Universal Credit System

una moneda criptográfica de nueva generación

¡Bienvenido!

En este documento encontrará todo lo que necesita saber sobre la nueva e innovadora criptomoneda de nueva generación: **el Universal Credit System**. Contiene toda la información que necesita para comprender y confiar en el Universal Credit System.

Este documento es una especie de documento técnico que contiene una especificación precisa de la criptomoneda. Además, los procesos lógicos se presentarán de manera comprensible para todos en este documento.

El Universal Credit Standard

El ***Universal Credit Standard*** es un estándar de criptomoneda digital independiente. La norma permitirá a todos los usuarios participar en el comercio y acumular riqueza. El ***Universal Credit System*** es el software subyacente para administrar la moneda (billetera) y la moneda pagada en este software se llama ***Universal Credit Coins (UCC).***

Sin embargo, el *Universal Credit Standard* y los principios detrás de él son fundamentalmente diferentes en comparación con otras criptomonedas. En lugar de *extraer* nuevos bloques en cualquier forma y obtener una *recompensa*, a todos los participantes simplemente se les *acredita* una cantidad fija de Universal Credit Coins todos los días.

Estas Universal Credit Coins no son acreditadas ni otorgadas por una autoridad central; los participantes se gestionan a sí mismos en base a un algoritmo. Las Universal Credit Coins concedidas tienen una validez indefinida y pueden ser utilizadas para cualquier fin por parte del destinatario.

El pago por día sigue una regla muy sencilla:

1.000000000 UCC por usuario por día

Con esta regla es muy fácil determinar el valor de una cosa, pero también el valor de una moneda de crédito en cualquier momento. Si algo tiene un precio de 200 UCC, en realidad son pagos a 200 días. Y no importa si hoy, dentro de 3 años o incluso dentro de 10 años. 200 monedas son el pago de 200 días.

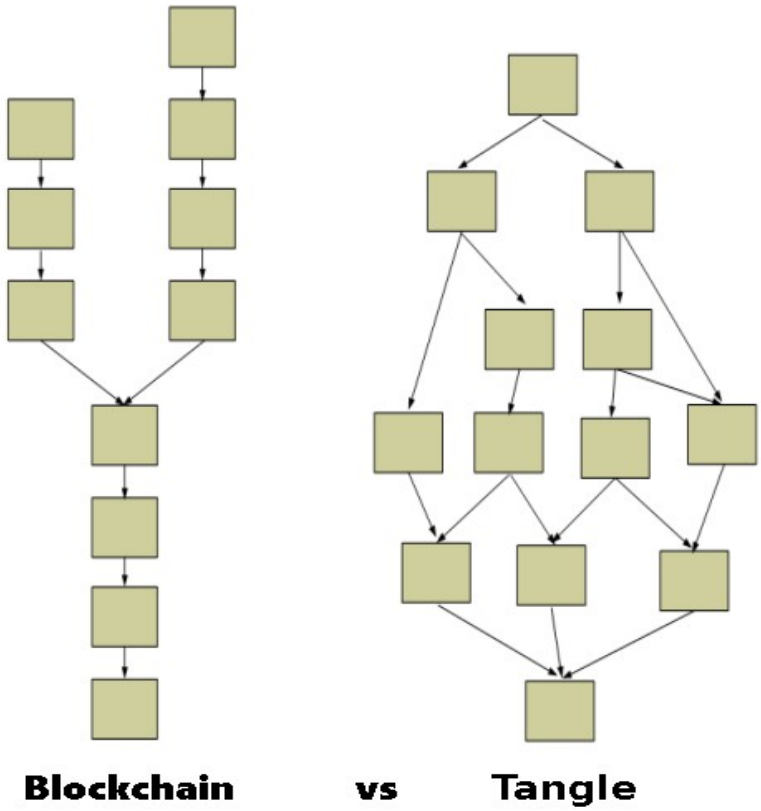
Debido a que el pago/recompensa está ligado al tiempo transcurrido y es consistente, Universal Credit Coins cumple con la definición de moneda estable.

El algoritmo de proof-of-Trust [poT]

Si bien la mayoría de las criptomonedas utilizan algoritmos de *proof-of-work* o *proof-of-stake / delegated-proof-of-stake* para llegar a un consenso, la tecnología utilizada en el Universal Credit System es fundamentalmente diferente. El algoritmo utilizado en la UCS se denomina **algoritmo de proof-of-Trust** y ha sido completamente rediseñado desde cero.

En lugar de construir el consenso a partir de un libro de contabilidad monolítico y central (blockchain) como Bitcoin, la arquitectura del Universal Credit System se basa en un **gráfico acíclico dirigido** (DAG) en el que cada usuario tiene su propia blockchain en el sentido de un autogestionado *blockgrid* (el llamado „true distributed ledger“). Cada bloque de un usuario corresponde a una transacción y los bloques **no están** vinculados entre sí.

La estructura utilizada aquí se puede comparar con la *tangle* de la criptomoneda IOTA. Pero en comparación con IOTA, el consenso común dentro de la red se alcanza de una manera totalmente diferente. El uso de un gráfico acíclico dirigido hace que la criptomoneda sea muy diferente de otras arquitecturas basadas en blockchain:



En cierto sentido, los usuarios en la UCS proporcionan prueba de trabajo (pow) firmando sus propias transacciones y verificando las transacciones de otros usuarios, pero el consenso sobre el saldo de una cuenta se determina solo parcialmente utilizando esta poof-of-work. Las monedas pagadas diariamente, que están determinadas por la fecha de creación certificada, tienen una influencia mucho mayor en el saldo de una cuenta. La fecha de creación certificada y las transacciones firmadas por el usuario, así como las transacciones dirigidas a él, junto con las confirmaciones de otros usuarios, forman la *proof-of-Trust*.

Dado que los participantes se gestionan ellos mismos, no se requiere una conexión permanente a Internet. Cada usuario gestiona su propia versión de blockgrid. Con cada acción, los usuarios se proporcionan mutuamente pruebas de confianza, que demuestran matemáticamente la validez del saldo de su cuenta ante los demás participantes.

Usuarios y la certificación de la fecha de creación por parte del TSA (Time Stamping Authority)

Cada entidad, en adelante denominada "usuario" neutral (un usuario puede ser cualquier cosa), puede crear un par de claves RSA de 4096 bits. El usuario debe revelar inmediatamente la clave pública a una Autoridad de Sellado de Tiempo (TSA) que cumpla con RFC-3161, que actúa como notario independiente y certifica la fecha en que se creó el perfil **dentro de los 120 segundos** posteriores a la fecha de creación.

La TSA certifica al usuario que su clave está disponible en el momento de su creación. Este tiempo de creación certificado sirve como base para calcular el pago diario.

La certificación de un nuevo usuario después de su creación es el único punto en el que se requiere una conexión a Internet. Cualquier otra acción se puede realizar sin estar conectado a internet.

Transacciónes

Un usuario puede crear una transacción que contenga su dirección como remitente, el monto, el destinatario y la marca de tiempo actual y luego firmar esta transacción con su clave privada. Luego, el usuario crea el archivo de transacción, que puede enviar al beneficiario del modo que elija. Para ello no es necesario estar conectado a Internet, el usuario puede utilizar un medio de su elección para intercambiar el archivo de transacción. El destinatario puede verificar la autenticidad de la transacción con la ayuda de la clave pública y verificar la transacción y el crédito asociado con la ayuda de la prueba de confianza.

Estrictamente hablando, el archivo de transacción es un archivo que contiene la clave pública del remitente, la autenticación de la TSA y todas las transacciones enviadas y recibidas previamente por el remitente para procesar la transacción. También contiene todas las claves recopiladas hasta el momento, sus autenticaciones TSA y las transacciones que estaban en posesión del remitente en ese momento. Esto se utiliza para desarrollar un conocimiento común de las transacciones.

Este conocimiento de transacciones comúnmente compartido se utiliza para determinar las dependencias de las transacciones y poder verificar los saldos asociados. Esto es particularmente importante para determinar saldos, ya que un usuario puede haber dependido de una transacción que se le envió.

A continuación se muestra un ejemplo de una transacción que depende de otras transacciones:

Saldo del usuario A	Transacción
0	
100	+100 otorgado por el sistema
200	+100 recibido del usuario B
50	-150 Enviado al usuario C

Como puede ver, el *Usuario A* solo pudo enviar la transacción de 150 Credit Coins porque previamente había recibido 100 Credit Coins del *Usuario B*. Esta última transacción (150 Credit Coins) depende de una transacción anterior. Estas dependencias se pueden determinar y verificar mediante proof-of-trusts recopiladas de otros usuarios.

Transacciones y Confirmaciones

Si una transacción es plausible, siempre será inmediatamente válida para el remitente. Entonces, si una transacción se creó exitosamente, el saldo de la cuenta del remitente se reduce inmediatamente. A cambio, el saldo de la cuenta del destinatario sólo aumenta si ha recogido el número necesario de confirmaciones de otros usuarios. A través de la sincronización y transacciones futuras, el conocimiento sobre esta transacción se difunde y otros usuarios la confirman/autentican.

Una transacción requiere una cierta cantidad de confirmaciones de otros usuarios para poder ser reconocida en el futuro por usuarios que previamente no estaban involucrados en una transacción. El problema es particularmente importante al comprobar pagos dependientes, ya que el pago del que depende el remitente puede no tener suficientes confirmaciones para ser considerado válido todavía. Pero también se pueden identificar los llamados *stale blocks* que se producen cuando alguien intenta gastar el doble.

Para que una transacción se tenga en cuenta al calcular el saldo de una cuenta, debe ser confirmada **por al menos 2 usuarios** para que sea lo más definitiva posible y el remitente ya no pueda negar esta transacción en el futuro ("double spend" y ataques "0 race").

El proceso de cambiar el estado de un pago (de pendiente a válido y final) es un proceso que nunca termina. Por lo tanto, una transacción nunca es totalmente definitiva, pero se vuelve cada vez más definitiva. En algún momento, hay suficiente confirmación de que puede considerarse válido.

Los reconocimientos de los demás usuarios sobre la existencia de una transacción se denomina **confirmación**. Depende del número de confirmaciones de una transacción si ésta puede considerarse válida. Una transacción se considera válida por defecto si tiene **al menos 2 confirmaciones de otros usuarios**. La transacción debe ser confirmada por usuarios que no participaron en la transacción (ni como remitente ni como destinatario). Estos usuarios actúan como una especie de notario y certifican/confirman/reconocen esta transacción al incluir el archivo de la transacción en su archivo de índice.

El hecho de que el receptor de 1 transacción necesite al menos 2 confirmaciones para procesarla garantiza la difusión exponencial del conocimiento de la transacción.

A continuación puede encontrar una descripción general del número de confirmaciones de una transacción y la validez (según la configuración predeterminada):

Confirmaciones	Validez
0	no válido (pendiente)
1	no válido (pendiente)
2	válido
3	válido
...	...
∞	final

El número actual de *confirmaciones* de una transacción se puede ver en *el historial de transacciones* del Universal Credit System. Para garantizar que todas las transacciones realizadas o recibidas estén suficientemente confirmadas, tiene sentido sincronizar con otros usuarios lo antes posible.

Calificativo

Para evitar que un usuario cree varias cuentas adicionales, se realiza la llamada puntuación del usuario. Esto significa que las transacciones enviadas, las transacciones recibidas y el saldo del usuario se comparan entre sí. El valor de la puntuación de un usuario se calcula según las siguientes 5 reglas:

- Cada día la puntuación de todos los usuarios aumenta por el pago.
- Inmediatamente después de crear una transacción, la puntuación se reduce según el monto de la transacción.
- Si la transacción ha recibido suficientes confirmaciones, la puntuación del remitente aumenta en el importe original.
- La puntuación no puede ser inferior a 0.
- La puntuación no puede ser superior al saldo del usuario.

La puntuación garantiza así que un usuario no pueda acumular un número infinito de créditos de otros usuarios y volver a gastarlos inmediatamente. En cambio, se desbloquean cada vez más créditos con el tiempo. Cuando un usuario no tiene fondos suficientes para comprar algo, es imposible evitarlo creando varias otras cuentas y recolectando los retiros, ya que el usuario no puede enviarlos todos a la vez.

A continuación se muestra un ejemplo sin puntuación:

- cuenta A tiene un saldo de 5 UCC La cuenta A quiere comprar algo por el precio de 10 UCC
- cuenta A crea las cuentas B, C, D, E y espera 1 día para el primer pago
- cuenta A tiene un saldo de 6 UCC al día siguiente, las cuentas B, C, D y E tienen cada una 1 saldo UCC
- las cuentas B, C, D, E envían cada una 1 UCC a la cuenta A y aumentan el saldo de 6 UCC a 10 UCC
- cuenta A ahora tiene un saldo de 10 UCC

En este ejemplo sin puntuación, la cuenta A ahora tiene 10 UCC y podría comprar el artículo.

A continuación se muestra un ejemplo <u>con</u> puntuación:

- cuenta A tiene un saldo de 5 UCC y una puntuación de 5 UCC
- cuenta A quiere comprar algo por el precio de 10 UCC
- cuenta A crea las cuentas B, C, D, E y espera 1 día para el primer pago.
- la cuenta A tiene un saldo de 6 UCC al día siguiente, las cuentas B, C, D y E tienen cada una 1 saldo UCC
- las cuentas B, C, D, E envían cada una 1 UCC a la cuenta A, aumentando el saldo de 6 UCC a 10 UCC
- cuenta A ahora tiene un saldo de 10 UCC, pero solo una puntuación de 6 UCC

A ahora tiene un saldo de 10 UCC, pero debido a la puntuación (el saldo es igual a la puntuación, por lo que la puntuación no se ve afectada), solo 6 UCC (los 5 UCC iniciales + 1 pago UCC después de 1 día) se desbloquean y se pueden gastar. Cuando gastes los 6 UCC, se desbloqueará el resto del crédito. Con la puntuación, un usuario sólo puede gastar los pagos diarios sin límite y debe activar los créditos recibidos. En el ejemplo sin puntuación, la cuenta A puede gastar el monto total en una transacción, mientras que la cuenta A con puntuación no puede gastar el monto completo.

<u>Es muy importante que el monto total se envíe en una sola transacción si no puede confiar en el remitente.</u> Esto garantiza que los atacantes no puedan retirar fondos de un número potencialmente infinito de cuentas que hayan creado. Este proceso de evaluación basado en puntuaciones lo protegerá a usted y a todos los demás participantes de usuarios fraudulentos.

Determinación del saldo de la cuenta

El saldo de una cuenta lo determinan los propios usuarios, que se controlan entre sí una y otra vez.

Para determinar el saldo de la cuenta de un usuario, primero se calcula *la creditload* para este primer día a partir de la fecha de creación certificada de la clave y luego se restan o suman las transacciones enviadas o recibidas. El resultado es el saldo de la cuenta al final de este día y sirve como saldo de la cuenta para el día siguiente, al cual primero se suma nuevamente la *creditload* y luego se restan o se suman nuevamente las transacciones salientes o entrantes.

Este cálculo continúa día a día hasta el día actual, por lo que el saldo de la cuenta nunca debe caer por debajo del límite de saldo 0. El Universal Credit System está programado de manera que un usuario nunca pueda gastar más monedas de las que tiene saldo. Por el contrario, las transacciones de cuentas que, según el consenso general, no tienen fondos, no pueden acreditarse, ya que no recibirían confirmación.

Consenso comunitario

Los usuarios se verifican entre sí durante una transacción o después de la sincronización verificando las pruebas de confianza de cada uno. Para hacerlo simple:

Si un usuario quiere enviar una transacción, debe demostrar a los demás participantes, y en particular al destinatario, que existen créditos suficientes para realizar esta transacción.

Proporciona esta prueba a través de las pruebas de fideicomiso recopiladas. La validación de una transacción la realizan una y otra vez los demás participantes. Calculando los saldos de las cuentas y verificando las transacciones teniendo en cuenta las confirmaciones hasta la fecha y la puntuación, se logra un consenso común.

Sincronización con otros usuarios

Un usuario puede sincronizarse con otros usuarios independientemente de las transacciones intercambiadas previamente para generar confianza y conocimiento. El usuario también debería hacer esto de forma regular.

Un usuario que se sincroniza con otro usuario ayuda a desarrollar conocimientos sobre transacciones comúnmente compartidos y ayuda a difundir las transacciones de otros usuarios. Al mismo tiempo, se protege de ataques de doble gasto al tener conocimiento sobre otras transacciones que antes desconocía.

El conocimiento de transacciones comúnmente compartido también puede reducir significativamente el tamaño de un archivo de transacción, ya que, en el mejor de los casos, el usuario A ya no tiene que enviar las pruebas de confianza necesarias para la transacción al usuario B porque ya está allí.

Cuanto más sepa un usuario sobre este usuario y las transacciones vinculadas a este usuario, más creíble será la confirmación de un usuario y su saldo. Cuantos más usuarios conozcan una transacción y la confirmen, más definitiva será la transacción. Un usuario que ha realizado una transacción y posteriormente la elimina de su historial no puede evitar la rápida difusión de este conocimiento por parte de otros usuarios. Además, el usuario atacante ya no tiene influencia sobre la rapidez con la que se difunde el conocimiento de la transacción. En el mejor de los casos, el siguiente socio de transacción ya ha sido informado de la última transacción mediante la sincronización o mediante un pago de un socio comercial/amigo anterior, de modo que el usuario atacante no puede negarlo.

Además de la sincronización con UCA/usuarios, en este contexto también son imaginables **modelos de sincronización como servicio**, en los que los sitios web actúan como punto de encuentro para los usuarios que desean sincronizar y actuar como notario para varias monedas.

PREGUNTAS FRECUENTES

¿Por qué no existe una cadena de bloques central?

La arquitectura utilizada en UCS se basa en una estructura de cuadrícula de bloques descentralizada en lugar de una cadena de bloques monolítica central. No se requiere una cadena de bloques central para formar un consenso común o verificar una transacción o cuenta específica. Las *proofs-of-Trust* (archivos TSA, archivos de transacciones y archivo de índice) son suficientes. Como resultado, un usuario sólo puede confirmar transacciones desde la red confiable en la que se encuentra. El usuario sólo puede ver las redes y los participantes conectados a esta red de confianza. No es como Bitcoin, donde puedes ver el historial completo de transacciones de todos los usuarios gracias a la cadena de bloques monolítica. Por supuesto, las redes de confianza que se formen crecerán y se conectarán a través del comercio y la sincronización. Esto crea con el tiempo un conocimiento de transacciones más o menos central, pero el concepto básico no es central. La cadena de bloques de un usuario consta de todas las transacciones enviadas y recibidas, que se gestionan como parte de un concepto de *distributed ledger*.

¿Qué TSA son compatibles?

Actualmente, solo FreeTSA es compatible como TSA. Actualmente se están debatiendo conceptos para otras TSA.

NOTA: Ya se ha discutido extender la selección de TSA a OpenTimestamp o brindar a los usuarios la oportunidad de definir las TSA ellos mismos. Sin embargo, lo primero significaría que habría que integrar el cliente OpenTimestamp, que a su vez accede a la cadena de bloques de Bitcoin, lo que implica una mayor dependencia de un servicio en línea o la necesidad de instalar el cliente, incluido el cliente de Bitcoin, localmente. La capacidad de definir TSA usted mismo permitiría a los usuarios utilizar TSA comprometidas. ¡Ambas soluciones no son buenas!

¿Qué es el algoritmo de proof-of-Trust?

El algoritmo de proof-of-Trust garantiza que todo sea correcto y que los usuarios no puedan hacer trampa. Una prueba de confianza consiste en la clave pública del remitente, que ha sido certificada por la TSA, el archivo de índice del usuario y todas las transacciones entrantes y salientes de un usuario y sus contactos. Esto es suficiente para determinar el saldo actual de una cuenta y/o para determinar si una transacción relacionada con este usuario es plausible o no.

¿Qué contiene la proof-of-Trust?

Una proof-of-trust siempre se compone de varios archivos. La proof-of-trust de un usuario consta de al menos:

- clave pública del usuario en la carpeta /keys

  opcional: claves públicas de otros usuarios si las transacciones son dependientes

- archivo de consulta freeTSA (*.tsq) y archivo de respuesta (*.tsr) de claves públicas en la carpeta /proofs

  opcional: archivos de consulta y respuesta de otras claves públicas si las transacciones son dependientes

- transacciones de usuario en la carpeta /trx

  opcional: transacciones de otros usuarios si las transacciones son dependientes

- archivo de índice de cada usuario en la carpeta /proofs

  contiene una lista de todas las transacciones plausibles y se utiliza para determinar las confirmaciones.

Utilizando estos archivos, es posible consultar un saldo y las transacciones asociadas en cualquier momento.

¿Qué sucede si un usuario elimina manualmente una transacción del historial? ¿Puede el usuario volver a gastar la misma cantidad?

Si has seguido todas las reglas: ¡No! Si un usuario envía una transacción a otro usuario, el destinatario distribuirá esa transacción en el futuro. Si el usuario emisor simplemente elimina una transacción de su historial, los usuarios que ya conocen la transacción aún difundirán el conocimiento de esta transacción en el futuro. El remitente ya no puede influir en la rapidez con la que esto sucede. La sincronización con otros participantes reduce significativamente el riesgo de tal ataque, ya que un participante lógicamente no puede retener una transacción que otros usuarios ya conocen en la red de confianza.

¿Por qué Universal Credit System?

No se requieren cálculos intensivos para obtener Universal Credit Coins. Las monedas de credits se otorgan a todas las entidades que hayan creado una cuenta con éxito. Es independiente de una autoridad central, un estado o un país. Es independiente del lugar donde se utilice. Nadie puede prohibirlo, nadie puede cerrarlo y nadie puede cambiar el consenso. Por un lado, puede actuar como medio monetario y, por otro, puede utilizarse para la especulación estimulada por la escasez artificial. La falta artificial de credits ofrece a los usuarios potenciales un incentivo para participar lo más rápido posible y al mismo tiempo no excluye a los participantes tardíos. Es una especie de moneda democrática, porque todos reciben la misma cantidad y nadie sale favorecido ni desfavorecido. No existen tendencias de centralización en términos de creación de dinero como en las criptomonedas existentes. Alguien con mucho dinero obtiene la misma cantidad de credits que alguien con poco dinero. Es un nuevo comienzo desde cero y cada usuario comienza con saldo 0 y las mismas oportunidades. Es un estándar monetario universal basado en matemáticas y confianza descentralizada. Es transparente cuando es necesario para la trazabilidad y para llegar a un consenso, pero al mismo tiempo, los participantes fuera de la red de confianza establecida no necesitan estar informados sobre las transacciones, etc. Esto lo hace menos propenso al fraude y, en general, mucho más atractivo. que las criptomonedas existentes.