

Módulo 1

LECCIÓN 1

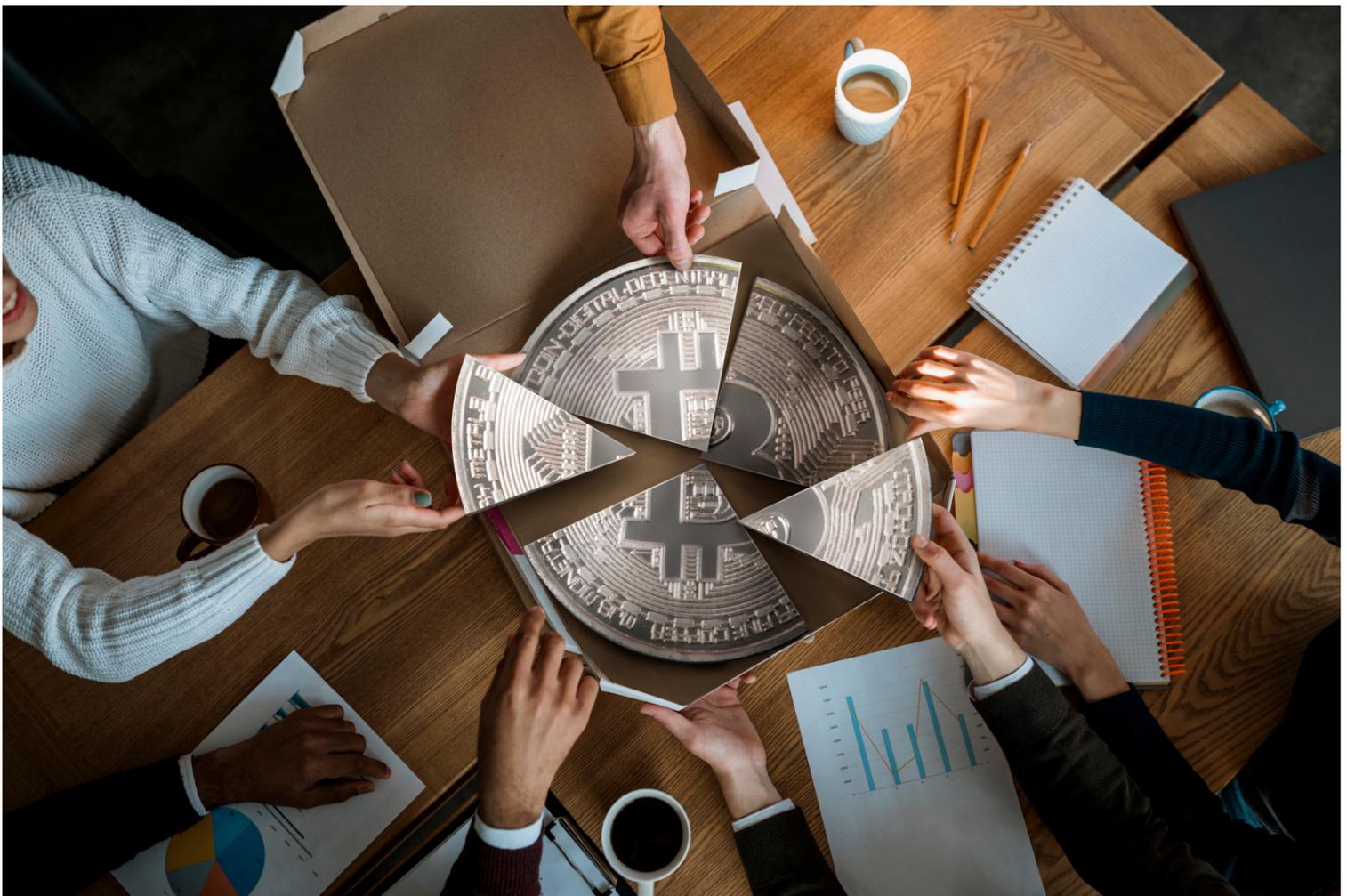
Pool de Mineros y Recompensas

Pool de Mineros y Recompensas

Tiempo de ejecución: 2 horas

Planteamiento de la sesión:

En esta lección se profundizará en los Mining Pools, mostrando cómo algunos mineros unen su capacidad computacional y reparten la recompensa de manera equitativa basados en el nivel de participación que tuvo cada uno durante el proceso.



Desarrollo de la sesión: 2 horas

Pool de Mineros

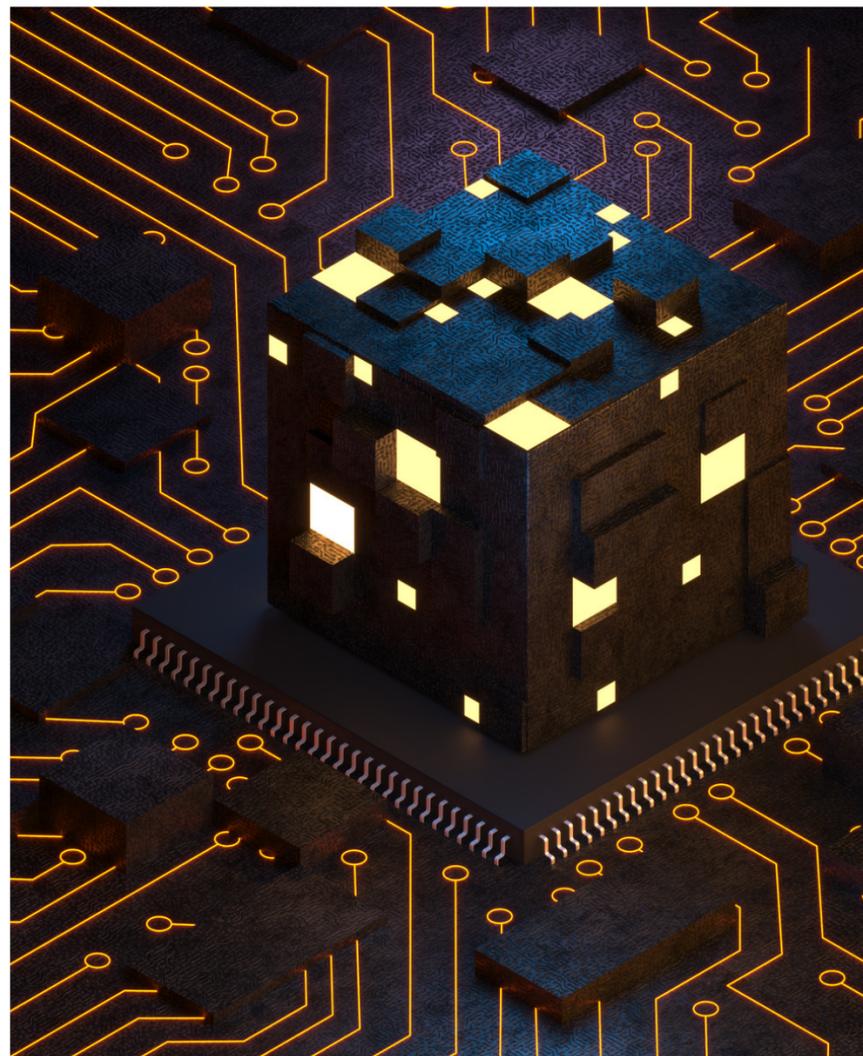
Un pool de minería es una entidad que reúne a un grupo de mineros de criptomonedas como la moneda de Ethereum o Bitcoin. En este sistema los mineros se unen para sumar sus capacidades de cómputo y minar como si fueran uno solo.

Este sistema existe en respuesta al hardware más potente y especializado de la actualidad. La diferencia entre los pools de mineros es cómo los mismos reparten sus recompensas entre los participantes.



Gracias a la colaboración de varios equipos ASIC conectados a la red eléctrica, se logran obtener recompensas, por ejemplo, en bitcoins. Estas recompensas son generalmente compartidas entre los participantes que aportaron su potencia de hashrate (es un indicador de la potencia de una red blockchain y también de su seguridad). Sin embargo, existen modalidades donde el pago se limita a la recompensa dividida, ya que las comisiones, que varían según el usuario, son dirigidas a los administradores del grupo minero.

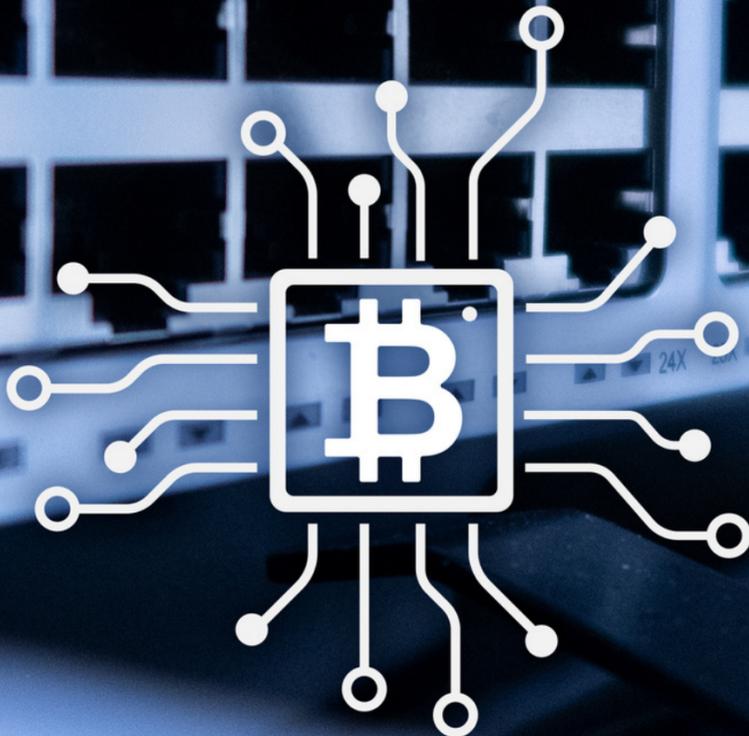
El concepto de pool de minería se puede entender como un modelo de negocio que recompensa financieramente a aquellos encargados de resolver bloques en una red que utiliza el consenso de "Prueba de trabajo" (PoW). Esto refleja la idea de que unirse y colaborar es más beneficioso, ya que intentar realizar esta actividad de manera individual resulta simplemente imposible por la capacidad de cómputo requerida, en consonancia con el principio de "unidos es mejor".



Estas alianzas surgieron como respuesta a la competencia generada por la introducción de hardware avanzado y como una solución al aumento de la dificultad en la minería de Bitcoin. Este aumento se aceleró a medida que la actividad digital se expandió globalmente. No es posible determinar cuál de estos factores influyó primero, ya que ambos se desarrollaron prácticamente simultáneamente, dando origen a la industria minera que se observa en la actualidad.

En la década del 2010, cuando la dificultad de la minería comenzó a aumentar y los mineros emigraban de las CPU a las tarjetas de video (GPU), aquellos operadores rezagados se unieron para competir en potencia de hashrate con aquellos que ya utilizaban hardware diseñado para juegos de computadora (tarjetas de video o GPU), diseño y otras aplicaciones, con el propósito de llevar a cabo la actividad de minería.

Blockchain Revolution



Primer pool de la minería:

Durante ese periodo surgió Slush Pool, considerado como el pool de minería de Bitcoin más antiguo en el ecosistema. La tarea de los mineros individuales que usaban sus computadoras personales (CPU) para obtener bitcoins se complicó, ya que los mineros con GPU estaban empezando a dominar el panorama. Ante esta situación, el desarrollador Marek Palatinus anunció en el foro Bitcoin Talk la creación del pool de minería cooperativa Bitcoin.cz, con el objetivo de hacer frente a estos operadores mediante el concepto de minería agrupada.

Este pool logró minar tres bloques en su primer día de funcionamiento en diciembre de 2010. En el año 2016, el grupo cambió oficialmente su nombre a Slush Pool y, a partir de ese momento, surgieron nuevos pools que también incluyeron la minería de otras criptomonedas.



Llegada de los ASIC

El modelo de minería agrupada se replicó con la introducción de los ASIC (Circuito Integrado para Aplicaciones Específicas). Este hardware especializado marcó un cambio significativo en la minería, al ser diseñado exclusivamente para la extracción de bitcoins.

En este punto, los pools desempeñaron un papel importante al facilitar la distribución del poder de procesamiento generado por la activación de estas nuevas máquinas. Estos dispositivos dejaron obsoletas a las tarjetas de video (GPU) para la minería de Bitcoin, ya que no podían competir con la eficiencia de los ASIC.

Los pools de minería, como en la actualidad, desempeñan la función de equilibrar la potencia de procesamiento en la red para fomentar la descentralización. Aunque en el pasado se registraron instancias de concentración de poder en un solo grupo, como el ya desaparecido GHash.io, que llegó a controlar más del 50% del hashrate y fue disuelto por esta razón

Funcionamiento de un pool de Minería



El funcionamiento de los pools se basa en una función específica del protocolo de Bitcoin llamada `getblocktemplate`. Esta función, una actualización de `getwork`, posibilita que los mineros coordinen y concentren la potencia de procesamiento en un solo bloque, el cual se extrae de manera colaborativa. Es esencialmente una herramienta que notifica a un conjunto de equipos de minería que hay trabajo disponible para realizar.

El administrador del pool de minería tiene la tarea de que los mineros equilibren sus potencias, de manera que no desperdicien su poder de procesamiento. Asimismo, son quienes tienen la responsabilidad de dividir las recompensas obtenidas por la resolución de un bloque y hacerlas llegar a quienes conforman la organización.

Actualmente, uno de los desarrollos más novedosos y actualizados para minar en un pool es Stratum V2. Este se encarga de otorgarle más poder de decisión a los mineros, al tiempo que evita la censura en las transacciones por parte del administrador del grupo y, además, hace más eficiente el registro y la propagación de las transferencias



Cualquier persona que tenga la capacidad de cómputo necesaria puede participar en una pool de minería. En la mayoría de los pools, el acceso se encuentra disponible sin costo alguno, aunque los detalles relacionados con las comisiones y el funcionamiento específico varían según cada grupo.

Al momento de unirse, el minero establece discusiones con la empresa respecto a aspectos clave, como el método y la periodicidad de los pagos, así como la distribución de las ganancias. Además, se aclara la proporción que retendrá el pool como parte de su organización. Una vez que se llega a un acuerdo mutuo, se inicia la operación en conjunto.

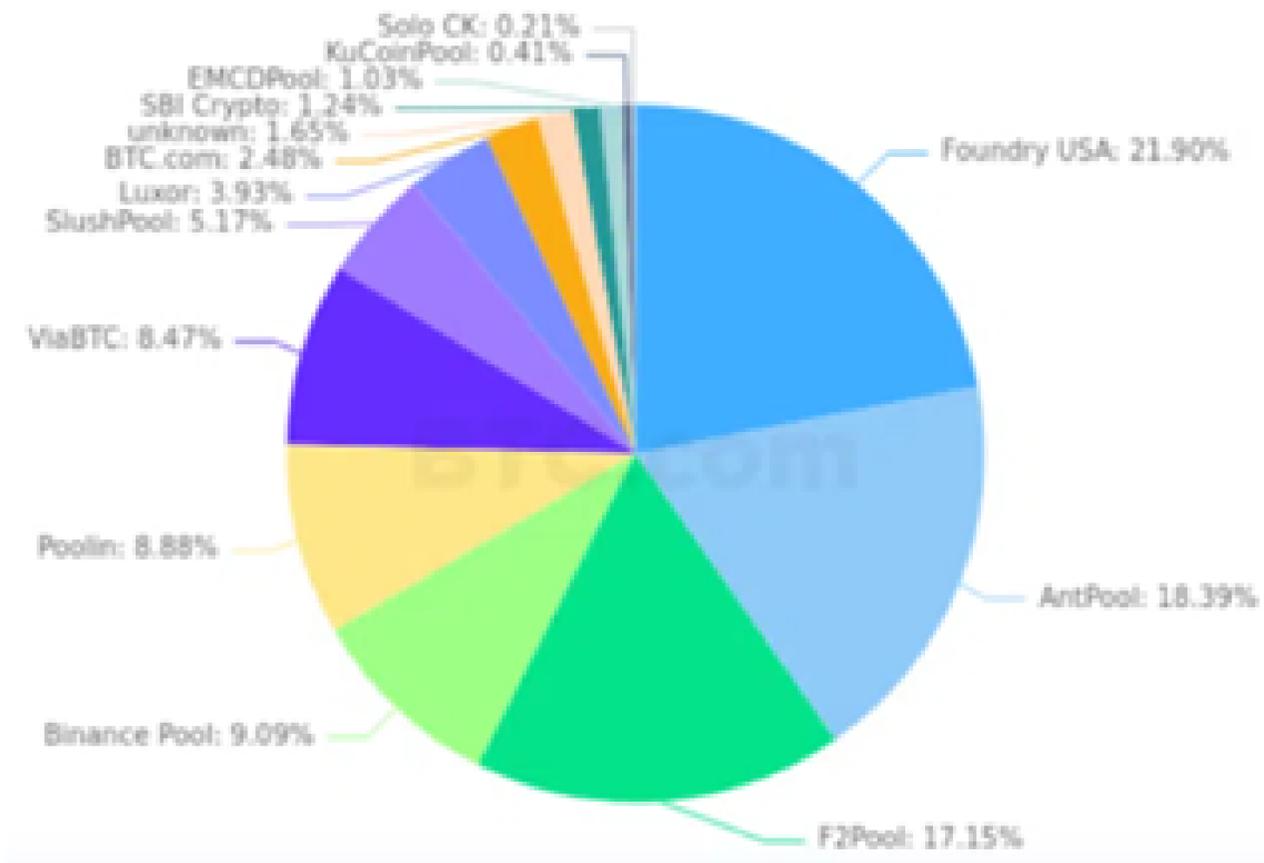


Figura 1: Gráfico de participación de los pools de minería.

En la figura 1 se puede ver un gráfico tomado de la BTC.com del año 2022, en el cual se muestra la distribución de los pools de minería más relevantes de ese momento. Como se ve en la figura, solo el 1.65% se encuentran en estado desconocido, esto quiere decir que son granjas de minería autónomas que no han formado pools con otros mineros, esto debido a su capacidad de cómputo propia, la cual es suficiente para cubrir sus necesidades.

Para los demás, hay participaciones de pools con el 0.21% en el caso de Solo CK, y una participación del 21.90% por parte de Foundry USA, la cual tiene la mayor participación de todas las pools.



Límites de participación:

En el caso de que una pool llegara a superar el 50% de la participación total de la red, se tendría que disolver para mantener el sistema descentralizado.

Es importante que los mineros comprendan que la centralización de la red y los riesgos asociados a los ataques del 51% no benefician al sistema. Estos elementos pueden provocar la disminución de los precios de Bitcoin y disminuir la confianza de los potenciales nuevos inversores.



Tipos de pagos o recompensas:

Otro enfoque es el pago por las últimas "N" participaciones (PPLNS), que se calcula según el porcentaje de participación de los mineros en el pool, permitiéndoles contribuir al conjunto de acciones realizadas por el grupo minero.

Un último tipo es el pago completo por participación (FPPS), similar al share. En estos pools, los mineros reciben un porcentaje por su participación en la actividad, además de las comisiones pagadas por transacción por bloque.

Esto incrementa significativamente las ganancias de los mineros y respeta su derecho sobre las tarifas de transacción.

