uPlexa

Incentivando la potencia informática masiva de los dispositivos IoT para formar un medio de pago anónimo basado en la cadena de bloques basada en el navegador.

El Descargo de Responsabilidad:

Está viendo una versión del documento técnico a partir del 27 de noviembre de 2018. Es posible que se realicen cambios en los modelos comerciales, técnicos y legales en el futuro. Consulte el sitio web de uPlexa para obtener la última versión de este documento técnico.

Table of Contents

Introducción y Visión

uPlexa es un sistema de pago electrónico p2p enfocado en aprovechar el poder de IoT y el anonimato. Construido en su propia cadena de bloques que utiliza una versión modificada del algoritmo CryptoNight, uPlexa se desarrolló para vincular el poder colectivo de los dispositivos IoT (Internet de las cosas) en su conjunto, al tiempo que admite pagos basados en el anonimato, especialmente para proveedores de servicios de Internet y telecomunicaciones. Mientras que también apoya el comercio electrónico basado anónimo. Hay más de 9 mil millones de dispositivos IoT en el mundo en 2018, con una expectativa de más de 20 mil millones para 2020.uPlexa es un sistema de pago electrónico p2p enfocado en aprovechar el poder de IoT y el anonimato. Construido en su propia cadena de bloques que utiliza una versión modificada del algoritmo CryptoNight, uPlexa se desarrolló para vincular el poder colectivo de los dispositivos IoT (Internet de las cosas) en su conjunto, al tiempo que admite pagos basados en el anonimato, especialmente para proveedores de servicios de Internet y telecomunicaciones. Mientras que también apoya el comercio electrónico basado anónimo. Hay más de 9 mil millones de dispositivos IoT en el mundo en 2018, con una expectativa de más de 20 mil millones para 2020.

Al igual que Bitcoin, uPlexa es un sistema de pago electrónico peer-to-peer (p2p). Sin embargo, uPlexa también admite pagos anónimos y minería de transacciones IoT rentable. UPlexa ASIC no solo es resistente, sino que también aspira a ser la moneda más rentable para los usuarios con dispositivos IoT que utilizan un porcentaje específico de recursos no utilizados. La cadena de bloques de uPlexa será accesible y se podrá acceder directamente a través de la web, sin necesidad de descargar ningún recurso externo. Sin embargo, las aplicaciones descargables también estarán disponibles.

En diciembre de 2017, vimos la mayor adopción de cualquier criptomoneda, Bitcoin. En este momento, Bitcoin no estaba preparado para ser adoptado por una base tan amplia de usuarios, lo que provocó una gran congestión de la red, lo que resultó en tiempos de transacción más bajos y grandes tarifas. uPlexa planea con anticipación resolviendo estos problemas utilizando nuestro Modelo de Congestión Casi Cero (NZCM). El NZCM consiste en un poderoso avance a través del aprovechamiento de la potencia de los dispositivos de IoT, al tiempo que reduce los micropagos al tener el aumento de la tarifa para los micropagos a medida que aumentan las transacciones de la red. Cualquier pago que no se considere un micropago siempre tendrá tarifas relativamente bajas. NZCM también utilizará la API de uPlexa para utilizar transacciones fuera de la cadena para usuarios avanzados de uPlexa. Estas son sólo unas pocas capas sencillas de la NZCM. Para leer más, lea acerca de NZCM en la página 6.

El anonimato y la privacidad se encuentran entre uno de los mayores debates dentro del campo de la criptomoneda. uPlexa utiliza el algoritmo

CryptoNight para garantizar transacciones privadas no rastreables. Con uPlexa, nuestros objetivos son llevar el anonimato a los pagos de proveedores de servicios de telecomunicaciones e Internet, así como al comercio electrónico. Esto se logrará mediante la negociación de acuerdos con proveedores de TI y telecomunicaciones, así como con el lanzamiento de nuestra propia plataforma de comercio electrónico; respaldar transacciones anónimas, propietarios de tiendas anónimas y desaprobar el almacenamiento y la venta de información personal para fines de marketing y otros fines.

Cómo Funciona – Modelo IoT (funcionalidad Core)

uPlexa utiliza una versión modificada del algoritmo CryptoNight para proporcionar seguridad incuestionable y pagos anónimos. Después de auditar el algoritmo predeterminado de CryptoNight para nuestros propósitos, pronto nos dimos cuenta de que la extracción de dispositivos IoT fuera del algoritmo predeterminado de CryptoNight no es directamente viable ni rentable. Las modificaciones hechas al algoritmo son para hacer que la minería de IoT sea más rentable. A diferencia de otros sistemas de pago, la red troncal de nuestra red estará alimentada por los miles de millones de dispositivos IoT que existen en el mundo.

Nuestro objetivo principal es generar una cantidad rentable de uPlexa para ayudar a pagar la electricidad al ejecutar cualquier dispositivo IoT dado extrayendo una proporción de los recursos inactivos en cualquier dispositivo IoT dado. Esto puede no parecer mucho en los países desarrollados. Sin embargo, en los países en desarrollo, donde se construyen la mayoría de los dispositivos de IoT, también son más asequibles de comprar. Por ejemplo, las personas en el sudeste asiático y otras regiones tienen Smart TV, Smart Refrigeradores, Smart Cars y múltiples dispositivos móviles. Si pudieran obtener ganancias suficientes como mínimo para pagar una parte del costo de su administración, estarían en una situación mucho mejor, ya que los costos mensuales de electricidad pueden costar hasta el 20% de sus ingresos.

Planeamos dar soporte a la mayoría, si no a todos los dispositivos de IoT, desarrollando software específicamente para cada dispositivo para explotar uPlexa con un porcentaje de una CPU inactiva para dispositivos. La cantidad puede ser ajustada opcionalmente por el usuario, y tendremos límites para evitar el uso excesivo de un dispositivo IoT de usuarios. Los dispositivos que vamos a soportar son:

- Computadoras
- Teléfonos móviles y tabletas
- Televisores inteligentes
- Electrodomésticos de cocina inteligentes (Frigoríficos, hornos, cafeteras, gamas, etc)

- Autos inteligentes
- Raspberry Pi's
- Servidores (Los centros de datos y granjas de servidores)
- Otros

Cómo Funciona – Cuotas & modelo de congestión cercana a cero (NZCM)

Con el fin de eliminar la gran congestión de la red y mantener tarifas extremadamente bajas, hemos decidido crear un modelo conocido como Modelo de Congestión Cercana a Cero (NZCM) en el cual hay varias capas:

- Aprovechar el poder de la adopción masiva de IoT
- Utilización de la API NZCM de uPlexa para transacciones fuera de la cadena
- Desaprobación de microtransacciones extremadamente pequeñas.
- Fee Tarifa de escalamiento a tasas más altas para microtransacciones

Con la enorme cantidad de dispositivos de IoT existentes y la adopción continua de IoT, no tenemos ninguna duda de que obtendremos una cantidad sustancial de soporte de red para alimentar nuestra cadena de bloques. Sin embargo, otro aspecto positivo es que para los principales casos de uso de uPlexa, el uso de la API NZCM resultará en que no tenga que usar la cadena de bloques real para una gran parte de las transacciones.

La API de NZCM permitirá a los webmasters, desarrolladores de aplicaciones y organizaciones acreditar a sus usuarios en uPlexa, mientras que sus usuarios eligen buscar un servicio, aplicación o negocio específico. Cuando un usuario opta por buscar una organización específica utilizando la API de NZCM, la organización actúa como un grupo de minería. Los mineros están minando en una billetera singular, como una tienda de comercio electrónico en línea. Todas las monedas acuñadas se envían a la organización en lugar de a los mineros individuales. El uPlexa se acredita al usuario individual en su plataforma a través de nuestra API, en lugar de hacerlo en la propia cadena de bloques. Por lo tanto, cuando un usuario gasta su uPlexa extraído en la plataforma de las organizaciones, una transacción no necesita ser empujada a través de la cadena de bloques. Más bien, la transacción se procesa a través de la base de datos de la organización.

El caso de uso de uPlexa es principalmente para pagos anónimos tanto para proveedores de internet como de telecomunicaciones, así como para comercio electrónico. Por lo tanto, las micro-transacciones no son una prioridad importante. DEBEMOS centrarnos en una red de rayos CryptoNight en el futuro para soportar uPlexa y otras micro-transacciones de CryptoNight. Sin embargo, como uPlexa no admite directamente las micro-transacciones, habrá un límite mínimo sobre la cantidad de uPlexa que se puede enviar (no menos de 1 uPlexa).

Esta cantidad se puede cambiar en cualquier momento mediante un bifurcación debido al valor de uPlexa. Para micro-transacciones bajo 5 uPlexa, habrá una tarifa de escalado. Por lo tanto, si está enviando menos de 5 uPlexa cuando la red se está inundando de micropagos, la tarifa de estas micro-transacciones aumentará 2 veces más que cualquier pago estándar. La idea detrás de esto, es negar los ataques de red y disminuir el uso de micropagos con uPlexa. uPlexa no es, sin embargo, una criptomoneda que se enfoca en micro-transacciones (<$0.15 USD)

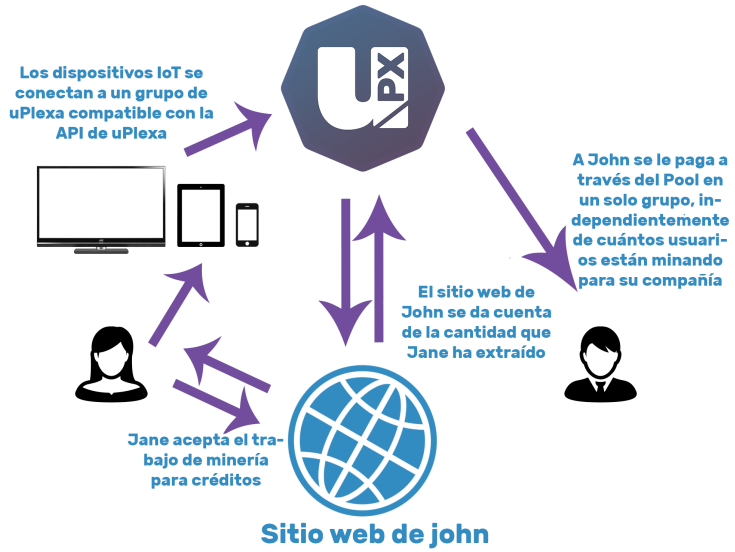
uPlexa NZCM API

La API de uPlexa se puede usar para ayudar a proporcionar menos congestión de red al usar menos transacciones en la cadena, lo que reduce las tarifas para compañías y proyectos.

Cómo Funciona

Si el propietario de johnswebsite.com desea proporcionar un sistema de crédito a sus usuarios para que puedan comprar bienes, servicios o hacer donaciones. Puede pedir a sus usuarios que conecten sus dispositivos IoT a su sitio web en línea para extraer monedas de uPlexa. A cambio, los usuarios serán recompensados con créditos en el sitio utilizando la API de uPlexa. Una vez que los usuarios obtienen suficientes JohnCredits, el usuario puede hacer una compra o usar algunos de los créditos para obtener un descuento en el sitio web de John.

La minería durante este proceso se envía a una billetera, la billetera de John. Sin embargo, cada usuario individual y la cantidad de hashes que han resuelto se rastrean a través de la API de uPlexa. Así, cuando la usuaria Jane, desea realizar una compra; la cantidad se deduce del saldo de los usuarios a través de la API en lugar de realizar una transacción por separado de su billetera a la billetera de John.



Presentando el comercio electrónico

La industria del comercio electrónico representa más de $ 2.3 trillones de dólares de los ingresos mundiales, con estimaciones de más de $ 4.88 trillones de dólares para 2021. Fuente: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

El equipo de uPlexa presentará su propia plataforma de comercio electrónico basada en el apoyo masivo de múltiples criptomonedas, fiat y también utilizando uPlexa como una puerta de enlace privada, segura y anónima para los webmasters y sus clientes. No habrá KYC para nuestros webmasters, y se pagarán de forma anónima a través de uPlexa. Otras cosas como desarrolladores, complementos y diseños también estarán disponibles en el mercado de comercio electrónico para que los webmasters compren con uPlexa para su propia tienda.

El sistema uPlexa eCommerce no cobrará a los usuarios hasta que dicho usuario esté ejecutando una tienda rentable. Lo que significa que la tienda es GRATUITA hasta que empieces a ganar un mínimo de 3 veces la tarifa mensual de la tienda, que será de alrededor de $ 29 USD / mes para las tiendas básicas. Los pagos se realizarán diariamente si supera una cantidad de> $ 29 USD. De lo contrario, los pagos serán quincenales.

Nuestro equipo ha trabajado anteriormente en la industria del comercio electrónico, desde BigCommerce hasta Wordpress (WooCommerce) y Shopify. Nos centraremos en hacer una personalización y una experiencia de comercio electrónico anónima para superar a otros sistemas de comercio electrónico existentes escuchando las sugerencias de los clientes y las quejas que estas empresas han ignorado por siempre. Personalmente hemos tenido muchas ideas para impulsar la conversión de dichos sistemas en los cuales los sistemas no eran capaces de realizar modificaciones importantes. Algunos de los cuales están actualmente en producción para tiendas en vivo.

Dicho esto, el enfoque prioritario de uPlexa con respecto al comercio electrónico será tanto las criptomonedas como las mayores conversiones para nuestros clientes.

Sistema de pago anónimo

uPlexa finalmente cerrará la conexión entre los pagos anónimos y los proveedores de servicios. Esto se logrará al hacer varias asociaciones con nuevas empresas en desarrollo que permitirán a los usuarios pagar sus servicios sin KYC y utilizar uPlexa como un método de pago opcional.

¿Por qué los pagos de servicio deben ser anónimos?

- El anonimato brinda protección contra programas espía con el único propósito de robar su información privada
- Ayuda a protegerlo de la venta de sus datos para fines de marketing u otros fines
- Pague servicios en otros países cuando viaje sin tener que pagar tarifas de "turista", ya que uPlexa es una moneda global y no saben quién es usted
- Evite que otras compañías sepan a quién está pagando, o qué compañía está adquiriendo
- Mantenga en secreto a sus proveedores de negocios.
- Escapar de la represión gubernamental y las prohibiciones de servicio
- Evite el chantaje de los ISP o empleados que espían sus datos
- Pague los servicios de los miembros de la familia con su propia cuenta
- Los piratas informáticos no podrán rastrear un número de teléfono a su nombre, o secuestrar su acceso móvil con sus datos personales para obtener más acceso a sus cuentas en línea

Las funciones anónimas de uPlexa van mucho más allá de la base de código, a los reinos de las grandes corporaciones, y las políticas con respecto a KYC y el anonimato. Los desafíos más difíciles serán encontrar compañías y socios dispuestos a brindar una opción segura y anónima a sus sistemas y servicios. Por lo tanto, tendremos un fuerte enfoque en las alianzas estratégicas, al tiempo que recompensaremos las recompensas para aquellos que ayudan a uPlexa a alcanzar su verdadero potencial.

Viabilidad y rentabilidad de IoT

uPlexa entregará minería a una variedad de dispositivos IoT, desde teléfonos inteligentes y tabletas hasta televisores inteligentes e incluso autos inteligentes. Esto se logra mediante la ejecución de nuestro software de minería. El software de minería uPlexa utiliza un conjunto específico de fallos para evitar que dichos dispositivos se sobrecalienten y se vuelvan menos receptivos al usar solo una parte específica de los recursos inactivos de los dispositivos. En nuestras pruebas, el software de minería uPlexa requiere menos CPU que las aplicaciones de uso común, como la cámara de sus teléfonos, Facebook y Netflix.

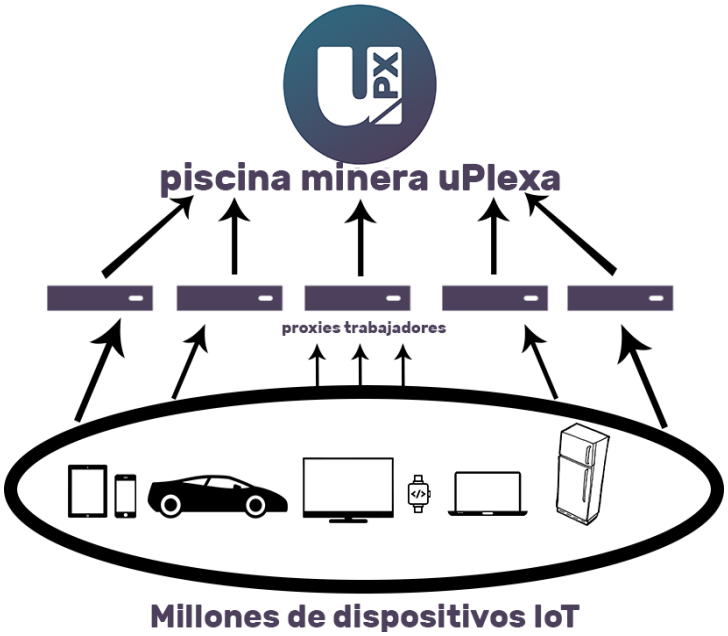
Las Matemáticas

Teléfono inteligente estándar: 28H/s al máximo o 10H/s al 35% de uso de CPU
Portátil estándar en torno a 45H/s al máximo o 16H/s al 35% de uso de CPU

Usando el 35% de la CPU proporciona un promedio de hashrate de 13H/s. Si Alice tiene 15 dispositivos; Ella tiene 13 * 15 = 195H/s.

La tecnología que hace esto posible y liviano es un grupo de CryptoNight bifurcado combinado con un protocolo de proxy avanzado para disminuir las conexiones al grupo. Con nuestro software, podemos aceptar más de dos millones

de conexiones simultáneas en cinco instancias de Amazon m5.2xlarge como proxies y dos instancias de Amazon m4.16xlarge (una para el grupo, una para la validación de recursos compartidos y el equilibrio de la carga de trabajo).



Rentabilidad del Minero

La rentabilidad implica nuestra versión modificada del protocolo CryptoNight para proporcionar la forma más rentable y anónima de minería de IoT. El protocolo CryptoNight es bastante resistente al ASIC. Sin embargo, es posible que se requieran futuras tareas obligatorias que toda la red siga para evitar la minería de ASIC en nuestra plataforma. Dichas horquillas no serán intrusivas ni arriesgadas.

Nuestro objetivo con nuestro algoritmo es equilibrar la GPU con la CPU lo más cerca posible, en términos de costo por dólar para el hardware de minería de los usuarios. La idea detrás de la minería de IoT es tener muchos dispositivos de IoT conectados en todo el mundo para ayudar a minimizar la centralización de la minería mientras se mantiene un flujo constante de ganancias para nuestros mineros para ayudar continuamente a procesar transacciones en la cadena de bloques uPlexa.

Con uPlexa, las personas pueden usar una cadena de bloques que es rentable minar conectándose directamente a uno de los grupos públicos de uPlexa. También pueden elegir conectarse a una compañía o sitio web / grupo de juegos para obtener créditos en esa plataforma.

Explicación técnica - Descripción general de CryptoNight

CryptoNote Algoritmo

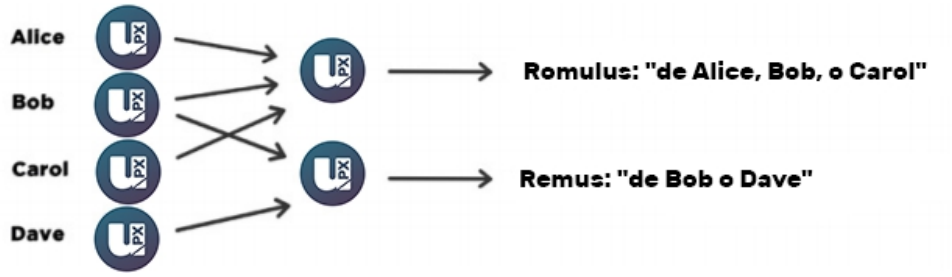
El algoritmo CryptoNote se publica bajo una licencia de código abierto y se ha adoptado e incorporado en uPlexa, ya que forma la base de un núcleo de criptomoneda sólido y bien probado. Es la misma tecnología de blockchain básica que utilizan tanto Monero (una de las 10 mejores criptomonedas) como Bytecoin (una de las mejores 15 criptomonedas).

Pagos no rastreables

El proceso de verificación de firma digital ordinaria (por ejemplo, DSA, Schnorr, etc.) implica la clave pública del firmante.
Es una condición necesaria, porque la firma en realidad prueba que el autor posee la clave secreta correspondiente. Pero no siempre es una condición suficiente.

La firma de anillo es un esquema más sofisticado, que de hecho puede requerir varias claves públicas diferentes para la verificación. En el caso de la firma del anillo, tenemos un grupo de individuos, cada uno con su propia clave secreta y pública. La declaración probada por las firmas de anillo es que el firmante de un mensaje dado es un miembro del grupo. La distinción principal con los esquemas de firma digital ordinarios es que el firmante necesita una única clave secreta, pero un verificador no puede establecer la identidad exacta del firmante. Por lo tanto, si encuentra una firma de anillo con las claves públicas de Alice, Bob y Carol, solo puede reclamar que una de estas personas fue el firmante, pero no podrá ubicarlo.

Este concepto se puede utilizar para hacer que las transacciones digitales enviadas a la red no sean rastreables mediante el uso de las claves públicas de otros miembros en la firma de timbre, uno se aplicará a la transacción. Este enfoque prueba que el creador de la transacción es elegible para gastar la cantidad especificada en la transacción, pero su identidad será indistinguible de los usuarios cuyas claves públicas usó en sus firmas de anillo.



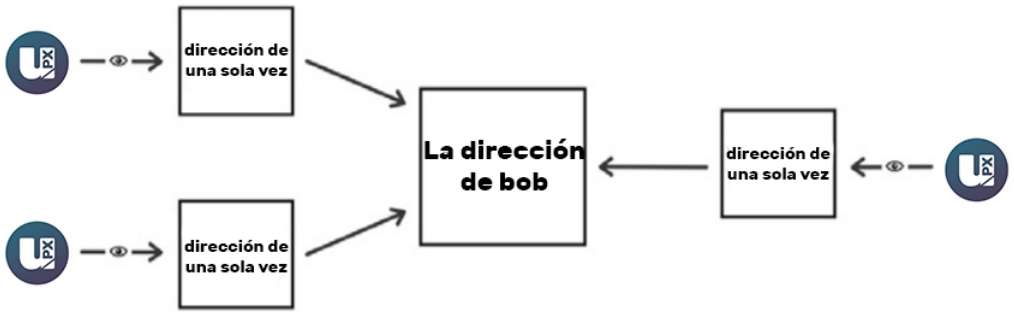
Transacciones no rastreables

Debe tenerse en cuenta que las transacciones en el extranjero no le impiden gastar su propio dinero. Su clave pública puede aparecer en docenas de firmas de anillo de otros, pero solo como un factor de confusión (incluso si ya usó la clave secreta correspondiente para firmar su propia transacción). Además, si dos usuarios crean firmas de anillo con el mismo conjunto de claves públicas, las firmas serán diferentes (a menos que usen la misma clave privada).

Normalmente, cuando publica su dirección pública, cualquier persona puede verificar todas sus transacciones entrantes, incluso si están ocultas detrás de una firma de timbre. Para evitar la vinculación, puede crear cientos de claves y enviarlas a sus pagadores de forma privada, pero eso le priva de la conveniencia de tener una única dirección pública.

CryptoNote de uPlexa resuelve este dilema mediante la creación automática de múltiples claves únicas únicas, derivadas de la clave pública única, para cada pago p2p. La solución radica en una modificación inteligente del protocolo de intercambio Diffie-Hellman. Originalmente, permite que dos partes produzcan una clave secreta común derivada de sus claves públicas. En nuestra versión, el remitente utiliza la dirección pública del destinatario y sus propios datos aleatorios para calcular una clave de una sola vez para el pago.

El remitente puede producir solo la parte pública de la clave, mientras que solo el receptor puede calcular la parte privada; por lo tanto, el receptor es el único que puede liberar los fondos después de que se comprometa la transacción. Solo necesita realizar una comprobación de una sola fórmula en cada transacción para establecer si le pertenece. Este proceso implica su clave privada, por lo que ningún tercero puede realizar esta comprobación y descubrir el vínculo entre la clave de una sola vez generada por el remitente y la dirección pública única del receptor.



Una parte importante de nuestro protocolo es el uso de datos aleatorios por parte del remitente. Siempre resulta en una clave única diferente, incluso si el remitente y el destinatario permanecen iguales para todas las transacciones (es por eso que la clave se llama "una sola vez"). Además, incluso si ambos son la misma persona, todas las claves de un solo uso también serán absolutamente únicas.

Doble gasto es imposible

Las firmas totalmente anónimas permitirían gastar los mismos fondos muchas veces, lo que, por supuesto, es incompatible con los principios de cualquier sistema de pago. El problema se puede solucionar de la siguiente manera.

Una firma de anillo es en realidad una clase de algoritmos criptográficos con diferentes características. La que utiliza uPlexa es la versión modificada de la "firma de anillo rastreable". De hecho, transformamos la trazabilidad en vinculación. Esta propiedad restringe el anonimato de un firmante de la siguiente manera: si crea más de una firma de timbre usando la misma clave privada (el conjunto de claves públicas externas es irrelevante), estas firmas estarán vinculadas entre sí, lo que indica un intento de duplicación de gastos.

Para admitir la capacidad de enlace, CryptoNote de uPlexa introdujo un marcador especial creado por un usuario mientras firmaba, lo que llamamos una imagen clave. Es el valor de una función criptográfica de una sola vía de la clave secreta, por lo que en términos matemáticos es en realidad una imagen de esta clave. Unidireccional significa que, dada la imagen clave, es imposible recuperar la clave privada. Por otro lado, es computacionalmente imposible encontrar una colisión (dos claves privadas diferentes, que tienen la misma imagen). El uso de

cualquier fórmula, excepto la especificada, dará como resultado una firma no verificable. A fin de cuentas, la imagen clave es inevitable, no ambigua y, sin embargo, un marcador anónimo de la clave privada.

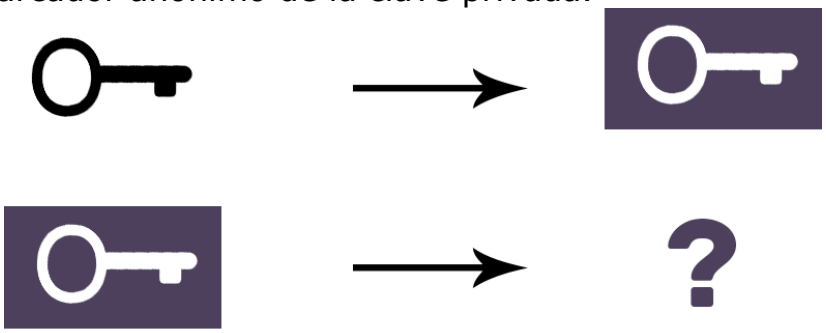
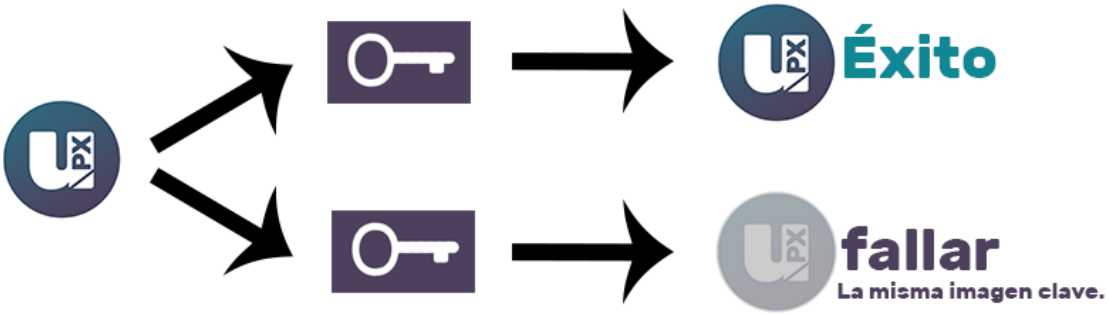


Imagen clave a través de una función unidireccional

Todos los usuarios mantienen la lista de imágenes clave utilizadas (en comparación con el historial de todas las transacciones válidas que requiere una cantidad insignificante de almacenamiento) y rechace inmediatamente cualquier nueva firma de timbre con una imagen de clave duplicada. No identificará al usuario que se comporta mal, pero evita cualquier intento de doble gasto, causado por intenciones malintencionadas o errores de software.

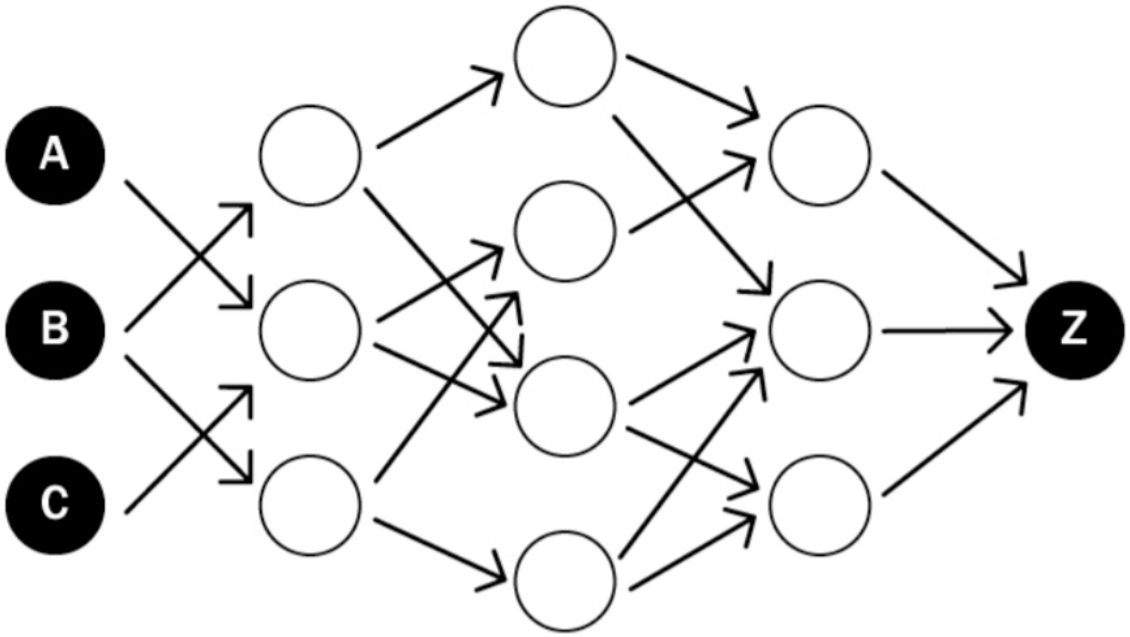


Resistencia al análisis de blockchain

Hay muchos trabajos académicos dedicados al análisis de la cadena de bloques de Bitcoin. Sus autores rastrean el flujo de dinero, identifican a los propietarios de monedas, determinan los saldos de billetera y así sucesivamente. La capacidad de realizar dicho análisis se debe a que todas las transferencias entre direcciones son transparentes: cada entrada en una transacción se refiere a una salida única. Además, los usuarios a menudo reutilizan sus antiguas direcciones, recibiendo y enviando monedas de ellos muchas veces, lo que simplifica el trabajo del analista. Ocurre involuntariamente: si tiene una dirección pública (por ejemplo, para donaciones), está seguro de usar esta dirección en muchas entradas y transacciones.

CryptoNote de uPlexa está diseñado para mitigar los riesgos asociados con la reutilización de claves y el seguimiento de una entrada a una salida. Cada dirección para un pago es una clave única y única, derivada de los datos del remitente y del destinatario. Puede aparecer dos veces con una probabilidad de colisión de hash de 256 bits. Tan pronto como utiliza una firma de timbre en su entrada, se genera la incertidumbre: ¿qué salida se ha gastado recientemente?

Al intentar dibujar un gráfico con direcciones en los vértices y las transacciones en los bordes, se obtendrá un árbol: un gráfico sin ciclos (porque no se usó la clave / dirección dos veces). Además, hay miles de millones de gráficos posibles, ya que cada firma de anillo produce ambigüedad. Por lo tanto, no puede estar seguro de a qué remitente llega el borde de la transacción al vértice de la dirección. Dependiendo del tamaño del anillo, adivinarás de "uno de dos" a "uno de cada mil". Cada próxima transacción aumenta la entropía y crea obstáculos adicionales para un analista.



Transacción Estándar de CryptoNote

Se genera una transacción estándar de uPlexa CryptoNote mediante la siguiente secuencia que se describe en este documento técnico.

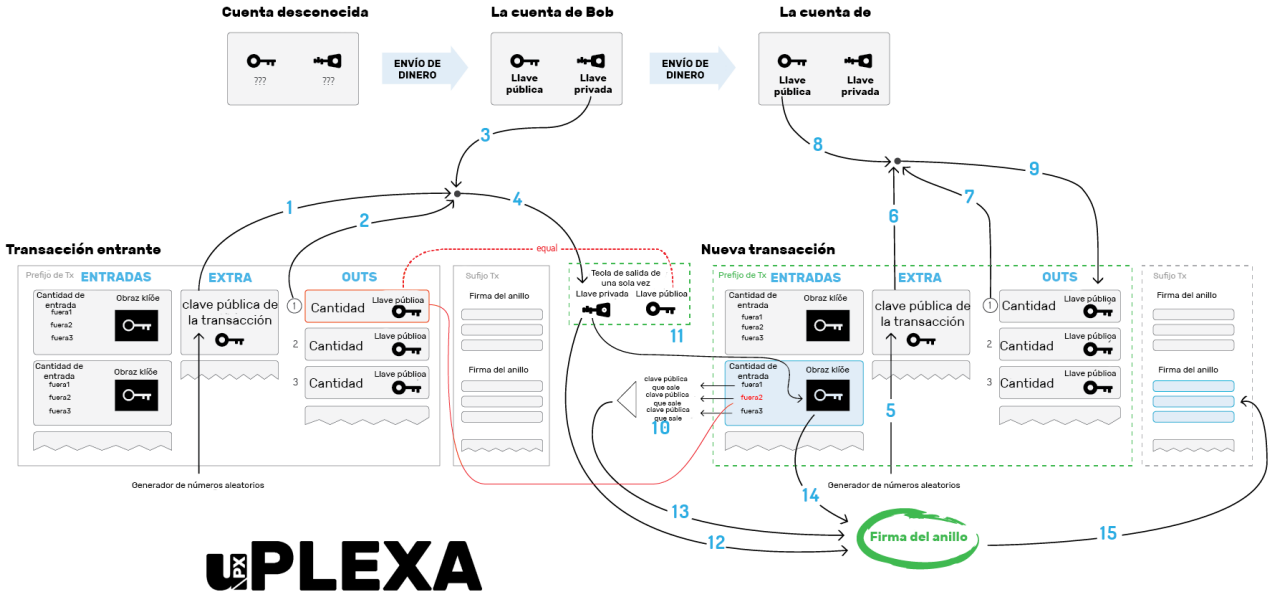
Bob decide gastar una salida, que fue enviada a la clave pública única. Necesita Extra (1), TxOutNumber (2) y su clave privada de Cuenta (3) para recuperar su clave privada de una sola vez (4).

Al enviar una transacción a Carol, Bob genera su valor Extra al azar (5). Utiliza Extra (6), TxOutNumber (7) y la clave pública de cuenta de Carol (8) para obtener su clave pública de salida (9).

En la entrada, Bob oculta el enlace a su salida entre las claves externas (10).

Para evitar el doble gasto, también empaca la imagen de la clave, derivada de su clave privada única (11).

Finalmente, Bob firma la transacción, utilizando su clave privada única (12), todas las claves públicas (13) y la imagen clave (14). Agrega la Firma de anillo resultante al final de la transacción (15).



Límites adaptativos

Un sistema de pago descentralizado no debe depender de las decisiones de una sola persona, incluso si esta persona es un desarrollador central. Las constantes difíciles y los números mágicos en el código impiden la evolución del sistema y, por lo tanto, deben eliminarse (o al menos reducirse al mínimo). Todos los límites cruciales (como el tamaño máximo de bloque o la cantidad de tarifa

mínima) se deben volver a calcular en función del estado anterior del sistema. Por lo tanto, siempre cambia de forma adaptativa e independiente, lo que permite que la red se desarrolle por sí misma.

CryptoNote de uPlexa tiene los siguientes parámetros que se ajustan automáticamente para cada nuevo bloque:

1. Dificultad. La idea general de nuestro algoritmo es sumar todo el trabajo que los nodos han realizado durante los últimos 720 bloques y dividirlo por el tiempo que han dedicado a lograrlo. La medida del trabajo es el valor de dificultad correspondiente para cada uno de los bloques. El tiempo se calcula de la siguiente manera: ordene todas las 720 marcas de tiempo y elimine el 20% de los valores atípicos. El rango de los 600 valores restantes es el tiempo que se gastó en el 80% de los bloques correspondientes.

2. Tamaño máximo del bloque. Sea MN el valor mediano de los últimos N bloques de tamaños. Entonces el "límite duro" para el tamaño de los bloques de aceptación es 2 * MN. Evita la hinchazón de las cadenas de bloques, pero aún así permite que el límite crezca lentamente con el tiempo si es necesario. El tamaño de la transacción no tiene que estar limitado explícitamente. Está limitado por el tamaño del bloque.

Emisión suave

El límite superior para la cantidad total de todas las monedas digitales también es digital:

$$\mathbf{MProvisión = 264 - 1 \text{ unidades atómicas}}$$

Esta es una restricción natural basada solo en los límites de implementación, no en la intuición como "Las monedas N deberían ser suficientes para todos". Para hacer que el proceso de emisión sea más suave, CryptoNote de uPlexa utiliza la siguiente fórmula para recompensas de bloque:

$$\mathbf{RecompensaBase = (MProvisión - A) >> 18}$$

Donde A es la cantidad de monedas generadas previamente. Da un crecimiento predecible de la oferta de dinero sin ningún punto de ruptura.

Conclusión

uPlexa se centra en proporcionar una moneda anónima con utilidad complementaria con pagos de comercio electrónico y proveedores de servicios. Estas utilidades se ubicarán en la parte superior de las capas fundamentales de las transacciones masivas de hashpower y fuera de cadena de IoT.

Referencias

Documento técnico de cryptonote:
https://cryptonote.org/whitepaper.pdf

Cryptonote Inside:
https://cryptonote.org/inside

Documento técnico de Bitcoin:
https://bitcoin.org/bitcoin.pdf

Statistica: Dispositivos Conectados IoT 2015-2025:
https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

PRISM (programa de vigilancia):
https://en.wikipedia.org/wiki/PRISM_(surveillance_program)