques y mejorar la eficiencia en el almacenamiento y la transmisión de datos.



Actividad: Simulación de Minería de Bitcoin y Exploración de Soluciones de Escalabilidad

El propósito de esta actividad es que los participantes adquieran una comprensión práctica de los desafíos y soluciones vinculados a la escalabilidad y el consumo de recursos en blockchain, con un enfoque específico en el caso de estudio de Bitcoin. Previo a esta actividad, se realizará una explicación detallada sobre las plataformas y herramientas que se emplearán.



Plataformas y Herramientas:

CGMiner

Es un software de minería de criptomonedas de código abierto que permite a los usuarios minar Bitcoin y otras criptomonedas utilizando equipos ASIC, FPGA y GPU. CGMiner es altamente configurable y ofrece funciones avanzadas de monitoreo y control de minería.

BFGMiner

Similar a CGMiner, BFGMiner es otro software de minería de criptomonedas de código abierto que admite una amplia gama de dispositivos de minería. Ofrece características avanzadas como la detección automática de hardware y la capacidad de ajustar la frecuencia de reloj y la tensión para optimizar el rendimiento. La información la encontrará en un repositorio de github.

Red de Prueba de Bitcoin

Es una red alternativa de Bitcoin diseñada para probar nuevas características y aplicaciones sin poner en riesgo los fondos reales. Permite a los desarrolladores y usuarios experimentar con la blockchain de Bitcoin en un entorno controlado y sin consecuencias financieras.

Lightning Network:

Es una red de canales de pago de capa 2 construida sobre la blockchain de Bitcoin. Permite realizar transacciones instantáneas y de bajo costo fuera de la cadena principal de Bitcoin, mejorando la escalabilidad y la eficiencia de la red.

Procedimiento:

Introducción y Explicación de Plataformas:

CGMiner y BFGMiner

- **Propósito:** CGMiner y BFGMiner son dos populares software de minería de Bitcoin diseñados para extraer criptomonedas utilizando el algoritmo de Prueba de Trabajo (PoW), que es el mismo algoritmo utilizado por Bitcoin. Estos programas permiten a los mineros conectarse a la red de Bitcoin, resolver complejos problemas matemáticos y confirmar transacciones, a cambio de recompensas en forma de nuevas monedas.
- **Características:** Ambos programas ofrecen una amplia gama de características, incluyendo configuraciones avanzadas de minería, monitoreo del rendimiento del hardware, ajuste dinámico de la frecuencia del reloj de la GPU, y soporte para múltiples dispositivos de minería.

Red de Prueba de Bitcoin

- **Propósito:** La red de prueba de Bitcoin es una réplica de la red principal de Bitcoin, pero diseñada específicamente para realizar pruebas y experimentos sin involucrar moneda real. Permite a los desarrolladores y usuarios probar nuevas aplicaciones, realizar experimentos de minería y realizar transacciones sin preocuparse por pérdidas financieras.
- **Características:** La red de prueba de Bitcoin opera de manera similar a la red principal, pero utiliza bitcoins de prueba (BTC) que no tienen valor económico. Esto permite a los participantes experimentar con todas las funcionalidades de Bitcoin sin riesgo financiero.



Lightning Network

- **Propósito:** La Lightning Network es una solución de escalabilidad de segunda capa diseñada para mejorar la velocidad y eficiencia de las transacciones en la red de Bitcoin. Permite transacciones instantáneas y de bajo costo fuera de la cadena principal de Bitcoin, aliviando así la congestión y reduciendo las tarifas de transacción.
- **Características:** La Lightning Network utiliza canales de pago bidireccionales que permiten a los usuarios realizar transacciones directas sin necesidad de confirmaciones en la cadena principal. Esto agiliza el proceso de transacción y reduce los costos asociados con las transacciones en la red de Bitcoin.

Simulación de Minería de Bitcoin:

Durante esta fase de la actividad, los participantes seguirán instrucciones detalladas para instalar y configurar CGMiner o BFGMiner en sus máquinas virtuales. Se les proporcionarán pasos claros y concisos para garantizar una instalación sin problemas de estas herramientas de minería de Bitcoin. Esto incluirá la descarga del software desde fuentes confiables, la instalación de dependencias necesarias y la configuración de parámetros específicos para la minería eficiente de Bitcoin.

Una vez que CGMiner o BFGMiner estén correctamente instalados, los participantes serán guiados a través del proceso de conexión a la red de prueba de Bitcoin. Se les proporcionará información sobre cómo acceder a la red de prueba y cómo configurar sus programas de minería para conectarse a ella. Esto puede implicar la especificación de la dirección del nodo de la red de prueba y la configuración de otros parámetros relevantes.



Después de establecer la conexión a la red de prueba de Bitcoin, los participantes procederán a la configuración de parámetros de minería dentro de CGMiner o BFGMiner. Se les proporcionará orientación sobre cómo ajustar estos parámetros para optimizar el rendimiento de la minería, como la frecuencia del reloj de la GPU, el factor de dificultad y la asignación de potencia de procesamiento.

Durante la simulación de minería, los participantes tendrán la oportunidad de observar de cerca el consumo de recursos y el rendimiento de la minería en sus máquinas virtuales. Podrán monitorear el uso de CPU, GPU y energía, así como la velocidad de hashing y la tasa de éxito en la resolución de bloques. Esto les permitirá comprender mejor cómo funcionan los programas de minería de Bitcoin en términos de consumo de recursos y eficiencia de la minería.

Exploración de la Lightning Network:

Instalación del Software de Lightning Network:

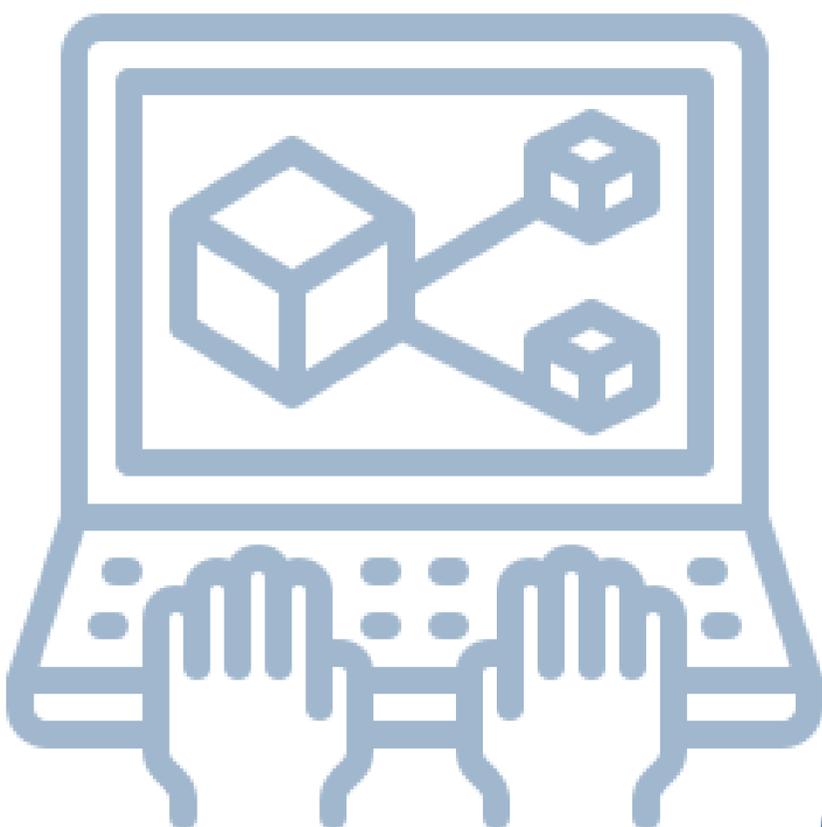
Para configurar nodos de Lightning Network, se puede utilizar software como LND (Lightning Network Daemon) o c-lightning. Ambos son populares y bien documentados.

Se debe seguir la documentación oficial para la instalación específica del software seleccionado, asegurándose de cumplir con todos los requisitos del sistema.

Configuración y Puesta en Marcha:

Una vez instalado el software, se debe generar una billetera de Lightning Network y asegurarse de tener fondos disponibles para las transacciones.

Se procede a configurar el nodo con la información requerida, como la dirección IP, los puertos de escucha y las claves de autenticación.



Conexión a la Red:

Después de configurar el nodo, se conecta a la red de Lightning Network para empezar a realizar transacciones.

Se establecen conexiones con otros nodos de la red para facilitar las rutas de pago y la transferencia de fondos.

Realización de Transacciones Prácticas:

Selección de Escenario:

Se presentarán varios escenarios de uso, como realizar un pago a otro usuario de la red o abrir un canal de pago bidireccional con un nodo diferente.

Ejecución de la Transacción:

Se sigue el proceso específico del escenario seleccionado para ejecutar la transacción. Esto puede implicar la selección del destinatario, la cantidad a transferir y la confirmación de la transacción.

Monitoreo y Verificación:

Después de realizar la transacción, se monitorea el estado de la misma para asegurarse de que se complete correctamente.

Se verifican los detalles de la transacción, como el tiempo de confirmación y los costos asociados, para evaluar la eficiencia y la velocidad de la Lightning Network en comparación con las transacciones tradicionales en Bitcoin.

