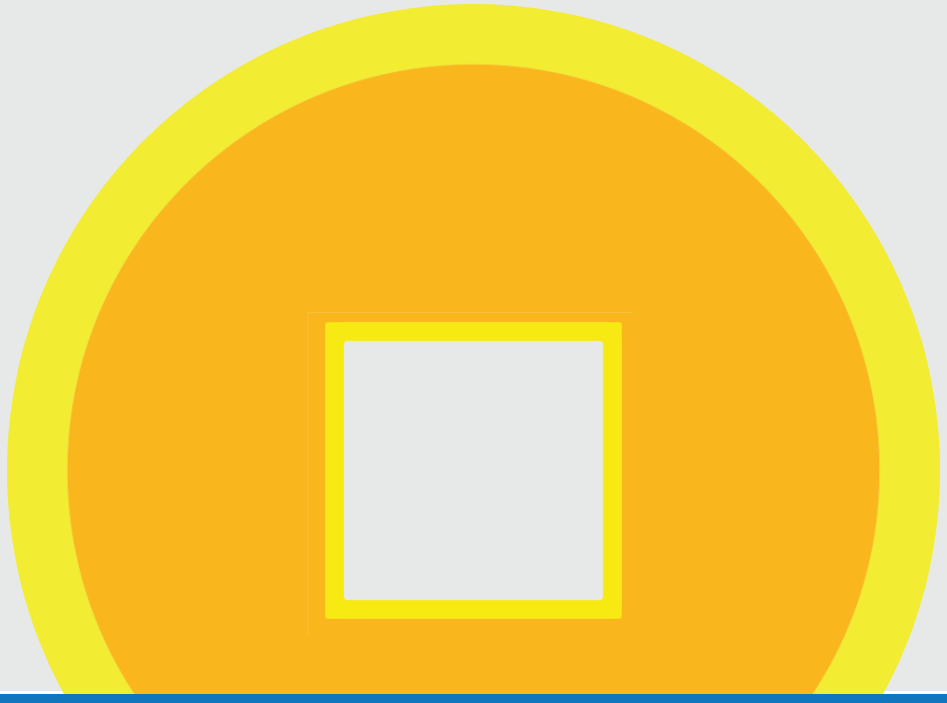
FLASH Whitepaper

La tecnología de la Cryptomoneda para desarrollar pagos más rápidos



Resumen

FLASH es una plataforma basada en blockchain que permite a los usuarios y los desarrolladores aprovechar esta tecnología para redes sociales, sitios web, blogs y sitios de comercio electrónico. Esta limitado solo por la imaginacion del usuario, pero al mismo tiempo se crea un campo de juego nivelado adjunto donde cada contribucion es bastante valorada por la comunidad de una manera totalmente transparente

1 de Septiembre, 2016

Contenido

Introducción

El principio fundamental de FLASH es que todo el trabajo y/o contribucióna la red debe ser valorado por la comunidad de manera objetiva. Permitiendo el proceso de libre mercado en función de crear un mecanismo a lo cual todas las formas de trabajo puedan ser reducidas a un común denominador.

Lo que esto significa es que cualquier forma de trabajo, ya sea por un tiempo valioso del usuario, su atención, una habilidad especial establecida como herramientas de desarrollo, varias formas de energía (es decir, procesamiento) y la moneda, pueda ser valorada en tiempo real, basados en la oferta y demanda del mercado para una tarea o contribución especifica.

Las formas de contribuir a la comunidad sólo están limitadas por la imaginación y la valoración colectiva de la misma. En su núcleo FLASH es sencillo de entender, completamente transparente, sin reglas y con condiciones que no son difíciles para trabajar. Dado que FLASH tiene un sistema de solución muy simple y rápido (<2 segundos!), Y construido en la escalabilidad (~ 25.000 transacciones por segundo) que tendra muchos casos de uso.

Conformidad Legal

FLASH fue diseñada desde el principio para ser legalmente compatible a través de cada fase de su vida. Mientras que las monedas de FLASH fueron entregadas inicialmente a los primeros donantes y no tienen ninún valor de redención, ya que las monedas se mueven en los intercambios, es posible que tengan algún valor en el futuro. Para proteger nuestros usuarios, existen políticas y procedimientos que estamos poniendo en práctica hoy, para asegurarnos de que todo se haga legalmente.

Los 900 millones de monedas FLASH se distribuyeron a los probadores y los donantes después de la pre-venta. No se permitieron participantes de Estados Unidos. Otro millón de monedas que se utilizaron para las pruebas internas, a los donantes se les proporcionó monedas para propósitos de prueba - ninguna de las monedas fue retenida por los desarrolladores. Las monedas tenían un valor de cero al momento de su distribución y el proyecto no mantiene un inventario de las monedas en absoluto. Una fundación se ha establecido en Liechtenstein para ayudar a promover y dar soporte a Flash, las donaciones son bienvenidas.

Como contribuir y dar

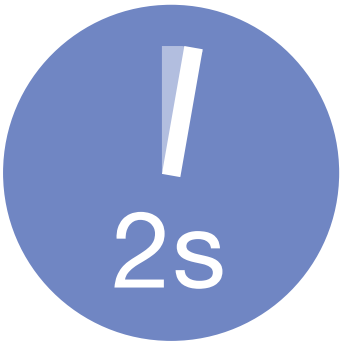
Flash ha sido diseñado pensando en el único modelo económico exitoso y probado, el sistema de libre mercado. Ha habido muchos intentos fallidos en el pasado para replicar en parte este mecanismo o eludirlo completamente mediante la creación de sistemas de votación y los complicados acuerdos de propiedad. FLASH es único, ya que el mercado es el único árbitro de valor que es libre de fluctuar basado puramente en las fuerzas de oferta y demanda en la comunidad. La unidad fundamental de la cuenta en la plataforma Flash es la criptomoneda FLASH. Aunque esperamos que habrá muchas maneras diferentes de contribuir, limitadas solamente por la imaginación.
Aquí hay algunos casos de uso:

En resumen, todo lo que requiere seguridad de extremo a extremo, asentamiento en tiempo real, cierto transporte de valor o información, y una pista de auditoría permanente son condiciones ideales para flash. Cuando desarrollas una aplicación con FLASH, puedes construir también tu pago en la aplicación.

- Registrarse para la cuenta con su correo electrónico (necesario para la cuenta)
- Opcionalmente agregar y validar su teléfono celular
- Almacenar hasta 40 bytes de datos de una transacción
- Al igual que un botón de visitante para recompensar al propietario de un blog / sitio web fuente de publicidad para el usuario y para apoyar a los escritores pagados por el anunciante
- Registro y validación de la propiedad de los medios de comunicación digitales o bienes físicos
- Pago por contenido
- Registro y validación de la propiedad de los medios de comunicación digitales o bienes físicos
- Un sello de correo electrónico para validar el remitente y compensar el receptor

FLASH Descripción de Arquitectura

FLASH es una PREMINED, PERMISSIONED BLOCKCHAIN, Basada en el Bitcoin original y la cadena de bloques de Litecoin, además ha sido optimizada para casos de uso específico como:



1. Alto rendimiento. Las transacciones se asientan en menos de 2 segundos y capaces hoy de 25.000 transacciones por segundo.

2. De alta seguridad. Una serie de fallos de seguridad con la cadena de bloques bitcoin original se han parcheado. La plataforma ha sido mejorada con encriptación Curve25519 de curva elíptica. Todas las comunicaciones entre la cartera y blockchain están en túnel seguro CE con curva ZeroMQ (http://curvezmq.org/).

3. Escala comercial con capacidad de rendimiento. La plataforma FLASH ha sido probado con éxito en 25.000 trans / seg. En base a los análisis de laboratorio estamos seguros de que la plataforma puede ser optimizado a más de 100.000 trans / seg en un futuro próximo, si surge la necesidad.

4. Una cartera Web con funciones fáciles de usar, incluyendo el historial de transacciones, solicitudes FLASH, contactos, autenticación de 2 factores y recuperación de claves.

Para alcanzar estos parámetros críticos para el uso a gran escala por millones de participantes, la plataforma FLASH se basa en los principios de la cadena de bloques operada por la comunidad. La plataforma aprovecha la empresa existente con tecnologías de control descentralizado, base de datos, la inmutabilidad y la creación y el movimiento de los activos digitales. FLASH ha pre-minado 900 millones de monedas que han sido totalmente regalados.

El sistema de FLASH se basa en tres plataformas de nivel de aplicación. Como la mayoría de de los sistemas estándar que tenemos: **Interfaz de usuario, Comunicaciones y la lógica de negocio.**

Los niveles de interfaz de usuario permite al usuario final disponer de la aplicación para interactuar con el sistema de FLASH. La plataforma de FLASH aprovecha HTML5, CSS3 y JavaScript en los navegadores, sin extenciones, que permite el soporte de navegadores sin problemas. Hemos desarrollado y adoptado todas las tecnologías que permiten a JavaScript adoptar funciones comunes entre C/C++ y Java. Además el sistema de FLASH usa Twitter Bootstrap para proporcionar un marco de respuesta Web que funcione en cualquier dispositivo.

Los **Niveles de comunicación** permiten un túnel seguro entre el nivel de interfaz de usuario y el nivel de almacenamiento sin la necesidad de OpenSSL. Los protocolos seguros utilizados por el FLASH incluye:

HTTP / Web Sockets utilizando la curva ZeroMQ y Libsodium. Nuestro trabajo en el área de la comunicación también significa que somos los primeros en adoptar nuevos protocolos de seguridad que se ejecutan sobre el uso de JavaScrpt HTML5

El nivel de almacenamiento permite que todos los flujos de la operación y sistemas de redes sean operados dentro de esta capa. Este nivel es responsable de ejecutar algoritmos propios para almacenar en la base de datos distribuida, con la potencia de FLASH

- Los Cluster de intercambios de claves es un conjunto de servidores que proporcionan el intercambio de claves o búsqueda de claves para cada transacción en el sistema FLASH, como un directorio. Debido a la naturaleza de los pares de claves criptográficas en el sistema transaccional de Bitcoin, cada transacción requiere una busqueda de direcciones de carteras públicas. El Cluster key también permite el intercambio de divisas, mensajes, el fideicomiso público y otro flujo de información. El motor de mensajes ha activado el registro y la notificación de todas las actividades relativas a la comunicación del monedero mediante la notificación por correo electrónico SendGrid. El servidor de claves utiliza NodeJS, ZeroMQ, Redis y MySQL.

- La aplicación Flash Wallet es una aplicación de servidor que permite que todas las carpetas FLASH sean utilizadas por diferentes navegadores Web. La aplicación Wallet Flash tiene la mayoría de las funcionalidades de la carpeta Bitcoin e intercambio de claves. Es una billetera virtual usando como conectores protocolos Web HTTP. Además, billeteras QT con código fuente se han proporcionado sin minería para Windows, Mac y Linux. Las billeteras QT con nodos de minería estan disponibles para los titulares de GovNode cualificados.

- El proceso de servidores API de servicios web se encarga de converitr e indexar todas las transacciones de FLASH desde la interfaz web y enviarlas en cadena de bloques. Esto acelera significativamente las transacciones, ya que cada monedero no tiene que sincronizar todos los bloques de la cadena del servidor local. Todas las carteras pueden compartir la cadena de bloques en el servidor API blockchain. Esto mejora el rendimiento de las transacciones de manera significativa debido a que la latencia de la red se ve reducida para cada sincronización de la billetera. Otro aspecto muy importante de la tecnología es la reducción significativa en la posibilidad de "duplicar el gasto". Todas las transacciones de bloques de cadena se indexan y son procesados y validados a travéz del servior de una manera similar a Bitcoin.

- La cadena de bloques FLASH se ha basado en la tecnología Litecoin. Se han realizado una serie de modificaciones significativas. La configuración se ha cambiado con el fin de agilizar las transacciones a los bloques en cadena. Todas las monedas han sido previamente extraidas y la minería se ha restablecido al grado mínimo de dificultad. La cadena de bloques se fija detras de los cortafuegos en multiples centros de datos seguros. Un consenso tradicional junto con la detección de intrusos, se usa para que la cadena de bloques sea tomada por un atacante. El proposito de la cadena de bloques de FLASH es reemplazar la base de datos transaccional tradicional con una base de datos de almacenamiento en red e incluir una estructura de datos de seguridad a los extremos finales.

- Las tarifas de transacción se establecen en 0.001 FLASH por transacción, esta tarifa puede ser elevada o bajada en el futuro, dependiendo de ls nodos distribuidos.

FLASH Estructura de la Cuenta

Las cuentas en FLASH se almacenan en un servidor centralizado (CAS).

Cada cuenta CAS tiene los siguientes datos:

id: ID de la cuenta.

email: cuenta de correo

role: Según sea la autoriazación.Ejem.: USER o ADMIN

privateKey: clave privada de cifrado (cifrada por la contraseña del usuario)

publicKey: EC criptografía de la clave pública..

sc1: Procedimiento de recuperación del usuario (cifrada por las respuestas de seguriad del usuario).

sc2: Parte del servidor utilizada para la recuperación.

sc3: Participación del administrador en caso de que sc1 no pueda recuperarse.

Además de los perfiles de usuario descritos que se almacenan en el servidorde claves FLASH, la información incluye: nombre para mostrar, avatar,país...que varía de una aplicación a otra.

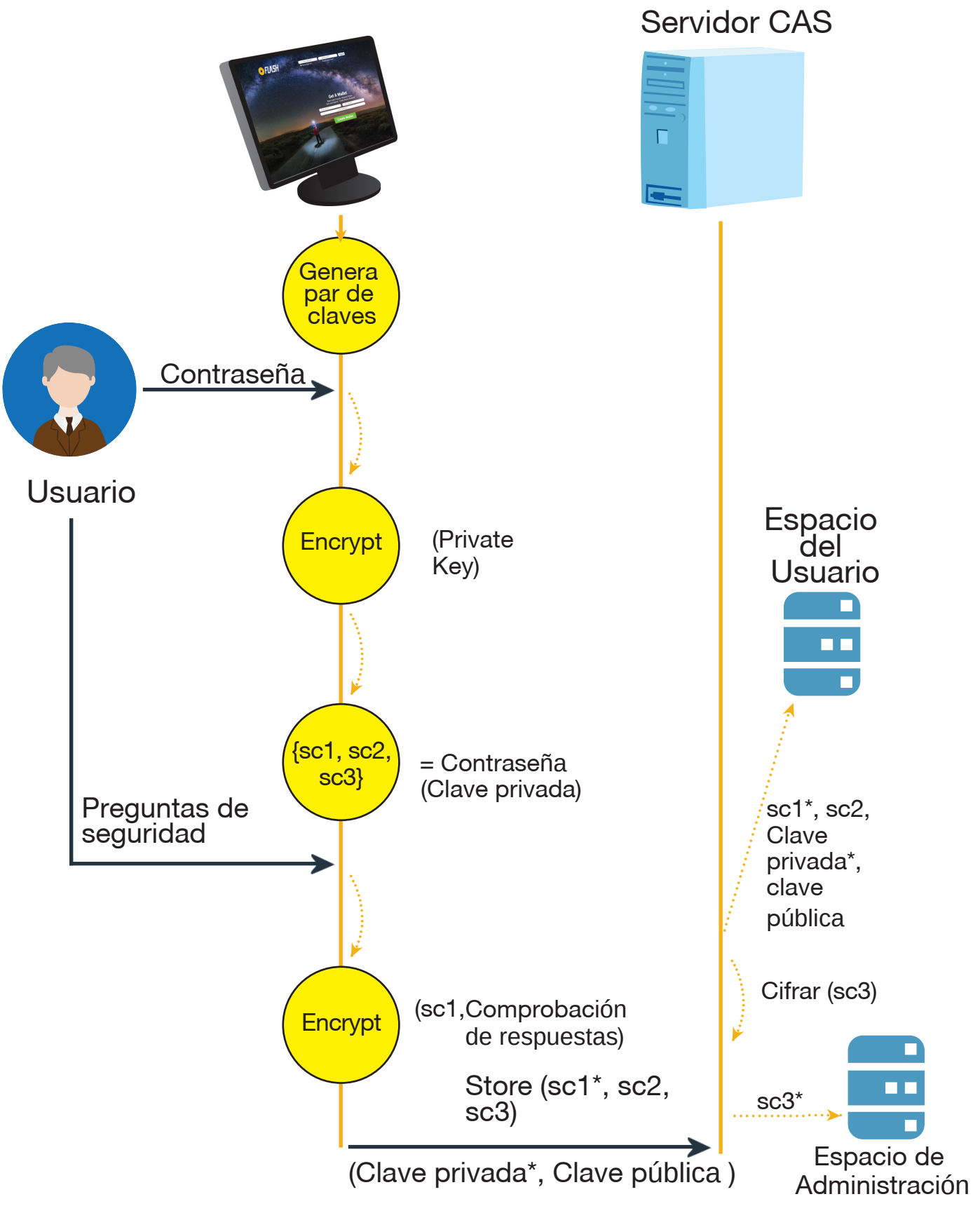
Generación de claves FLASH, almacenamiento y recuperación.

Generación de claves al registrarse

El par de claves cifradas se genera en el cliente al registrarse. La clave privada se cifra mediante la contraseña del usuario. Las claves de recuperación también se generan a partir de la clave privada. Después que el usuario responde las preguntas de seguriad, las respuestas se utilizan para cifrar sc1

Almacenamiento de claves

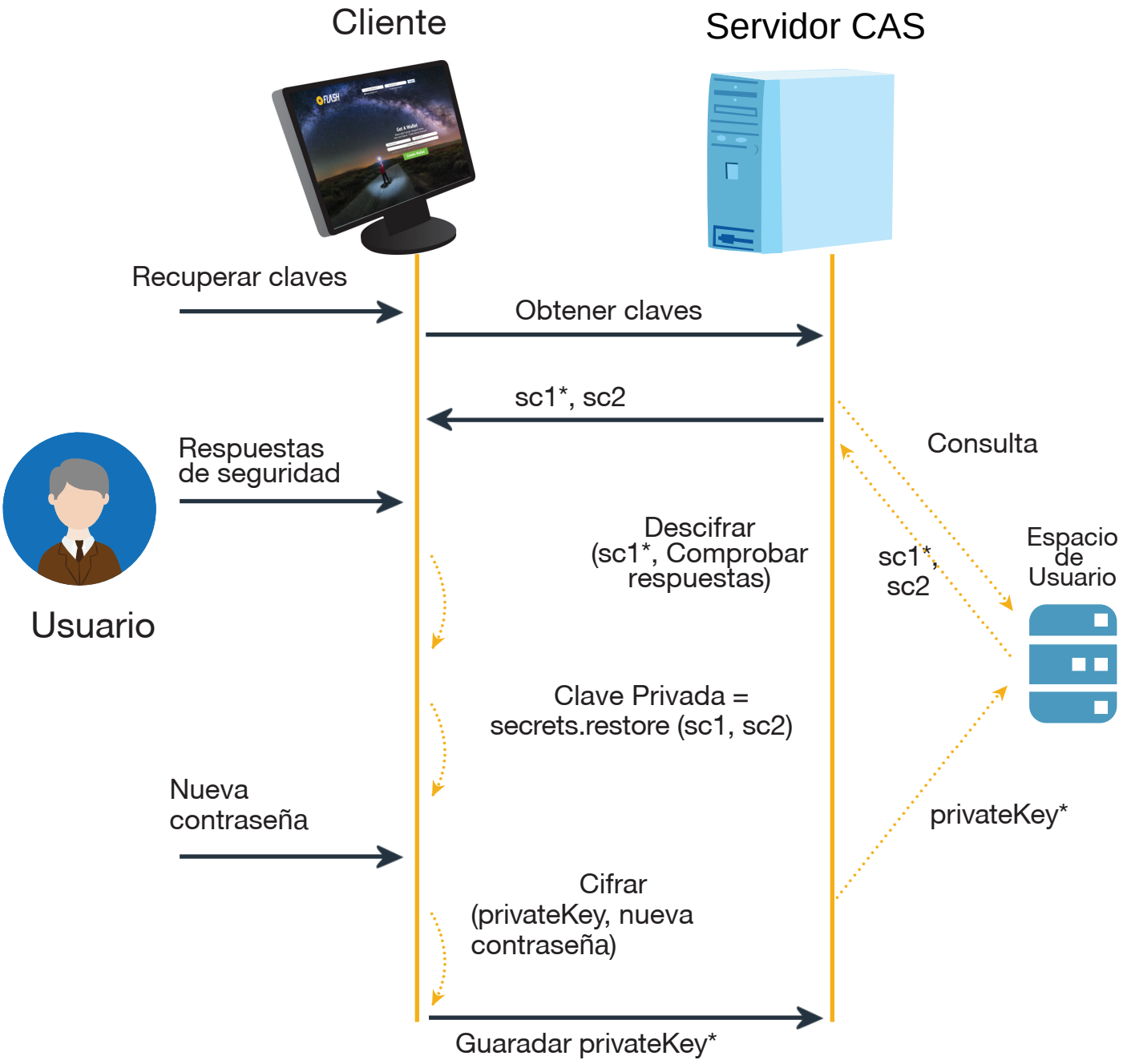
El servidor almacena lo siguiente: La clave privada encriptada, clave pública, sc1 encriptado, preguntas de seguridad, sc2 y sc3 (que luego se cifra por separado por el administrador).



Recuperación de claves

El proceso de recuperación se activa automáticamente por el usuario. Despúes de verificar el correo electrónico, el cliente recibe SC1 y SC2 cifradas y las preguntas de seguridad. Al responder las preguntas de seguridad correctamente la respuesta se utiliza para descifrar SC1. De SC1 y SC2, se restaura la clave privada. A continucación, el usuario tiene que proporcionar una nueva contraseña e iniciar el proceso de protección y almacenamiento de claves siguiendo el mismo paso que el anterior

El usuario también puede elegir un modo super-seguro en el que el servidor almacena una única sc. Cuando se activa el modo de recuperación, el usuario debe proporcionar su parte para combinar con la parte del servidor. Si el usuario pierde el SC1 (dado el proceso de registro), entonces nadie puede recuperar su contraseña. Por lo tanto la participación obligatoria del usuario en el proceso de recuperación garantiza la seguridad de la parte del usuario, así como la contraseña.



FLASH Suministro de monedas

El suministro de monedas FLASH es generado previamente y se limita a 900 millones de monedas. Todas las monedas se entregaron a los donantes en las preventas.

FLASH Distribución de monedas

TODAS LAS MONEDAS HAN SIDO DISTRIBUIDAS. CON FLASH, HAY:

1. Inflación cero - No se crearan monedas nuevas.

2. No hay mineria - no se emiten monedas.
   Todas las monedas existentes han sido distribuidas a la comunidad.

3. Ningún fondo desarrollador - Eso solo motiva al abuso y el amiguimismo.

4. Una comunidad de personas afines que donan sus monedas para apoyar proyectos valiosos que apoyan FLASH.

¿Qué ocurre despúes de que las monedas de nueva emisión se quedan?

Las personas que deseen monedas para sus proyectos o negocios, necesitarán inducir a otros usuarios para darles monedas FLASH alternativamente, en el futuro podría potencialmente comprarlos de los usuarios o en una bolsa a un precio de mercado.

FLASH Blockchain

FLASH tiene la versión blockchain de Litecoin para uso como un sistema de red de almacenamiento distribuido. Un número de modificaciones significativas al código se han hecho con el fin de abordar las deficiencias de las redes totalmente decentralizadas:

- **Latencia de conexión** - Bloques de sincronización entre los nodos relentiza drásticamente la velocidad de validación de transacción (doble gasto). FLASH es una red cerrada con el tubo de red de un 1 Gbs garantizados entre los nodos. Debido a que usamos la blockchain como una base de datos de red transaccional de la latencia de la red se garantiza que sea mas bajo de 200 ms (ventana de tiempo de propagación)

- **Rendimiento** - Dos factores que determinan el rendimiento de la Blockchain son: La sincronización de bloques y el bloque de minería. FLASH utiliza servidores de caché e índice para sincronizar los nodos y reiniciar el algoritmo de minería para el factor de menor dificultad. Debio a que tenemos la red de confianza entre los nodos, no hay necesidad de seguir aumentando el grado de dificultad de la minería para el proceso de verificación de bloques. FLASH proporciona una solución única para asegurar la integridad de datos de almacenamiento de red distribuida.

- **Riesgo de seguridad** - Bloquear la minería hace vulnerable a la red Blockchain distribuida de manera abierta. FLASH Blockchain no esta abierta al público para extraer o manipular el blockchain por la ventaja computacional.

El cifrado de extremo a extremo

Con el fin de garantizar un único punto de debilidad, el diseño del sistema de seguridad y de todas las funciones de cifrado se tiene que hacer desde el monedero (nodo del cliente)...como resultado, las transacciones están codificadas por la clave pública del destinatario que a su vez están inscritos en la cadena de bloques de FLASH. Esta metodología protege de intrusos y de la obtención de datos cifrados en las bases de datos FLASH. Para que un atacante o intruso decifre la información debe poner en peligro el sistema y romper su curva elíptica.

La Cryptografía (ECC) permite algoritmos en cada tecla. Incluso si alguien tuviera una computadora cuántica y fuese capaz de romper la ECC para decifrar una transacción que supera con mucho, la posible ganancia. Para un equipo promedio se tardaría mas de 100 millones de años de esfuerzo de cálculo. Por lo tanto el costo de crackeo de la ECC en cada transacción excede con mucho el rendimiento potencial.

Tokens pre-minados

Hemos extraido aproximadamente 900 millones de monedas que seran distribuidas principalmente de forma gratuita para desarrolladores y usuarios.

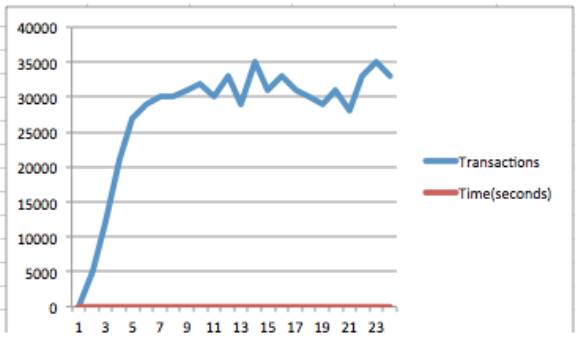
Blockchain API

Un protocolo que permite a la aplicación WEB comunicarse con la red FLASH Blockchain. Todas las transacciones se han indexado en la capa API Blockchain para comprobar la validez de cálculo y acelerar las búsquedas de transacción tales como registros dobles de verificación, gastos y de transacción.

Minería

FLASH posee la piscina de la minería para toda la Blockchain FLASH. A los efectos de la ampliación y redundancia de los sistemas de almacenamiento de datos de la red. FLASH utiliza suficiente potencia de CPU/ Servidores, para configurar una red de autoridad para todo los servidores de bloqueo del nódulo. Debido a que hemos de restablecer el grado de dificultad de minería a casi 0, el tiempo de validación por bloques es varias órdenes de magnitud más rápido que el Litecoin típico o el procesamiento de transacciones de Bitcoin. La minería sera designada por los nodos de gobierno, que a su propia discreción determinaran las tasas de transacción.

Escalabilidad y Rendimiento



Resultados de referencia para FLASH corriendo en un i7 processor Brix cube a 3.9 Ghz con 16GB RAM y 240GB SSD.

Los bloques de cadena de FLASH han sido optimizados para un rendimiento y escalabilidad muy alta. La liquidación final con blockchains es un concepto basado en el número de confirmaciones por varios nodos en la cadena de bloques. Una moneda no puede ser reutilizada hasta que llegue a los asentamientos suficientes para tener confianza muy alta de la autenticidad de la transacción y la aprobación por la red. FLASH se ha optimizado para el tiempo de ajuste final de menos de 2 segundos, incluyendo la capacidad para volver a enviar la moneda

El rendimiento es una consideración importante, ya que una moneda en escala, llegara a "romper hitos". FLASH ha sido probada y optimizada para procesar.

25.000 transacciones por segundo y con pequeñas modificaciones podrían llegar fácilmente a 100.000-200.000 transacciones por segundo. Para poner esto en perspectiva, el pico de carga de red VISA es de aproximadamente 50.000 tras/seg y el pico de Paypal es en los bajos miles de transacciones por segundo.

APENDICE

Wallet Webservice API

Crear Cuenta

Name: create_unverified_account
Description: Create unverified account (need to verify via email)
Request params: name, email, ip, callbackLink, g_recaptcha_response (Google recaptcha response)
Response: {rc: Number}

Establecer contraseña y verificar correo

Name: set_password
Description:
Request params: password, privateKey (encrypted private key), publicKey, token
Response: {rc: Number}

Obtener una sesión Token (sso)

Name: get_session_token
Description:
Request params: idToken, resource
Response: { rc: Number, profile : Object { sessionToken: String } }

Compruebe la sesión Token (sso)

Name: check_session_token
Description:
Request params: sessionToken, resource
Response: {rc: Number, profile: Object{username: String, email: String} }

Inicio de sesión (sso)

Name:
Description:
Request params: email, password, ip, resource
Response:
Success: {rc: Number, profile: Object{email: String, display_name: String, gender: String, ...} }

Actualizar cuenta

Name: update_account
Description: Update user profile
Request params: display_name, gender, profile_pic_url, about, timezone ...
Response: {rc: Number }

Ver Perfil

Name: get_profile
Description: Get user profile
Request params: {}
Response: {rc: Number, profile: {username: String, email: String, display_name: String, profile_pic_url: String …} }

Establecer PIN

Name: set_pin
Description: Set PIN
Request params: pin
Response:
Success: {rc: Number}

Verificar PIN

Name: check_pin
Description: Check if PIN is correct
Request params: pin
Response:
Success: {rc: Number}

Cabiar PIN

Name: change_pin
Description: Change the PIN
Request params: old_pin, new_pin
Response:
Success: {rc: Number}

Obtener los detalles de contacto

Name: get_contact_detail_by_email
Description: Get contact details by email
Request params: contact_email
Response:
Success: {rc: Number, profile: {username: String, email: String, display_ name: String, gender: String, profile_pic_url: String, …} }

Ver perfil

Name: get_profile
Description: Get user profile
Request params: {}
Response: {rc: Number, profile: {username: String, email: String, display_ name: String, profile_pic_url: String …} }

Ver usuarios

Name: get_users_by_uid
Description: Get users information by user id
Request params: [‘user1’, ‘user2’, …]
Response:
Success: {rc: Number, accounts: [account1, account2, …] }

Obtener lista

Name: ros_get
Description: Get contact list of a user
Request params: {}
Response:
Success: {rc: Number, roster: {total_subs: Number, subs: [], …}

Operación de lista

Name: ros_op
Description: operate roster, where operation could be REQUEST, APPROVE, REMOVE
Request params: op, from, to
Response:
Success: {rc: Number}
Notification: notify to related users

Crear Monedero

Name: create_flash_wallet
Description: Create a new wallet
Request params: idToken, wallet_secret
Response:
Success: {rc: Number, wallet: {passphrase: String, wallet_id: String, address: String }

Buscar Monedero

Name: search_wallet
Description: Search for wallet by keyword, to send money to
Request params: start, size, term
Response:
Success: {rc: Number, criteria, wallets: [wallet1, wallet2, ..], total_wallets: Number }

Obtener mis monederos

Name: get_my_wallets
Description: Get my wallets (currently only support 1 wallet)
Request params: {}
Response:
Success: {rc: Number, my_wallets: [], total_wallets: Number}

Añadir Transacción

Name: add_txn
Description: Push transaction to blockchain and add transaction log
Request params: receiver_id, amount, currency_type, receiver_public_address, transaction_id, memo, request_id, transaction_hex (signed)
Response:
Success: {rc: Number, id: String}
Notification: notify to the recipient about the new transaction

Obtener Log de Transacciones

Name: get_txns
Description: Get transaction log of current user
Request params: date_from, date_to, order, start, size
Response:
Success: {rc: Number, txns: [tx1, tx2, ...], total_txns: Number}

Obtener transacciones por ID

Name: get_transaction_by_id
Description: Get transaction detail by id
Request params: transaction_id
Response:
Success: {rc: Number, txn: {...} }

Crear una Transacción sin firmar

Name: create_unsigned_raw_txn
Description: Create a unsigned transaction to be signed by the owner later
Request params: from_address, to_address, amount
Response:
Success {rc: Number, transaction: {...} }

Obtener detalles de transacción

Name: get_transaction_details
Description: Get transaction details from blockchain
Request params: transaction_id
Response:
Success: {rc: Number, transaction: {...} }

Obtener balance

Name: get_balance
Description: Get wallet balance from blockchain api
Request params: {}
Response:
Success {rc: Number, balance: Number}

Añadir solicitus de dinero

Name: add_money_request
Description:
Request params: to, amount, note
Response:
Success: {rc: Number, id: String }
Notification: notify to the requested user

Recibir Solicitudes de dinero

Name: get_requests
Description:
Request params: date_from, date_to, status, start, size, type
Response:
Success: {rc: Number, money_requests: [req1, req2, ...], total_money_reqs: Number}

Marcar un solicitud de dinero como aprobada

Name: mark_accepted_money_requests
Description:
Request params: receiver_id, request_id, note_processing
Response:
Success {rc: Number}

Marcar un solicitud de dinero como rechazada

Name: mark_rejected_money_requests
Description:
Request params: receiver_id, request_id, note_processing
Response
Success {rc: Number}

Marcar un solicitud de dinero como cancelada

Name: mark_cancelled_money_requests
Description:
Request params: sender_id, request_id, note_processing
Response
Success {rc: Number}

Marcar un solicitud de dinero como leída

Name: mark_read_money_requests
Description:
Request params: receiver_id, request_ids: Array<{request_id, sender_bare_uid}>
Response
Success {rc: Number}

Blockchain APIs (en progreso)

Empujar transacción a la blockchain

Name: push_transaction
Description: push a transaction raw format (hexa encoding) to the blockchain
Request params: transaction hex
Response: {}

Enviar token

Name: send_token
Description: send token (coin) to a wallet identified by public address
Request params: to_public_address, amount, message
Response: {}