COLOMBIA POTENCIA DE LA VIDA

TIC

Módulo 1

LECCIÓN 2
Mining pools y conceptos de minería en blockchain

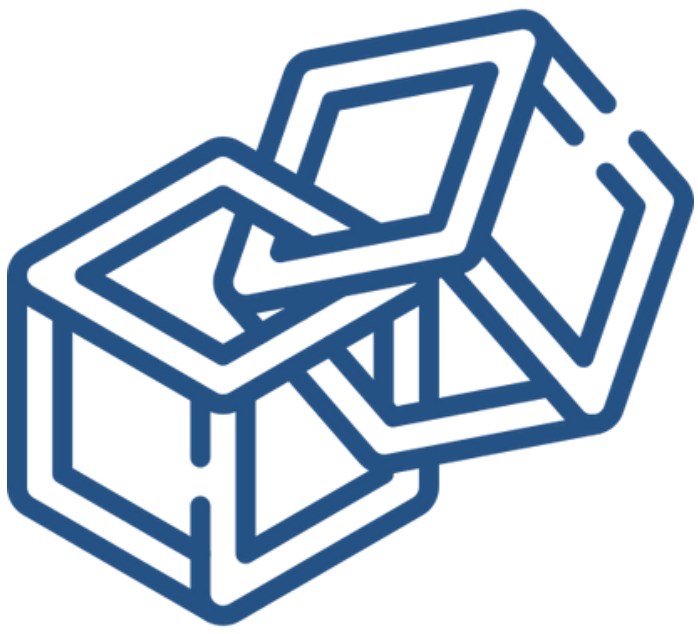
TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

Blockchain

La cadena de bloques de Ethereum es una sucesión de todos los bloques que han sido añadidos a la red a lo largo de su historia. Se denomina así debido a que cada bloque incluye una referencia al bloque anterior, lo que facilita la preservación de un orden en la totalidad de los bloques, proporcionando un registro preciso de la historia.

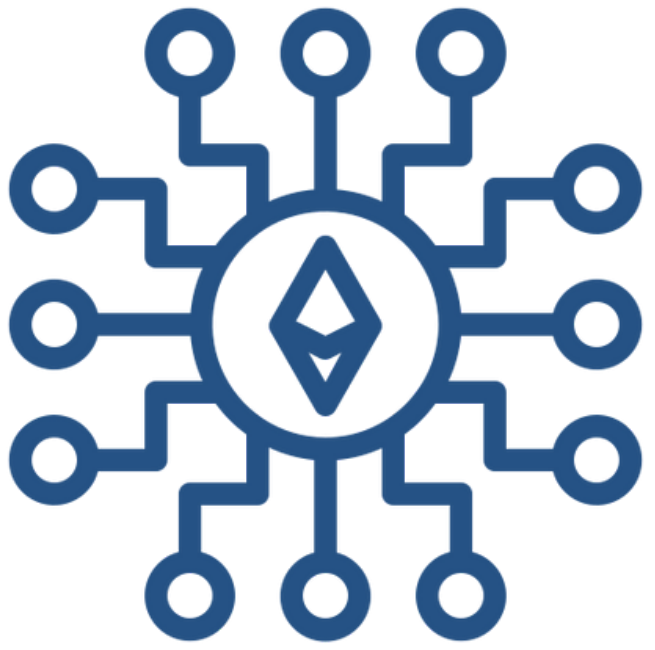


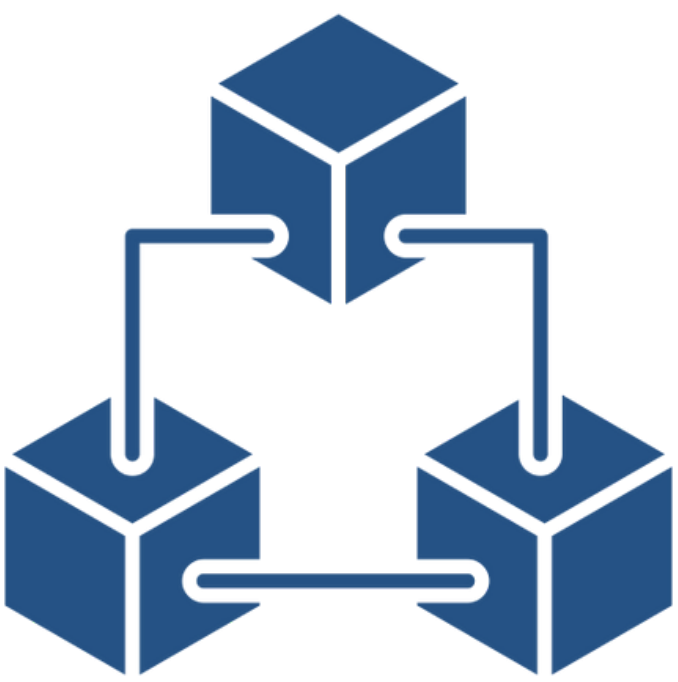
ETH

El Ether (ETH) es la criptomoneda nativa de Ethereum. Los usuarios de la plataforma pagan ETH a otros usuarios para que se cumplan sus solicitudes de ejecución de su código.

EVM

La Máquina Virtual de Ethereum (EVM) funciona como un ordenador virtual a nivel global, y su estado está respaldado por todos los participantes en la red Ethereum. Cualquier miembro de la red tiene la capacidad de pedir la ejecución de código diverso en la EVM, y dicha ejecución provoca cambios en el estado de la EVM.



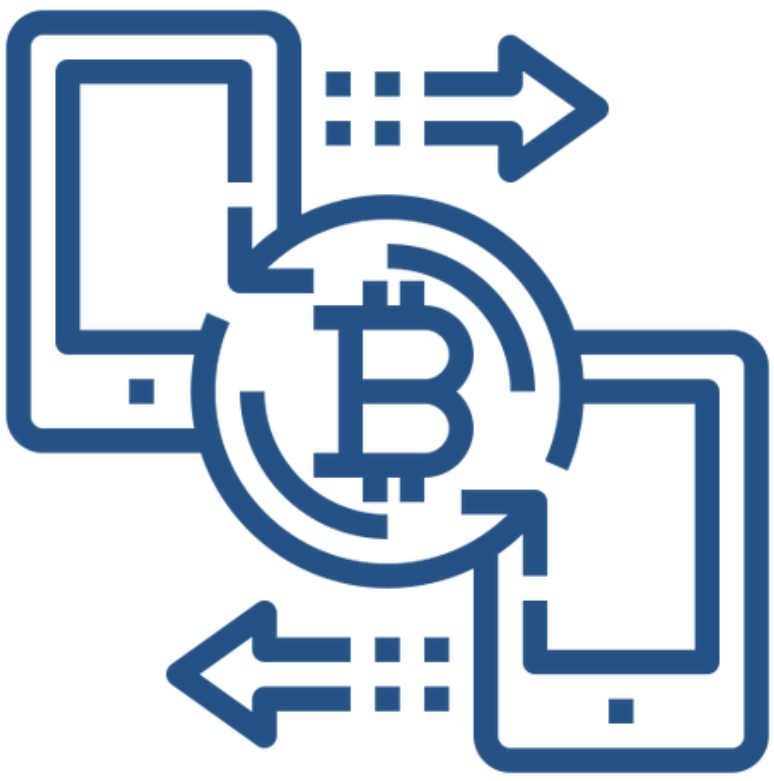


Nodos

Se trata de máquinas físicas que retienen la información, y se mantienen en contacto para difundir detalles acerca del estado actual de la EVM y las recientes modificaciones en dicho estado. También, cualquier usuario tiene la posibilidad de requerir la ejecución de código al enviar la solicitud desde uno de los nodos. La red de Ethereum engloba a todos los nodos de Ethereum y sus interacciones.

Cuentas

Las cuentas son espacios de almacenamiento del ETH. Los usuarios tienen la capacidad de crear cuentas, depositar y transferir en ellas desde sus cuentas a las de otros usuarios. Una extensa tabla en la EVM guarda información sobre las cuentas y sus saldos, contribuyendo así al estado general de la EVM.



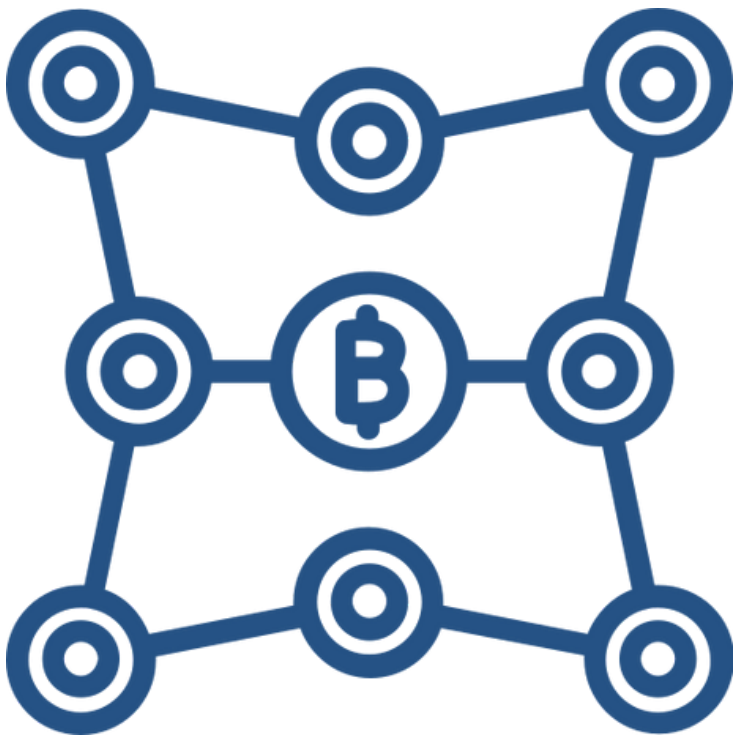
Transacciones

La solicitud de transacción es el procedimiento formal para pedir la ejecución de código en la EVM. Una “transacción” es esencialmente una solicitud de transacción que ha sido completada junto con los cambios asociados en el estado de la EVM. Cualquier usuario puede enviar una solicitud de transacción desde un nodo a la red.

Para que esta solicitud afecte al estado acordado, debe ser validada, ejecutada y enviada a la red por otro nodo. La ejecución de código provoca cambios en el estado de la EVM, y mediante el consenso, estos cambios se transmiten a todos los nodos de la red. Algunos ejemplos de transacciones incluyen enviar una cantidad específica de ETH desde una cuenta a la de otra persona, publicar código de contrato inteligente en la EVM y ejecutar el código de un contrato inteligente en una dirección específica con argumentos dados.

Bloques

Dado el elevado volumen de transacciones, estas se agrupan en bloques. Por lo general, un bloque contiene varias docenas o cientos de transacciones. Cada bloque tiene un hash que lo identifica y se conecta al bloque anterior a través de su hash para generar la cadena de bloques.



Contrato inteligente

Es un fragmento de código reutilizable, también conocido como programa, que un desarrollador sube al entorno EVM. Cualquier persona puede solicitar la ejecución del código del contrato inteligente al realizar una solicitud de transacción. Dado que los desarrolladores pueden crear diversas aplicaciones ejecutables en la EVM, como juegos, mercados e instrumentos financieros, mediante la publicación de contratos inteligentes, a menudo se les conoce como DApps o Aplicaciones Descentralizadas.

Mecanismo de consenso

El consenso en Ethereum se refiere a un acuerdo general entre nodos de la red sobre el estado de la cadena de bloques. Es como un grupo que decide qué película ver juntos. Ethereum utiliza un mecanismo de consenso basado en la prueba de participación, donde el 66 % de los nodos debe coincidir en el estado de la red. Este mecanismo incluye recompensas y sanciones para fomentar la honestidad de los participantes y hacer costoso cualquier intento de ataque a la red. El protocolo rige la selección de validadores, la propuesta y validación de bloques, y la resolución de bifurcaciones. En resumen, estos componentes forman el mecanismo de consenso.

Prueba de trabajo

La prueba de trabajo es el algoritmo fundamental que establece la dificultad y las reglas para la labor de los mineros, que consiste en agregar bloques válidos a la cadena. La minería, o dicho trabajo, es crucial para determinar la longitud de la cadena y seguir la bifurcación correcta de la cadena de bloques. Cuanto más trabajo se realiza, más larga será la cadena, y con un mayor número de bloques, se incrementa la seguridad de la red para adaptarse al estado actual.

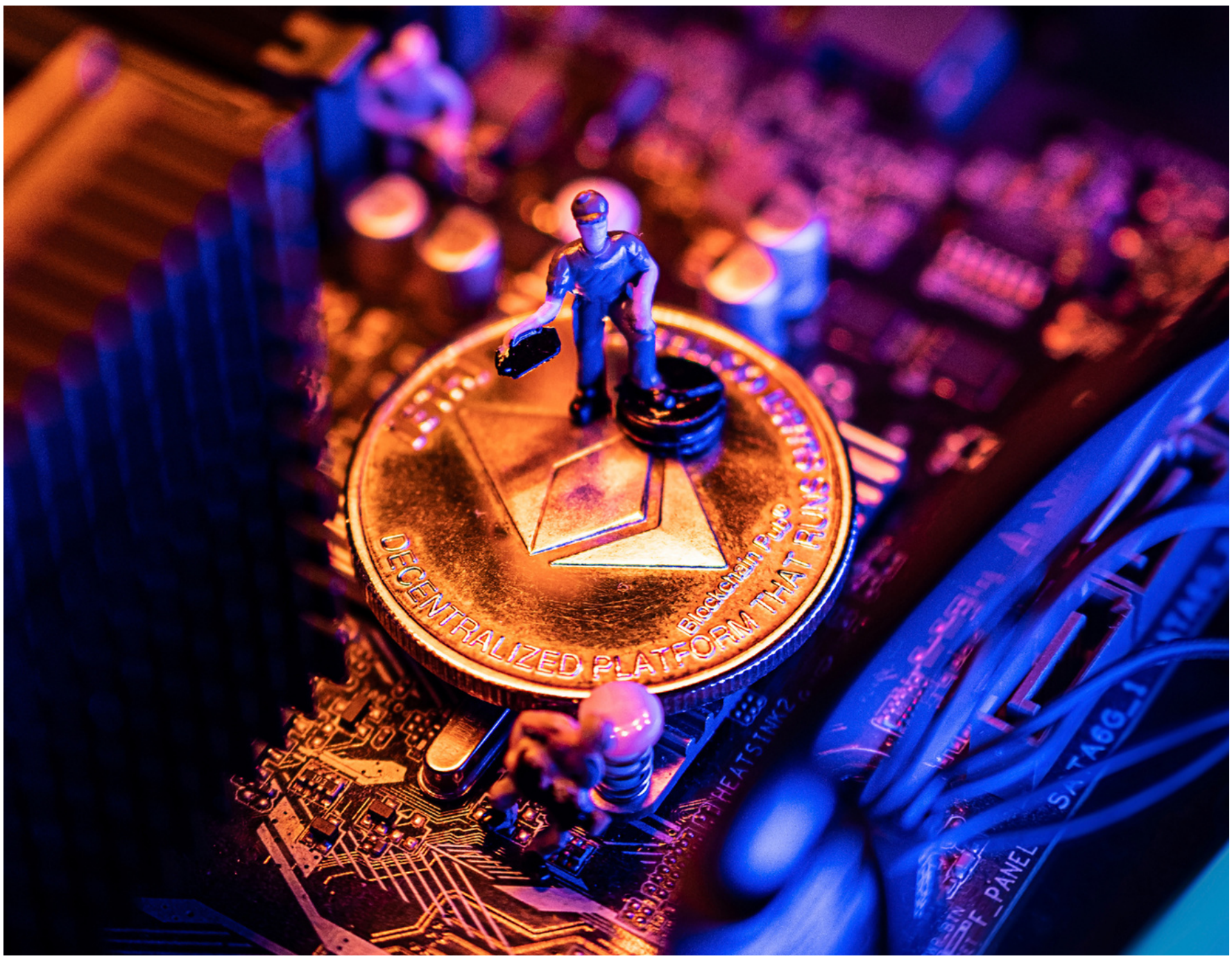
La minería en la blockchain

La minería es un proceso esencial en las redes blockchain descentralizadas, como Bitcoin o Ethereum Classic (ETC) y Ethereum Work (ETHW), que busca emitir unidades de la criptomoneda de la red y validar las transacciones. Los mineros, nodos de la blockchain, emplean equipos para crear bloques con transacciones y resolver problemas matemáticos únicos asociados a esos bloques.

El primero en resolver el problema envía su bloque al resto de los mineros para su confirmación y adición a la cadena de bloques. Esta descentralización es mantenida por mineros que reciben incentivos en forma de comisiones por transacciones y recompensas en la criptomoneda de la red, como Bitcoin en el caso de la red Bitcoin. Estos incentivos motivan a los mineros a invertir en la infraestructura necesaria para sostener la red.

Los mineros y las mining pools

Los mineros en la red Bitcoin fueron inicialmente impulsados por desarrolladores de software que instalaron el software en computadoras personales. Con el aumento de mineros, la competencia creció, disminuyendo la probabilidad individual de resolver problemas de bloques.



Surgieron dos modalidades de minería en grupo: las granjas, que son grupos inversores con data centers y equipos de alto rendimiento, y los mining pools, grupos que permiten a quienes tienen equipos de bajo rendimiento unirse para aumentar conjuntamente la capacidad de cómputo y la probabilidad de resolver bloques, al combinar su poder computacional trabajan como si fueran uno solo. Las recompensas se distribuyen proporcionalmente en las granjas y de manera equitativa en los mining pools.

¿La minería en un negocio rentable?

Para evaluar la viabilidad de un proyecto de minería, es esencial considerar variables clave que afectan los ingresos y costos. En términos de ingresos, el precio de la criptomoneda minada y el crecimiento de la red son fundamentales. A medida que el precio aumenta, los ingresos en dólares también aumentan, pero el crecimiento de la red puede reducir la cantidad de recompensas por minero.

En cuanto a los costos, la inversión en hardware y el costo de la energía eléctrica son críticos. La elección de la ubicación geográfica puede influir en el costo de la electricidad. La variabilidad en estos costos es baja y se puede controlar eficientemente. A diferencia de los costos, los ingresos dependen principalmente del rendimiento de la industria cripto y la red específica.

El análisis de casos de uso de la red, su potencial futuro y la comprensión de su historial son elementos clave para evaluar la viabilidad a largo plazo de un proyecto de minería. Este enfoque permite anticipar y comprender mejor el panorama para tomar decisiones informadas.