Kii Whitepaper

Resumen.

Kii es una criptomoneda basada en Dash, con varias mejoras que permiten un aumento en la cantidad total de monedas emitidas y mayor velocidad de liberación de bloques. Conservando la red incentivada de dos niveles denominada red de Nodos Maestros y envíos instantáneos KiiSend, lo cual facilita la confirmación instantánea de las transacciones sin una autoridad centralizada.

1. Introducción

Bitcoin es una criptomoneda cifrada que se ha convertido en un medio popular de intercambio, siendo la primera criptomoneda digital en captara un número considerable de usuarios. Desde sus principios en elaño 2009, Bitcoin ha experimentado un rápido crecimiento en suadopción por la mayoría y su uso en la venta al por menor. Un problema esencial para la aceptación de Bitcoin surge en situaciones con puntos de venta donde la red requiere un tiempode espera para confirmar que la transacción realizada es válida. Diversas empresas de pago han creado métodos alternativos para permitir a los vendedores efectuar transacciones de cero confirmaciones, pero estas soluciones utilizan una contraparte deconfianza para mediar en la transacción fuera del protocolo.

Bitcoin ofrece transacciones pseudoanónimas en un libro de contabilidad público, con una relación uno a uno entre el emisor y el receptor. Esta estructura facilita un registro permanente de todas las transacciones que han tenido lugar en todo momento en la red. Bitcoin es ampliamente conocido en círculos académicos por ofrecer un nivel bajo de privacidad, pero aun existiendo esta limitación muchas personas confían su historial financiero a la cadena de boques.

Dash es la primera moneda criptográfica enfocada en la privacidadbasada en Bitcoin y ofrece servicios adicionales de privacidad

través de su opción de PrivateSend y envíos instantáneos InstantSend. En este paper proponemos una serie de mejoras para Dash cuyo resultado es una divisa cifrada descentralizada, fuertemente anónima, con transacciones instantáneas seguras y una red secundaria entre pares incentivada para ofrecer servicios a la red Kii.

2. Red de Nodos Maestros

Los nodos completos son servidores que funcionan en una red p2p, los cuales permiten su uso a pares para recibir actualizaciones sobre los eventos en dicha red. Estos nodos requieren un volumen de tráfico significativo y otros recursos anexos que conllevan un coste sustancial. Como consecuencia, en la red Bitcoin se ha observado una disminución constante en el número de estos nodos a lo largo del tiempo y el consiguiente aumento en la propagación del bloque hasta alcanzar los 40 segundos. Muchas soluciones se han propuesto para ello, como un plan nuevo de recompensa por Microsoft Research y el programa de incentivo de Bitnodes.

Estos nodos son muy importantes para la salud de la red. Ellos ofrecen a los clientes la capacidad de sincronizar y propagar rápidamente los mensajes a través de la red. Proponemos añadir una red secundaria, la red de Nodos Maestros de Kii de la misma forma como la propone Dash. Estos nodos tendrán una alta disponibilidad y proporcionan un nivel de servicio determinado a la red para formar parte del Programa de Recompensa de Masternode.

2.1 *Programa de Recompensa de Nodos Maestros - Costes y Pagos*

La causa en mayor medida de la disminución en el número de nodos completos de la red Bitcoin es la ausencia de incentivos para operar uno de ellos.

El coste de mantenimiento de un nodocompleto aumenta con el transcurso del tiempo ya que el uso dela red es mayor, creando más ancho de banda y suponiendo más dinero a su operador. Conforme el coste crece, los operadores consolidan sus servicios de forma que resulten más baratos de operar o emplean un cliente ligero, el cual no ayuda a la red en absoluto.

Los nodos maestros son nodos completos, análogos a sus contrapartidas en la red Bitcoin, con la diferencia de que proporcionan un nivel de servicio a la red y tienen un vínculo establecido con un colateral para poder participar. La garantía es fija y es segura siempre y cuando el nodo maestro esté funcionando. Esto permite a los inversionistas servir a la red, producir rendimiento de su inversión y reducir la volatilidad de la moneda.

Para operar un Nodo Maestro, el nodo debe almacenar 150,000Kii. Cuando están activos, los nodos proporcionan servicios a los clientes de la red y a cambio se les paga en forma de un dividendo. Esto permite a los usuarios pagar por los servicios y obtener un retorno de la inversión. Los Nodos Maestros reciben los pagos de la misma reserva de dinero, un 45% de la recompensa total del bloque se dedica a este programa.

Debido al hecho de que el programa de recompensa del Nodo Maestro es un porcentaje fijo y la cifra total de nodos presentes en la red fluctúa, las recompensas esperadas variarán según el recuento actual de todos los Nodos Maestros activos. Los pagos para un día estándar por operar un Nodo Maestro se pueden calcular mediante la fórmula siguiente:

$$(n/t)* r*b*a$$

Donde: *n* es el número de Nodos Maestros controlados por un operador t es el número total de Nodos Maestros *r* es la recompensa del bloque actual (actualmente es 300 KII) *b* es la media de bloques en un día. Para la red Kii es generalmente 1440. *a* es el pago promedio del Nodo Maestro (45% de la cuantía promedio del pago por bloque).

El retorno de inversión por operar un Nodo Maestro se calcula con

$$((n/t)*r * b*a*365) / 1000$$

Donde las variables son las mismas de arriba.

El coste asociado por operar un Nodo Maestro implica unos límites duro y suave en los nodos activos en la red. En estos momentos con 1,350 millones de KII en circulación, un máximo de 9.000 nodos podría funcionar en la red. El límite suave lo impone el precio que cuesta adquirir un nodo y la liquidez limitada en las casas de cambio debido al uso de Kii como divisa y no simplemente como una inversión.

2.2 *Ordenación Determinística*

Un algoritmo determinístico especial se usa para crear una ordenación aleatoria de los Nodos Maestros. Usando el hash de la prueba de trabajo de cada bloque, la seguridad de esta funcionalidad queda garantizada por la red de minado.

Pseudocódigo para seleccionar un Nodo Maestro:

```
Para(nodo_maestro en nodos_mestros){
n = nodo_maestro.CalcularPuntuación();

   si(n > la_mejor_puntuación){
la_mejor_puntuación = n; nodo_ganador = nodo_maestro; } }

CNodoMaestro::CalcularPuntuación(){
n1 = ObtenerHashPruebaDeTrabajo(nAlturaBloque); // obtener el hash de este bloque n2
= Hash(n1); //hash del hash de POT para aumentar la entropía n3 = valorabsoluto(n2 -
vin_del_nodo_maestro);

devolver n3; }
```

El código de ejemplo se puede extender para proporcionar una clasificación de los Nodos Maestros, seleccionando un “segundo”, “tercero”, “cuarto” Nodo Maestro de la lista.

2.3 *Quorums sin Necesidad de Confianza*

Actualmente la red Kii tiene ~50 Nodos Maestros activos. Exigiendo una garantía de 150,000 KII para convertirse en un Nodo Maestro activo, creamos un sistema en el cual nadie puede controlar toda la red. Por ejemplo, si alguien quiere controlar el 50% de la red de Nodos Maestros debe comprar 3.750.000 KII en el mercado abierto. Todas las transacciones se verifican mediante Quorums temporales, guiado por una formula determinística de voto que lo hace casi imposible tener la mayoría de participación dentro del Quorum.

Con la incorporación de la red de Nodos Maestros y los requisitos de colateral, podemos usar esta red secundaria para realizar tareas delicadas sin necesidad de confianza, donde ninguna entidad es capaz de controlar el resultado. Seleccionando *N* Nodos Maestros pseudoaleatorios del total en el grupo para llevar a cabo la misma tarea, estos nodos pueden actuar como un oráculo, sin que la red entera desarrolle la tarea.

Puede verse un ejemplo de implementación de un quorum sin necesidad de confianza *KiiSend*, el cual utiliza quorums para ratificar transacciones y bloquear las entradas o la implementación de prueba de servicio.

2.4 *Roles y Prueba de Servicio*

Los Nodos Maestros pueden proporcionar cualquier número de servicios adicionales a la red. Como prueba de concepto, nuestra primera implementación incluyó *KiiSend*. A través de lo que denominamos prueba de servicio, podemos requerir que estos nodos estén en línea, respondiendo e incluso en la altura de bloque correcta.

Actores malignos podrían también operar Nodos Maestros, pero no ofrecer la calidad de servicio requerida por el resto de la red. Para disminuir la posibilidad de personas usando el sistema para su exclusivo beneficio, los nodos deben hacer ping al resto de la red para asegurar que permanecen activos. Este trabajo lo realiza la red de Nodos Maestros seleccionando 2 quórums por bloque.

El Quorum A comprueba el servicio del Quorum B en cada bloque. El Quorum A son los nodos más próximos al hash del bloque actual, mientras que el Quorum B son los más alejados de dicho hash.

Nodo Maestro A (1) comprueba Nodo Maestro B (rango 2300) Nodo Maestro A (2) comprueba Nodo Maestro (rango 2299) Nodo Maestro A (3) comprueba Nodo Maestro B (rango 2298)

Todo el trabajo necesario para comprobar si los nodos de la red están activos lo realiza la propia red de Nodos Maestros. Aproximadamente el 1% de la red será comprobada en cada bloque. Esto resulta en que la red se comprueba por completo más de siete veces al día. Con el propósito de mantener el sistema sin confianza, seleccionamos nodos aleatoriamente con el sistema de Quorum. Después también requerimos un mínimo de seis violaciones para desactivar un nodo.

Para engañar al sistema un atacante necesitará ser seleccionado seis veces seguidas. En caso contrario, las violaciones serán neutralizadas por el sistema conforme otros nodos sean seleccionados por el sistema de Quorum.

La selección de Nodos Maestros es pseudoaleatoria basada en el sistema de Quorum.

2.5 *Protocolo de Nodos Maestros*

Los Nodos Maestros se propagan en la red mediante una serie de extensiones del protocolo incluyendo un mensaje de anuncio y el mensaje de ping del Nodo Maestro. Estos dos mensajes son todo lo necesario para poner activo un nodo en la red. Aparte de estos mensajes se encuentran los destinados a efectuar una petición de prueba de servicio, *KiiSend*.

Los Nodos Maestros se forman originalmente enviando 150,000KIIa una dirección específica de un monedero, el cual "activará" el nodo haciéndolo así capaz de ser propagado por la red. Se crea una clave secundaria privada para firmar todos los mensajes

posteriores. La clave anterior permite bloquear completamente el monedero cuando funciona en un modo autosuficiente.

Un modo en frío es posible gracias a la clave privada secundaría almacenada en dos máquinas separadas. El cliente "caliente" primario firma la entrada de 150,000 KII incluyendo la clave privada de firma secundaria en el mensaje. Poco después el cliente "frío" ve un mensaje que incluye su clave secundaria, y, se activa como un nuevo Nodo Maestro. Esto permite que el cliente "caliente" se desactive (cliente desconectado) y no deja posibilidad alguna a un atacante de que obtenga los 150,000 KII consiguiendo el acceso al Nodo Maestro tras su activación.

En cuanto se inicia, un Nodo Maestro envía un mensaje a la red "Anuncio de Nodo Maestro", conteniendo lo siguiente:

Mensaje: (Entrada 150.000 KII, Dirección IP Accesible, Firma, Tiempo de Firma, Clave Pública de 150,000 KII, Clave Pública Secundaria, Clave Pública de Donación, Porcentaje de Donación)

Cada 15 minutos y posteriores, se envía un mensaje de ping para demostrar que el nodo aún está activo.

Mensaje: (150.000 KII de Entrada, Firma (usando clave secundaria), Tiempo de Firma, Parada)

Después de que un tiempo de vida ha expirado la propia red eliminará el nodo inactivo de la misma, provocando que el nodo no sea usado por los clientes o reciba pagos. Los nodos también pueden hacer ping a la red constantemente, pero si no tienen sus puertos abiertos, con el tiempo serán marcados como inactivos y no cobrarán.

2.6 *Propagación de la lista de Nodos Maestros*

A los clientes nuevos que se incorporan a la red Kii hay que avisarles de los Nodos Maestros actualmente activos en la misma para poder utilizar sus servicios. Tan pronto como se unen a la red en malla, se envía una orden a sus pares solicitando la lista conocida de Nodos Maestros. Los clientes usan un objeto caché

para registrar los Nodos Maestros y su estado actual, así cuando los clientes se reinician simplemente cargan este archivo en lugar de preguntar la lista completa de Nodos Maestros.

2.7 *Pagos mediante Minería e Imposición*

Para garantizar que cada Nodo Maestro cobra su parte equitativa de la recompensa por bloque, la red debe hacer cumplir el pago de los bloques al Nodo Maestro correcto. Si un minero no cumple las normas sus bloques deben ser rechazados por la red, si no se incentivaría el hacer trampas.

Proponemos una estrategia donde los Nodos Maestros forman quórums, seleccionan un Nodo Maestro ganador y propagan su mensaje. Después de que N mensajes se han propagado para seleccionar el mismo beneficiario, se formará un consenso y dicho bloque en cuestión se le exigirá que pague al Nodo Maestro.

Cuando se mina en la red, el software del grupo (sitios web que combinan los esfuerzos de mineros individuales, Pool de Minería) usa la API RPC para obtener la información sobre cómo debe generarse un bloque. Para pagar a los Nodos Maestros, este interfaz debe extenderse añadiendo un beneficiario secundario (GetBlockTemplate). Posteriormente los grupos propagan sus bloques minados con éxito, incluyendo un pago que se reparte entre ellos y un Nodo Maestro.

3. Transacciones Instantáneas mediante KiiSend

A través de quórums con Nodos Maestros, los usuarios son capaces de enviar y recibir transacciones instantáneas irreversibles. Una vez se forma un quorum, las entradas de la transacción se bloquean a una transacción específica única, un bloqueo de transacción requiere unos 2 segundos para que sea establecido en la red. Si se alcanza consenso del bloqueo en la red de Nodos Maestros, a partir de ese momento todas las transacciones o bloques conflictivos serían rechazados, salvo si coincidiesen con el ID exacto de la transacción asignada al bloqueo que toma lugar.

Esto permitirá a los vendedores utilizar los dispositivos móviles en sus ubicaciones tradicionales con sistemas de punto de venta

(POS) para el comercio en la vida cotidiana, y a los usuarios pagar rápidamente transacciones no comerciales en persona como sucede con el efectivo tradicional. Todo ello se realiza sin una autoridad central.

4. Algoritmo de hashing X11

X11 es un algoritmo de hashing ampliamente utilizado, el cual toma una aproximación diferente, conocida como encadenado de algoritmos. X11 consiste en todos los 11 contendientes de SHA3, calculando cada hash particular y luego enviándolo al algoritmo siguiente de la cadena.

5. Suministro de Minería

La cantidad máxima total de KII es de 1,800,000,000 KII de los cuales se consiguieron 1,326,960,000 KII con la liberación del bloque génesis y los otros 473,040,000 KII se conseguirán por concepto de minería en la liberación de cada bloque posterior. La recompensa de minería inicial es de 300 KII por cada bloque minado, con un Target Spacing promedio de 1 minutos. El halving será cada 788,400 Bloques.

La producción de Kii está programada para que prosiga en este siglo, decelerándose hasta cerca de finales del año 2074, cuando ésta cesará.

6. Conclusión

Este paper presenta varios conceptos para perfeccionar el diseño de Bitcoin y Dash que dan como resultado una privacidad y fungibilidad mejoradas para el usuario medio, menor volatilidad en el precio y una propagación de mensajes más rápida por la red. Todo esto se consigue mediante un modelo de dos niveles incentivado, en lugar del modelo de un solo nivel presente en otras criptomonedas cifradas como Bitcoin.

Utilizando este diseño de redalternativo es posible añadir muchos tipos de servicios tales comola mezcla de monedas descentralizada, transacciones instantáneas y oráculos descentralizados a través de quórums con nodos maestros.

Referencias

1. A peer-to-peer electronic cash system (2008)
2. http://eprints.qut.edu.au/69169/1/Boyen_accepted_draft.pdf
3. https://www.cryptocoinsnews.com/3-solutions-instant-bitcoin-confirmations/
4. http://research.microsoft.com/pubs/156072/bitcoin.pdf
5. http://www0.cs.ucl.ac.uk/staff/s.meiklejohn/files/imc13.pdf
6. https://getaddr.bitnodes.io/nodes/incentive/
7. https://medium.com/zapchain-magazine/why-don-t-people-run-bitcoin-nodes-anymore-d4da0b45aae5
8. https://dashninja.pl/
9. https://www.dash.org/wp-content/uploads/2014/09/InstantTX.pdf
10. https://github.com/dashpay/dash/blob/master/src/Masternode-pos.cpp
11. https://blockchain.info/tx/4eb3b2f9fe597d0aef6e43b58bbaa7b8fb727e645fa89f922952f3e57ee6d603
12. https://blockchain.info/tx/1694122b34c8543d01ad422ce600d59f8d8fde495ac9ddd894edc7139aed7617
13. http://en.wikipedia.org/wiki/NIST_hash_function_competition#Finalists
14. http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf
15. https://docs.dash.org/en/stable/introduction/about.html#whitepaper