UNA CRIPTOMONEDA CENTRAL RAPIDA, LIVIANA Y PORTATIL.

Sam Segura
Francia

admin@xiropht.com
www.xiropht.com

Escrito: 18/03/2019
Actualizado: 07/09/2019
Versión: 1.4

El Whitepaper puede modificarse durante la fase de prueba de Xiropht y también puede modificarse después de la última fase si se implementa una actualización significativa en su protocolo operativo.

Resumen

Xiropht es una **criptomoneda centralizada**.

Los pagos se procesan y verifican en un solo punto central. **Xiropht** está completamente desarrollado bajo el lenguaje de programación C #, creado y desarrollado por **Microsoft**. Las herramientas de **Xiropht** no están limitadas a los sistemas de Windows y pueden ser portadas a otros sistemas como **Linux**, **Android** y otros mediante tecnologías externas y válidas como **Xamarin y Mono.**

Varios puntos proporcionan acceso a la red del **Blockchain** centralizado. **Xiropht** tiene como objetivo demostrar que la minería puede protegerse en tiempo real contra **ASIC** sin pasar por **Soft / Hard Fork** y sin la necesidad de enviar actualizaciones significativas a los usuarios o a puntos de red importantes de la criptomoneda, como los Nodos Semilla y los Nodos Remotos para mantenerlos compatibles y sincronizados con la red.

El propósito también es proponer la posibilidad de que las transacciones enviadas puedan recibirse de manera rápida, ya que solo están vinculadas a la actividad natural de los usuarios en el envío de las transacciones y no a la operación de minería. Además, es posible vincular cada cantidad contenida en un saldo de billetera total a un número de identificación del bloque minero para garantizar que la cantidad exista y no se duplique.

Una de las funciones principales es también proporcionar el saldo total del usuario vinculado a una lista de montos de minería masiva sin la necesidad de sincronizar todos los datos del **Blockchain**, al mismo tiempo que se proporciona el historial a los usuarios, mientras se cifran las transacciones realizadas para que sólo sean leidos por los usuarios interesados en una transacción específica.

Sin embargo, es posible realizar una bifurcación (copia) de la cadena de bloques sin obtener el código fuente de esta, a pesar de estar centralizada gracias a la historia completa de los bloques y las transacciones realizadas sin descubrir el monto total en la billetera de un usuario.

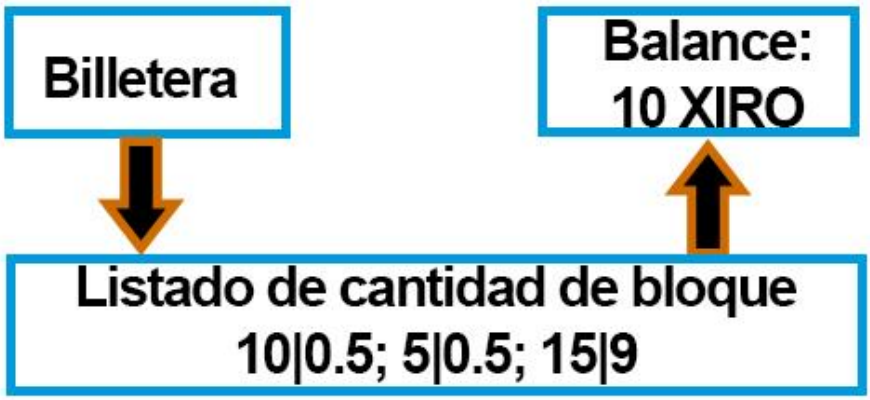
El usuario debe proporcionar su dirección de billetera y su clave pública para que el sistema pueda descifrar las transacciones relacionadas para obtener el saldo de los usuarios, es decir, teóricamente, puede obtener la cantidad total de dinero operada por la minería sin obtener el saldo de sus usuarios si intenta hacer una copia de la **Blockchain.**

Así que puede comenzar desde el punto de su copia y dar la bienvenida a los nuevos usuarios sin penalizar a los usuarios existentes que podrán obtener los montos de sus transacciones gracias a su dirección de billetera y clave pública si ese es su deseo y que su copia sea correcta y consistente con toda la información.

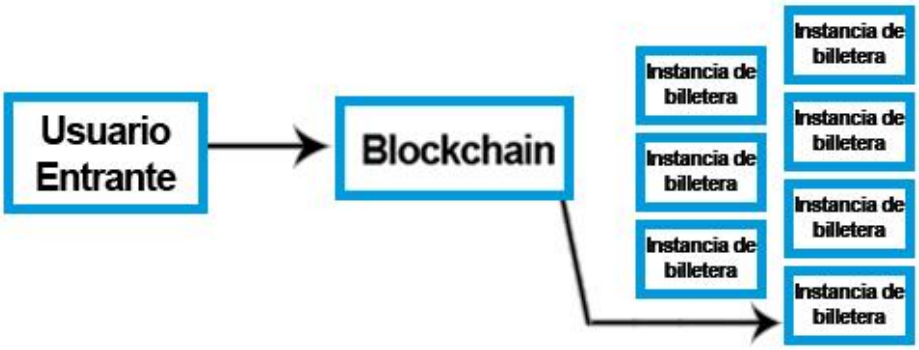
A continuación, revisamos las características de **Xiropht**

I. Características del Blockchain y su red.

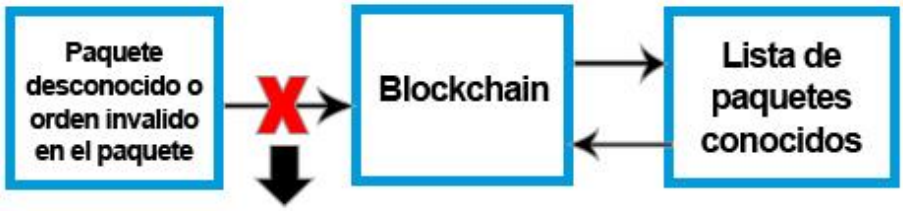
1. La cadena de bloques calcula el saldo total del usuario mediante una lista de bloques en contraste con una cantidad única que podría ser fácilmente falsificada o comprometida por un error. Vincula cada cantidad que forma un saldo de billetera a una ID de un bloque obtenido durante una operación de minería, esto permite reducir la cantidad de este bloque y enviar una parte de él mientras mantiene su ID. Esto también permite no obtener una cantidad de bloque mayor que la recompensa del mismo al extraer una. Cada cantidad de bloque debe corresponder al importe total de la recompensa de este último cuando se repone en uno durante la verificación de los importes.



2. La **Blockchain** crea una instancia para cada billetera existente para que pueda procesarse en tiempo real y conectarse más fácilmente para realizar una transacción. Sin embargo, el usuario tendrá que usar su **código PIN** para desbloquear la instancia a la que está conectado.

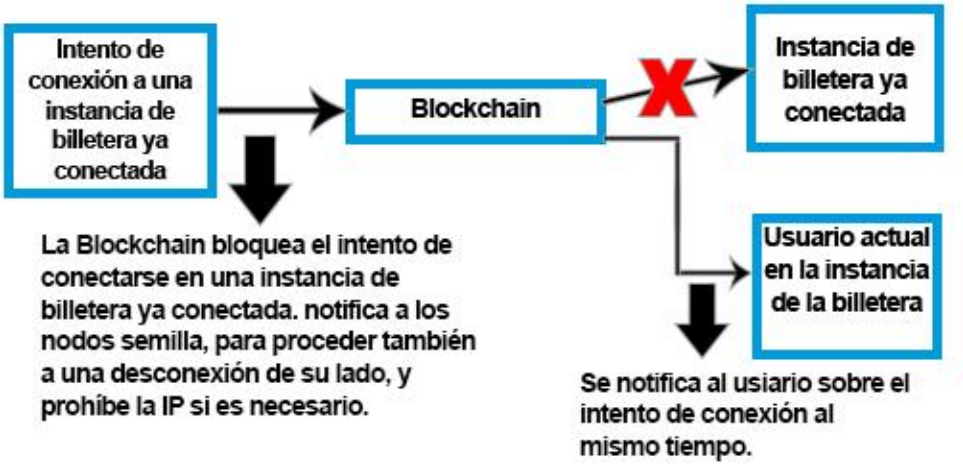


3. La **Blockchain** solo procesa comandos de paquetes estáticos, es decir, cualquier tipo de paquete recibido que no sea compatible no está permitido como válido y provoca una desconexión intencional del que lo envía y también la posibilidad de ser prohibido a través de los **Nodos Semilla**. Esto también es válido si los paquetes enviados no se envían en el orden de los procedimientos estáticos.

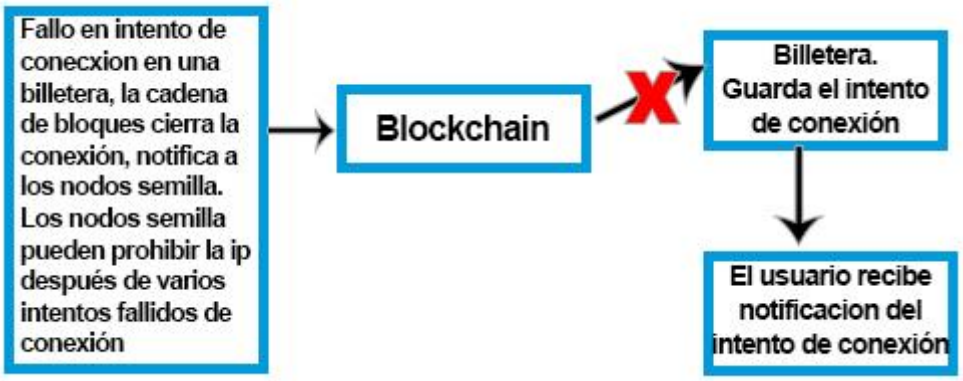


Paquete desconocido.
Resultado de inundación a una desconexión forzada, se envía una notificación a los nodos semilla para proceder a la prohibición.
Desconexión de su lado también

4. La **Blockchain** solo permite una conexión activa por billetera y tiene la posibilidad de informar al usuario cuando se realiza un intento de conexión durante el inicio de sesión de los usuarios, incluso si el intento no es completamente válido. De hecho, el solo enviar un intento de conexión específico en una dirección de monedero hace que se envíe automáticamente una notificación a la conexión activa.



5. El **Blockchain** también rastrea cualquier intento de inicio de sesión no válido de una dirección de billetera válida e informa al propietario de los intentos no válidos cuando se conecta a su billetera con credenciales válidas.

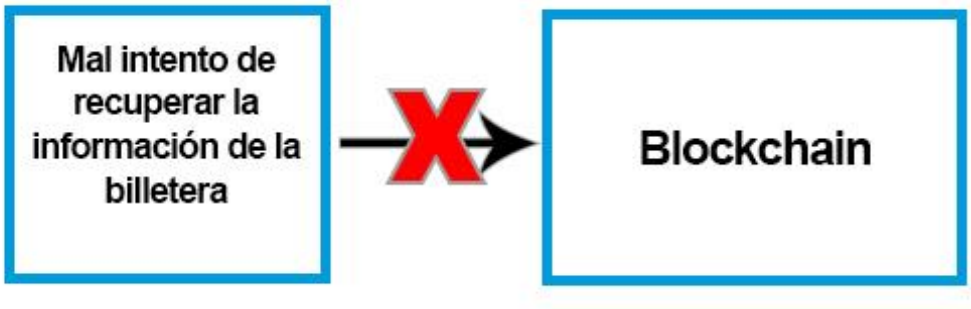


6. El **Blockchain** no tiene la capacidad de recuperar la información de una billetera del usuario sin proporcionar la clave privada asociada con él. También tiene el derecho de notificar a los **Nodos Semilla (Seed Nodes)** en caso de repetidos intentos no válidos para causar una prohibición temporal de la IP. La dirección relacionada con el usuario que intenta crear un Bruteforce en ella. Por otra parte, el tamaño de una clave pública / privada tiene diferentes tamaños y es único, para mejorar aún más la seguridad del sistema.

   - Número mínimo de caracteres de una clave pública / privada: 128
   - Número máximo de caracteres de una clave pública / privada: 288
   - Número mínimo de caracteres de una dirección de billetera: 48
   - Número máximo de caracteres de una dirección de billetera: 96

- Número de posibles combinaciones mínimas de caracteres en diferentes claves públicas / privadas: 62 ^ 128
- Número de posibles combinaciones máximas de caracteres en diferentes claves públicas / privadas: 62 ^ 288
- Número de posibles combinaciones mínimas de caracteres en las direcciones de la cartera: 62 ^ 48
- Número de posibles combinaciones de caracteres máximas en las direcciones de la cartera: 62 ^ 96

(Esta limitación se puede cambiar en tiempo real si es necesario).



En caso de problemas, el usuario con su clave privada puede generar nueva información, obtendrá un nuevo código PIN y una nueva clave privada.

Desde la versión 1.1 del sistema de restauración de **Xiropht**, la seguridad se ha incrementado en comparación con las técnicas de detección de redes locales.

En la billetera del lado del usuario:

a. Genera un código QR que represente la clave privada de la billetera y su nueva contraseña de billetera para su instancia en el **Blockchain**.
b. Convierta la imagen del código QR en Base64String y cifre ésta con AES256bit con su clave privada actual.
c. Envíe el código QR encriptado con su identificación única de billetera (número de identificación) o una pequeña parte del final de la clave privada (para la versión antigua de la clave privada).

Del lado de la blockhain:

a. Busca la clave desde la identificación única de la billetera o desde la pequeña parte de la clave privada recibida e intente descifrar el código QR cifrado.
b. Convierte el código QR cifrado en un mapa de bits y compare la representación con las informaciones reales de la billetera.
c. Genera una nueva clave privada y un código PIN, encripta cada nueva información con el cifrado AES de 256 bits con la clave privada anterior del usuario

7. El **Blockchain** que se comunica con el usuario de una billetera encripta los paquetes a través de la información que solo el usuario tiene como una sola clave de encriptación, pero también con un sistema para modificar el contenido de la clave en tiempo real con el usuario. La información que respecta a él usuario conoce de antemano la clave de cifrado para que no se vuelva a intercambiar. La composición de esta clave de cifrado se modifica ligeramente en un intervalo irregular de tiempo para mejorar la seguridad y modificar la apariencia general de los paquetes de red entre el **Blockchain** y el usuario.

8. El **Blockchain** funciona, por seguridad, cuando el usuario envía una transacción, bloqueando cualquier otro intento de enviar una transacción hasta que la transacción pendiente esté en la lista. Esto evita, por ejemplo, que el usuario envíe por error varias veces la misma transacción.

9. El **Blockchain** calcula el tiempo de recepción de una transacción enviada en relación con la actividad global de las transacciones pendientes, este sistema hace posible no sobrecargar el **Blockchain** sino también dar una estimación en tiempo real del tiempo de recepción de la transacción antes de que se envíe. Este sistema se aplica a todos los tipos de transacciones, ya sea a partir de una recompensa de bloque minero, una recompensa de sincronización otorgada a los hosts del Nodo remoto, una transacción regular o una transacción anónima.

10. **Blockchain** ofrece la posibilidad de ocultar su dirección de billetera a la persona que recibe una transacción a través de una opción disponible en el software oficial de billetera Xiropht. Esta opción incluye una transacción de tarifa fija de 0.00001000 XIRO por transacción, esta tarifa se envía a la

dirección de la billetera de un desarrollador Xiropht o probador oficial que se selecciona al azar del lado de **Blockchain**.

11. **Blockchain** impone una tarifa de transacción obligatoria de una cantidad mínima de 0.00001000 XIRO, esta cantidad de transacción influye en el tiempo de recepción de la transacción. El tiempo mínimo para recibir una transacción será de un segundo.

    Este monto se enumera para su inclusión en el saldo de tarifa total acumulado por **Blockchain**. Este saldo se utiliza para pagar hosts de nodo remoto y crear nuevos bloques para extraer una vez que se alcanza el suministro máximo

12. **Blockchain** impone una tarifa de desarrollo obligatoria del 5% en cada bloque extraído. Esta cantidad de monedas se almacena para nuestros Fondos de desarrollo para facilitar la lista de nuestras monedas en los intercambios.

13. **Blockchain** solo proporciona contenido útil sobre transacciones y bloques para sincronizar de modo que sean rápidos de obtener y livianos, con tamaños prácticamente constantes de aproximadamente 0.4 KB por transacciones, 0.23 KB por bloques mientras se encriptan los intercambios dentro de la red. La parte no encriptada de las transacciones disponibles para la sincronización tiene los siguientes elementos:

    i. - Número de identificación único del remitente
    ii. - Cantidad falsa enviada
    iii. - Cantidad de impuesto de transacción falsa
    iv. - Número de identificación única de la fecha de envío del receptor
    v. - Hash de transacción.
    vi. - Fecha de recepción.
    vii. - Altura del bloque al enviar la transacción.

    Esto permite que los Nodos de Semilla y los Nodos Remotos clasifiquen las transacciones según los números de identificación únicos de los usuarios de una billetera, por lo que los usuarios solo tendrán que sincronizar los datos que corresponden a su billetera.

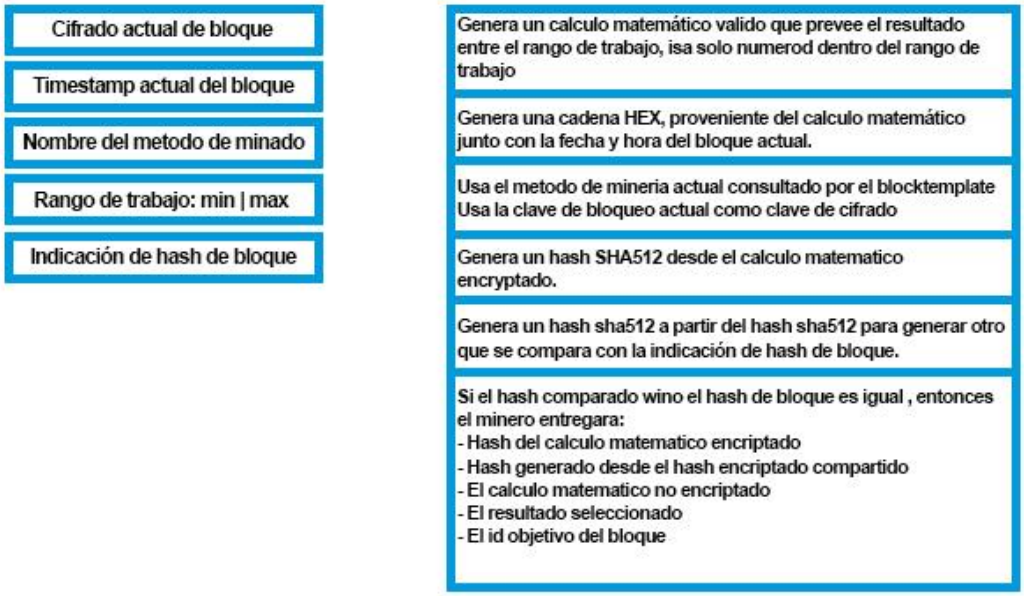
Este número de identificación único entre cada billetera se obtiene solo a través de la conexión entre el usuario de una billetera y **Blockchain**. El número de identificación utilizado por las transacciones que utilizan la opción de anonimato es diferente del utilizado para las transacciones básicas, a fin de no establecer un vínculo entre las transacciones enviadas, para ocultar su dirección de billetera a quien recibe la transacción y la básica.

14. La **Blockchain** tiene un sistema de copia automática de datos dentro de su propio servidor y también un sistema espejo dispuesto en varios servidores externos que permite la redundancia de los datos en tiempo real para asegurar la **Blockchain** en caso de problemas.

15. La **Blockchain** tiene un sistema de inflación que aumenta la oferta máxima todos los días. La inflación aumenta el máximo entre +0.1 XIRO a +0.5 XIRO máximo. El sistema de inflación está vinculado a las actividades comerciales. Por ejemplo, si la actividad del día actual es más alta que la del día anterior, habrá una inflación cercana a +0.1 XIRO, si la actividad comercial es menor, entonces la inflación estará más cerca de +0.5 XIRO.

16. La **Blockchain** emite la Blocktemplate actual y el último método de cifrado de minería en tiempo real a los mineros, lo que permite que Xiropht se actualice en tiempo real para bloquear la minería de ASIC. Se supone teóricamente que, al cambiar la cantidad de bucles de cifrado, la clave de cifrado y el tamaño de cifrado requerido, este método bloqueará efectivamente la minería ASIC. Los algoritmos de cifrado utilizados por Xiropht son: AES y XOR. También se acepta que Todos los programas de minería puestos en línea tienen la función de solicitar el último método de minería en tiempo real, así como la plantilla de bloque actual para mantenerse actualizado sin realizar una actualización completa del programa. La vida de un bloque es dinámica y se basa en 60 segundos. Aumenta según la dificultad. Cuanto mayor es la dificultad de la minería, mayor es la vida útil del bloque actual. Si se alcanza la vida, el bloque actual se renovará y la dificultad disminuirá. Aunque se está extrayendo el mismo

bloque, como si fuera un bloque nuevo, la dificultad disminuye. Este proceso continúa hasta que se encuentra la solución para el bloque.



17. Los nodos de semillas sirven como un punto de acceso seguro y proxy, y son las únicas herramientas que pueden acceder a la red del programa **Blockchain**. con una lista de direcciones IP de Nodos de Semilla pre registrada de antemano en el programa de **Blockchain** y también en su firewall.

18. Los nodos de semillas sirven como caché de datos para los bloques obtenidos en la operación de minería y las transacciones realizadas por los usuarios al distribuirlos de la misma manera que la **Blockchain** a los usuarios. Los nodos remotos también sirven como un punto de acceso a estos datos y pueden ser alojados por usuarios externos.

19. Los nodos de semillas no tienen la capacidad de leer los intercambios entre los usuarios que usan una billetera y la **Blockchain**. Los intercambios de datos se cifran de antemano con los datos creados durante la creación de la billetera y se entregan al usuario solo una vez y no ya no es enviado por la **Blockchain** o por el usuario.

20. Los nodos de semillas no tienen ningún derecho sobre la **Blockchain**. Solo tienen la capacidad de pasar datos cifrados entre los usuarios y la

Blockchain; sin embargo, pueden servir como un firewall para la **Blockchain**. La **Blockchain** comunica ciertos errores de paquetes recibidos a los Nodos de Semilla para desconectar o prohibir las direcciones IP si es necesario.

21. Los nodos de semillas enumeran públicamente los nodos remotos alojados y administrados por terceros si siempre están sincronizados de forma idéntica a los nodos de semillas. Los nodos de semillas tienen la capacidad de verificar los nodos remotos para determinar la integridad del nodo remoto. Para que los nodos de semillas puedan verificar los hosts de los nodos remotos que desean ser listados, el host del nodo remoto DEBE configurar su sistema para que sea visible en la red con puertos apropiados abiertos y enrutados a Internet público. La configuración de un Nodo Remoto para que el Nodo Semilla lo incluya como público es responsabilidad del operador del nodo. Se sugiere abrir y enrutar los puertos 18000-18002 a la dirección IP pública del sistema de nodo remoto. También es necesario que el tiempo de respuesta y la conexión del nodo remoto respondan rápidamente a los nodos semilla. Los hosts de nodo remoto que tienen un ancho de banda limitado pueden aparecer en la lista, pero los nodos semilla pueden prohibirlos o no usarlos. Se recomienda un mínimo de 10 kb / s. Este sistema también permite recompensar a los anfitriones de los nodos remotos que participan para ampliar la red de emisión de los datos que se sincronizarán gracias a un porcentaje deducido de las tarifas de transacción recopiladas durante 24 horas mediante la comunicación de un informe del tiempo preciso de sincronización entre los Nodos de Semilla y los Nodos Remotos en la **Blockchain**.

22. Los nodos remotos permiten redistribuir los datos de sincronización de la cadena de bloques obtenidos con los nodos semilla y distribuirlos a los usuarios de billetera sin pasar por la red centralizada.

23. Los nodos remotos se pueden enumerar en una lista de nodos de semillas que les permite ser utilizados por los usuarios usando una billetera, deben sincronizarse de la manera más precisa en comparación con los datos puestos en línea por los nodos de semillas, esta funcionalidad permite la participación de nodos remotos en la distribución de datos de la **Blockchain**.

24. Los nodos remotos pueden ordenar las transacciones sincronizadas por un número de identificación único de la dirección de la billetera del usuario

para devolver el número de transacciones mantenidas por el usuario y sus datos.

II. Token Network de la Blockchain (Beta).

(El sistema Token Network está en Beta y debería recibir actualizaciones para aumentar su seguridad)

La Red Token de la **Blockchain**, es un sistema que permite recuperar información de billetera / enviar transacciones sin mantener una conexión abierta y en línea 24h / 24 solo por solicitud HTTP GET cifrada con un esquema preciso de solicitud de respeto.

El token requiere ser usado antes de su vencimiento de 10 segundos y solo se puede usar una vez. Cada solicitud GET requiere incluir también la fecha y hora de envío dentro de la solicitud encriptada, es decir, permitir una fecha de vencimiento de los paquetes encriptados antiguos enviados.

Para recuperar una información o enviar una transacción:

1. Información requerida para recuperar un nuevo token válido:
   - En la clave de cifrado:
     → Dirección de la billetera + Clave pública de la billetera + Contraseña de la billetera actual
   - En la solicitud cifrada:
     → ask-token | vacío | fecha del paquete.
   - Solicitud enviada:
     → TOKEN- RED | dirección de billetera | solicitud encriptada
   - Solicitud recibida (por ejemplo):
     {"resultado": “4egdSyb464Az1jly8Z9ts8xHbWCL7e9ViyEA3JjIajwu3sRdFdRvVRKm4wms5DJm", "versión": "2.0.0.1"}
     clave de un encadenado recibida en el interior de la billetera recibida. Dirección + Clave pública de Walet + Contraseña de billetera actual

2. Información requerida para usar un token válido:
   - La clave de encriptación de la solicitud:

→ Dirección de la billetera + Clave pública de la billetera + Contraseña de la billetera actual

- En la solicitud encriptada:

→ ask-wallet-balance | token-recibido | fecha del paquete. (Por ejemplo)

- Solicitud enviada:

→ TOKEN-NETWORK | dirección de billetera | solicitud encriptada - Solicitud recibida (Por ejemplo): {"resultado": "gFsal9bHEIUJC3aXlovMRSatUnxxc5cnbaTQYPC++Xs=", "versión": "2.0.0.1"}

- La clave de descifrado del resultado recibido encapsulada dentro de una cadena json: → Dirección de billetera + Clave pública de Walet + Contraseña de billetera actual + token anterior utilizado

3. Solicitud disponible que se puede enviar a la red de tokens:

TOKEN-ASK: Solicite un nuevo token.

TOKEN-ASK-BALANCE: solicite información del saldo actual de la billetera.

TOKEN-ASK-WALLET-ID: solicite la identificación única de la billetera de la billetera.

TOKEN-ASK-WALLET-ANONYMOUS-ID: solicite una identificación de billetera anónima única de la billetera.

TOKEN-ASK-WALLET-SEND-TRANSACTION: solicite el envío de una transacción.

También cada solicitud incorrecta notifica al usuario de la billetera. Token Network respeta el sistema de conexión único de **Blockchain**, es decir, no se puede enviar una solicitud de token si el objetivo de la billetera está conectado y notificar al usuario. Los nodos de semillas también reciben una notificación de un «paquete no válido» para proceder a los desterros

III. Bifurcación blanda / dura de Blockchain.

Cuando se configura una bifurcación suave / dura en la cadena de bloques Xiropht, el código fuente de la versión anterior se publicará en línea. La versión actual implementada durante el Soft / Hard Fork no se pondrá en línea, por las siguientes razones: Por seguridad, cada Soft / Hard Fork cambia los procedimientos de seguridad y los mejora para que siempre sean diferentes de

las versiones anteriores. Para incluir nuevas características para mantener un distancia a la competencia. El Libro Blanco puede modificarse durante la fase de prueba de Xiropht y también puede modificarse después de la fase de prueba si se implementa una actualización significativa en su protocolo operativo. Sin embargo, es posible llevar a cabo una bifurcación de la **Blockchain** con la sincronización datos que se pueden obtener completamente con Nodos de semilla y Nodos remotos. Entonces, puede volver al punto de su copia sabiendo cuántos bloques de minería se han encontrado y, por lo tanto, obtener la cantidad total en circulación. Luego, con el historial completo de transacciones, cuando su **Blockchain** obtiene la dirección de la billetera y esa clave pública, puede descifrar las transacciones de esta dirección para identificar las cantidades enviadas y recibidas, y recomponga así el saldo total de usuarios que desean usar su Fork. Con este método, puede lanzar su Fork al público mientras continúa sirviendo a nuevos usuarios sin penalizar a los usuarios "antiguos" que desean unirse a su copia

IV. Mantenimientos en la Blockchain.

Como se mencionó anteriormente, Xiropht es una criptomoneda centralizada, por lo que es posible que se realice el mantenimiento y, por lo tanto, pueda bloquear temporalmente el acceso a la **Blockchain**. Para garantizar la seguridad de los datos, se han configurado varios sistemas de respaldo, a saber, una copia interna de los datos cifrados durante un intervalo regular, y un sistema espejo que permite copiar los datos de la **Blockchain** en tiempo real en varios servidores. . Estos mantenimientos también están destinados a mejorar la **Blockchain**, y puede que, si es necesario, se configure un Soft / Hard Fork para este propósito. Mover la **Blockchain** a servidores más potentes también puede ocurrir si es necesario.