KRON: Sistema electrónico para la Creación y Transferencia de activos (peer to peer)

(PROTOTIPO EXPERIMENTAL)

Agradecimiento al fundador y desarrolladores de Bitcoin. El proyecto Kron se lanzó sobre la base de Bitcoin y ha sido trabajo duro y esfuerzo continuo.

Kron es una cadena de bloques experimental optimizada para transferir activos, como tokens, de un titular a otro. Basado en el extenso desarrollo y prueba del Modelo UTXO del protocolo Bitcoin, Kron se basa en una bifurcación del código Bitcoin. Los cambios incluyen un tiempo de recompensa en bloque de cinco minutos, un cambio en la cantidad de monedas emitidas y la adición de creación de activos y capacidades de mensajería. Las billeteras de Kron son gratuitas y de código parcialmente abierto. Todos los Kron han sido minados en los nodos principales del entramado de red mediante el Protocolo SND utilizando el algoritmo Rx19r. Kron tiene como objetivo priorizar la seguridad, el control del usuario, la privacidad y Resistencia a la censura. Está abierto a su uso y desarrollo en cualquier jurisdicción, al tiempo que permite funciones adicionales simples para los usuarios según sus necesidades.

Desde décadas antes de que se creara **Bitcoin**, la obsesión por crear un dinero puramente digital rondaba la cabeza de muchas personas. Pero uno de los principales problemas con el que todos se chocaban de frente era el famoso **doble gasto**. Fue **Satoshi Nakamoto** quien, gracias a un conjunto de técnicas, solventó este gran problema, pudiendo crear el primer dinero descentralizado puramente digital. Las UTXO de Bitcoin desempeñan un gran papel en la creación de las transacciones para que los Kron puedan viajar de forma segura dentro del protocolo blockchain.

Activos Tokenizados

El protocolo Ethereum ERC20 y otros proyectos muestran activos tokenizados que utilizan otra cadena de bloques, se puede crear con una amplia variedad de propósitos y estructuras. Los tokens ofrecen varias ventajas a acciones tradicionales u otros mecanismos de participación, p. ej. velocidad de transferencia más rápida, mayor control del usuario y resistencia a la censura, y reducción o eliminación de la necesidad de un tercero de confianza. Bitcoin también tiene la capacidad de servir como rieles para tokens mediante el uso de proyectos como Omnilayer, RSK.

Sin embargo, ni Bitcoin ni Ethereum fueron diseñados específicamente para facilitar la propiedad de activos adicionales, y los usuarios y equipos de desarrollo generalmente priorizan otras características.

Kron está diseñado para manejar de manera eficiente una función específica: la transferencia de activos de una parte a otra. Uno de los objetivos del protocolo Kron es crear una cadena de bloques centrada en casos de uso y esfuerzo de desarrollo que puede crear código, proporcionando ventajas para casos de uso específicos.

Si la economía global está influenciada por actores que utilizan varias cadenas de bloques, entonces la forma en que los mercados de capitales trabajan hoy también podría cambiar. Las fronteras y jurisdicciones pueden volverse menos relevantes a medida que más activos se convierten en comerciables y el comercio transfronterizo se vuelve cada vez más libre de fricciones. En una época donde la gente puede mover cantidades significativas de riqueza al instante utilizando Bitcoin, es probable que los consumidores globales demanden la misma eficiencia para sus valores y tenencias de activos similares.

Tokens de fondo y otros activos

El 3 de enero de 2009, Bitcoin se lanzó como un sistema de efectivo electrónico de igual a igual. Años después, después alcanzó un nivel notable de seguridad, se reconoció que los activos se podían crear "encima de" o incrustado en la cadena de bloques de Bitcoin. Se pueden agregar nuevos activos a la cadena de bloques de Bitcoin creando transacciones de bitcoins seguras, firmadas e inmutables que también contienen información sobre la emisión de activos, y transferencias.

Hubo varios proyectos que agregaron tokens a la cadena de bloques de Bitcoin. El primero fue Mastercoin por JR Willett, seguido de Counterparty y otros proyectos. Una categoría de protocolos desarrollado para facilitar la creación de activos en la cadena de bloques de Bitcoin se conoció como Monedas de Colores, ya que marcan transacciones de bitcoins con transacciones especialmente diseñadas en OP_RETURN, que es como un campo de comentarios en el protocolo Bitcoin.

La ventaja de incrustar activos en la cadena de bloques de Bitcoin es el alto nivel de seguridad. Bitcoin es considerado por muchos como la blockchain más segura porque hay una enorme cantidad de poder de minería distribuido que asegura cada bloque con un "hash de alta dificultad". Porque Los nodos de Bitcoin distribuidos reconocen el nivel de esfuerzo para crear un hash de alta dificultad, esto lo hace casi imposible reescribir o modificar la cadena de bloques sin una minería prohibitivamente alta en inversión.

Manipular la cadena de bloques de Bitcoin, reescribir o modificar su libro mayor, llevaría esfuerzos significativos de un inversor a nivel de un estado nacional. **La desventaja de incrustar activos en la cadena de bloques de Bitcoin es que las reglas de Bitcoin deben ser seguidas como se escribieron originalmente, y los nodos de Bitcoin desconocen que los activos se están incrustando.**

Esto significa que una transacción de Bitcoin debe usarse para cada transacción de activos, y debe enviar suficientes bitcoins para ser considerada una transacción válida, aunque el propósito principal de la transacción sea enviar el activo. Eso es un inconveniente, y una gran desventaja porque un cliente de Bitcoin que gasta ese bitcoin sin ser consciente de la transacción del activo integrado, destruirá el activo.

Por ejemplo, un titular de las claves privadas de Bitcoin que mantienen los activos de la Contraparte, podría enviar accidentalmente ese Bitcoin a un intercambio o billetera y perder esos activos. Una solución parcial para resolver este problema es crear un formato de dirección especial que se utiliza para el activo, pero eso no evitar el error que pueda destruir el activo. Solo proporciona más pistas de que hay un activo incrustado en la transacción.

Otros estándares de tokens como ERC20, ERC721 y ERC223 se basan en Ethereum u otras cadenas de bloques que admiten contratos inteligentes. Existe un problema diferente al usar estos contratos inteligentes. **La red Ethereum no reconoce de forma nativa estos tokens de contrato inteligente, actualmente no puede proteger contra algunos problemas comunes. Los contratos inteligentes pueden ser confusos para los usuarios, ya que puede haber múltiples tokens ERC20 con nombres idénticos.** La única distinción entre contratos con idénticos nombres es el hash del contrato.

Sistema de nivel de protocolo con reconocimiento de activos completo

La solución es crear un sistema similar a bitcoin que sea plenamente consciente de los activos. Un sistema consciente de los activos proporciona dos ventajas principales.

Primero, permite que el cliente y los comandos RPC protejan el activo de ser destruido accidentalmente.

Segundo, permite que un solo cliente nativo emita, realice un seguimiento y transfiera los activos. Por último, para brindar seguridad a los activos subyacentes, el sistema similar a bitcoin funciona solo con un valor sugerido.

Activos

Los activos son tokens que los usuarios del protocolo Kron pueden emitir sin necesidad de extraerlos. Los usuarios del protocolo Kron crean estos activos y deciden su propósito y reglas independientemente del protocolo. Estos activos o tokens existen en la cadena de bloques de Kron y podrían tener cualquier nombre, denominación o propósito seleccionado por los creadores de cada activo, moneda o ficha. Los tokens son transferibles y se mueven con la misma facilidad que bitcoin u otras criptomonedas que funcionan de manera similar.

En Kron, un activo es solo una cantidad limitada de un símbolo único y transferible a cualquier Dirección de Kron. Los activos han estado disponibles durante algún tiempo en otras plataformas como Mastercoin y como token ERC20 o ERC223 en Ethereum 2.0.

Los activos creados en el protocolo Kron tienen varias ventajas: son más fáciles de usar, están estrechamente integrados con una moneda nativa y están asegurados por un protocolo de consenso validador seguro y estable de SND la cual se ejecuta en los servidores principales.

Los estandares de tokens son:

kr10: Token principal, (el más común)
kr12: Subtoken (respaldado por el token kr10)
kr5: Token NFT (respaldado por un token kr10)
kr17: Activo calificado especial
kr18: Subactivo calificado (Respaldado por un kr17)
kr23: Criptoactivo Restringido especial (Evita la Legitimación de Capitales)

Al momento de la creación de los criptoactivos en la Red Kron se generan 3 transacciones:

1. Se reciben de la red (por la quema de monedas) la cantidad de activos emitidos a una direccion propia de la billetera creadora.

2. Se recibe el Token administrativo tipo **kr117**, el cual nunca se muestra en billetera ya que es una ficha interna que habilita la administración de los activos creados, dicho token se reconoce porque tiene el simbolo (**!**) al final del nombre y esta ficha es transferible a cualquier otra persona a quien se desee delegar los derechos sobre los activos creados.

3. La operación lleva un costo de red direfente a la quema de los Kron para crear los activos es por eso que se necesita la operación de la comisión de red.

Comisiones

La Cadena Kron tiene una configuración por defecto de 0.3 Kron/Kb para cualquier envio de activos y monedas, esta comisión es basada en **espacio en bloque.** Generalmente las transacciones pesan mucho menos de 1Kb **(aprox. 0.435Kb, 0.391Kb)** es decir que en una transaccion normal el costo aproximado será de unos 0.04 Kron. Existe la posibilidad de que los usuarios puedan ajustar las comisiones a pagar **hasta un mínimo de 0.01 Kron/Kb**, también se ha dejado la opción de poder hacer envios con **cero comisiones,** por supuesto, este tipo de transacciones será transmitida a la red siempre y cuando haya suficiente mempool disponible y por ende especio en el siguiente bloque, pero en caso de que el mempool este casi lleno, aún asi se puede incluir este tipo de transacciones con la particularidad de ser removida si estando en mempool otro usuario hace una operación, entonces es desplazada y podría sacarse del mempool a la espera del siguiente bloque.

Usos de activos

Los activos o tokens se pueden usar para cualquier cosa que la imaginación del creador pueda conjurar. Las ideas presentadas
aquí hay una muestra.

Representar activos físicos o digitales custodiados en el mundo real en tokens

- Barras de oro
- Monedas de plata
- Euros físicos
- Escrituras de la tierra
- Créditos de energía (electricidad, madera, gas, petróleo, eólica)

Representar una parte de un proyecto

- Fichas de valores: acciones o acciones de una empresa donde las acciones están representadas por una ficha en lugar de un certificado de acciones físico.

- Valores o intereses de sociedades con la capacidad incorporada de pagar dividendos en Kron (legal en muchos países de libre mercado).

- Tokens que representan una plataforma cooperativa, de sociedad limitada, de reparto de regalías o de reparto de beneficios.

- Un token que representa un artículo financiado colectivamente con la capacidad de transferir o revender el artículo.

Representando bienes virtuales

- Entradas para un evento como un partido de basebal, con la posibilidad de revender
- Una licencia para permitir una actividad.
- Un token de acceso para usar un servicio
- Moneda y elementos del juego, transferibles fuera de la plataforma del juego

Representando un crédito

● Tarjetas de regalo
● Millas aéreas
● Puntos de recompensa

Satoshi Nakamoto describió bitcoin como una implementación del bmoney de Wei Dai, diseñado para ofrecer a los usuarios más control, seguridad y privacidad que los sistemas más centralizados. Un diseño con el potencial para prevenir la violencia y la discriminación, dado que el titular de bitcoin sigue siendo privado.

Kron tiene como objetivo continuar con esta implementación centrándose en activos distintos al efectivo, proporcionando una plataforma en la que los usuarios pueden emitir fácilmente los activos que controlan según las reglas que establecen de forma segura: la Blockchain.

Lanzamiento y algoritmo de Kron

Kron se creó el 08 de marzo de 2021. Kron es un Sistema similar a bitcoin que permitirá a los usuarios emitir e integrar activos en su blockchain. Esto será realizado en fases que se construyen unas sobre otras.

Se garantiza que los nombres de los tokens son únicos

El primero en emitir un token con un nombre de pila es el propietario de ese token. El emisor de un token quema Kron y debe proporcionar un nombre de token único. El emisor determina la cantidad emitida, el número de decimales y si se les permitirá emitir más del mismo token en el futuro.

Integración firme de los activos con la billetera GUI y nuevas llamadas RPC, lo que proporciona un a administración del activo intuitiva. Emisión fácilmente de nuevos activos, información de los saldos actuales y transferencia a otros usuarios. La combinación de código parcialmente abierto y los mecanismos de incentivos compartidos habilitados basados en la blockchain. Los tokens permiten que los intereses se alineen de formas que las estructuras tradicionales no pueden.

Los proyectos de token pueden reemplazar a los jefes, gobernantes, empleados y la estructura corporativa con intereses alineados y opciones económicas para los participantes. Kron permitirá proyectos que emitan tokens para representar cooperativas, corporaciones o asociaciones. Las cooperativas, por ejemplo, son una forma de organización común en la que los empleados y participantes son propietarios. Grandes organizaciones como Credit Agricole, REI, Land O 'Lakes, Ace Hardware, Co-op Kobe, Sunkist y Ocean Spray están estructurados como cooperativas. A pesar de ofrecer muchas ventajas a participantes, las cooperativas a veces son difíciles de estructurar y mantener.

Tokenizar intereses cooperativos abre muchas nuevas formas en que esta estructura se puede utilizar para asignar recursos y capital. Dado que las reglas para cada token puede ser cambiada por cada emisor y el mantenimiento de registros se realiza en la Cadena de bloques de Kron las organizaciones pueden adaptar e implementar una variedad de participación y estructuras. Además, dado que el emisor puede hacer que los tokens sean únicos, limitados o fungibles, los gerentes de proyecto podrán tener categorías de titulares de tokens como "Accionistas de Clase A", "Socios vitalicios del club social", "Benefactores" o "Titulares de __ en el artículo del juego".

Los tokens permiten una emisión más fácil de ofertas públicas a pequeña escala.

“En el futuro, la distribución del tamaño de las multinacionales se acercará a la de las empresas locales. El cambio entre estos estados puede ser bastante rápido ya que los costos de telecomunicaciones y transporte pasan por un "punto de fusión", creando una amplia variedad de nuevas pequeñas empresas e industrias multinacionales para apoyar esos negocios”. **Esto también podría disminuir el fraude, el economista Dr. Robert Shapiro señaló evidencia significativa de que el fraude de Wall St. puede estar relacionado con cuestiones de custodia (Patrick Byrne, PhD).** Solo un protocolo abierto funcionará en una economía global donde hay múltiples jurisdicciones, cada una con regulaciones complejas y conflictivas.

Recompensas

Permitir el pago de recompensas (o dividendos) en el token nativo. Con un solo comando la recompensa, denominada en Kron, se divide automáticamente en partes iguales y se envía a prorrata a los titulares del activo.

Ejemplo:

Un niño pequeño, en un país que lo permita, podría crear una ficha que represente un puesto de limonada. Suponga que crea 10,000 tokens LIMON. Estos tokens podrían usarse para aumentar fondos para el puesto de limonada a $0.01 por token de LIMON, lo que le permite recaudar $100 para construir su negocio. Estos tokens pueden ser vendidos y transferidos fácilmente por los propietarios. Supongamos que el puesto de limonada lo hace extraordinariamente bien porque el vecindario está invertiendo en este proyecto emprendedor.

Ahora nuestro niño ficticio de ocho años quiere recompensar a quienes creyeron en el proyecto. Con un comando, puede enviar ganancias, denominadas en cualquier valor que Kron pueda tener, al Portador de fichas de LIMON. Incluso podría haber nuevos poseedores de tokens LIMON que él nunca conoció.

La facilidad de uso incorporada debería permitir que cualquier persona, en cualquier parte del mundo, pueda hacerlo en un dispositivo móvil, o computadora con Windows, Mac o Linux.

Para que un sistema global de este tipo funcione, deberá ser independiente de las jurisdicciones reguladoras. Esto no es debido a creencias ideológicas, sino a la practicidad: si los rieles para la transferencia de activos blockchain no son resistentes a la censura y agnóstico de la jurisdicción, cualquier jurisdicción determinada puede entrar en conflicto con otra. En sistemas heredados, la riqueza generalmente se limitaba a la jurisdicción del titular y, por lo tanto, era de fácil control basado en las políticas de esa jurisdicción. Debido a la naturaleza global de la tecnología blockchain, cualquier capacidad a nivel de protocolo para controlar la riqueza potencialmente colocará jurisdicciones en conflicto y no podrá operar de manera justa.

Fichas únicas (NFT)

Los tokens únicos permiten a los poseedores de tokens crear activos únicos. Al igual que los tokens ERC721, los tokens únicos son garantizados para ser únicos y solo existirá uno (**kr5**). Los tokens únicos pueden cambiar de propiedad enviando el token único a la dirección de otro usuario.
Algunos ejemplos de tokens únicos:

● Imagine que un mercader de arte emite el activo denominado ART. El comerciante puede entonces hacer un arte único adjuntando un nombre o un número de serie a cada obra de arte. Estos tokens únicos se puede transferir al nuevo propietario junto con la obra de arte como prueba de autenticidad. Los tokens ART: MonaLisa y ART: VenusDeMilo no son fungibles y representan piezas distintas del arte.

● Un desarrollador de software puede emitir el activo con el nombre de su software GAME, y luego asigne a cada token GAME una identificación o clave de licencia única. Los tokens del juego podrían ser transferidos a medida que se transfiere la licencia. Cada ficha GAME: 398222 y GAME: 423655 son tokens únicos.

● En activos del juego. Un juego ZYX_GAME podría crear activos únicos en el juego de edición limitada que son propiedad y son utilizados por el jugador del juego. Ejemplo: ZYX_GAME: SwordOfTruth005 y ZYX_GAME: HammerOfThor. Estos activos en el juego podrían guardarse, intercambiarse con otros jugadores a través de códigos QR y billeteras o subido a una actualización o versión diferente de un juego.

● Los activos únicos basados en Kron se pueden vincular a activos del mundo real. Crea un activo llamado GOLDVAULT. Cada moneda de oro o barra de oro en una bóveda se puede serializar y auditar.
Se pueden crear activos únicos asociados GOLDVAULT: 444322 y GOLDVAULT: 555994 para representar los activos específicos en la bóveda de oro física. El carácter público de la cadena permite una transparencia total.
Ejemplo:
El titular del token CAR podría emitir un token único para cada automóvil al incluir el número de serial.
Ejemplo: CAR: 19UYA31581L000000

Algunos casos de uso de activos únicos incluyen:

- Licencias de software
- Matriculación de vehículos
- Tokens de prueba de autenticidad para transferir junto con artículos que podrían ser falsificados
- Un token que permite la comunicación en un canal

Partes interesadas en la mensajería

Un problema común con los tokens / activos es que el emisor del token no puede comunicarse con los titulares de los tokens. Esto debe manejarse con mucho cuidado porque los poseedores de tokens no siempre desean ser identificado. La comunicación debe permitir al titular del token optar por no participar en cualquier momento. El sistema solo debe permitir que determinadas partes utilicen el canal de mensajes para que no sea un conducto de spam. El sistema de mensajería utiliza tokens únicos para permitir la comunicación en el canal principal de token.

Por ejemplo, el token de EMPRESA tendría un ~ EMPRESA: token de alerta que permite que las alertas sean enviado a todos los titulares de EMPRESA. Boletines, desarrolladores de juegos, organizaciones sin fines de lucro, organizaciones activistas, corporaciones y otras entidades pueden emitir tokens para usuarios específicos y luego enviar mensajes a esos usuarios, pero a diferencia del correo electrónico u otros servicios de mensajería, la mensajería en sí se habilitará solo para los titulares de tokens, lo que hace el token transferible.

Los mensajes a los titulares de tokens por remitentes autorizados se superpondrán a los activos únicos. Los activos únicos actuarán como un "bastón parlante" que permitirá que el propietario del canal envíe mensajes a los poseedores.

Votación

Uno de los problemas, entre muchos, con el sistema financiero actual de muchos paises es que todas las acciones están celebradas en nombre de la calle. En esta era de comunicación rápida, esto hace que la celebración de una votación sea ridículamente difícil. Una empresa pública que emite acciones en Nasdaq, por ejemplo, tendrá que pagar un cuasi empresa monopolista solo para obtener las direcciones de correo de sus propios accionistas en un momento dado. Luego, se debe enviar un correo físico (árbol muerto) a los accionistas con información sobre cómo para votar junto con un formulario de voto por poder.

Mediante el uso del sistema de mensajería, los titulares de un token pueden ser notificados del voto, y emitiendo automáticamente un token de VOTO a cada titular de un token, el voto se puede automatizar desde el cliente a través de una interfaz web o móvil utilizando el protocolo integrado en Kron.

Los tokens se crean para representar votos. Kron creará un número exacto de tokens VOTE 1: 1 a los titulares de las fichas. Estos votos se pueden enviar a través del protocolo a direcciones que cuenta los votos. Debido a que los tokens de votación se mueven de la misma manera que los activos, la delegación de votos a veces conocida como democracia “delegativa o líquida” - es posible.

Privacidad

La privacidad es clave en inversiones y tokens porque los sistemas financieros funcionan mejor cuando los activos son fungibles y pueden comerciar sin fricciones. El proyecto debe buscar fortalecer la privacidad en cualquier manera posible a medida que se realicen futuras mejoras tecnológicas. A medida que se agreguen capacidades como mensajería, activos y recompensas, la privacidad se mantendrá de la misma forma en que las criptomonedas basadas en UTXO que separan la identidad de las direcciones públicas.

Dado que deseamos privacidad, debemos asegurarnos de que cada parte de una transacción tenga conocimiento solo de lo que es directamente necesario para esa transacción. Puesto que se puede hablar de cualquier información, debemos asegurarnos de revelar lo menos posible aunque en la mayoría de los casos, la identidad personal no es relevante.

“Cuando mi identidad es revelada por el mecanismo subyacente de la transacción, no tengo privacidad. Y aquí no puedo revelarme selectivamente; Siempre debo revelarme. Por lo tanto, la privacidad en una sociedad abierta requiere sistemas de transacciones anónimos. Hasta ahora, el efectivo ha sido el principal sistema de

este tipo. Un sistema de transacciones anónimo no es un sistema de transacciones secretas. Un sistema anónimo permite a las personas revelar su identidad cuando lo deseen y solo cuando sea deseado; esta es la esencia de la privacidad ". (E. Hughes).

Kron es una moneda de plataforma construida sobre el modelo UTXO de Bitcoin. Modificar el código de Bitcoin para agregar estas capacidades no es práctico, pero Kron es una plataforma construida a partir de una bifurcación del código de Bitcoin. Kron agregará activos, recompensas, activos únicos, mensajes y votaciones.

El proyecto Kron también puede servir como base y punto de partida para proyectos, soluciones de segunda capa, experimentos e ideas de negocios que podrían beneficiarse de Kron con ajustes o las características adicionales nativas agregadas a la cadena de bloques Kron.

Modelo UTXO, un concepto para evitar el doble gasto

Una transacción está compuesta de entradas y salidas. El conjunto de entradas y salidas, junto a monedas a enviar y firmas criptográficas, dan como resultado un hash de transacción, normalmente llamado HASH ID. Las entradas son HASH ID de una transacción que recibió el monedero y que no han sido usadas previamente, es decir que son UTXO, mientras que la salida es la dirección de destino, a la cual se le crearán UTXO que posteriormente podrá usar en una transacción. Una misma dirección puede tener infinitas UTXO. Es por esto que a las UTXO se las define como un conjunto de transacciones.

Cuando una persona necesita enviar una transacción, ésta ha de nutrirse de UTXO. Es decir, de transacciones que ha recibido y que no han sido gastadas. Esto significa que una persona puede usar para una misma transacción una o más UTXO. De hecho esos UTXO pueden formar parte de una o más direcciones de tu monedero.

Y vamos más allá, incluso una transacción podría ser creada con UTXO de direcciones de diferentes monederos, siempre que se firme cada una con su correspondiente clave privada claro. Todo esto lleva a un lugar: una UTXO solo puede ser usada una vez. Y esto es fundamental dentro del funcionamiento de la tecnología blockchain, pues es parte del conjunto de herramientas que garantiza que unas monedas no sean usadas más de una vez (el famoso doble gasto).

Es tal la fiabilidad de usar este mecanismo para identificar las monedas no gastadas que esta es la forma en la que en Kron puede contarse cuántas monedas existen en circulación. Lo que se hace es sumar todos las monedas que hay en las UTXO, es decir, en las transacciones que no han sido gastadas.

A continuación un ejemplo sencillo:

“María quiere pagar a Pedro un total de $100 en Kron por un trabajo. María espera recibir el pago de algunas personas que le deben Kron y de ese dinero pagará por el trabajo de Pedro. Al recibir María esos pagos, ella ha tenido unas “Entradas” de dinero, y de esas entradas hará una “Salida” para pagar a Pedro. A María le pagaron las deudas, las cuales eran un pago de $75y otro de $50”.

Cuando pague a Pedro, María tiene que usar las dos entradas, dado que con ninguna de ellas tiene suficiente, y pondrá a Pedro como salida. Tras eso, Pedro tendrá una entrada UTXO (ha recibido el pago).

¿Dónde van las monedas que sobran?

Como has podido observar María tenía un total de $125 repartido en dos UTXO, pero solo necesitaba mandar $100. Ha tenido que utilizar las dos UTXO, poniendo como Output o salida la dirección de Pedro, pero su monedero habrá hecho otra cosa de forma transparente a María. Su monedero habrá puesto una dirección de María también como salida, a la que le habrá asignado los $25 restantes. Es lo que se conoce como dirección de cambio.

Por cierto, existen unas transacciones que se convierten en una UTXO pero no vienen generadas por una UTXO previa. Con lo descrito anteriormente se puede entender cómo este modelo de "**Entradas"** y "**Salidas"**, puede servir para establecer relaciones de posesión y concesión del dinero. Unas relaciones que en blockchain están marcadas por el uso de criptografía y que brindan la seguridad absoluta de que el dinero ha llegado a destino y que está efectivamente bajo el control del destinatario.

UTXO y su importancia en Kron

En Kron todas las transacciones tienen esta estructura de entradas y salidas. En las "Entradas" de una transacción Kron, se puede ver los orígenes del saldo que se manejan con el monedero. Mientras que en las "Salidas", se puede ver hacía donde enviamos nuestro dinero. Adicional a esto, también se puede ver el dinero restante que es devuelto. Todo ello es visible y trazable por cualquier persona, ya que la blockchain de Kron es pública y transparente.

Este modelo permite tener un control total en la forma en como se puede usar el dinero y en qué condiciones se puede usar. En primer lugar, para poder usar un saldo en Kron ese saldo debe estar considerado como una UTXO dentro del monedero. Es decir, alguien debe realizarse un pago (una salida o UTXO) para que este pago se transforme entrada y así tener saldo disponible que gastar.

Este es un proceso es recursivo. Es decir, se repite desde el momento en que la moneda es generada como resultado de un bloque minado. Por ejemplo, una transacción coinbase es en realidad una UTXO creada por el minero para enviar ese saldo a una dirección bajo su control. Así esa transacción de salida se convierte en una entrada de dinero para el minero que posteriormente podrá gastar. El mismo proceso se repite para el resto de usuarios de Kron. Con esto se puede ver que las UTXO son parte esencial de las transacciones de Kron y sin ellas, su funcionamiento sería imposible.

Ampliando el ejemplo de cómo funciona una UTXO en Kron

Se puede ver el funcionamiento de una UTXO en Kron de la siguiente forma: Daniel quiere pagar por el coche de Luis, valorado en 1000 Kron, y en su monedero tiene disponible un total de 1500 Kron. El saldo de Daniel está dividido en dos direcciones la A con 800 Kron y la B con 700 Kron.

Así, Daniel va donde Luis y realiza el pago por 1000 Kron. En este punto, el monedero de Daniel no puede enviar 1000 Kron de forma directa porque el saldo está dividido en dos direcciones. Así que toma ambos saldos y los convierte en las entradas de la transacción de pago. Seguidamente toma la dirección de Luis y asigna a la misma el envío de 1000 Kron, adicional asigna un total de 499,5 Kron a la dirección de cambio, y el resto queda como la comisión de minería.

Una vez que Daniel envíe su transacción, esta será procesada y confirmada por la red, comenzando su camino a la irreversibilidad. Y en este punto, será fácil ver dónde están las UTXO de la transacción.Las primeras UTXO que se puede detectar en el ejemplo son los saldos de Daniel. Esas direcciones con 800 Kron y 700 Kron de saldo, son dos UTXO que están bajo su control y son las que les permiten hacer el pago a Luis. Como Daniel tiene el control de esos saldos, él puede transformar sus UTXO en “Entradas” para un nuevo pago como efectivamente lo hace en este ejemplo.

Inmediatamente después de que la red confirma la transacción de Daniel la situación cambia. Ahora, Daniel ya no tiene bajo su control los saldos que tenía en principio, y en su lugar, su transacción ha generado nuevas UTXO que sobrescriben las anteriores. Las nuevas UTXO en cuestión están representadas primero, por la dirección de Luis y los 1000 Kron que ha recibido en ella de parte de Daniel. Y segundo, por la dirección de cambio y los 499,5 Kron que Daniel ha recibido de la red, porque es lo que le resta del pago que realizó. El resto para completar el 1500 Kron que tenía Daniel en principio quedan como pago de comisión para el minero.

Kron Scripts y su relación con las UTXO

Todo el funcionamiento de las UTXO en Kron está garantizado por los **Kron Script**, el lenguaje de programación que se usa para escribir todas las operaciones en Kron. Cada transacción tiene un script asociado que nos permite:

1. Validar que realmente el saldo usado es nuestro.
2. Garantizar que los saldos enviados solo puedan ser gastados por la persona a quien se lo enviamos.

Validando el saldo

La primera tarea para poder usar un saldo en Kron es demostrar que efectivamente ese saldo es nuestro. Para ello, lo primero a tener en cuenta es que cada UTXO que se transforma en una entrada (saldo a gastar) en realidad es la salida de una transacción anterior que dio acceso a esos Kron. Es decir, todo saldo en Kron tiene una UTXO asociada al mismo, y dicho UTXO tiene asociado un script de bloqueo.

Este script de bloqueo es un candado digital que se debe abrir para entonces poder hacer uso del saldo de dicha UTXO. Los script de bloqueo en Kron son variados, pero el más común es el **P2PKH (Pay to Public Key Hash)**. Aunque también existen el **P2SH (multisig)**, el **P2PK** (el más primitivo de todos). Este script de bloqueo podrá ser abierto con la clave privada que dé como resultado la dirección indicada en la UTXO.

Así que para poder desbloquear dicho script lo que se debe es tomar la dirección de Kron, tomar nuestra clave privada y generar la clave pública de dicha dirección. Al final se estampa la firma digital y con todos esos datos verificados, se desbloquea el saldo de dicha dirección para que se pueda usar. Es decir, los nodos aceptarán la transacción y la pondrán en el mempool a espera del siguiente bloque.

Por el contrario, si se falla al hacer ese procedimiento, simplemente la transacción es rechazada por los nodos y no se puede usar el saldo. A este proceso se llama script de desbloqueo. Por supuesto, este proceso criptográfico es automático y transparente para los usuarios de un monedero, todo el proceso lo realiza el propio monedero.

Creando el script de bloqueo

Al demostrar que se puede gastar UTXO, sigue con el proceso de creación de la transacción, creando un script de bloqueo para la nueva UTXO dirigida a destino. En este caso, lo que hace el monedero es crear un script similar al que nos crearon a nosotros previamente, el cual indique que el único que puede gastar esta nueva UTXO es quien tenga en su poder las claves privadas con controlen las direcciones a donde hemos enviado.

De esta forma, lo que se crea es una cadena de validación, donde los Kron al pasar de una dirección a otra, quedan bloqueados para ser utilizados por la última persona que toma posesión de ellos.

El modelo UTXO ¿Está presente en todas las criptomonedas?

No, El modelo de las UTXO tal como está planteado en Kron no está presente en todas las criptomonedas. Un ejemplo de esto es Monero. En esta moneda, su protocolo de privacidad y anónimato hace este modelo imposible de funcionar. En su lugar, los creadores de Monero hallaron una solución criptográfica que permite ocultar la información de gasto y saldos de monedas (UTXO) y al mismo tiempo controlar el uso indebido de transacciones para realizar operaciones indebidas como el doble gasto, entre otros problemas de privacidad y anónimato.

Transacciones que no vienen de un UTXO

Existen unas transacciones especiales, unas que no se generan con unos UTXO, pues las monedas aparecen “mágicamente”. Este particular caso se da en las transacciones coinbase, que son creadas en el momento de minar un bloque y sirven para obtener la recompensa del bloque.

Conclusión

Kron es una cadena de bloques dirigida a la creación de una transferencia de activos (***kr10, kr12, kr17, kr18, kr5, kr23, kr117***). Es un fork de Bitcoin y como tal utiliza el modelo UTXO de Bitcoin. Kron es una criptomoneda que toma su caso de uso principal como la tokenización segura y la transferencia de activos del mundo real en la cadena de bloques.

Tiene la capacidad de reconocer activos, y diferenciarlos entre ellos en transacciones normales. El Blockchain también tiene la capacidad de enviar mensajes entre usuarios, lo cual hace fácil dictar y organizar contratos y acuerdos.

Básicamente, Kron permite crear y comercializar cualquier activo del mundo real (por ejemplo, lingotes de oro, títulos de propiedad) y activos digitales (por ejemplo, artículos de juego, licencias de software) en una red.

No se requieren Smart Contracts, ya que la cadena principal está diseñada para ejecutar sus funciones principales de forma nativa, y no se necesitan transacciones de criptomoneda reales para mover los activos.

Los derechos de nomenclatura en la cadena de bloques se analizan por orden de llegada y son títulos totalmente únicos que no se pueden replicar.

Kron es la moneda nativa de la su Blockchain. Como en la mayoría de las blockchains, sirve como incentivo y se utiliza para pagar las tarifas de la red y para recompensar el trabajo de los desarrolladores y de los servidores principales.