Jørgen Halse & Henrik Skog

Criptomonedas y banca tradicional

Las criptomonedas son activos digitales que utilizan la criptografía para realizar transacciones financieras seguras. Funcionan en redes descentralizadas, lo que significa que no están controladas por una única entidad, como un gobierno o una institución financiera. En su lugar, se basan en una red de usuarios para verificar y registrar las transacciones. Esto las convierte en una fuerza potencialmente disruptiva en el sector bancario tradicional, ya que ofrecen a particulares y empresas una forma alternativa de enviar y recibir dinero. [1]

Por el contrario, la banca tradicional es un sistema centralizado en el que las instituciones financieras, como bancos y cooperativas de crédito, desempeñan un papel central en la facilitación y regulación de las transacciones financieras. Estas instituciones mantienen y gestionan los depósitos de los clientes, prestan dinero y facilitan el cambio de divisas. También desempeñan un papel clave en el sistema de pagos, actuando como intermediarios entre compradores y vendedores para garantizar que las transacciones se realizan de forma fluida y segura.

Hay varios aspectos clave de la banca tradicional que las criptomonedas pueden sustituir potencialmente. Uno de los más significativos es el papel de los bancos como intermediarios en las transacciones financieras. Dado que las criptomonedas operan en redes descentralizadas, pueden permitir a particulares y empresas

[1] https://www.jpmorganchase.com/news-stories/could-blockchain-have-great-impact-as-internet

realizar transacciones directas entre sí, sin necesidad de que los bancos actúen como intermediarios. Esto podría reducir las comisiones y los tiempos de transacción, así como aumentar la accesibilidad financiera y la inclusividad, al permitir que los particulares y las empresas de zonas subbancarizadas o no bancarizadas participen en la economía mundial.

Las criptomonedas también pueden sustituir potencialmente a la banca tradicional en la emisión y gestión de moneda. Al estar descentralizadas y no estar controladas por una única entidad, las criptomonedas pueden ofrecer una forma de dinero más estable y segura. Esto se debe a que su oferta es limitada y no puede ser manipulada fácilmente por gobiernos o instituciones financieras. [2]

Este texto examinará los aspectos clave de la banca tradicional y presentará cómo o si las criptodivisas podrían sustituirlos. Examinará las principales diferencias, ventajas y desventajas entre ambos enfoques. También examinará los retos técnicos que aparecen en la implantación de una moneda descentralizada y cómo se resuelven. Se utilizarán como ejemplos las criptomonedas Ethereum, Bitcoin y Monero, ya que tienen diferentes propiedades que resultan interesantes en el debate.

Introducción a las criptodivisas

Como se indica en la introducción, una criptodivisa es una moneda digital o virtual que utiliza criptografía para su seguridad y está descentralizada, lo que significa que funciona sin una autoridad central como un banco o un gobierno. Cada transacción se firma digitalmente para garantizar su autenticidad y se registra en un bloque junto con otras transacciones. Una vez que un bloque se llena de transacciones, se añade a la cadena de bloques y no puede alterarse. Esto crea un registro seguro y transparente de todas las transacciones dentro de la red, permitiendo el seguimiento y la verificación de las transacciones sin necesidad de una autoridad central como en la banca tradicional. Bitcoin, Ether y Monero son ejemplos de criptomonedas que han ganado popularidad y adopción en los últimos años. Cada una de estas criptodivisas tiene sus propias características y utiliza la criptografía de diferentes maneras para lograr sus objetivos.

Es importante señalar que, aunque a menudo se habla de blockchain y criptomonedas a la vez, no son lo mismo. Blockchain es una tecnología de base de datos descentralizada y distribuida que permite el registro seguro y transparente de las transacciones. Las criptomonedas, por su parte, son activos digitales que utilizan la tecnología blockchain para permitir transacciones financieras seguras. En otras palabras, las criptomonedas son un tipo de aplicación que se ejecuta sobre una plataforma de cadena de bloques. Mientras que la tecnología blockchain tiene el

[2] https://www.investopedia.com/terms/c/cryptocurrency.asp

potencial de revolucionar una amplia gama de industrias, las criptomonedas se utilizan principalmente como medio de intercambio y depósito de valor. Entender la diferencia entre estos dos conceptos es importante para comprender el debate.

En la siguiente sección se hará una introducción a las tres criptomonedas Bitcoin, Ether y Monero.

Bitcoin

Bitcoin es una criptomoneda descentralizada que fue creada en 2009 por un individuo o grupo de individuos desconocidos utilizando el seudónimo "Satoshi Nakamoto". Una de sus características clave es que tiene un suministro limitado. Sólo habrá un total de 21 millones de Bitcoin, y en diciembre de 2022 ya se habían acuñado alrededor de 19,2 millones.[3] Esto contrasta con las monedas fiduciarias tradicionales, que pueden ser emitidas en cantidades ilimitadas por los bancos centrales. La oferta limitada de Bitcoin pretende garantizar que su valor se mantenga en el tiempo y evitar la inflación.

La oferta limitada de Bitcoin tiene implicaciones significativas para su uso como depósito de valor y medio de intercambio. Significa que, a diferencia de las monedas fiduciarias, que pueden perder valor debido a la inflación, se espera que el valor de Bitcoin aumente a medida que crece su demanda. Esto lo ha convertido en un vehículo de inversión popular, ya que muchas personas compran Bitcoin como una forma de protegerse contra la inflación y la incertidumbre económica.

Bitcoin es una moneda digital descentralizada que utiliza un algoritmo de consenso de prueba de trabajo (PoW) para lograr un consenso distribuido en la cadena de bloques. Utiliza la función criptográfica SHA-256 para registrar las transacciones y producir valores hash únicos para cada bloque de la cadena de bloques. Estos valores hash se incluyen en la cabecera del bloque y permiten verificar las transacciones del bloque y crear un vínculo criptográfico entre cada bloque y el bloque anterior de la cadena.

Ether

Ether es la criptomoneda nativa de la plataforma Ethereum, que es una plataforma de blockchain descentralizada y de código abierto que permite la creación de contratos inteligentes y aplicaciones descentralizadas (dApps). Fue creada en 2015 por Vitalik Buterin y desde entonces se ha convertido en una de las criptodivisas más utilizadas y valoradas.

---

[3] https://buybitcoinworldwide.com/how-many-bitcoins-are-there/

El Ether tiene un suministro limitado, con un total de alrededor de 115 millones de Ether en circulación a partir de 2021. La oferta de Ether no es fija, sino que viene determinada por su demanda como medio de pago por el uso de la plataforma Ethereum. Esto significa que la oferta de Ether puede aumentar o disminuir con el tiempo en función de la demanda de la plataforma Ethereum y del número de transacciones que se procesen en ella. A diferencia del Bitcoin, que se utiliza principalmente como depósito de valor y medio de intercambio, el Ether se utiliza principalmente para facilitar la ejecución de contratos inteligentes en la plataforma Ethereum. Esto significa que los validadores de los nuevos bloques se eligen en función de su participación y no de su potencia de cálculo.

Monero

Monero es una criptomoneda descentralizada creada en 2014 como una bifurcación de la criptomoneda Bytecoin. Se centra en la privacidad y el anonimato, y utiliza diversas técnicas para ocultar el remitente, el destinatario y el importe de cada transacción en su blockchain.

Monero opera en una red descentralizada entre pares y, al igual que Bitcoin, utiliza un mecanismo de consenso de prueba de trabajo para asegurar la cadena de bloques y validar las transacciones. Tiene una oferta limitada, con un total de unos 18,4 millones de Monero en circulación en 2021. El suministro de Monero aumenta a un ritmo decreciente con el tiempo, con un máximo de alrededor de 18,5 millones de Monero que se espera que estén en circulación en el año 2030.

Es una criptomoneda centrada en la privacidad que utiliza técnicas criptográficas avanzadas, como firmas en anillo y direcciones ocultas, para proteger la privacidad de sus usuarios. Utiliza la función hash criptográfica RandomX para su algoritmo de consenso de prueba de trabajo, que está diseñado para ser más privado y escalable que el algoritmo SHA-256 utilizado por Bitcoin, que se explora más adelante en el texto.

El enfoque de Monero en la privacidad y el anonimato lo ha convertido en una opción popular para aquellos que buscan una alternativa segura y privada a los sistemas financieros tradicionales. Sin embargo, también ha suscitado controversia y escrutinio normativo debido a su posible uso con fines ilícitos. A pesar de ello, sigue siendo una criptomoneda muy utilizada y valorada, con una capitalización de mercado de miles de millones de dólares..[4]

El intermediario de confianza

Además de almacenar su dinero, el papel central de los bancos es ser un intermediario de confianza a la hora de transferir dinero. Cuando un particular o una

[4] https://www.getmonero.org/resources/about/

empresa quiere enviar dinero a otra persona, puede iniciar una transferencia a través de su banco. El banco verifica la autenticidad de la transacción y garantiza que los fondos se transfieren de forma segura desde la cuenta del remitente a la del destinatario.

¿Cómo se puede implementar esta funcionalidad en una red descentralizada? Las cadenas de bloques se basan en una red de usuarios para verificar y registrar las transacciones. Esto se consigue mediante un proceso llamado "consenso", que permite a la red llegar a un acuerdo sobre el estado de la cadena de bloques. Garantizar la integridad y seguridad de esta red se resuelve principalmente de dos formas diferentes: prueba de trabajo, empleada por las blockchain Bitcoin y Monero, y prueba de participación, implementada por la blockchain Ethereum.

En la prueba de trabajo, un grupo de usuarios llamados "mineros" compiten para resolver un problema matemático complejo. El primer minero que resuelve el problema añade el siguiente bloque de transacciones a la cadena de bloques y es recompensado con una pequeña cantidad de criptomoneda. Para que un nuevo bloque sea aceptado, la mayoría de los mineros de la red deben verificarlo. Por lo tanto, para que alguien lleve a cabo con éxito una transacción ilegal en la cadena de bloques, tendría que convencer a la mayoría de los mineros para que participen en ella.

Una de las principales críticas al sistema de prueba de trabajo (PoW) utilizado por la red Bitcoin es que consume mucha energía. El proceso de minar nuevos bloques en la red Bitcoin requiere una cantidad significativa de potencia de cálculo, y esta potencia suele ser suministrada por ordenadores y servidores que consumen mucha energía. Según estimaciones de Digiconomist, la red Bitcoin es responsable de unos 73 millones de toneladas de dióxido de carbono al año, lo que equivale a las cantidades generadas por Suiza. [5]

También preocupa la centralización del poder minero en la red Bitcoin[6], ya que el proceso de minería consume muchos recursos y requiere hardware especializado. Esto ha provocado la aparición de grandes pools de minería, que son grupos de mineros que aúnan sus recursos para aumentar sus posibilidades de encontrar una solución al problema de la prueba de trabajo. La concentración del poder de minería en un pequeño número de pools de minería ha suscitado preocupación sobre la descentralización de la red Bitcoin. Sin embargo, como se ha dicho antes, se necesita una mayoría para poder manipular la blockchain, que es muy difícil de obtener.

---

[5] https://digiconomist.net/bitcoin-energy-consumption
[6] https://www.investopedia.com/investing/why-centralized-crypto-mining-growing-problem/

En un sistema Proof of Stake (PoS), que es el empleado por la blockchain de Ethereum, el proceso de validar transacciones y añadir nuevos bloques a la cadena se denomina "staking". En lugar de resolver acertijos matemáticos, los nodos de un sistema PoS son elegidos para validar transacciones y añadir nuevos bloques a la cadena en función del número de monedas que poseen, o su "estaca". Este proceso está diseñado para ser más eficiente energéticamente que PoW, ya que no requiere que los mineros gasten cantidades significativas de potencia de cálculo para resolver puzles.

La criptografía es un aspecto importante de los sistemas PoS, ya que se utiliza para asegurar la red y protegerla contra el fraude y los ataques. Por ejemplo, a los nodos de un sistema PoS se les puede pedir que proporcionen firmas criptográficas como parte del proceso de apuesta para demostrar que son los propietarios legítimos de su participación. Además, se utilizan hashes criptográficos para asegurar la integridad de la cadena de bloques y evitar la manipulación del historial de transacciones.[7]

Uno de los principales inconvenientes de no tener una autoridad central en el caso de las criptomonedas es que no hay una única entidad que pueda intervenir para anular o cancelar transacciones. Esto puede ser un problema si alguien comete un error al enviar una transacción, como enviarla a la dirección equivocada o enviar una cantidad incorrecta. En estos casos, no suele haber forma de recuperar los fondos, ya que la transacción se considera definitiva e irrevocable una vez que se añade a la blockchain.

Esta falta de recurso puede ser especialmente frustrante para los usuarios que son nuevos en el mundo de las criptomonedas y no están familiarizados con los detalles técnicos de su funcionamiento. También puede ser un problema para los usuarios que son objetivo de estafadores o piratas informáticos, ya que no existe una autoridad central a la que denunciar el problema o pedir una indemnización.

En general, la ausencia de una autoridad central en el caso de las criptomonedas puede ser tanto una ventaja como un inconveniente. Aunque permite una mayor descentralización y autonomía, también significa que los usuarios son responsables de la seguridad y exactitud de sus propias transacciones y no tienen el mismo nivel de protección o recurso que en un sistema financiero tradicional.

Privacidad personal

La privacidad personal es un concepto clave a la hora de analizar las diferencias entre el sistema bancario tradicional y las criptomonedas, ya que se gestionan de forma muy diferente. Con la banca tradicional, nadie puede acceder a sus

---

[7] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

transferencias. Sin embargo, los bancos pueden compartir información sobre sus transacciones financieras con terceros en determinadas circunstancias. Por ejemplo, los bancos están obligados a informar de determinadas transacciones a organismos gubernamentales, como la Red de Represión de Delitos Financieros (FinCEN) en Estados Unidos, como parte de sus esfuerzos para combatir el blanqueo de capitales y la financiación del terrorismo. Los bancos también pueden compartir información sobre sus transacciones con agencias de información crediticia, que pueden utilizar la información para calcular su puntuación de crédito y proporcionar servicios relacionados con el crédito a otras organizaciones.

Una de las principales características de la tecnología blockchain es que se trata de un sistema transparente y abierto. Esto significa que las transacciones se registran públicamente en la cadena de bloques y cualquiera puede verlas. Esta transparencia es una de las principales razones por las que la tecnología blockchain se considera segura y fiable, ya que permite a cualquiera verificar la autenticidad y exactitud de las transacciones, pero también significa que cualquiera y todo el mundo puede rastrear los detalles de cada transacción en el libro mayor. Si la identidad del emisor y el receptor quedara al descubierto, todas sus transacciones serían públicas.

Hay varias razones por las que alguien podría no querer esto. Algunas personas valoran su privacidad financiera y no quieren que sus transacciones financieras sean visibles para el público. Por ejemplo, alguien puede querer hacer una donación a una organización política, o una empresa quiere mantener sus transacciones financieras en privado por razones de competencia. Otros pueden estar preocupados por la posibilidad de que su información financiera sea utilizada para el robo de identidad u otras actividades fraudulentas.

Bitcoin y Ether son bastante similares con respecto a la privacidad de las transacciones en sus respectivas redes, con la excepción de algo llamado pruebas de conocimiento-cero, que se discutirá más adelante. Las transacciones de ambas monedas se publican en su libro mayor público, que registra todas las transacciones de la red. Esto significa que cualquiera puede ver las transacciones que se han producido en la red, incluidas las direcciones del emisor y el receptor y el importe de la transacción. Sin embargo, las direcciones no están directamente vinculadas a las identidades reales de las personas u organizaciones que las utilizan. Esto significa que no es posible determinar la identidad de las personas u organizaciones que están detrás de una dirección concreta simplemente mirando la blockchain, pero que en el caso de que la identidad de la persona que está detrás de una dirección quede expuesta, todas sus transacciones también lo estarán. En la blockchain de Monero se toman medidas adicionales para evitarlo.

Seguridad personal con Monero

Monero tiene varias características para proporcionar la privacidad de sus usuarios, y en comparación con Bitcoin y Ethereum, Monero se considera generalmente más seguro porque ofrece un mayor nivel de protección de la privacidad.

Ocultar la dirección del receptor de la transacción

En una transacción típica de criptomoneda, las direcciones de los receptores son visibles en la cadena de bloques. Esto significa que cualquiera puede ver todas las transacciones realizadas a una dirección, exponiendo también su saldo. El blockchain de Monero utiliza un concepto llamado direcciones ocultas para evitar esto. Una dirección oculta es una dirección generada aleatoriamente una sola vez que crea el emisor basándose en información pública sobre el receptor. Y aunque la dirección esté relacionada con el receptor, no hay forma de detectar esta similitud mirando sólo las direcciones por separado. Entonces, el receptor recibe automáticamente los fondos de la dirección aleatoria. Esto puede hacerse ya que son los únicos en posesión de su clave privada, que está conectada a su información pública de la que se derivó la dirección temporal. Esto significa que cualquiera que consulte la cadena de bloques no podrá ver la dirección real del receptor. En su lugar, sólo verán la dirección oculta aleatoria de un solo uso que se utilizó para la transacción. Sin embargo, el receptor podrá gastar los fondos.[8]

Ocultar la dirección del remitente de la transacción

Las firmas digitales son un tipo de mecanismo criptográfico que se utiliza para asegurar y verificar transacciones en diversos contextos, incluido el mundo de las criptomonedas. En una transacción de criptomoneda, se crea una firma digital utilizando una combinación de la clave privada del remitente y los datos de la transacción. Sin embargo, el uso de firmas digitales en este sentido significa que cualquiera que tenga acceso a la clave pública puede verificar la firma y vincularla a la clave privada correspondiente, exponiendo al público el remitente de la transacción. Para evitar esto, Monero utiliza firmas en anillo.

Monero utiliza firmas en anillo para crear una firma firmada por un grupo de usuarios. En una firma en anillo, el remitente selecciona un grupo de usuarios (denominado "anillo") y crea una firma que puede verificarse utilizando las claves públicas de cualquiera de los usuarios del anillo. Sin embargo, nadie puede determinar cuál de los usuarios firmó realmente la transacción, ya que la firma es una combinación de las firmas de todos los usuarios del anillo.

---

[8] https://serhack.me/articles/what-is-stealth-address-technology-monero/

Esto significa que cualquiera que consulte la cadena de bloques no podrá determinar cuál de los usuarios del anillo firmó realmente la transacción. Esto hace que sea mucho más difícil para cualquiera rastrear la transacción o vincularla a una persona o entidad específica. [9]

Ocultar el importe de la transacción

Para evitar que el importe de la transacción sea público en el libro mayor, Monero utiliza un protocolo llamado RingCT.

Los retos criptográficos en la implantación de las criptomonedas

En el contexto de las criptomonedas, el hash se refiere al proceso de utilizar una función hash criptográfica para asignar datos de entrada (es decir, una transacción o un bloque de transacciones) a una salida de tamaño fijo (es decir, un valor hash). Este resultado es único para los datos de entrada y se utiliza para verificar la autenticidad de los datos y garantizar que no han sido manipulados. El hash es una parte fundamental de muchos sistemas criptográficos, incluidas las criptomonedas, y desempeña un papel clave para garantizar la seguridad e integridad de los datos en la cadena de bloques.

Cuando se crea un nuevo bloque de transacciones en una cadena de bloques, las transacciones del bloque se someten a un hash criptográfico. Esto produce un valor hash único que se asocia con el bloque de transacciones, y este valor hash se incluye en la cabecera del bloque. Ethereum utiliza el algoritmo Keccak-256[10] mientras que Bitcoin utiliza el algoritmo SHA-256. Monero, por otro lado, utiliza un algoritmo hash llamado Blake2b como parte de RandomX, que exploraremos más adelante.

La inclusión del valor hash en la cabecera del bloque tiene varios propósitos. En primer lugar, permite verificar las transacciones del bloque. Un nodo de la red puede verificar si las transacciones del bloque coinciden con el valor hash de la cabecera del bloque. Esto garantiza que las transacciones del bloque son auténticas y no han sido manipuladas.

En segundo lugar, la inclusión del valor hash en la cabecera del bloque crea un vínculo criptográfico entre cada bloque y el bloque anterior de la cadena. Este vínculo se crea incluyendo el valor hash del bloque anterior en la cabecera del bloque actual. Esto crea una cadena de bloques a prueba de manipulaciones, en la

---

[9] https://localmonero.co/knowledge/ring-signatures
[10] https://ethereum.org/en/glossary/#keccak-256

que cualquier intento de alterar un bloque de la cadena provocaría la ruptura del enlace criptográfico entre ese bloque y el anterior.

En las cadenas de bloques de Bitcoin y Ethereum, el esquema general para verificar los bloques de la cadena de bloques es el mismo: cada bloque de transacciones se somete a un proceso de hash para obtener un valor hash único, que se incluye en la cabecera del bloque. Sin embargo, hay muchas otras diferencias de implementación ahora que Ethereum ha cambiado a Proof-of-Stake.

En resumen, el hash se utiliza para la verificación de bloques en una cadena de bloques mediante la producción de un valor hash único para cada bloque de transacciones y la inclusión de este valor hash en el encabezado del bloque. Esto permite verificar las transacciones del bloque y crea un vínculo criptográfico entre cada bloque y el bloque anterior de la cadena.

La función hash SHA-256 utilizada en Bitcoin es resistente a las colisiones, lo que significa que es extremadamente difícil encontrar dos valores de entrada diferentes que produzcan el mismo hash de salida. Dado que la base de Proof-of-work es que tienes que producir trabajo para poder minar un bloque y que el sistema sea de confianza, esta es una propiedad muy importante de la función hash. Si la función no fuera resistente a las colisiones, no se podría confiar en que los bloques son correctos, ya que un bloque con datos de transacción manipulados podría tener el mismo hash que un bloque correcto en tal caso.

La función RandomX

El enfoque en la privacidad de Monero es evidente en su elección de utilizar el algoritmo RandomX. Está diseñado para ser resistente al uso de hardware de minería especializado (ASICs) mediante el uso de técnicas de ejecución de código aleatorio y de memoria dura. Está optimizado para su uso en CPU de uso general, lo que tiene como objetivo hacer que la red Monero sea más descentralizada e igualitaria en la distribución de las recompensas de los bloques. Mediante el uso de RandomX, Monero es capaz de evitar el uso de ASICs y otro hardware de minería especializado, lo que hace más difícil para cualquier persona obtener una ventaja de minería sobre otros usuarios y ayuda a mantener la red más descentralizada.

Una de las características clave del protocolo RandomX es su uso de cálculos de memoria dura, que requieren almacenar y acceder a una gran cantidad de memoria para resolver el rompecabezas de la minería. Esto hace que sea difícil para los fabricantes de hardware optimizar su hardware para la minería RandomX, ya que tendrían que incluir una gran cantidad de memoria en sus diseños.

En general, el protocolo RandomX está diseñado para ser resistente al hardware especializado y para promover un ecosistema de minería más descentralizado, dificultando que una sola entidad o grupo de entidades domine el proceso de minería.

En resumen, Monero se considera generalmente más seguro que Bitcoin y Ethereum porque ofrece un mayor nivel de protección de la privacidad mediante el uso de direcciones ocultas y firmas en anillo, y porque utiliza un algoritmo de consenso de prueba de trabajo diferente que es más privado.

Zero Knowledge Proofs

Las pruebas de conocimiento cero (ZKP, por sus siglas en inglés) son un tipo de técnica criptográfica que permite a una parte (el prover) demostrar a otra (el verifier) que posee cierta información, sin revelar realmente la información en sí. Un ejemplo práctico podría ser demostrar a una empresa que se es ciudadano de un Estado sin revelar el pasaporte, por si se hace un uso indebido de él. Este concepto se utiliza a menudo en el contexto de la cadena de bloques y las criptomonedas para garantizar la privacidad y la seguridad.

En el caso de Bitcoin, los ZKP son cruciales en la implementación de la red relámpago, por ejemplo. Aquí los ZKP se utilizan para verificar que una transacción es válida sin revelar los detalles de la misma, como las identidades del remitente y el destinatario o la cantidad que se transfiere. Esto significa, que puedo confiar en que otra persona tiene la cantidad suficiente de Bitcoin, sin revelar el número exacto que tiene, o cualquier otro detalle sobre la transacción. Esto ayuda a mantener el anonimato de los usuarios de Bitcoin y a proteger su privacidad.

Las ZKP no son una parte esencial del diseño de Ethereum. Sin embargo, pueden usarse en Ethereum para transacciones fuera de la cadena que están destinadas a ser añadidas a la cadena de bloques en un momento posterior. En este contexto, los ZKP pueden utilizarse para verificar la autenticidad y validez de la transacción sin revelar los detalles de la misma, como las identidades del remitente y el destinatario o la cantidad transferida.

Por ejemplo, supongamos que Alicia y Bob quieren realizar una transacción fuera de la cadena utilizando un contrato inteligente en la plataforma Ethereum. Pueden utilizar un ZKP para demostrarse mutuamente que la transacción es válida sin revelar los detalles de la misma. Una vez completada la transacción, pueden enviar el ZKP a la cadena de bloques de Ethereum, junto con una prueba de que la transacción se ha realizado. Esto puede ayudar a aumentar la privacidad y seguridad de la transacción, ya que los detalles de la misma no se revelan a terceros.

Monero, por otro lado, utiliza ZKPs como parte clave de su diseño. Monero utiliza ZKPs para ocultar los detalles de las transacciones, incluyendo las identidades del remitente y el destinatario y la cantidad que se transfiere. Esto ayuda a mantener la privacidad de los usuarios de Monero y la convierte en una opción más atractiva para aquellos que valoran el anonimato.

Una diferencia clave entre estas tres criptomonedas es la forma en que utilizan los ZKP y el nivel de privacidad que proporcionan. Mientras que Bitcoin y Monero utilizan ZKPs para ocultar los detalles de las transacciones, Monero va un paso más allá utilizando ZKPs para ocultar completamente las identidades del remitente y del destinatario. Esto convierte a Monero en una opción más privada que Bitcoin.

En general, las ZKP son una herramienta clave para garantizar la privacidad y la seguridad en el mundo del blockchain y las criptomonedas. Aunque las distintas criptomonedas las utilizan de formas diferentes, desempeñan un papel fundamental a la hora de mantener la integridad y la privacidad de las transacciones.

Conclusión

Las criptomonedas son divisas digitales que utilizan la criptografía para permitir las transacciones entre iguales y descentralizar los sistemas bancarios tradicionales. Las distintas criptomonedas se centran más o menos en la privacidad, y algunas dan prioridad a la seguridad personal y al anonimato en las transacciones.

Bitcoin es la primera y más conocida criptodivisa, creada en 2009 por un individuo o grupo de individuos desconocidos con el seudónimo de "Satoshi Nakamoto". Tiene un suministro limitado de 21 millones de monedas y se utiliza principalmente como depósito de valor y medio de intercambio. Utiliza un algoritmo de consenso de prueba de trabajo (PoW) y la función hash criptográfica SHA-256 para asegurar y validar las transacciones en la cadena de bloques.

Ether es la criptomoneda nativa de la plataforma Ethereum, una plataforma de blockchain descentralizada y de código abierto que permite la creación de contratos inteligentes y aplicaciones descentralizadas (dApps). Creada en 2015, tiene una oferta limitada, pero no fija, que viene determinada por la demanda de la plataforma Ethereum. Se utiliza principalmente para facilitar la ejecución de contratos inteligentes en la plataforma Ethereum y utiliza un algoritmo de consenso proof-of-stake (PoS).

Monero es una criptomoneda descentralizada centrada en la privacidad y el anonimato, creada en 2014 como una bifurcación de la criptomoneda Bytecoin. Utiliza diversas técnicas para ocultar el remitente, el destinatario y el importe de

cada transacción en su blockchain. Monero utiliza un algoritmo de consenso de prueba de trabajo (PoW) y la función criptográfica RandomX para asegurar y validar las transacciones en la cadena de bloques. Cuenta con un suministro limitado de unos 18,4 millones de monedas, y se espera un suministro máximo de unos 18,5 millones de monedas para 2030.

En general, mientras que Bitcoin, Ether y Monero son criptomonedas descentralizadas que utilizan diferentes algoritmos de consenso y funciones hash criptográficas para asegurar y validar las transacciones en sus respectivas cadenas de bloques, tienen diferencias significativas en términos de sus casos de uso, capitalización de mercado y base de usuarios. Bitcoin se utiliza principalmente como depósito de valor y medio de intercambio, Ether se utiliza para facilitar la ejecución de contratos inteligentes en la plataforma Ethereum, y Monero se centra en la privacidad y el anonimato.

Las criptodivisas son monedas digitales que utilizan la criptografía para permitir las transacciones entre pares y descentralizar los sistemas bancarios tradicionales. Las distintas criptomonedas se centran más o menos en la privacidad. Algunas, como Monero, dan prioridad a la seguridad personal y al anonimato en las transacciones. En comparación, Bitcoin y Ethereum se centran menos en la privacidad en sus transacciones, debido a que presentan diferencias significativas en cuanto a sus casos de uso, capitalización de mercado y base de usuarios. Será interesante seguir el desarrollo y la adopción de las criptomonedas en el futuro.

Fuentes del artículo

JPMorgan Chase. (2022) "Could Blockchain Have as Great an Impact as the Internet?" Obtenido de https://www.jpmorganchase.com/news-stories/could-blockchain-have-great-impact-as-internet

Investopedia. (2022). “Cryptocurrency Explained”. Obtenido de https://www.investopedia.com/terms/c/cryptocurrency.asp

Buy Bitcoin Worldwide. (2022). “How many bitcoin are there?”. Obtenido de https://buybitcoinworldwide.com/how-many-bitcoins-are-there/

Monero. (2022). "About Monero." Obtenido de https://www.getmonero.org/resources/about/

Ethereum. (2022) “PROOF-OF-STAKE (POS)” Obtenido de https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

Ethereum. (2022). “Official Go implementation of the Ethereum protocol.” Github. Obtenido de https://github.com/ethereum/go-ethereum

Bitcoin. (2022). “Bitcoin Core integration/staging tree.” Github. Obtenido de https://github.com/bitcoin/bitcoin

Monero. (2022). “Monero: the secure, private, untraceable cryptocurrency.” Github. Obtenido de https://github.com/monero-project/monero

Serhack. (2022). “What is Stealth Address technology and Why Does Monero Use It?” Obtenido de https://serhack.me/articles/what-is-stealth-address-technology-monero/

Localmonero. (2022). “How Ring Signatures Obscure Monero's Outputs”. Obtenido de https://localmonero.co/knowledge/ring-signatures

Digiconomist. (2022). "Bitcoin Energy Consumption Index." Obtenido de https://digiconomist.net/bitcoin-energy-consumption

Ethereum. (2022). “Glossary”. Obtenido de https://ethereum.org/en/glossary/#keccak-256