Global **R**eal-time **A**uthorizations and **F**und **T**ransfers

Blockchain Descentralizada para Procesamiento de Pagos, a Tiempo Real, con Crypto, Crédito y Débito

Slava Gomzin, Dan Itkis

Versión 3

Octubre 2018

Initial version was published in June 2017

Resumen

Autorizaciones y Transferencia de Fondos, Globales, a Tiempo Real (GRAFT - Global Real Time Authorizations and Funds Transfers) es una plataforma de procesamiento de pagos, descentralizada, global, de código abierto y basada en la tecnología blockchain que todo el mundo puede usar. Todos los compradores y comerciantes pueden hacer uso de GRAFT de manera descentralizada y sin coste alguno. El ecosistema GRAFT es completamente abierto, por lo que cualquiera puede participar manteniendo la blockchain o implementando nuevos servicios dentro de la red.

GRAFT utiliza métodos y protocolos de procesamiento de pagos muy similares a los sistemas tradicionales de pago electrónico, como las tarjetas de crédito/débito y prepago, cuyo uso ya es familiar y se ha ganado la confianza de millones de usuarios y comerciantes en todo el mundo. Seguir esta estrategia facilita una rápida adopción de GRAFT como una plataforma de pago habitual, eliminando a la vez la necesidad de los intermediarios centralizados (proveedores de servicios y pasarelas de pago) que en la actualidad son necesarios para procesar las transacciones entre compradores y comerciantes.

Introducción

Bitcoin [1] se creó como una "moneda digital", así como un sistema de contabilidad muy seguro, pero relativamente lento, que no ha sido capaz de reemplazar las tarjetas de pago online o competir con las tarjetas de plástico y la moneda en metálico en las tiendas físicas (Figura 1).

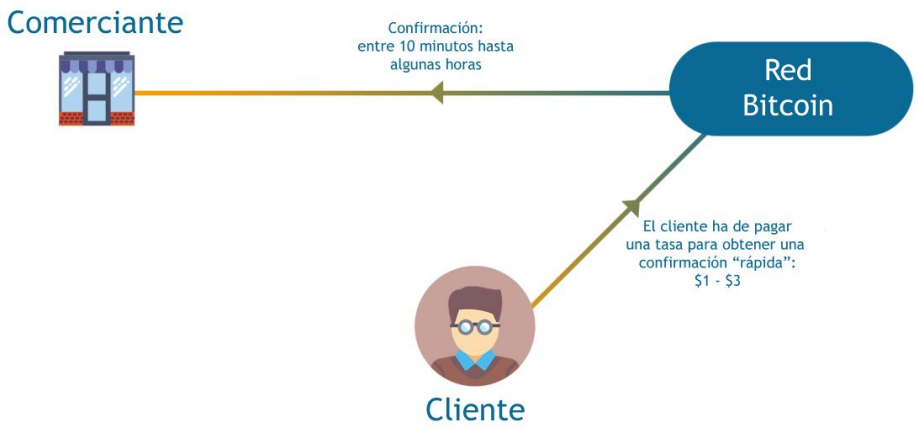

Figura 1: Procesado de las transacciones con Bitcoin sin intermediario centralizado

Aunque en la actualidad algunas criptomonedas o tokens criptográficos [2] han mejorado considerablemente los tiempos de confirmación, aún son incapaces de procesar, a tiempo real, transacciones básicas desde la autorización a la finalización del proceso, haciendo imposible su adopción por parte de los minoristas, el sector hostelería o los pequeños supermercados, sin la necesidad de intermediarios - proveedores de servicios y pasarelas de pago [3] – que solucionen ese problema (Figura 2). Sin embargo, el uso de proveedores de servicios y pasarelas de pago – que generalmente son organizaciones comerciales centralizadas, reguladas por el gobierno y controladas por los accionistas – como un elemento de la transacción criptográfica contradice algunos de los principios fundamentales de las criptomonedas o tokens criptográficos: descentralización, privacidad e independencia.

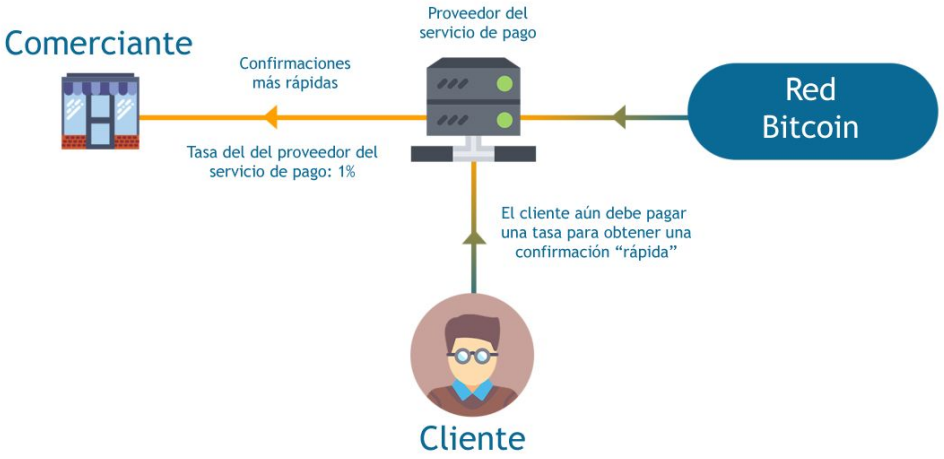

Figura 2: Procesado de las transacciones con Bitcoin con un intermediario centralizado

La mayoría de comerciantes se ven incapaces de aceptar criptomonedas sin requerir la participación de terceras personas que gestionen los pagos debido a la singular forma procesar las transacciones en las blockchain. Esta forma de procesar es conceptualmente diferente a los sistemas de pago electrónico tradicionales, los cuales, a pesar de sus defectos, han creado útiles herramientas a su alrededor que les ha permitido acumular una enorme experiencia en el ámbito de los comerciantes y ganar la confianza de los usuarios.

Existen algunas diferencias principales entre la manera de procesar las transacciones en el sistema de pagos electrónico tradicional y como se realizan en un sistema criptográfico, estas diferencias convierten el sistema de pagos criptográfico en menos atractivo para los comerciantes y/o consumidores. En la siguiente lista se muestran algunas de las limitaciones técnicas o defectos de los sistemas de pago criptográfico existentes, comparando con los sistemas de pagos electrónico tradicionales:

- No existe una codificación básica de tipos de transacciones
- Procesado de pagos inadecuado
- Tiempos de confirmación largos
- Tasas por transacción impredecibles e inadecuadas
- Incapacidad para procesar micro-pagos o pagos periódicos (suscripciones).
- No existe soporte para transacciones fuera de línea
- Escalabilidad baja
- Volatilidad
- Sistemas de seguridad incompletos
- Falta de privacidad debido a la trazabilidad de la blockchain
- Falta de confianza entre comerciantes y consumidores
- Utilidad cuestionable
- Baja estabilidad en la interfaz de usuario
- Ausencia de soporte al usuario

Con la idea de romper las limitaciones y corregir los defectos anteriormente descritos, el objetivo de GRAFT es la creación de una plataforma que permita, por primera vez, una adopción masiva y global de los pagos criptográficos, por comerciantes y consumidores, y al mismo tiempo respetando los principios fundamentales de las criptomonedas y tokens criptográficos.

El Valor del Procesamiento de Pagos Descentralizado

Por qué motivo un comprador querría empezar a utilizar criptomonedas y tokens criptográficos en vez de (o además de) tarjetas de plástico convencionales, PayPal o Apple Pay? y por qué un comerciante querría aceptar criptomonedas y tokens criptográficos en vez de (o además de) los métodos de pago ya existentes? Obviamente, si no tenemos respuesta a estas simples cuestiones, crear este documento carece de sentido.

Mientras que la respuesta a la primera pregunta ha de tener en consideración muchos elementos -tantos como las múltiples razones (o combinaciones de ellas) por las que cada individuo puede elegir mantener su dinero en forma de criptomoneda o token criptográfico-, la respuesta a la segunda pregunta es relativamente simple. Los comerciantes quieren ampliar su base de clientes para poder aumentar sus ingresos, si identifican un grupo de potenciales clientes que prefieren, por cualquier razón, usar criptomonedas, esto les motivará a empezarán a aceptar estas criptomonedas. En este sentido, GRAFT brinda a los comerciantes la oportunidad de aceptar pagos con criptomonedas y tokens criptográficos, directamente de sus clientes y con unos costes extremadamente bajos.

GRAFT es un sistema de procesamiento de pagos descentralizado cuyas funciones se basan y controlan a través de sus propios tokens digitales. Esto le permite implementar ciclos completos de pago sin involucrar otras criptomonedas, tokens criptográficos o activos externos. Sin embargo, GRAFT también soporta Bitcoins y muchas de las criptomonedas y tokens más importantes, brindando a los consumidores otras opciones de pago y creando la infraestructura necesaria para que los comerciantes puedan aceptar los pagos. Esta característica permitirá a los comerciantes integrar diferentes sistemas de pago en uno, además de eliminar la necesidad, a los usuarios, de registrarse en distintos servicios centralizados y aprender a mantener múltiples wallets.

Terminología

Conjunto de Autorización

Grupo de supernodos completos (full supernode) seleccionados para aprobar una transacción, en tiempo real y garantizar que el comprador no puede gastar la misma cantidad de fondos más de una vez, antes de que la transacción se haya escrito en la blockchain.

DAPI

API descentralizado y no gubernamental, implementado por los supernodos para dar soporte a las aplicaciones cliente como el GRAFT Wallet, GRAFT Point of Sale y otras aplicaciones de punto de venta desarrolladas por terceros. GRAFT SDK facilita la integración con la red GRAFT, a los desarrolladores de aplicaciones externos, tanto en el lado de lo comerciantes, como en el de los clientes.

Broker de Exchange

Extensión del protocolo de GRAFT, alojado en un supernodo o en un grupo de supernodos. El broker exchange implementa y lleva a cabo algunas características que no pueden ser ejecutadas de manera automática en una red totalmente descentralizado y/o requieren de un marco regulatorio especial. Como ejemplo los brokers para procesar el pago con Bitcoin o con moneda fiduciaria (fíat).

Supernodo Completo (Full Supernode)

Servidor independiente y siempre on-line que ejecuta, de manera combinada, un nodo de la blockchain de GRAFT y un nodo DAPI; procesando las autorizaciones a tiempo real; gestionando las llamadas DAPI entre compradores, agentes de cambio y comerciantes; y alojando los servicios de terceros como los intercambios instantáneos entre criptomonedas dentro de la red GRAFT, integración con tarjetas de crédito/débito y otros métodos aceptados por los comerciantes. Los supernodos, de manera colectiva, mantienen la segunda capa de la red GRAFT usando el algoritmo POS (Proof of Stake).

GRAFT

1. Autorizaciones y Transferencia de Fondos, Globales, a Tiempo Real (GRAFT - Global Real Time Authorizations and Funds Transfers) es una plataforma descentralizada, global y de código abierto para procesar, a tiempo real, autorizaciones, pagos de mercancías y transferencia de fondos, y que usa tecnología blockchain, imposible de rastrear. Soporta variedad de métodos de pago, incluyendo criptomonedas, tokens criptográficos y métodos tradicionales como tarjetas de crédito/débito y transferencia bancarias.

2. Una planta que tiene, unidad a ella, una ramita o brote de otra planta de manera que se fusionan y crezcan juntas (injerto) [4]. El injerto (grafting) es una técnica avanzada en botánica, agricultura y jardinería que se usa para añadir tejido vivo de una planta a otra [5]. Esta técnica permite unir los mejores rasgos de diferentes plantas para crear algo mejororado y con más valor que las partes originalmente separadas.

Punto de venta GRAFT (GRAFT Point of Sale)

Aplicación cliente para móvil y escritorio que permite a los comerciantes aceptar pagos con tokens GRAFT, bitcoin, altcoin o tarjetas de débito/crédito, generar y canjear tarjetas regalo, puntos por lealtad y créditos de la tienda; y configurar pagos y devoluciones en GRAFT, bitcoin, altcoin o moneda fíat local.

GRAFT Wallet

Aplicación cliente para móvil, escritorio y navegadores de internet, que permite hacer pagos y transferir fondos usando tokens GRAFT, otras de las criptomonedas y tokens más importantes, o tarjetas de crédito/débito a través del DAPI de GRAFT.

GRFT

Token criptográfico nativo, soportado por la blockchain de GRAFT y utilizado en las autorizaciones de los pagos a tiempo real, las transferencias de fondos y las liquidaciones de fondos entre compradores y comerciantes.

Tokens de comerciante

Contrato inteligente predefinido que permite al comerciante crear un token privado que pertenece a su propietario. Los tokens del comerciante permiten implementar importantes funciones de pago y crear un sistema privado y cerrado de puntos de lealtad, tarjetas regalo, créditos de la tienda y cupones descuento.

Pasarelas de pago (Payment Gateway)

Permite a los comerciantes y a los proveedores de servicios de pago controlar la configuración de sus terminales de pago (como la dirección del wallet) y establecer las tasas específicas del servicio, además de proporcionar información y análisis de las transacciones que se realizan.

Tokens de pago de “Valor Estable”

Representa a la moneda fíat local y puede operarse dentro de la blockchain de GRAFT, a tiempo real, usando los supernodos. Los tokens de pago se basan en los tokens de comerciante GRAFT y funcionan de forma parecida a las tarjetas regalo, puntos de lealtad y otros tokens del comerciante.

Supernode Proxy

Es un tipo de supernodo que facilita las transacciones con los comerciantes, comunicándose, por un lado, con sus puntos de venta (POS) y con las wallets de los compradores y por otro lado, con los supernodos del conjunto de autorización.

VChain

Hace referencia a una cuenta de usuario para los comerciantes, descentralizada e independiente, donde ellos pueden crear sus tokens y establecer las autorizaciones y las reglas de pago, así como los umbrales y avisos que afectan a las transacciones específicas de dicho comerciante.

Tasas por Transacción

En primer lugar, por qué ha de ser necesaria una tasa por transacción? Después de todo, no hay ningún negocio detrás de una blockchain, entonces, por qué los usuarios deben pagar esta tasa? Quién la recibe? Y cómo de alta debe ser?

Añadir una Tasa o no Añadir una Tasa

Potentes nodos (servidores) distribuidos por todo el mundo son necesarios para mantener y soportar, de una manera segura y con alta disponibilidad, la red de cualquier criptomoneda o token criptográfico. Entonces, quién mantiene estos servidores? y cuál es la motivación o incentivo para establecer un nodo de la blockchain? En Bitcoin y otras criptomonedas, los fondos e incentivos se consiguen a través del minado y de las tasas por transacción -el propietario de un nodo consigue dinero a través del minado de un nuevo bloque y cobrando las tasas al procesar las transacciones. Por otro lado, el minado tiene otro objetivo, la inyección constante y controlada de nuevos tokens en el sistema, con el objetivo de mantener la liquidez de forma paralela a la demanda creciente, tal y como se va produciendo la adopción. Tal y como el sistema vaya cogiendo impulso, el operador del nodo irá recibiendo más incentivos provenientes de la tasa por transacción, por lo que la recompensa de minado irá cayendo gradualmente, cuando el número máximo de tokens definido se vaya alcanzando.

En un mundo ideal, las criptomonedas o los tokens criptográficos deberían estar disponibles para cualquier usuario, de una manera gratuita, de hecho, siguiendo esta linea, existen redes que prometen transacciones gratuitas [6]. En la realidad, incluyendo Bitcoin, las tasas se usan para priorizar cierta transacción y “resolver” el problema de la escalabilidad.

En la red GRAFT, sin embargo, las tasas se implementan por dos razones. La primera es para evitar el abuso de la red y los problemas de rendimiento asociados en la blockchain - por ejemplo, usar la red real para pruebas, si las transacciones son completamente gratuitas, alguien podría mover la misma cantidad de dinero entre dos cuentas de manera indefinida. La segunda razón es para mantener el incentivo a los nodos una vez las recompensas de minado sean demasiado bajas.

Imponiendo Tasas al Tipo Equivocado

El problema de las tasas en la red Bitcoin y otros tokens criptográficos es que la tasa se cobra en el lado equivocado de la transacción, siendo incluso más injustas que en los métodos tradicionales. Al contrario que el los pagos con tarjeta de débito/crédito, en las transacciones criptográficas tanto el comprador como el comerciante han de pagar tasas: el comprador abona la tasa a la red, mientras que el comerciante paga al proveedor de servicios. Este método es confuso para el comprador medio, que, en muchos casos, lo ve como una estafa. Además, encontrar una explicación clara y sencilla a este sistema es difícil, lo que convierte las criptomonedas o tokens criptográficos en mucho menos atractivas como métodos de pago.

Micropagos: Como Pago con Crypto una Taza de Café?

Otro problema que en la actualidad experimenta Bitcoin es la inviabilidad para manejar micropagos debido a sus elevadas tasas por transacción [7]. GRAFT soluciona este problema introduciendo una estrategia única para definir las tasas por transacción.

Tasas por Transacción en GRAFT

En el ecosistema GRAFT, **el emisor no paga las tasas**. Todas las tasas se trasladan y cargan al receptor (comerciante o beneficiario). Por otro lado, GRAFT aborda el problema de los micropagos estableciendo tasas muy bajas (en comparación con las tarjetas de crédito/débito, los proveedores de servicio online, criptomonedas y otros tokens criptográficos) [8].

Tabla 1: GRAFT - Tasas por transacción/estructura de incentivos

		1	2	3
		Transferencia Regular P2P	**RTA (Autorización a tiempo real) Tx (GRFT)**	**RTA Tx con altcoin, exchange broker (p.e., bitcoin)**
a	**Incentivo Supernodo Proxy**	0.1 GRFT *	0.05% *	0.05% *
b	**Incentivo Supernodo completo (miembro del conjunto de autorización)**	N/A	0.0625% **	0.0625% **
c	**Incentivo al Exchange Broker**	N/A	N/A	0.25% **
d	**Incentivo Minado (Bloque)**	Variable, basado en el tamaño del Tx en KB	Configurable *** Min: 0.1 GRFT	Configurable *** Min: 0.1 GRFT
e	**Incentivo Comerciantes POS/Supernodo Proxy** ****	N/A	0.05% ****	0.05% ****
	Tasa total a pagar por el que envía la Tx (comprador en RTA)	a1 + d1	0	0 *****
	Tasa total a pagar por el que recibe la Tx (comerciante en RTA)	0	a2 + b2*8 + d2 + e2	a3 + b3*8 + c3 + d3 + e3
	Cantidad total requerida al que envía la Tx	Cantidad en Tx + a1 + d1	Cantidad en Tx	Cantidad en Tx
	Fondos totales disponibles por el receptor de la Tx	Cantidad en Tx	Cantidad en Tx– (a2 + b2*8 + d2 + e2)	Cantidad en Tx – (a3 + b3*8 + c3 + d3 + e3)

* el supernodo proxy puede estar alojado en un servidor privado o un conjunto público gestionado por un proveedor de servicios. Cada uno puede operar y usar su propio supernodo proxy para evitar dicha tasa. Para poder cobrar estas tasas, el supernodo debe tener fondos (stake).

** los fondos (stake) son necesarios para operar un supernodo completo o un exchange broker y así recibir el incentivo por participar en procesado de transacciones a tiempo real (RTA Tx).

*** tasa establecida por el proveedor de servicios o el propietario del supernodo proxy que enlaza con el POS

**** el supernodo proxy que enlaza con el POS puede pertenecer a un servidor privado, ser parte de la infraestructura del comerciante o propiedad de un proveedor de servicios. Para poder cobrar estas tasas, el supernodo debe tener fondos (stake).

***** no incluye la tasas de la red altcoin

Los incentivos de los supernodos proxy (a1, a2, a3, e2 y e1 en la Tabla 1) mantienen una infraestructura de red completamente descentralizada. Si por algún motivo, se prefiere evitar los clusters de supernodos proxy alojados por proveedores de servicio particulares, existirán proveedores alternativos preparados para proveer este servicio a los wallets o los POS. Para obtener los incentivos, los supernodos proxy deben probar que los fondos linkado a la dirección IP pública de dicho supernodo son únicos. La cantidad requerida es de 250,000 GRFT

A diferencia de los supernodos del conjunto de autorización, los supernodos proxy son operables aún sin tener fondos, sin embargo un supernodo proxy sin fondos no puede cobrar las tasas de las transacciones. Esta opción se reserva para los propietarios de supernodos proxy cuyos usuarios necesiten un elevado nivel de privacidad, de manera que puedan alojar su punto de entrada a la red GRAFT. Sin fondos, los incentivos derivados serán enviados al wallet de donaciones de la comunidad GRAFT. De esta manera, la tasa total por transacción se mantiene consistente, independientemente del estado del supernodo proxy que la gestione.

A los mineros se les paga una tarifa plana (d2 y d3) por confirmar las transacciones RTA (transacciones a tiempo real). Tradicionalmente el incentivo a los minero se calcula en base al tamaño del registro de la transacción en KB (d1). Com las RTA, no podemos hacer que este incentivo sea variable, ya que provocaría que la tasa total pagada por el comerciante fuera inconsistente e impredecible (algo inaceptable en la mayoría de situaciones). Además, tampoco podemos hacer que esta tasa sea proporcional a el valor de la transacción (similar a lo que se hace con las tasas para los supernodos) porque los incentivos para los mineros son visible en la blockchain, lo que significa que la cantidad involucrada en la transacción puede ser estimada de manera proporcional (a pesar de que se planea ocultar la visibilidad de esta cantidad en el futuro). Por lo tanto, hemos decidido aplicar una tasa plana, configurable, con una valor mínimo de 0.1 GRFT.

Las tasas asociadas con las transacciones RTA, involucrando un exchange broker, son las mismas que las tasas RTA (columna 2), pero con una tasa extra de 0.25% que se transfiere al broker (pagada también por el comerciante).

Proveedores de Servicios y Tasas a los Comerciantes

Los proveedores de servicio de pago pueden definir el esquema de tasas que se adapte mejor a su modelo de negocio, las tasas pueden estructurarse en niveles, como por ejemplo:

Transacciones por debajo de $10: 2%
Transacciones por arriba de $10: 1%
Cantidad mínima por transacción: $1
Mineros: 0.1 GRFT
Transacciones en altcoins: +0.25%
Pagos inmediatos en altcoin o fíat: +0.25%

Basándose en el esquema de tasas anterior, el siguiente ejemplo muestra una transacción de $20 con altcoin y sus tasas asociadas.

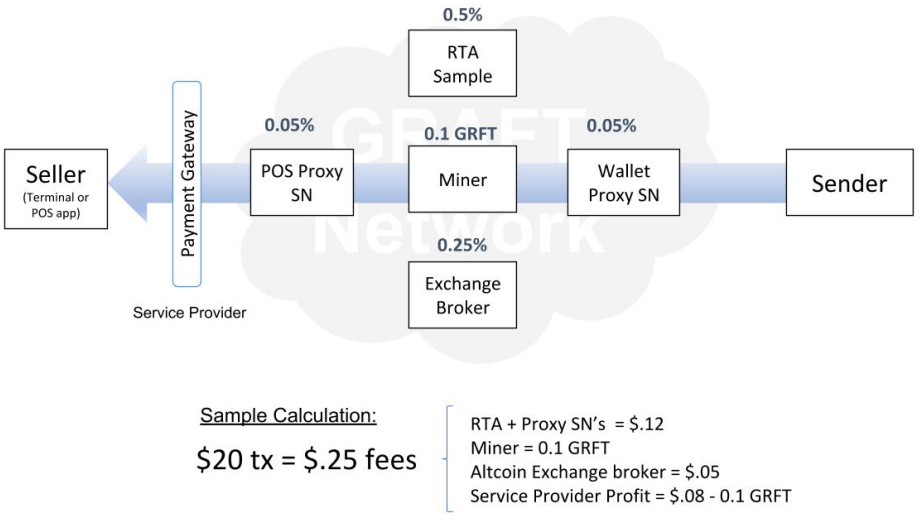

Figura 3: Ejemplo de Transacción en la red GRAFT, distribución de tasas/incentivos.

Transferencia de fondos gratuita: Transacciones Autentificadas

Algunos sistemas de pago, como Automated Clearing House (ACH) o PayPal ofrecen transferencias de fondos gratuitas entre cuentas de usuarios. Para poder competir con dichos sistemas tradicionales, GRAFT ofrecerá un número fijo de transacciones gratuitas entre miembros autentificados.

En general, las redes de criptomoneda, normalmente no pueden "permitirse" transacciones gratuitas por tres razones principales:

- Falta de incentivos para los mineros
- Amenaza de ataque por denegación de servicios (DDoS attack)
- Crecimiento descontrolado de la blockchain

GRAFT ha solucionado el primer problema -falta de incentivo para los mineros- separando en otro tipo los pagos a través de transferencias, por lo que los mineros siguen recibiendo incentivos por los pagos instantaneos que constituyen la mayoría de todas las transacciones. Las transferencias gratuitas se procesan con baja prioridad.

El segundo problema - Ataques DDoS- se puede resolver a través de la autentificación y identificación voluntaria de los usuarios. Por supuesto, esto tiene consecuencias, ya que el usuario tiene que proveer su identidad a la red para asegurar un uso razonable (limitando el número y la frecuencia de las transferencias gratuitas por usuario), previniendo el abuso. Añadiendo una autentificación por prueba de conocimiento cero (zero-knowledge proof-authentication - ZKP) permitirá a los usuarios autentificarse sin comprometer su privacidad.

El último problema -crecimiento descontrolado de la blockchain- se puede solucionar de diferentes maneras, incluyendo intervalos entre bloques más pequeños, tamaño por bloque ilimitado y tamaño de transacción estándar y restringido para ciertos tipos de transacciones. Además, una las partes implicadas en la transferencia gratuita ha de ser verificada, comprobando que ha llevado a cabo alguna transacción del tipo "pago comercial" en el pasado.

Privacidad

A menudo hay un error de percepción en la necesidad de privacidad. En realidad, la mayoría de los compradores legítimos no les importa revelar su identidad a los comerciantes, especialmente si se benefician de ello o si dicha información se requiere para proceder con la transacción. De manera similar, los compradores quiere estar seguros de que el comerciante, al que le han enviado un pago, es el receptor verdadero y no un imitador. Pero ni los comerciantes, ni los compradores quiere que cualquier otra persona, ajena a la transacción, tenga la capacidad de reconocer sus identidades y ver los detalles de las transacciones realizadas, escaneado una blockchain pública.

La privacidad es un tema delicado para las criptomonedas y las industria de los pagos en general. La privacidad puede cubrir desde el anonimato extremo hasta la completa transparencia, según decidan ambos, el vendedor y el comprador. El vendedor, por ejemplo, puede tener la obligación de cumplir ciertos requerimientos regulatorios, pedir y verificar ciertos datos personales, como la edad para poder comprar bebidas alcohólicas o cigarrillos o el código postal para calcular los impuestos aplicados al hacer una compra online. El comprador, por otro lado, puede estar de acuerdo en compartir cierta información o puede no estarlo, independientemente, tiene que tener el derecho a decidir. Si el vendedor y el comprador pueden acordar que información va a ser compartida, entonces, la transacción puede procesarse. Además, los comerciantes, en la mayoría de casos, necesitan un sistema que establezca la autenticidad de la información requerida.

En GRAFT pensamos que la mejor manera de abordar dicho problema pasa por utilizar sistemas de verificación de identidad y información compartida que sean consistente con las pautas de identidad establecidas por las regulaciones gubernamentales en este ámbito (p.e., NIST 800-63 en USA o GDPR en UE). Estos estándares exigen pruebas de identidad y autentificación diferenciadas [9].

GRAFT implementa un perfil de identidad digital, que va unido al wallet de GRAFT, con la capacidad de compartir cierta información, siempre partiendo del permiso del usuario, en el momento de la transacción. Esta autorización permite compartir ciertos atributos (como la edad, localización, dirección o nombre) selectivamente y en cada transacción.

GRAFT ha implementado el protocolo **CryptoNote** [10] como sistema de registro de transacciones subyacente, el cual se caracteriza por el alto grado de privacidad cuando se compara con Bitcoin o otras criptomonedas, ya que esconde la información relativa al emisor y al receptor

Por qué una Blockchain Privada es Necesaria?

La clave de la innovación del Bitcoin es crear un libro de cuentas abierto y accesible a todos los nodos que participan en la red, ya que las transacciones deben ser verificadas para asegurar que no es posible gastar dos veces los mismos fondos. Pero esto, también implica que cualquier persona del mundo puede ver todas las transacciones y los balances de todos los wallets. A diferencia de las tarjetas de plástico, los wallets de Bitcoin son anónimos ya que las transacciones no se guardan directamente relacionadas a la identidad del propietario. A primera vista, esta característica parece compensar el hecho de que cualquiera pueda consultar los registros de transacciones, sin embargo, existen técnicas que permiten a los observadores relacionar direcciones de wallets con sus respectivas identidades [11]. Una vez esto pasa, todas tus transacciones anteriores quedan identificadas para siempre, ya que la blockchain siempre es visible y no se puede borrar.

CryptoNote es totalmente necesario para poder competir con los métodos tradicionales de pago como la red VISA o PayPal, que de hecho, proporcionan mucha mayor privacidad a sus clientes que la mayoría de la criptomonedas existentes.

Cuando insertas tu tarjeta de pago en un terminal de venta o haces click en el botón de pagar de Paypal, hay dos entidades en el mundo que están al tanto de la transacción que acabas de realizar: la red de pago (Visa o PayPal en este caso) y el comerciante. En realidad hay más organizaciones que "conocen" los detalles de tu transacción porque la red de pagos es mucho más compleja. Esta lista incluye, por lo menos, el banco emisor (el banco que te suministra la tarjeta de pago), el banco receptor (el banco que aprueba el pago), la pasarela de pago (el sistema que enruta adecuadamente la transacción al procesador de pagos o banco receptor) y el procesador de pagos (el cual procesa el pago y la recepción por parte comerciante). Aunque son varias las entidades implicadas, la lista es limitada, además, como tiene que cumplir las leyes y regulaciones sobre seguridad y privacidad, estas compañías han desarrollado algunos sistemas de seguridad relativamente buenos que protegen los registros de tus transacciones de ojos indiscretos. Por supuesto, cualquiera de los miembros de esta lista puede ser hackeado o puede ceder toda tu información a las agencias gubernamentales. Simplificando, la privacidad con los métodos tradicionales se puede resumir en que alguien aleatorio, en casi todos los casos, no va a ser capaz de acceder a los registros de tus transacciones, lo que en la mayoría de las blockchain no es ni siquiera así.

CryptoNote como la Base de la Privacidad

CryptoNote destaca por encima de los demás protocolos de blockchain porque proporciona algo que todos necesitamos: privacidad. Normalmente asumimos que la privacidad está garantizada y solo la echamos en falta cuando la perdemos. Irónicamente, Bitcoin y sus derivados han retrocedido en términos de privacidad si comparamos con las tecnologías de pago tradicionales, como el dinero en metálico o las tarjetas de crédito/débito, lo que se ha convertido en un ignominioso símbolo que compromete la seguridad y la privacidad. Los creadores de Bitcoin no se plantearon el tema de la privacidad o simplemente no tuvieron tiempo de resolver el problema, lo que es totalmente comprensible teniendo en cuenta que tenían que resolver un problema mayor: la creación de la tecnología blockchain.

CryptoNote, por su parte, mantiene todos los beneficios de la tecnología de blockchain, los cuales son bien conocidos, pero además recuperando las características de privacidad anteriormente pérdidas: **pagos no rastreables, transacciones imposibles de linkar, resistente al análisis de la blockchain y cuantía de la transacción confidencial**. Encima de todo esto y para completar la escena, GRAFT **añade tasas por transacción confidenciales**.

En resumen, CryptoNote ha creado los cimientos perfectos para construir encima una gran variedad de aplicaciones relacionadas, donde GRAFT ha aparecido para traer luz y conquistar el mundo de los pagos.

Transacciones Privadas

GRAFT ha utilizado diversos mecanismos diseñados por CryptoNote y Monero para ocultar los registros de las transacciones y hacerlas solo visibles al propietario:

Destinatarios de un solo uso, con direcciones fantasma.

En vez de mandar pagos al receptor directamente se crea para cada transacción una clave única y de un solo uso. Esta clave se deriva criptográficamente de la dirección pública del receptor, de manera que es imposible de linkar con una dirección o con otra clave. Por lo tanto, **el receptor puede publicar una dirección única y recibir pagos no linkables**, además, **ningún observador puede determinar si alguna de estas transacciones fue enviada a alguna dirección en específico o relacionar dos direcciones.**

Anillo de signatura de un solo uso

Este conjunto de signaturas **ocultan la identidad de emisor**. Cada transacción en todas las blockchain queda firmada por la llave privada del emisor, de manera que la red pueda confirmar que la transacción es genuina. En vez de crear una signatura única, se crean diversas signaturas ("anillo"), siendo todas ellas igualmente válidas, ya que representan la misma transacción pero con distintos emisores. El observador, sin embargo, no puede discernir quién ha sido el emisor real. La red tampoco es capaz de saber que output en particular se ha usado ya que esta información se oculta entre todas las demás signaturas del anillo. En vez de esto, la red comprueba que las cantidades que hay en el anillo no se han utilizado más de una vez. Esto evita de manera eficiente el duplicado de gastos.

Transacciones confidenciales dentro del anillo

Convierte las cantidades enviadas, en cada transacción, en invisibles dentro de la blockchain. La cuantía de cada transacción queda encriptada por el emisor. Solo el receptor del pago es capaz de decodificar esa cantidad. Los observadores externos no pueden desencriptar dicha información, pero si que pueden comprobar que ese dinero no se ha gastado más de una vez, evitando la creación de "nuevo dinero" en esta transacción.

Procesado de Transacciones

La tecnología tiende hacia la creación de dispositivos más pequeños y manejables. La gente en todo el mundo utiliza cada vez más smartphones y tablets y menos ordenadores de sobremesa y portátiles. Por este motivo, pensamos que un sistema de pagos criptográficos descentralizado ha de descansar sobre nodos pequeños e individuales alojados en dispositivos personales y basarse en potentes supernodos dedicados y alojados por profesionales, destinados a conectar las apps de los usuarios a los conjuntos de autorización -grupo de supernodos seleccionados aleatoriamente por un algoritmo especializado en prevención de fraude- vía llamadas DAPI.

El Problema de los Tiempos de Confirmación: Introducción a las Autorizaciones en Tiempo Real (RTA)

Tiempos largos de confirmación [12] (desde algunos minutos hasta varias horas, dependiendo de la tasa aplicada a la transacción), es una de las principales razones para explicar la baja adopción que sufren las criptomonedas y tokens criptográficos en el sector servicios y la hostelería. A los clientes no les gusta esperar, como consecuencia, los comerciantes exigen procesamiento de pagos casi instantáneos. A diferencia de otras redes de criptomoneda que intentan resolver el problema

utilizando sistemas adicionales o tipos específicos de transacciones, GRAFT es capaz de procesar todas las transacciones de pago a “tiempo real” (esperamos que la mayoría de transacciones se completen en alrededor de 3 segundos), además, sin cargar ninguna tasa extra al consumidor.

Para conseguir esto se necesita del consenso de supernodos (“conjunto de autorización”) con la habilidad de bloquear fondos en el wallet del comprador, de manera distribuida e instantánea y comunicarse y responder al cliente, típicamente en milisegundos. Los supernodos también monitorizan la blockchain de GRAFT de manera que ninguna transacción se pueda autorizar fuera de la blockchain.

Supernodos

Todas las transacciones en tiempo real se procesan a través de una red, siempre online, de nodos GRAFT -supernodos. Las tasas de la transacción, pagadas a los supernodos participantes en el conjunto de autorización, son abonadas por el receptor (el comerciante) y también se abonarán las tasas a los Exchange Brokers que participen (de manera opcional) en el procesado de la transacción. El propietario de un supernodo es el responsable de cada transacción que procesa. Esta responsabilidad se ve incentivada por un interés financiero (las tasas de la transacción).

DAPI

A diferencia de las APIs regulares, que están alojadas en servidores o granjas de servidores, DAPI no tiene una dirección única y se ejecuta en múltiples supernodos. Cualquier nodo puede mandar una llamada DAPI cuando lo desee. Las llamadas DAPI no tienen una autoría fija, lo que significa que los supernodos no mantiene una sesión permanentemente abierta con el cliente, toda la información necesaria para procesar la transacción se distribuye de manera que, instantáneamente, queda disponible para todos los supernodos. Las apps cliente, que interactúan con la DAPI, mantienen una lista de los proxy supernodos con los que se comunican. Sin embargo, el cliente app es libre de elegir un supernodo de confianza y lanzar las transacciones a través de él. Por ejemplo, un comerciante o un usuario pueden decidir alojar su propio supernodo proxy para comunicarse con su POS o wallet. Sin embargo, estos supernodos privados pueden no tener derecho a participar en los conjuntos de autorización, debido a sus recursos limitados (ver la sección de Algoritmo de Selección de los Conjuntos de Autorización), pero sí que pueden ser utilizados para proporcionar una capa extra de privacidad a sus propietarios

Aprobación a Tiempo Real por los Conjuntos de Autorización

Existen criptomonedas con intervalos entre bloques de menos de dos minutos. Sin embargo, reducir dichos intervalos no convierte dichas transacción en “transacciones a tiempo real”. Los supernodos de GRAFT resuelve este problema, definiendo conjuntos de autorización, cuando se requiere, capaces de aprobar la transacción realizada, a tiempo real. Creemos que, con esta estructura, se puede garantizar que el mismo dinero no puede gastarse más de una vez, hasta que el bloque se establece (se escribe en la blockchain). La escritura de cada bloque (minado) se realiza en un intervalo de típico de varios minutos.

A diferencia de la mayoría de los sistemas de pago criptográficos, y con más similitud a los métodos electrónicos de pago tradicionales, cada pago realizado en la red GRAFT se divide en dos fases: autorización y establecimiento (escritura del bloque). De manera similar al mundo de los pagos tradicionales, en GRAFT la autorización sucede a tiempo real, mientra que el establecimiento de la transacción sucede más adelante, normalmente en dos minutos (comparando con las horas o incluso días que tardan las redes de pago tradicionales).

Autorización de Bloqueo en Cuenta

CryptoNote utiliza el mecanismo de imágenes de clave para validar las nuevas transacciones y prevenir el gasto duplicado sin comprometer la privacidad del emisor. Cada imagen de la clave crea una “huella” única que representa la dirección de comprador y la cantidad involucrada, sin revelar ningún detalle acerca del comprador o la cantidad. Por definición cada imagen de la clave solo puede utilizarse una vez, para evitar el gasto de fondos duplicado. Al proporcionar la llave única a la red de supernodos seleccionados para la siguiente transacción, el wallet emisor queda temporalmente bloqueado, para que no se pueda generar otra transacción con la misma imagen de clave (p.e. desde la misma cuenta) hasta que la transacción queda establecida o el bloqueo queda deshabilitado por otros medios. Si el comprador intenta finalizar la transacción con una imagen de clave diferente a la que se usó en el bloqueo original, la transacción quedará automáticamente anulada por los supernodos.

Por otro lado, la imagen de clave no contiene información acerca de comprador o el wallet del comprador, lo que garantiza la seguridad, el anonimato y la imposibilidad de rastreo. Además, cualquier rastro de comunicación entre compradores (app wallet), comerciantes (app de punto de venta - POS) y supernodos (conjunto seleccionado) durante el proceso de autorización, se eliminará una vez la transacción se haya establecido (escrito en la blockchain y confirmado 10 veces).

Niveles de Supernodos

Los nodos GRAFT se llaman “supernodos” porque realizan más funciones que los nodos de una blockchain tradicional. Por lo que existe un aumento de los requerimientos sobre lo propietarios de los mismos. Ya que GRAFT es una red abierta y descentralizada, que permite a cualquiera operar un supernodo, se han creado diferente niveles de supernodos con distintos requerimientos y incentivos asociados a cada nivel.

Supernodo Proxy (Proxy Supernode) es el “nivel de entrada”, cualquiera puede instalar el software del supernodo para alojarlo. Los Supernodos proxy proporcionan los siguientes servicios:

- Enlace de confianza para aquellos que busquen el mayor grado de privacidad posible, de tal modo que puedan alojar su propio servidor wallet.
- Para grande comerciantes, pueden usarse como “servidor de tienda” que acelere y haga más fiable el procesado de las transacciones.
- Como un “nodo de salida” público que conecte las apps de wallet y la del punto de venta con la red GRAFT (una IP pública es necesaria). El supernodo proxy público puede conseguir incentivos si se dispone de fondos (stake) asociados.

El **Supernodo Completo** ejerce la función de autorizador y proveedor de servicios. Además, para poder operar, los supernodos completos requieren de fondos (stake) -balance colateral asociado a la dirección del supernodo. Las tasas por transacción y servicio se pagan a los supernodos completos que tengan estos fondos asociados y realicen autorizaciones a tiempo real.

Nodos de Minado

Mientras que la segunda capa de la red GRAFT consiste en los supernodos de POS que realizan las autorizaciones y funciones de exchange, la primera capa, consiste en una red de nodos Proof of Work (PoW) que se encargan de establecer las transacciones, generando nuevos bloques y añadiéndolos a la blockchain.

Incentivos Minado

Los nodos de minado reciben la recompensas por haber minado un bloque a través de PoW y también reciben las tasas por “establecer” o escribir una transacción en el bloque, tanto en transferencias regulares como en RTA.

Incentivos por establecimiento (RTA Tx): variable

Determinada por el proveedor de servicios a través de la pasarela de pago, no puede ser menor que 0.1 GRFT.

Tasas de Minado por transacción (transferencia no-RTA): variable

Variable, basada en el tamaño del Tx en KB

Incentivo por Minar un Bloque (Coinbase)

La recompensa por minar un bloque se le paga al nodo de minado que ha resuelto este nuevo bloque. La recompensa por bloque se va reduciendo gradualmente con cada bloque usando la siguiente fórmula: $(M - A) * 2^{-19} * 10^{-10} / 2$, donde A = circulación actual y M = circulación total $(2^{64} - 1)$ en unidades atómicas (10^{-10}). La idea detrás de esta estrategia es que en el futuro habrán más transacciones, lo que mantendrá un flujo de dinero hacia los mineros a través de las tasas por transacción.

Niveles de Supernodos Completos

GRAFT ha diseñado cuatro niveles de supernodo, en función de los fondos, donde lo niveles más altos tendrán mayor probabilidad de ser seleccionados para un conjunto de autorización, aunque siendo la selección un proceso completamente aleatorio.

50,000 GRFT – Nivel 1 (tier 1)
90,000 GRFT – Nivel 2 (tier 2)
150,000 GRFT – Nivel 3 (tier 3)
250,000 GRFT – Nivel 4 (tier 4)

Cada nivel participa en la selección aleatoria de 2 supernodos por conjunto (donde N es el nivel). Por esta razón, un supernodo de nivel 4 tendrá más posibilidades de ser seleccionado debido a su número más limitado (cantidad menor de supernodos de nivel N que de niveles N-1). Los huecos vacíos se llenarán con supernodos de los niveles más altos (o más bajos en ausencia de los anteriores). El algoritmo es adaptativo y el mismo "regulará" el número medio de supernodos de cada nivel.

Fondos Delegados

Los fondos de diversos wallets pueden "delegarse" a un único supernodo para conseguir un balance suficientemente alto como para operar un supernodo completo. Las ganancias se distribuirán entre los wallet en proporción a los fondos aportados. La cantidad mínima para delegar son 5,000 GRFT.

Conjuntos de Autorización

Para poder realizar autorizaciones, a tiempo real, la red GRAFT se apoya en los conjuntos de autorización: un grupo seleccionado de supernodos de confianza que “representan” la red, validando la transacción, evitando el uso duplicado de los fondos y firmando una autorización instantánea antes de que la transacción quede confirmada dentro de la blockchain de GRAFT (antes de ser añadida a un bloque y que este bloque sea añadido a la blockchain).

El conjunto de autorización consiste en ocho supernodos seleccionados aleatoriamente de un lista dinámica de supernodos. La selección se hace de manera aleatoria mientras que el resultado es determinista para cualquiera que calcule la fórmula. El propietario del supernodo debe mantener un balance colateral mínimo en el wallet asociado al supernodo. La mínima cantidad requerida empieza con 50,000 GRFT.

Cuando se inicia una transacción en uno de los puntos de venta (POS) de un comerciante, esta se asigna al tamaño actual del bloque que define el conjunto de autorización. El tamaño puede incrementarse mientras la transacción se está procesando, pero este hecho no cambia el tamaño de la muestra que inicialmente se asignó al inicio de la solicitud. El supernodo proxy del comerciante que inicialmente dio formato a la solicitud de transacción selecciona en conjunto de supernodos, aunque esta selección ha de ser validada por cada miembro del conjunto y por el supernodo proxy del wallet.

Para acelerar el proceso de autorización, la aplicación de POS del comerciante puede pedir a los supernodos del conjunto de autorización que ignoren las respuestas del resto del conjunto siempre que se hayan recibido más de un 50 por ciento de respuestas aprobadas de los supernodos más rápidos y ninguna respuesta rechazada.

Supernodes Proxy

Cualquier supernodo de conjunto de autorización puede también actuar como supernodo proxy -esto facilita las transacciones con los comerciantes, comunicándose, por un lado, directamente con el POS y/o el wallet del cliente y por el otro lado, con el resto de los supernodos del conjunto de autorización. El supernodo proxy puede ser seleccionado aleatoriamente por el POS o el wallet dentro del conjunto de autorización actualmente linkado con la transacción. Aunque, en realidad, el POS o el wallet puede seleccionar cualquier otro supernodo que no sea parte del conjunto de autorización. De hecho, un POS o wallet pueden alojar su propio supernodo proxy si buscan mayor seguridad y privacidad. El supernodo proxy puede obtener incentivos por transacción si tiene fondos asociados.

Incentivos a los Supernodos

Cada supernodo recibe un parte de las tasas de cada transacción que procesen. Los incentivos son pagado por parte del receptor de los fondos (comerciante).

Supernodo Completo, incentivo RTA (todas las RTA Tx): 0.5%

Una octava parte de esta tasa, o 0.0625% del total de los fondos transferidos en la RTA Tx van a cada supernodo que haya participado en la conjunto de autorización.

Supernodo Proxy, incentivo RTA (todas las RTA Tx): 0.1%

La mitad de esta tasa, o 0.05% del total de los fondos transferidos en la RTA Tx van a cada supernodo que proporcionan conectividad entre la red (supernodos proxy del wallet y del POS).

Supernodo Proxy para wallets, incentivo (no RTA Tx): 0.1 GRFT

Esta tasa será transferida al supernodo proxy que comunica el wallet con la red y la abonará el emisor de la transacción, adicionalmente tendrá que cubrir las tasas de la red (incentivo a los mineros)

Escalabilidad

La escalabilidad de una red de pagos se refiere a la habilidad para procesar una gran cantidad de transacciones, simultáneamente, sin perder rendimiento. Una de las estrategias que la red GRAFT implementa para conseguir alta escalabilidad es fijar el intervalo de creación de los bloques en dos minutos y eliminar el límite de tamaño por bloque, de manera que los bloques de transacciones se generan más frecuentemente y cada uno puede acomodar más transacciones. Esta estrategia no es única en GRAFT ya que se ha implementado de manera similar en otra criptomonedas o tokens criptográficos. Sin embargo, GRAFT también se basa en potentes supernodos que siempre están on-line y que se encargan de validar y autorizar las transacciones a tiempo real. Por lo tanto, cada supernodo mantiene una copia actualizada de la blockchain completa y también una lista de todas las transacciones pendientes de incluirse en la blockchain. Esta arquitectura de dos capas permite absorber grandes picos the peticiones de transacciones (por ejemplo, cambios estacionales, eventos, y otros cambios en las actividades de los compradores y vendedores).

Aprobación de Transacciones Offline

La gente familiarizada con los métodos de pago con tarjeta sabe que a veces las transacciones pueden ser aprobadas por el comerciante sin obtener una aprobación simultánea por parte del banco. Esto se llama aprobación offline o local, autorización local o, a veces, S&F ("store and forward"), ya que este tipo de autorizaciones se reenvían al servidor una vez la red vuelve a ser accesible.

Los pagos criptográficos, por otro lado, asumen que la red está disponible 24/7, sin interrupción. Sin embargo, esta afirmación no siempre es verdad. En algunas situaciones, los comerciantes deciden arriesgarse y aprobar transacciones localmente, porque el riesgo de encontrar una transacción sin fondos es menor que el riesgo de perder múltiples compradores. Normalmente, hay un máximo de dinero que se puede autorizar localmente. Cuando el sistema alcanza ese límite (el riesgo máximo), el sistema deja de aprobar transacciones hasta que la red vuelve a estar operativa otra vez. Pero, en caso de periodos sin conexión cortos, el sistema de autorizaciones locales pasa inadvertido tanto para el cajero como para el comprador.

Un punto de venta (POS) GRAFT y un supernodo proxy serán capaces de procesar transacciones criptográficas offline, basándose en los mismos principios antes explicados y suponiendo que no se puede mantener comunicación con el conjunto de autorización para obtener el consenso necesario. Se autorizará si el comerciante está dispuesto a asumir dicho riesgo. La decisión sobre la aprobación offline se basará también en la reputación (reputation score) tanto del comprador como del supernodo.

Pasarela de Pago para Proveedores de Servicios a Comerciantes

Uno de los perfiles importantes dentro del ecosistema GRAFT son los Proveedores de Servicios al Comerciante (Merchant Service Provider - MSP). El papel del MSP consiste en proporcionar y mantener la red de servicio de pago al comerciante y asegurar la calidad de la red (normalmente se refiere al Acuerdo de nivel de servicio o Service Level agreement - SLA) y proporcionar y mantener los equipamientos (p.e. terminales de pago), así como mantener un seguimiento.
Para permitir al MSP cumplir que esto, se necesitan otro tipo de servidores, uno que:

- Administre la configuración de los terminales (incluyendo las direcciones de las wallets).
- Gestione el modelo de tasas del MSP (un MSP puede definir diferentes niveles de servicios y cargar diferentes tasas en función de los fondos involucrados en la transacción).

- Mantenga un seguimiento de las transacciones y analice y reporte dicha información a los comerciantes.

Este sistema de pasarela de pago puede ser diseñado e implementado por terceros, como pueden ser los procesadores de pago tradicionales que quieran añadir pagos con criptomonedas a su conjunto de servicios. Para ello, GRAFT ha creado una “implementación de referencia” para permitir una adopción más rápida dentro de la estrategia “go-to market”.

Ya que GRAFT es un red de pago descentralizada, las pasarelas de pago son aplicaciones multi-propietario, multi-instancia y de código abierto, para que cualquiera puede alojar su propio sistema de pasarela de pago y convertirse en un proveedor de servicios en la red. La pasarela de pago es el “quinto elemento” necesario para gestionar las aplicaciones GRAFT en los terminales de pago y la interface e-commerce de GRAFT, y así poder comunicarlos con los supernodos de la red GRAFT. Estas aplicaciones se consideran parte del "back office" del comerciante.

Tipos de Transacciones y Flujos de Pagos

GRAFT introduce los siguientes tipos y flujos de pago para facilitar las transacciones de los comerciantes, apoyar los métodos de pago y las aplicaciones de punto de venta (POS) existentes.

Authorize

Authorize, se usa cuando cuando no se conoce de manera exacta la cuantía final de la transacción en el momento en que se inicia la compra. Por ejemplo, cuando se paga por repostar en una gasolinera, se alquile un coche, se reserva una habitación de hotel o se paga en la mesa de un restaurante.

Este es un método análogo al de las tarjetas de débito. El comerciante inicia un tipo de transacción autorizada (Authorize) y confirmada por el pagador. En la cuenta del pagador se bloquea una cantidad, durante un cierto tiempo (número de bloques) a petición del comerciante y confirmado por el pagador, o hasta que la transacción sea confirmada a través de una transacción tipo “Complete” ulterior. Estos fondos también se pueden desbloquear a través de otra transacción tipo “Cancel”, antes de que expire la fecha/tiempo. Los fondos se devuelven automáticamente al pagador después de que expire la fecha/tiempo y si el comerciante no reclama los fondos a través de una transacción tipo “Complete”.

PreAuth

Método similar al Authorize a largo plazo, pero con la diferencia que el pagador no garantiza que los fondos estarán disponible cuando llegue el momento. PreAuth es un contrato a largo plazo entre el pagador y el beneficiario. Sin embargo, a diferencia del método Authorize, el cual no puede ser cancelado por el pagador, PreAuth sí puede ser cancelado, en cualquier momento, moviendo los fondos desde la cuenta asociada con la transacción preautorizada.

PreAuth es adecuado para acuerdos de pago a largo plazo como servicios de suscripción mensual o facturación diaria de habitaciones de hotel. El beneficiario especifica (el pagador confirma) la cantidad máxima de cada cargo simple, el número de cargos y el intervalo mínimo entre ellos.

Complete

Complete finaliza el pago iniciado con una transacción tipo Authorize o PreAuth. La cantidad de la transacción “Complete” actual, puede ser menor que la previamente autorizada ya que pueden haber múltiples transacciones de “Complete” pero la cantidad total no podrá exceder el máximo bloqueado por Authorize.

Complete se usa después de que una transacción autorizada sea finalizada con la cuantía real conocida -por ejemplo, cuando se paga en un gasolinera después de llenar completamente el depósito, se devuelve un coche alquilado, se procede al check-out de un hotel o se paga en un restaurante añadiendo las propinas.

Sale

Sale es un proceso de tipo Authorize/Complete secuencial y automático creado por la red como una transacción simple. Sale es la típica transacción comercial que se produce en las tiendas on-line o una tienda cualquiera .

Transfer

Tranfer se utiliza para transferir dinero entre cuentas GRAFT. Funciona igual que sale pero en este caso la transacción queda inicializada por el emisor sin la autorización necesaria del receptor. Se puede utilizar para pagos a dos, intercambio o transferencia entre diferentes cuentas.

Cancel

Cancel se usa para cancelar transacciones tipo Authorize previas y liberar los fondos implicados (los desbloquea de la cuenta),

Issue

Issue genera las tarjetas prepago de GRAFT, cheques regalo, puntos de lealtad, créditos de tienda y cupones descuento.

Redeem

Redeem permite pagar utilizando tarjetas prepago de GRAFT, cheques regalo, puntos de lealtad, créditos de tienda y cupones descuento que previamente hayan sido generados con GRAFT (Issue).

Exchange

Echange permite cambiar fondos entre tokens GRAFT y otras criptomonedas o tokens criptográficos conocidos, y también cambiar a la moneda fíat local, eligiendo automáticamente la mejor oferta disponible.

Schedule

Schedule se usa para programar un transacción con el objetivo de que ocurra en un momento posterior (hora/fecha). Requiere de aceptación adicional por parte del usuario.

Escrow

Escrow sirve para generar un depósito de fondos, añadiendo un evento en el cual serán liberados.

Refund

Refund devuelve los fondo que están referenciados a cierto puntero de transacción. Este método requiere un sistema autorización de devolución de mercancía (return merchandise authorization - RMA) por parte del vendedor.

Procesado de Transacciones con tokens GRFT como Método de Pago

A diferencia de los Bitcoins, otras criptomonedas o tokens criptográficos y de una manera muy similar a las tarjetas de crédito/débito, las transacciones de pago son creadas y emitidas por el receptor de los fondos (comerciante), a excepción de los métodos Tranfer y Exchange, que son iniciados por el emisor (p.e. cualquiera que quiera mover fondos entre cuentas de GRAFT). Sin embargo, a diferencia de las tarjetas de crédito/débito, las peticiones de pago son explícitamente confirmadas por el comprador que recibe la petición en su Wallet de GRAFT, antes de firmar digitalmente la transacción y mandarla a la red. La única excepción es la función Redeem cuando se está utilizando un tarjeta de

regalo en papel o plástico o un cupón que puede ser escaneado por la app de pago del comerciante, en caso que el cliente no quiera utilizar su aplicación de móvil o simplemente no quiere tener una cuenta en GRAFT.

Procesado de Transacciones con Métodos Alternativos de Pago

Con el objetivo de proporcionar la mejor experiencia para el comprador y mejores tipos de conversión para los comerciantes, una transacción de pago utilizando GRAFT permite usar, como moneda de entrada, varias criptomonedas, tokens criptográficos o monedas fíat locales (en forma de tarjetas de crédito/débito), que se pueden seleccionarse en la app del wallet de GRAFT. Las tasas de cambio, las tasa de los bancos y las tasas de procesado con tarjeta de crédito/débito (definidas por el comerciante en GRAFT) pueden ser aplicadas adicionalmente a las tasas de transacción de GRAFT. Asumimos que estás tasas serán pagadas por el beneficiario y invisibles al pagador, ya que el método de pago no debería afectar al precio de venta. El sistema de conversión instantánea y automática de GRAFT ayuda a la adopción de los pagos con crypto, por la mayoría de usuarios que, aunque no están suficientemente familiarizados con los ecosistemas de criptomoneda y se siente más cómodos con los métodos tradicionales de pago, buscan mejor seguridad, privacidad y anonimato en sus transacciones.

Si un comprador decide pagar con una criptomoneda alternativa o con tarjeta de crédito/débito, la red GRAFT automáticamente hará el cambio entre criptomonedas o convertirá el pago en moneda fíat local, con tarjeta crédito/débito, a GRFT, a tiempo real y como parte del proceso de transacción, utilizando los Exchange Brokers. Los Exchange Brokers funcionan dentro supernodos GRAFT y son los responsables de ejecutar los procesos de intercambio, cobrando al comprador y ejecutando el pago al comerciante. Si el comprador elige un criptomoneda alternativa o tarjeta de crédito/débito como método de pago, el conjunto de supernodos de autorización automáticamente seleccionará la mejor oferta de entre todos los Exchange Brokers, basándose en las elecciones anteriores y combinando esta información con los mejores tipos de cambio y las reputaciones más altas.

Exchange Brokers

Si un cliente paga con GRAFT tokens, y el comerciante quiere recibir el pago en GRAFT tokens, los fondos se retiraran de manera inmediata de la cuenta del comprador y se depositarán en la cuenta del comerciante a través de la red GRAFT. Sin embargo, si el cliente quiere pagar usando un método alternativo y/o el comerciante quiere recibir el dinero en una moneda diferente, la red GRAFT usará unos mecanismos especiales.

Con el objetivo de facilitar ciertos elementos del procesado de pagos, que no pueden ser completamente descentralizado pero son muy demandados por los consumidores y comerciantes, la red GRAFT introducirá el Exchange Broker. Aún cuando la red GRAFT no pueda procesar una operación particular, de una manera completamente descentralizada, se cederá dicha operación a una red de exchange brokers. Los comerciantes podrán elegir un exchange broker en concreto (por ejemplo un exchange broker de confianza o más económico) o un grupo de posibilidades.

El exchange broker es el responsable de mantener la seguridad y operar conforme a la legislación referente a los pagos con tarjetas, incluyendo los estandares PCI DSS y la legislación contra el blanqueo de capitales [13].

A continuación se listan los diferentes tipos de exchange brokers:

Comerciante/POS exchange brokers:

- Pay-in broker
- Payout broker

Comprador/wallet exchange brokers:

- Interchange broker
- Top-up broker

En cada transacción se dispondrá de un grupo de exchange brokers para cada una de las criptomoneda más importantes listadas en https://coinmarketcap.com/, empezando por el principio del "top 10" ordenado por capitalización de mercado. El exchange brokers inyectará liquidez a cada criptomoneda, a través de varias opciones de pago en ambos lados de la transacción (comprador y comerciante).

Los exchange brokers de criptomoneda se han implementado en colaboración con los exchanges ya existentes o nuevos. Eventualmente, habrán disponible múltiples opciones para cada criptomoneda, de manera que puedan competir y reducir los tipos de cambio. La variedad de servicios y los sistemas de registro automático, selección y ejecución de los procesos mantendrán el carácter descentralizado de la red. Se espera que cada uno de los conjuntos incluya cuatro exchange brokers para cada criptomonedas.

Los brokers de Pay-in y Payout trabajan en el lado de las apps de POS y con los terminales de pago permitiendo a los comerciantes aceptar el tipo de criptomoneda, elegido por el cliente como método de pago, durante el proceso de transacción de pago en su wallet de GRAFT o en una wallet de otra criptomoneda.

Los brokers de Interchange y Top-up trabajan en el lado de el Wallet de GRAFT permitiendo a los compradores poder utilizar la criptomoneda seleccionada como método de pago, cuando se realiza una transacción con un POS de GRAFT, una app de wallet nativa, un POS no nativo pero integrado con la DAPI de GRAFT o un POS no nativo que acepte pagos con la criptomoneda seleccionada.

Broker Pay-in

El Broker Pay-in permite aceptar pagos con una criptomoneda diferentes al token nativo GRFT, convirtiendo, de manera inmediata, la cantidad pagada a tokens GRFT y depositandola en la cuenta del comerciante. Los brokers Pay-in trabajan a tiempo real y son parte de la transacción entre el comprador y el comerciante. Desde el punto de vista del comprador, la transacción es muy similar a una transacción estándar entre dos wallet con la misma criptomoneda nativa.

El Broker Pay-in funciona junto con el POS de GRAFT para permitirle aceptar la criptomoneda seleccionada como método de pago, en caso de que el comprador no tenga un Wallet de GRAFT. Las tasas de transacción de la red (criptomoneda seleccionada) las continuará pagando el comprador, siempre que no disponga de la aplicación del Wallet de GRAFT. Si el comprador utiliza un Wallet de GRAFT, la aplicación será capaz de reconocer el POS de GRAFT y automáticamente convertirá la transacción de pago a una transacción instantánea en GRFT.

El pago a los comerciante será procesado por el Broker Pay-in instantáneamente en GRFT (Si se activa la opción, el pago se podrá hacer en cualquier otra criptomoneda o moneda fíat).

Ejemplos de Broker Pay-in:

- Bitcoin Pay-in Broker
- Ether Pay-in Broker
- Tarjeta de crédito Pay-in Broker

Diseño y Económica de los Broker Pay-in y Payout

Los Brokers asumen cierto riesgo al aceptar, de manera inmediata, las criptomonedas del pago y transferir los GRFT a cambio (sin esperar a que llegue la confirmación de la red de la criptomoneda en cuestión). Este riesgo se ve disminuido si tenemos en cuenta que las transacción en comercios suelen ser relativamente pequeñas y están sujetas al conjunto de autorización que valida la transacción. Por otro lado, el riesgo para los comerciantes viene mitigado por la garantía en GRFT, igual a la cantidad del pago, que genera el Broker al inicio de la transacción. La garantía la bloquea el conjunto de autorización hasta que el Broker aprueba el pago. Tan pronto como la transacción con altcoin (desde el comprador al Broker) es recibida y validada, el conjunto de autorización aprueba la transacción al comerciante y libera el pago en GRFT (desde el Broker al comerciante). El Broker puede establecer límites de autorización para diferentes cantidades y niveles de riesgo.

A cambio de este servicio, el Broker Pay-in recibirá el 0.25% de los fondos en GRFT transferidos al comerciante, mientras que los nodos participante en la muestra de autorización aplicarán una tasa total en GRFT de 0.5%.

El siguiente diagrama de flujo muestra como un Broker Pay-in de bitcoin realiza la transacción de intercambio y para aceptar el pago con bitcoin en nombre del comerciante. El comprador puede usar cualquier wallet que soporte bitcoin. El comerciante recibe el pago el GRFT.

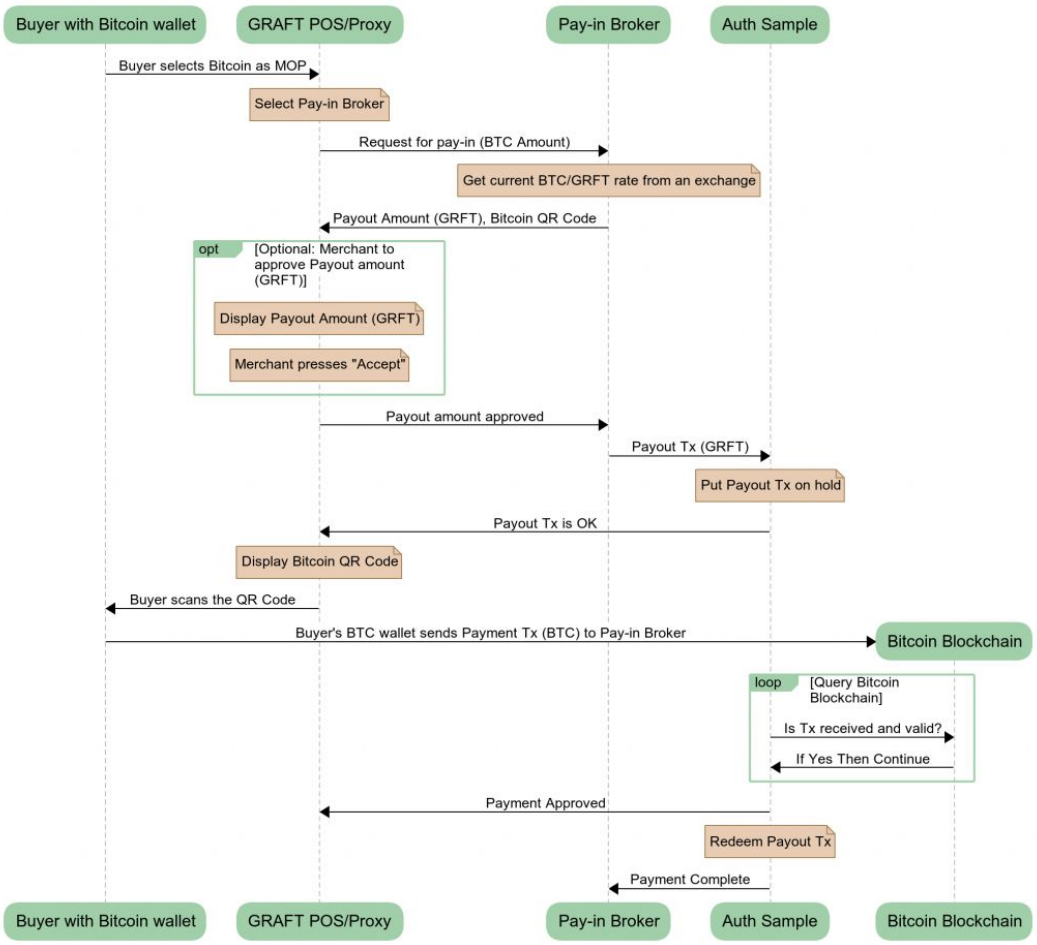

Figura 5: Flujo de la transacción GRAFT con Broker Pay-in de Bitcoin

Los Brokers Payout intercambian los GRFT enviados a la moneda en la que el comerciante quiere recibir el pago. La transacción es asimétrica -lo que significa la segunda fase de la transacción es generalmente más larga (a veces mucho más larga), porque depende del tiempo de confirmación de la moneda elegida. Para asegurarse que el Broker transfiere los fondos sin hacer ningún duplicado de gasto, el Broker tendrá que bloquear una cantidad de fondos igual a la implicada en la transacción. El conjunto de autorización bloqueará la misma cantidad en GRFT (stacking) de la cuenta del comerciante. Si el conjunto de autorización detecta (después del periodo de espera) que los fondos no han sido recibidos por el comerciante, la transacción se cancelará y el broker payout no recibirá el el equivalente en GRFT por parte del comerciante.

A cambio de este servicio, el Broker Payout retirará el 0.25% de los fondos. Además del 0.5% en tasas que los nodos participante en la muestra de autorización aplicarán.

Brokers Pay-in/Payout Duales

El mismo Exchange Broker (EB) puede operar (muy probablemente lo hará) tanto como pay-in como payout Broker. Por ejemplo, consideremos un Broker de Exchange de Bitcoins (EB) que quiere realizar ambos tipos de operaciones.

Supongamos que el Broker tiene un wallet con 0.01 BTC. El Broker recibe un petición de un comerciante para cambiar 100 GRFT a 0.01 BTC (asumiendo que el tipo de cambio en ese momento en de 0.01 BTC = 100 GRFT). El flujo de esta transacción se muestra en el siguiente diagrama.

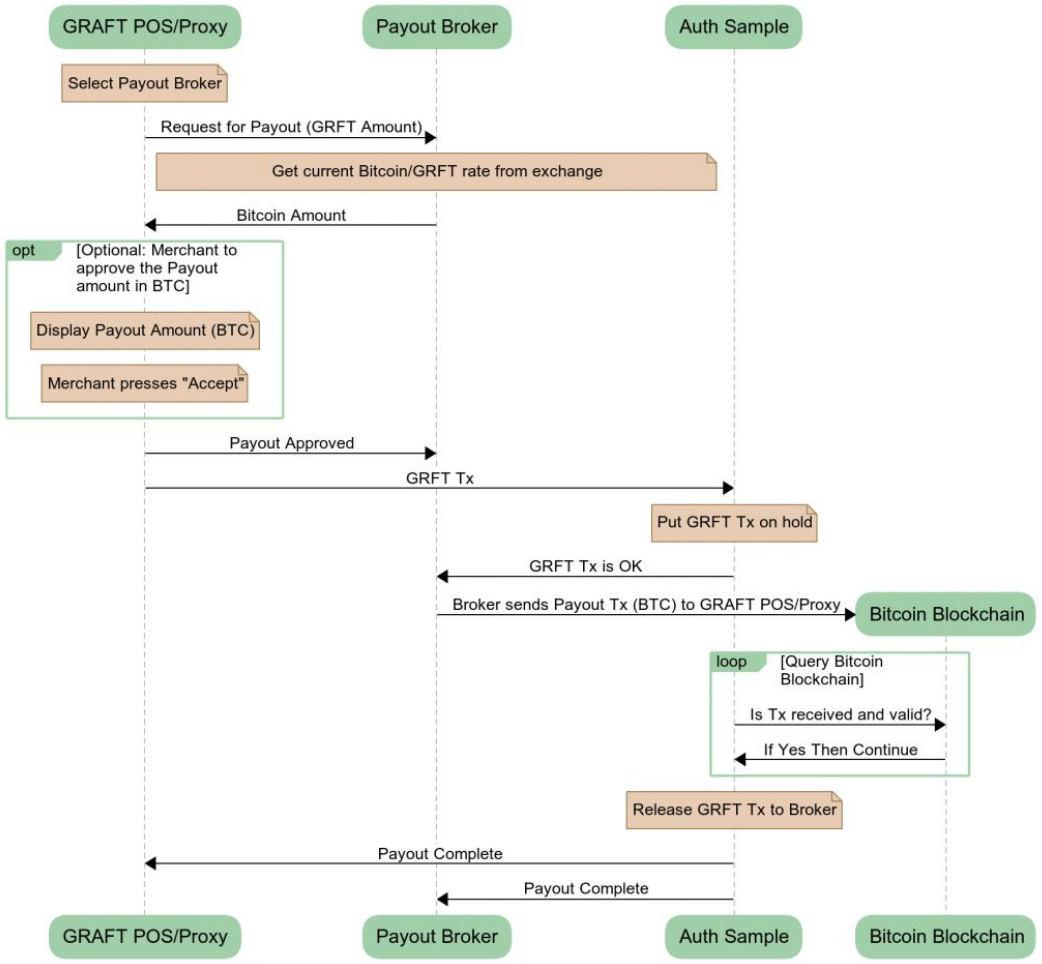

Figure 6: Flujo de transacción de pago GRAFT con Broker payout de Bitcoin

El broker acepta la solicitud y manda 0.01 BTC (menos las tasas de la red bitcoin) al comerciante, mientras, el comerciante bloquea un pago de 100.75 GRFT (100 GRFT + 0.25 GRFT tasa broker + 0.5 GRFT tasa conjunto de autorización) y lo envía al conjunto de autorización. Este retiene 100.75 GRFT y lo notifica al broker para que envíe 0.01 BTC al comerciante. Una vez la transacción no se establece (10-60 min dependiendo de la tasa enviada a la red bitcoin), los 100 GRFT se liberan y en ese momento el broker exchange tiene 100 GRFT más 0.25 GRFT en beneficio.

El broker puede cambiar a modo pay-in. Como pay-in broker, el EB recibe un petición para cambiar 0.01 BTC en 100 GRFT. El broker acepta la petición y transfiere 100 GRFT (menos tasas). Tan pronto como los fondos, en bitcoin, llegan al broker, este puede volver a modo payout otra vez, conservando sus 0.01 BTC más 0.5 GRFT de beneficio.

Asumiendo (siendo conservativos) que un ciclo pay-in/payout puede tomar 1 hora, el broker puede conseguir un **beneficio del 12% un periodo de 24 horas***, convirtiéndose en un negocio muy lucrativo para el Exchange Broker (*estimación).

Más allá del Pago a Comerciantes: DEX

El sistem de exchange brokers descrito anteriormente puede funcionar más allá del ecosistema de pago de GRAFT y convertirse en el primer exchange descentralizado a tiempo-real (real-time decentralized exchange - DEX). Teniendo en cuenta que los atomic swaps (operaciones de exchange si la intervención de terceros) están cerca de ser a tiempo real y aprovechando la capa de autorización/validación de GRAFT (la red de supernodos de GRAFT), el mismo sistema de atomic swaps se podría extender para ofrecer intercambios a tiempo real (ejemplo BTC <-> ETH).

Broker de Interchange

El Broker de Interchange trabaja sobre la aplicación del Wallet de GRAFT para facilitar el pago a un wallet de criptomoneda nativo o un POS ajeno a GRAFT que acepta cierta criptomoneda. El Broker de Interchange crea un transacción de criptomoneda regular en la red en particular y en formato nativo y la envía a la dirección de receptor. La tasa de transacción de la red, en este caso la paga el emisor, ya que la transacción no está comprendida completamente dentro de la red GRAFT. Este escenario es menos beneficioso que una transacción GRFT, tanto para el comprador como para el comerciante ya que la velocidad serà menor y las tasa la paga el comprador. Sin embargo, GRAFT las soporta y las integra para mantener la flexibilidad en cuanto a los Wallets aceptados, incluso si estos está fuera del ecosistema GRAFT.

El Broker de Interchange instantáneamente cambiará la cantidad necesaria de GRFT de la cuenta del comprador a la criptomoneda seleccionada. El comprador pagará una pequeña tasa de intercambio al Broker, que se puede incluir en el ratio de cambio.

Ejemplos de Brokers de Interchange:

- Broker de Interchange de Bitcoin
- Broker de Interchange de Ether

Broker Payout

El Broker Payout permite hacer los depósitos, en la cuenta de un comerciante, en Bitcoins, altcoins o moneda fíat local. Este mecanismo puede aplicarse de manera automática o manual.

Las tasas de Payout/Exchange, para cada depósito procesado, cambiará en función de la frecuencia de los mismo. Dependiendo del volumen de transacciones, un depósito diario puede costar significativamente menos que realizar depósitos instantáneos, ya que el Broker podrá acumular más fondos y depositarlos solo una vez, de manera que la tasa de la red sea única, comparando con las múltiples que se aplicarían, al elegir el pago instantáneo.

Ejemplos de Broker Payout:

- Broker Payout de GRAFT Tokens (“Valor Estable”)
- Broker Payout de USDT
- Broker Payout de Bank ACH (transferencia electronica)
- Broker Payout con PayPal
- Broker Payout con Bitcoin

Broker Top-Up

El Broker Top-up permite a los wallets cambiar Bitcoin, altcoins o moneda fíat local a GRFT. Utilizar este procedimiento de cambio es lo más beneficioso, tanto para el comprador, todas las tasas (incluyendo las de la red, o las de la criptomoneda deseada) las paga el comerciante, como para el vendedor, ya que el pago se aprueba instantáneamente. Para el comprador, el beneficio es obvio -no hay tasa asociadas con el pago, permitiendo el pago al comerciante con la moneda deseada aunque no la acepte. Para el comerciante, es muy importante el obtener una autorización instantánea que permita atender a más clientes a tiempo real y aceptar pagos en diferentes criptomonedas. El hecho de que todas las tasas las pague el comerciante solo sigue el método tradicional que utilizan las tarjetas de crédito/débito, que a fin de cuentas, mejora los ratios de conversión.

El Broker Top-up puede también procesar cambios, cuando se le solicita, con cantidades mayores y por ende, mejorando los rates.

Ejemplos de Broker Top-up:

- Broker Top-Up para Tarjetas de Crédito/Débito
- Broker Top-Up de Bitcoin
- Broker Top-Up para Bank ACH (transferencia electronica)

Pago a Comerciantes

Los comerciantes pueden elegir cómo quieren recibir el dinero de las transacciones realizadas en otras criptomonedas, como Bitcoin, otros tokens criptográficos, tokens de pago ("valor estable") o moneda local fíat. En este caso, el pago de la transacción podrá ser procesado por el Broker de Exchange, como parte de la transacción, o procesar el cambio posteriormente, dependiendo de la configuración preferida por el comerciante. Esto sirve para asegurar que el comerciante recibirá exactamente el dinero de la transacción menos las tasas correspondientes. El conjunto de supernodos elegirá la mejor oferta de entre los Brokers de Exchange, basándose en la combinación de características que el comerciante prefiere; mejores tipos de cambio, valor de la reputación del Broker.

Volatilidad

La mayoría de los comerciantes quieren que se les pague en su moneda local, ya que el uso de su moneda fíat (no Bitcoin y otras criptomonedas) es necesario, para poder reponer su stock, pagar sus factura o el salario de sus empleados. Además, tienen que disponer de moneda fíat para cubrir reembolsos. Por otro lado, la mayoría de comerciantes no pueden permitirse la alta volatilidad, sobretodo los comerciantes pequeños y como el token de GRAFT (GRFT) puede comprarse/venderse en los mercados, cuando se utiliza para comprar productos, su volatilidad puede ser un problema. GRAFT ha solucionado este problema a través de la implementación de las autorizaciones a tiempo real, lo que minimiza las posibles pérdidas debidas a la volatilidad de la moneda. Además, ha creado un tokens de pago de "valor estable". Las POS puede automáticamente ajustar la cantidad de la transacción a la tasa de cambio actual y pasarlo a la moneda local a través de un exchange online, inmediatamente después de finalizar la transacción.

Token de Pago (“Valor Estable”)

El token de pago es un tipo especial de token de comerciante que puede usarse para facilitar el pago a comerciantes en moneda local y de esta manera rellenar el hueco para conectar los dos mundos -transacciones con criptomoneda y operaciones con moneda local fíat. Estos tokens representan a la moneda local y se puede realizar con ellos transacciones en la blockchain de GRAFT, a tiempo real, utilizando los supernodos de la blockchain. Los tokens de pago se basan en la tecnología de tokens GRAFT para comerciantes, similar a las tarjetas regalo, recompensas y otros tipos.

Garantia de los Tokens de Pago

El objetivo principal para crear tokens de pago es proporcionar una manera fácil y fiable de que los comerciantes reciban los pagos en su moneda fíat local sin utilizar un procesador de pagos centralizado. Los tokens de pago son emitidos y mantenidos por el responsable de suscribirlos (como un banco). Cuando alguien (el broker de pago, por ejemplo) compra tokens de pago (al que los suscribe) este genera la cantidad necesaria de tokens y los transfiere al comprador por la cantidad equivalente en moneda fíat. Cuando alguien (el comerciante o el Broker que lo representa) vende tokens de pago al que suscribe los tokens, la compañía destruye los mismos y paga la cantidad equivalente al vendedor en moneda fíat local. Estos tokens siempre han de estar garantizados con suficiente fondos en moneda fíat local y su precio siempre es el mismo, referenciado a la moneda fíat. Por ejemplo 100 GRAFT.USD siempre se podrán comprar y vender por 100US$. Los tokens de pago serán generados por emisores autorizados y solo a cambio de la misma cantidad de moneda fíat local. Además, el derecho particular para generar estos tokens de pago puede, en realidad, delegarse a algún banco local o incluso a organizaciones gubernamentales.

Procesado de Pagos

Hay diferentes opciones de pago: tokens GRFT, otras criptomonedas, tokens de pago GRAFT o moneda fíat local (Tabla 2). Para cada una de estas opciones hay servicios de Brokers Payout disponibles en la red GRAFT. Cuando un comerciante selecciona el método de pago que quiere aceptar y define su preferencia para recibir los fondos (payout), la aplicación de Punto de Venta (POS) muestra al comerciante la lista de los diferentes brokers que hay disponibles -dependiendo de la identidad de comerciante y de los atributos locales- así mismo el comerciante podrá seleccionar los servicios de los brokers que más le convengan. En caso de que haya más de un Broker de pago que ofrece el mismo tipo de cambio que ha seleccionado el comerciante, la aplicación de POS automáticamente seleccionará la mejor oferta, todo esto durante el tiempo de ejecución de la transacción.

Tabla 2: Ejemplo de la variedad de métodos de pagos aceptados (Pay-in/Payout)

Métodos de pago seleccionados por el cliente	Métodos de pago seleccionados por el comerciante	Broker de Entrada	Broker de Payout
GRFT	GRFT	No (red GRAFT)	No (red GRAFT)
Tarjetas Regalo, Recompensas Lealtad, Crédito de la tienda	N/A	No (red GRAFT)	N/A
GRFT	USD	No (red GRAFT)	Broker Payout de Transferencia Bancaria
GRFT	Bitcoins	No (red GRAFT)	Broker Payout de Bitcoin
Bitcoins	GRFT	Broker que acepte Bitcoin	No (red GRAFT)
Bitcoins	GRFT	Broker que acepte Bitcoin	Broker Payout de Bitcoin
Bitcoins	USD	Broker que acepte Bitcoin	Broker Payout de Transferencia Bancaria
Tarjeta Crédito	GRFT	Broker que acepte la Tarjeta Crédito	No (red GRAFT)
Tarjeta Crédito	Bitcoins	Broker que acepte la Tarjeta Crédito	Broker Payout de Bitcoin

Tarjeta Crédito	USD	Broker que acepte la Tarjeta Crédito	Broker Payout de Transferencia Bancaria

Tokens de comerciante y VChains

Además de transacciones rápidas y de bajo coste, los comerciantes valoran mucho su marca y la fidelidad de sus clientes. Esta idea se implementa como una funcionalidad apoyada en la capa de tokens de la moneda GRAFT. Los tokens representan una parte (comerciantes) específica del uso de GRAFT y ofrecen variedad de smart-contracts, como puntos de lealtad que se acumulan y se pueden intercambiar, descuentos en tienda, aplicación de descuentos, cupones y créditos de la tienda.

Una cadena de cafeterías, puede crear, por ejemplo, un token de comerciante y ligarlo a las reglas de una promoción que provee al poseedor de un descuento en bebidas frías, en cierto momento del día (rango de horas). Dicha recompensa se ofrecería en función de la actividad del cliente, manteniendo la cuenta de las veces que ha comprado al establecimiento. Los tokens de comerciante de GRAFT proporcionan un método muy eficiente para hacer cupones, permitiendo al comerciante generar el cupón y las reglas de uso dentro del dominio de su red.

Tokens de Comerciante

Los tokens del comerciante son contratos inteligentes (smart-contracts) que permiten la creación de tokens privados del propietario. A diferencia de otros contratos inteligentes y otras plataforma de tokens, la creación de los tokens GRAFT no requieren de ningún tipo de programación y su creación es accesible a todo el mundo.

Los servicios para negocios descritos a continuación se asocian, típicamente, a la necesidad de contratar proveedores de servicios externos y con altos costos de implementación. Esto los convierte en servicios inaccesibles para pequeños y medianos negocios y muy costoso para grande empresas. Los tokens para comerciantes de GRAFT permiten a cualquier comerciante implementar estas importantes características minimizando el esfuerzo y el coste.

Tipos de Tokens de Comerciantes

Los tokens de GRAFT permitirán crear y usar su propio sistema cerrado o abierto de productos -tarjetas regalo, puntos de lealtad o créditos de tienda- en cuestión de minutos, sin ninguna inversión inicial, tasa o registros en entidades autorizadas. Los comerciante podrán vender y aceptar tarjetas regalo en sus páginas web o en sus tiendas y cambiarlos por la moneda local, otras criptomonedas o GRFT.

Todas las transacciones GRAFT, incluyendo la creación y aplicación de tarjetas regalo, puntos de lealtad y créditos de la tienda, se procesan a tiempo real utilizando una API estándar, que puede integrarse de manera rápida en la aplicación de punto de venta (POS) del comerciante.

Créditos de Tienda

Los créditos de la tienda son utilizados, típicamente, por los comerciantes para entregar el dinero de una devolución o cambio, cuando no se puede realizar en el método de pago original o la política interna de la tienda no lo permita. Los créditos de la tienda básicamente transforman las devoluciones en un cambio de manera que el comerciante no pierde al cliente ni los beneficios asociados.

Los tokens de los créditos de tienda se pueden linkar a el precio en moneda fíat, de tal manera que el cliente pueda usarlos en la siguiente compra en vez de realizar ningún pago adicional con moneda fíat local. Estos tokens, habitualmente, no caducan o tienen tiempos de caducidad muy largos, ya que básicamente reemplazan la moneda fíat.

Puntos por Lealtad

Los puntos por lealtad son un poderoso instrumento de marketing que puede atraer a clientes e incrementar las compras. Los puntos por lealtad se pueden entregar en cada compra, como un bonus puntual o de cualquier otra manera. Los puntos pueden usarse para comprar algunos items en particular o cualquier item, o convertirlos en fíat. Los puntos por lealtad pueden no estar linkados a una moneda fíat o una criptomoneda, de manera que también pueden usarse para recibir ciertos descuentos o comprar productos especiales que no están disponibles con otros métodos de pago.

Los puntos de lealtad, normalmente, tiene una fecha de expiración relativamente corta. Esto sirve para motivar al cliente a conseguir más puntos y elimina las posibilidad de acumulación de grandes cantidades, que les haría perder el objetivo original de los mismos.

Tarjetas Regalo

Las tarjetas regalo las puede generar el comerciant con el objeto de atraer más clientes. Para aumentar su impacto, las tarjetas regalo se pueden vender con un descuento (costar menos de su valor nominal). Los tokens de las tarjetas regalo, normalmente, no tienen fecha de expiración o es muy larga, ya que básicamente representan a la moneda fíat.

Los clientes pueden comprar tarjetas regalo de varios comerciante en tiendas generales, de manera online o físicamente, y pagar en moneda fíat local o criptomoneda. Las tarjetas regalo o el crédito de la tienda tiene un valor en moneda fíat garantizado por el comerciante que las genera y por la red, por lo que nunca van a perder su valor inicial nominal. Los clientes pueden utilizar las tarjetas regalo en los comercios propios y gastar su equivalente en moneda fíat local o venderlas, en cualquier momento, en algún mercado de intercambio por moneda fíat local o criptomoneda aplicando su valor de mercado.

Cupones de Descuento

Los cupones de descuento puede usarse puntualmente o el promociones de larga duración. Los cupones pueden distribuirse públicamente o individualmente, dentro de un wallet o físicamente en papel. Los cupones se pueden escanear en el punto de venta (POS) para obtener el descuento correspondiente o incluso algún producto gratuito.

Tipos de Transacciones para los Tokens de Comerciante

Create

Crear un nuevo token de comerciante (“smart-contract”). Puede hacerse a través de la aplicación de punto de venta (POS).

Renew

Renueva el token de comerciante (“smart-contract”). Puede hacerse a través de la aplicación de punto de venta (POS).

Add

Añade más tokens de comerciante a la circulación.

Issue

La aplicación de POS de comerciante envía los tokens al wallet del cliente o los imprime en papel.

Redeem

El cliente aplica los tokens de comerciante en el punto de venta del comerciante, utilizando la app del wallet o el papel impreso equivalente.

Las Tasas aplicadas a los Tokens del Comerciante

Todas las tasas de los tokes de comerciante se pagan al conjunto de supernodos de autorización.

Tasas de Transacción de los Tokes de Comerciante

Los comerciantes siempre pagan las tasas de transacción de los tokens (el cliente nunca pagará ningún tipo de tasa). Las tasas de transacción se pagarán en cada operación con los tokens, incluyendo add, issue and redeem.

Tasa de Inicialización y Renovación

La transacción inicial "Create" implica una tasa ligeramente más alta porque se asocia con la creación de un nuevo token. La tasa inicial tendrá un valor razonable para prevenir el uso masivo y el abuso ("domain squatting").

VChains

Las VChain permiten crear cadenas virtuales de tiendas, de manera que múltiples puntos de venta pueden conectarse a la misma "blockchain virtual". Por esta razón, la palabra VChain tiene varios significados: cadena virtual y blockchain virtual. La VChain sirve para crear una plataforma común de administración de tokens de comerciante y catálogos de productos.

Los comerciantes pueden crear su propia VChain privada, que será sólo accesible por este comerciante en particular y contendrá toda la información sobre sus tokens. VChain permite conectar varios puntos de venta (POS) creando una cadena de diferentes tiendas. Los puntos de venta que pertenezcan a la misma VChain pueden crear y aceptar los tokens del comerciante; utilizar un catálogo de la tienda común mantenido en su blockchain; generar informes de transacciones común y más.

Los compradores pueden utilizar la VChain para linkar múltiples wallets de manera que pueden gestionar múltiples cuentas y mover fondos de una a otra sin pagar tasas. Estas características son muy útiles para familias o las cuentas de corporaciones.

Tasas de la VChain

Habrá una tasa anual por crear una VChain y renovarla. Estas tasas son necesarias para garantizar la seguridad al procesar los contratos inteligentes y prevenir el uso abusivo. Habrá un tasa anual separada por añadir otro punto de venta o wallet a la VChain.

Todas las tasas de la VChain las recibirá el conjunto de supernodos de autorización.

Crédito Crowdfunded Descentralizado

Un ecosistema de crédito crowdfunded descentralizado engloba a consumidores de crédito (dueños de las tarjetas, compradores), suministradores de crédito, proveedores de identidad, y comerciantes (vendedores). La red GRAFT facilita la comunicación y transacción entre las partes y aplica un conjunto de normas comunes para minimizar el riesgo de fraude.

La red GRAFT conecta potenciales consumidores de crédito con proveedores que los ofrecan. Cualquiera, con un wallet de GRAFT (una app gratuita) puede pedir este tipo de créditos. Cualquiera con un wallet de GRAFT y un balance positivo puede conceder crédito. Cualquiera con un POS de GRAFT (una app gratuita), o un POS de terceros integrado con la SDK de GRAFT, puede convertirse en un comerciante. Además se añadirá un proveedor de identidad (identity provider) que se implementará como un capa extra en los supernodos GRAFT. Este proveedor en un API abierta, que ayuda a mantener el carácter descentralizado del ecosistema.

Los proveedores de crédito pueden requerir un mínimo de información sobre la identidad de consumidor para aceptar una petición de crédito, fijar un límite máximo de crédito o un límite máximo global (de múltiples proveedores), una puntuación crediticia o un mínimo de cuota de devolución, así como la frecuencia de pagos. Los consumidores de crédito pueden recibir créditos de diferentes proveedores siempre que cumplan con los requisitos del proveedor. Proveedores de identidad externos validan y confirman la información de identidad proporcionada por el consumidor, de esta manera se reduce el trabajo de validación que tendrían que hacer los proveedores de crédito y proporciona cierto grado de anonimato y privacidad consumidor. Estos proveedores de identidad, conocen la identidad real del consumidor y por lo tanto pueden saber la reputación de consumidor, a largo plazo e independientemente de la red o el proveedor de crédito. Los proveedores de crédito reciben un fracción de la tasa de cada transacción que se haga con el crédito dispuesto.

El consumidor de crédito tendrá asociado un puntuación de reputación, que se calculará, dinámicamente, basándose en el historial del mismo y los datos de la identidad que hayan sido validados por el proveedor de identidad. La puntuación inicial, antes de que se valide ninguna información o se hayan colectado datos, será 0. Cuantos más datos de identidad sean proporcionados y validados (por ejemplo, carnet de conducir, biométrica, número de la seguridad social), más alto será la puntuación inicial, lo que significa que tendrá acceso a un número mayor de crédito. Un historial de devoluciones positivas irá elevando la reputación.

Los comerciantes, simplemente, serán los receptores de las transacción realizadas por los consumidores de crédito, estando aislados de las relaciones entre lo consumidores de crédito, los proveedores de crédito y los proveedores de identidad. Esto elimina completamente el riesgo de fraude al comerciante. Los proveedores de crédito son los que asumen el riesgo potencial de fraude y los gastos, que se compensarán con los incentivos ganados en cada transacción y las tasa aplicadas al crédito. Sin embargo, los comerciantes podrán participar en el proceso, ofreciendo incentivos o incluso actuando como proveedores de crédito.

Seguridad

La seguridad es un elemento crucial en cualquier ecosistema de pago. Para alcanzar el nivel máximo de seguridad, los protocolos tienen que ser parte, intrínsecamente, del diseño del sistema y no añadirse posteriormente. La seguridad en los sistemas de pago, no solo se refiere a la seguridad de la información, sino también a la información financiera. Además de los protocolos de seguridad que son intrínsecos a sus predecesores, GRAFT plantea implementar otras mejoras para beneficiar a los compradores y comerciantes.

Disponibilidad

La red de supernodos distribuidos y siempre on-line asegura la disponibilidad de la misma. Las aplicaciones cliente se comunican con múltiples supernodos simultáneamente con el objetivo de obtener el consenso necesario para la autorización. Si uno de los supernodos del conjunto de autorización se desconecta, automáticamente será reemplazado por otro de la lista de candidatos, la cual será virtualmente infinita.

Administrador de Identidad

Transferir a los wallets la administración de usuarios puede generar un riesgo de seguridad, ya que los wallets, generalmente, son de código abierto y a, igual que pueden implementar sus propias

medidas de seguridad y estás pueden ser comprometidas. Para proteger la red y asegurar la integridad de la información de los usuarios, GRAFT implementará un servicio distribuido de proveedores de servicio de identidad (integrado en los supernodos) y disponible en los wallets como una API OpenID oAuth2.

Por supuesto, referente a la implementación de los wallets, la verificación y autentificación del usuario la llevará a cabo la red GRAFT, para prevenir el robo de identidades de usuario, spoofing, repeticiones y ataques como man-in-the-middle.

Identificación, Autentificación y Autorización

Los métodos de autentificación/autorización de las existentes criptomonedas se crearon en el ámbito de las aplicaciones de usuario, como los wallet, y en general su implementación fue tardía. En el contexto de transacciones financieras entre comprador y vendedor, donde debe establecerse cierto grado de confianza entre las partes, las regulaciones y obligaciones tienen que incluirse y los recursos han de estar disponibles, por lo que un buen sistema de autentificación/autorización es una parte crucial.

Prueba de Identidad

La prueba de identidad es un reto complicado ya que debe incluir las regulaciones diseñadas para salvaguardar la privacidad. Por lo que hacer un sistem de prueba de identidad efectivo no es trivial.

Para entender la necesidad de un sistema que verifique las identidades, consideremos un comerciante que requiere de muchos datos identificativos contrastados, para poder asegurarse que el comprador es adecuado para la compra de ciertos medicamentos o un para comprar un arma (como define el NIST Special Publication 800-63A en US). A la inversa, los clientes que compran productos de postventa, querrán asegurarse de que no compran productos robados, para ello tendrán que pedir al comerciante información verificada.

GRAFT espera que cada aplicación cliente cumpla con los estándares de verificación de identidad relevantes para la legislación local. Los supernodos funcionan como una fuente automática de verificación de identidad y detección de fraude, ayudando al comerciante (y usuario) con el cumplimiento de los pagos, asegurando la integridad de la red y la seguridad de las transacciones. Para limitar la exposición de los usuarios al compartir la información de la identidad completa, hecho no aceptable frente a algunas regulaciones (como GDPR), GRAFT cederá la información a petición de ciertos atributos en específico, como la edad y la dirección, siempre cumpliendo la normativa local.

También se plantea añadir otros apartados de metadata para poderlos compartirlos, de manera que se integren otras lógicas de negocios, como por ejemplo, recetas para medicamentos.

GRAFT permite un control multi-usuario, donde muchos usuarios pueden tener acceso a la misma cuenta de comerciante. Así mismo permite custodias multiusuario, donde dos o más usuarios podrán requerirse para desbloquear ciertas funciones, como por ejemplo transferir fondos de una cuenta.

Puntos de Reputación: Iluminando la Oscuridad

GRAFT ha decidido utilizar una estrategia basada en las estimación de riesgo para procesar las transacciones. Cada participante en la red tendrá asignada una puntuación basada en su reputación, que dinámicamente se irá actualizando en función de los nuevos datos que se obtengan. Los compradores, comerciantes y propietarios de supernodos, pueden agregar, opcionalmente, datos de su identidad en sus cuentas, con el objetivo de mejorar su reputación. Esta característica ha sido implementada para no comprometer la no trazabilidad de las transacciones.

El sistema de puntos por reputation ayuda a los participantes del ecosistema a tomar las decisiones con más información y sin comprometer la seguridad y la privacidad. Por ejemplo, los comerciantes pueden tener en consideración la reputación de un comprador, a la hora de fijar los límites de fondos durante el procesado de una autorización instantánea. De la misma manera, un comprador puede revisar la reputación de un comerciante, antes de hacer un pago por cualquier objeto que no se vaya a entregar inmediatamente. Ambos, comprador y comerciante, pueden consultar los puntos de reputación de cualquier nodo de la red que esté disponible, así mismo, los supernodos proxy pueden usar estas puntuaciones para decidir con qué Broker de Exchange se hace cierta transacción.

Otro elemento importante del uso de una puntuación por reputación es que aligerara el contexto de crédito peer-to-peer, donde la reputación incluirá puntuaciones referentes a los históricos por cumplimiento de los pagos de créditos.

Los supernodos participan en la monitorización, cálculo, actualización y validación de la reputación de los compradores, comerciantes y otros supernodos. Los puntos se calculan usando ciertos algoritmos analíticos, especialmente diseñados para devolver una puntuación de 0-100, fácilmente entendible y de la que no se puede extraer ningún tipo de información acerca del número, cantidad, tiempo o naturaleza de la transacción.

Soporte a Consumidores, Resolución de Disputas y Seguro de Pagos

Uno de los principales escollos que se encuentran las criptomonedas o los tokens criptográficos, para poder ser adoptados por los consumidores y comerciantes, es la ausencia de una autoridad central o de un responsable de negocio que pueda ayudar a responder cuestiones o problemas técnicos o de implementación. Así mismo, es importante que el ecosistema sea capaz de solucionar posibles problemas en una transacción ya sea en caso de error humano, actividad fraudulenta o problema técnico. Obviamente, esta falta de soporte está causada y justificada por la naturaleza descentralizada, anónima e independiente de pago criptográfico, pero una buena razón no ayuda a resolver los posibles problemas. Las comunidades open-sources solucionan esto con un sistema de soporte gratuito para sus productos open-source: Linux OS, soportado por Redhat y MySQL soportado por Oracle, son dos ejemplos donde se proporciona soporte a nivel comercial pero a productos open-source gratuitos.

Para facilitar la adopción de sistema de pagos GRAFT, la Fundación GRAFT proporciona soporte al consumidor gratuita y servicio de resolución de disputas entre usuarios de GRAFT. Los comerciantes con un volumen de transacciones alto, obtendrán soporte, a tiempo real, 24/7 y asistencia para la resolución de disputas. La Fundación GRAFT y/o los Brokers de Exchange deberán asegurar pagos hasta un equivalente de 100 USD para compensar a los consumidores o comerciantes en caso de que se pierdan sus fondos por fraude o problemas técnicos.

Aplicaciones de Usuario

Todos las aplicaciones de usuario GRAFT, son aplicaciones cliente que no guardan copia de la blockchain, ni procesan ninguna transacción. La aplicaciones de usuario utilizan una API remota para comunicarse con los nodos de GRAFT, lo cuales están on-line y se encargan de minar los nuevos bloques de transacciones y procesar peticiones RTA.

Los usuarios que requieran de un alto nivel de control de la privacidad, anonimato y disponibilidad (por ejemplo un gran comerciante o una organización secreta) deberán operar su propio supernodo, incluso multiples supernodos, que exclusivamente se van a comunicar con sus aplicaciones cliente, enviar mensajes a otros supernodos, hacer autorizaciones offline y mantener los GRAFT necesarios para operar y generar créditos de tienda, tarjetas regalo y puntos de lealtad.

Las apps de consumidores incluyen:

- Punto de venta para comerciantes móvil y de escritorio que permite aceptar pagos con los tokens GRAFT, Bitcoin, altcoin y tarjetas de crédito/débito, así como configurar la retirada de los fondos (payout) en Bitcoins, altcoins o moneda fíat local. Puede usarla tanto el comerciante como el comprador.
- Wallet para escritorio, móvil o una extensión del navegador Chrome, sirve para hacer el pago en tokens GRFT, Bitcoin, altcoin y tarjetas de crédito/débito (utilizando los Brokers de Exchange), también se puede utilizar para enviar y recibir transferencias tokens GRAFT.
- La SDK de GRAFT permitirá la integración con la mayoría de los puntos de venta de comerciantes para procesar transacciones online o en tiendas físicas. GRAFT incorporará un tarjeta inteligente como método de pago. Además la tarjeta almacenará una firma biométrica de usuario y un conjunto de datos secretos, esto se puede utilizar como método de autentificación en los terminales. La Fundación GRAFT y los Brokers de Exchange darán soporte a las tarjetas inteligentes y a los lectores de las mismas.

Además de aceptar transacciones orientadas al consumidor (B2C), GRAFT también aceptará transacciones de negocio a negocio (business-to-business - B2B) integradas en el flujo existente para negocios. Este flujo implementará transacciones simples, como recibir cobros de crédito en función de ciertos términos (p. e., Neto 30, 60, 90), hasta complicados flujos como liquidaciones de facturas adeudadas y contabilizarlo como parte de las transacciones generales, para distribuir los fondos según los méritos y ventas a clientes.

GRAFT también encaja bien en el espacio de los IoT, de manera que un sistema IoT cobre o pague automáticamente por los servicios que está ofreciendo. Un ejemplo podría ser una tienda física que solicitará un camión de mercancías basándose en los niveles de inventario determinados por el sistema de sensores del almacén.

Conclusiones

GRAFT nunca existiría sin sus predecessors. GRAFT se basa en ideas, principios y tecnologías introducidas y probadas por los creadores de otros tokens de utilidad criptográfica. Usando las más recientes tecnologías desarrolladas por las comunidad criptográfica y aplicando nuevas soluciones para el procesado de transacciones y la seguridad, GRAFT podrá competir con los métodos de pago tradicionales y los procesadores de pago centralizados.

References

1. Bitcoin. https://bitcoin.org/en/.

2. Dash. https://www.dash.org/.

3. Bitpay. https://bitpay.com/.

4. GRAFT Definition. Merriam-Webster (2017). https://www.merriam-webster.com/dictionary/graft#h2.

5. What Is GRAFTing? - Definition & Methods. Study.com (2017). http://study.com/academy/lesson/what-is-grafting-definition-methods-quiz.html.

6. IOTA. https://iota.org/.

7. Bitcoin, Ethereum, Litecoin, Dash, Monero Avg. Transaction Fee historical chart. Bitinfocharts.com. https://bitinfocharts.com/comparison/transactionfees-btc-eth-ltc-dash-xmr-sma7.html#1y.

8. PayPal. https://www.paypal.com/us/webapps/mpp/merchant-fees.

9. NIST Special Publication 800-63. Revision 3. Digital Identity Guidelines. NIST (2017). https://pages.nist.gov/800-63-3/sp800-63-3.html.

10. CryptoNote. https://cryptonote.org/.

11. Top Seven Ways Your Identity Can Be Linked to Your Bitcoin Address. 99 Bitcoins. https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/

12. Median Confirmation Time. Blockchain. https://blockchain.info/charts/median-confirmation-time?timespan=30days.

13. Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures. Version 3.2 PCI Security Standards Council (2016). https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf.

14. What are Open Loop and Closed Loop Gift Cards? Shelley Hunter. GiftCards.com. https://www.giftcards.com/gcgf/open-loop-versus-closed-loop-gift-cards.