Especificaciones de Actualización de Sistema

Aplicación de Plataforma Zen: Sistema de Nodo Multinivel y Cadenas Laterales para Descentralizar la Red

Abril 2018
Pier Stabilini, Robert Viglione y Alberto Garofolo

INTRODUCCIÓN

El sistema de Nodos Seguros de ZenCash es una red blockchain compensada única con encriptación mejorada de cliente a nodo y de nodo a nodo. El sistema fue diseñado para descentralizar de forma rápida y masiva la red blockchain para proporcionar una fuerte resistencia a la censura, capacidad de red y establecer la infraestructura para una plataforma orientada a la privacidad de alto rendimiento. En solo tres meses de operar este sistema, la red ya compite con el números de nodos de Bitcoin. A pesar de este gran éxito, es solo un punto de partida y este sistema de próxima generación proporcionará importantes mejoras al rastreo y pagos de los nodos, lo más importante es que estos cambios establecen las bases para una plataforma de aplicaciones completa.

Las mejoras tecnológicas incluyen:

- Creación de una nueva clase de nodos llamada Super Nodos que tienen requisitos significativamente mayores de fondos congelados ZEN (500 ZEN), computación y almacenamiento.
- Migración de la lógica de los clústeres de servidores fuera de la cadena hacia las cadenas laterales mantenidas en los nuevos Super Nodos. Las cadenas laterales multicapa también permitirán que ZenCash admita múltiples aplicaciones como por ejemplo: ZenPub, pagos de cero demora (InstantZen), ZenGrid (computación como servicio) y ZenXchange (un intercambio descentralizado creado en nuestra red).
- Proporcionar un sistema rastreador de nodos completamente descentralizado con su estado de nodo transmitido por sus nodos conectados y todos los mensajes en los nodos seguros que sean recibidos a través del protocolo principal.

Los cambios económicos incluyen:

- Los operadores de nodo recibirán el 20% de las recompensas del bloque, un aumento comparado con el porcentaje del 3.5% anterior. Esto se dividirá de modo que los operadores de los Nodos Seguros recibirán 10% y los operadores de los Super Nodos el 10% restante.
- La tesorería recibirá el 10% de las recompensas del bloque, un aumento del 8.5% anterior.
- Los mineros recibirán el 70% de las recompensas del bloque, un cambio del 88% anterior.

VISIÓN GENERAL ZENCASH

ZenCash es un sistema blockchain orientado a la privacidad basado en la criptografía de conocimiento cero (Zero-knowledge) y el consenso modificado de Satoshi. El sistema va mucho más allá de una criptomoneda tradicional, ya que está diseñado para ser una especie de nación “startup” o un sistema económico de persona a persona para el dinero, los medios y la mensajería.

El proyecto comenzó con su producto principal, ZenCash, que es una criptomoneda con privacidad o transparencia selectiva. Los usuarios eligen entre tipos de direcciones totalmente privadas o aquellas transparentes como las que posee Bitcoin. Además de la privacidad de las transacciones, el sistema introdujo el protocolo de comunicación SSL / TLS de encriptación de cliente a nodo y de nodo a nodo para proteger aún más los datos y las conexiones de los usuarios.

El consenso de Satoshi introdujo la escasez digital al evitar el gasto doble y alinear los incentivos de los mineros para participar honestamente en la creación de bloques. Sin embargo, el sistema no proporcionó tales incentivos a otras partes interesadas,

como los operadores de nodo completos. Nuestra innovación fue recompensar a los operadores de nodo completo directamente de las recompensas de bloque y también exigir que estos operadores de nodos tengan certificados válidos, capacidad computacional mínima y requisitos mínimos de tiempo de actividad. Esto creó una red de nodos de mayor calidad y más confiable, pero la debilidad del sistema es que toda la lógica está alojada fuera de la cadena (off-chain) en clústeres de servidores y bases de datos externas. El siguiente paso, es tener toda la lógica dentro de la cadena (on-chain) y automatizar todo el proceso.

La clase de Super Nodos introduce aplicaciones de plataforma y cadenas laterales (sidechaining). Esta es una mejora importante del sistema que mueve el proyecto mucho más allá de una simple criptomoneda.

NODOS SEGUROS

El sistema de los Nodos Seguros de ZenCash fue diseñado para descentralizar masivamente nuestra red para que el proyecto pueda ser resistente a la censura en jurisdicciones globales. Los operadores de nodos completos que obtuvieron un certificado SSL / TLS válido, tenían al menos 42 monedas Zen congeladas en una dirección transparente (dirección t) y respondieron con éxito al menos al 92% de los desafíos enviados a direcciones blindadas (direcciones z), los cuales obtenían la división de la recompensa del 3.5% de recompensa del bloque. Ninguno de estos requisitos cambia con esta nueva actualización del sistema, pero sí introducimos una mejora en las mediciones de tiempo de actividad de los nodos que se basan en la conectividad real de los pares de red en lugar de las conexiones de websocket.

La configuración actual del sistema aloja servidores de seguimiento (tracking) y pago en clústeres dedicados fuera de la cadena en varias regiones del mundo. Esto fue suficiente para la primera versión del sistema, pero la migración de toda la lógica en la cadena es importante para la verdadera resistencia a la censura, la resistencia de la red y para permitir un conjunto verificable y auditable de información utilizada para calcular la recompensa. Esta actualización trae todo dentro del protocolo y hace uso de las cadenas laterales administradas por los Super Nodos para rastrear nodos seguros, fila de nodos para pagos y coordinar la distribución autónoma de pagos con nodos de minería.

Para resumir, la nueva versión de los Nodos Seguros proporcionará muchas mejoras, incluyendo:

- Implementar toda la lógica a nivel de protocolo en el código central en lugar de mantenerlo dentro una base de código separada

- Proporcionar un sistema rastreador de nodos completamente descentralizado con su estado de nodo transmitido por sus nodos conectados y todos los mensajes en los nodos seguros que sean recibidos a través del protocolo principal.

La mayor parte del Nodo Seguro seguirá siendo igual:

- Mantener toda la cadena de bloques de ZenCash en el sistema.
- Que el usuario proporcione un certificado SSL válido al software ZenCash Node para utilizarlo en la comunicación con otros nodos y carteras.
- Que el usuario tenga que mantener al menos 42 ZenCash en una dirección t para poder operar el Nodo Seguro.
- Monitorear los mensajes de red para los mensajes del desafío computacional.
- 92% del tiempo en línea.

Cambios que se introducirán:

- Un nuevo mecanismo de desafío basado en la nueva versión de zk-snark que requerirá 1.7Gb de RAM. Este cambio se está introduciendo en una actualización de software precursora lanzada a testnet en marzo 2018 y programado para mainnet a partir de mayo de 2018.
- Tiempo de actividad calculado sobre la conectividad real de los pares de red y sobre la sincronizacion de cadena de bloques.
- Las recompensas de los Nodos Seguros aumentarán al 10% de las recompensas de bloque.

En el nivel de protocolo, el controlador de mensajes admitirá los mensajes necesarios para:

- Transmitir la información y el estado del Nodo Seguro a la red.
- Verificar una transacción específica, un conjunto de transacciones o un hash de bloque específico para verificar si el nodo está sincronizado
- Ejecutar un desafío u otra comprobación para verificar que los requisitos del nodo estén satisfechos.

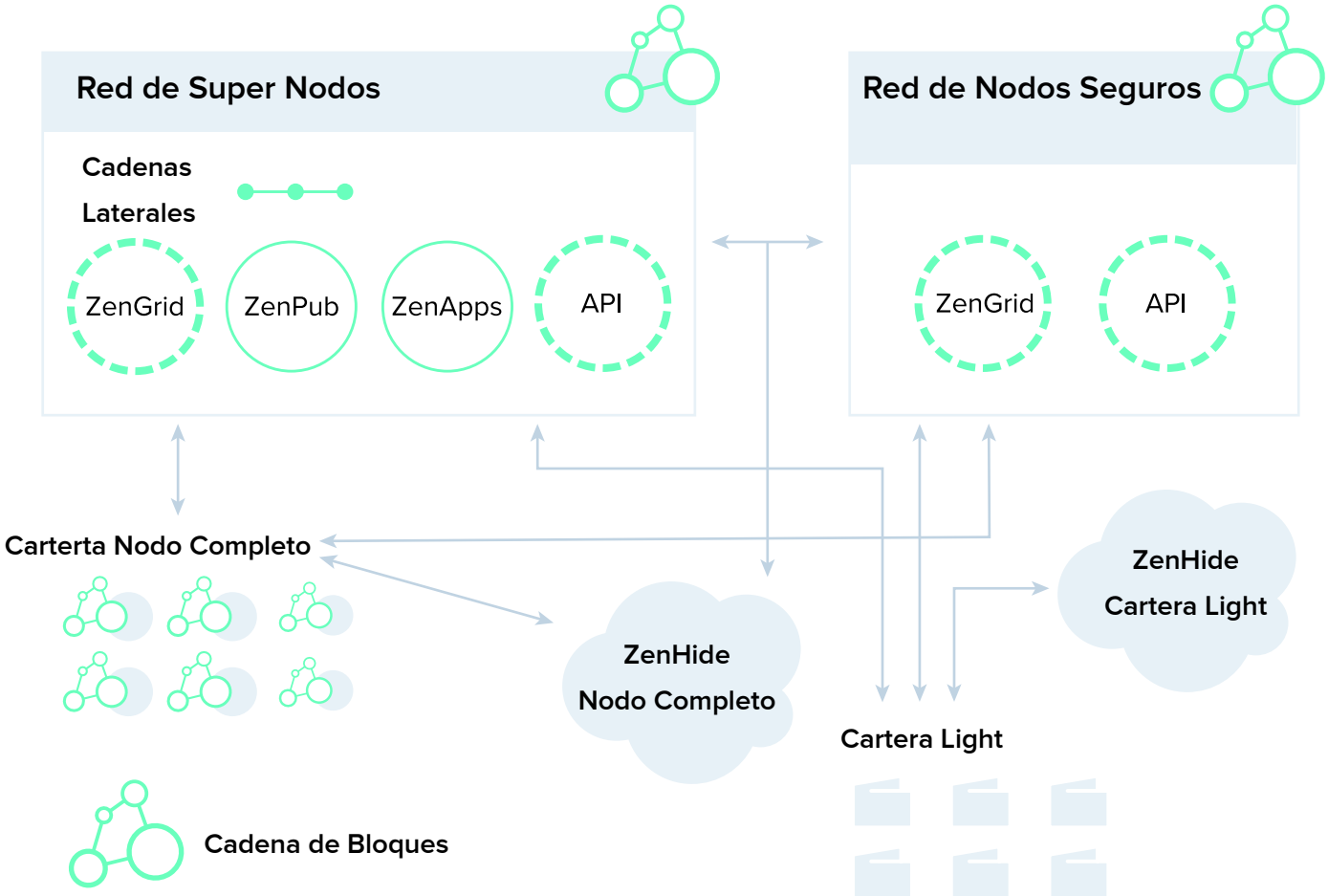
SUPER NODOS Y CADENAS LATERALES

Una de las principales características diferenciadoras de nuestro sistema fue el lanzamiento de una red de nodos compensada con encriptación punto a punto mejorada, que llamamos Nodos Seguros. La red ZenCash adquirió más de 9,000 Nodos Seguros, 3 veces más de lo esperado, solo en los primeros cuatro meses de lanzamiento de este sistema. Estos nodos especiales en la red se componen de sistemas de calidad lo suficientemente alta para cumplir con los requisitos mínimos, incluida la posesión de un certificado SSL válido, una gran mejora con respecto a otras cadenas de bloques actualmente en el mercado. La siguiente fase que presentamos aquí es crear una nueva clase de nodos especiales con requisitos más altos que llamamos Super Nodos. Los Super Nodos serán más potentes que los Nodos Seguros y tendrán la tarea de administrar funciones claves de red y sistema, como hospedar múltiples servicios en cadenas laterales, rastrear y medir el tiempo de actividad de los Nodos Seguros y poner en fila el horario de pago de nodos para los mineros.

Las dos principales mejoras que traen los Super Nodos es transicionar el rastreo y pagos a los Super Nodos dentro de la cadena (on-chain) o dentro del protocolo, un cambio importante con respecto al sistema actual donde tales funciones se ejecutan en clústeres de servidores externos; la introducción de las cadenas laterales (sidechaining) eleva el sistema ZenCash de una criptomoneda pura a una plataforma en la que se puede construir un conjunto ilimitado de servicios. La propuesta de valor del sistema pasa a ser algo más que la utilidad de la moneda, pero ahora incluye la utilidad de todos los servicios futuros que se incluirán en capas en nuestra infraestructura. Una pequeña

muestra de tales servicios que ya están en planificación incluyen un sistema de almacenamiento de archivos distribuidos (ZenPub), un sistema de mensajería segura (ZenChat), un sistema de computación de alquiler similar a las Funciones Lambda de AWS (ZenGrid), pagos sin demora (InstantZen) y un intercambio descentralizado (ZenXchange) con un activo de precio estable completamente colateralizado llamado ZenUSD (USDZ).

RED ZEN



ADMINISTRACIÓN DE PAGO DE NODOS

La red de los Super Nodos mantendrá una cadena lateral multicapa. Una de las capas se usará para almacenar toda la información sobre el estado de los Nodos Seguros y el estado de los Super Nodos. La idea es que la red de los Super Nodos hagan un seguimiento del estado de los Nodos seguros y de los otros Super Nodos en una cadena lateral. Esa red usará el consenso para verificar y validar toda la información de seguimiento necesaria.

Dicho proceso de fila podría funcionar de la siguiente manera:

- Cada n cantidad de bloques los Super Nodos leerán la cadena lateral para procesar los nodos que están listos para ser pagados y moverlos a la fila.
- Todos los Super Nodos deberían proporcionar un consenso sobre cada elemento de la fila.
- Los nodos de minería extraerán elementos de la fila (un subconjunto) y crearán el pago para los nodos en una transacción específica de coinbase (que no sean recompensas estándar de coinbase para el minero y para la comunidad), los nodos pagados se eliminan de la fila.

- Los nodos pagados se eliminan de la fila y se reiniciará en la fila desde los Super Nodos para la siguiente ronda de pago.

ADMINISTRACIÓN DE LA CADENA LATERAL (SIDECHAIN) Y REQUERIMIENTOS DEL SISTEMA

Los Super Nodos soportarán múltiples cadenas laterales en capas, que formarán la base para desarrollar el sistema como una plataforma. Estos se usarán para una variedad de aplicaciones y se expondrán a través de una interfaz común para incluir métodos RPC. La primera implementación se usará para consultar el estado del nodo desde adentro de la API. Las cadenas laterales en capas permitirán que ZenCash sea compatible con múltiples aplicaciones como se describe en la sección anterior. Además ZenCash podrá aprovechar las cadenas laterales para integrar otras tecnologías como FlowCrypt, una extensión de PGP para Gmail, para almacenar toda la llave pública establecida en la cadena lateral. Es importante tener en cuenta que inicialmente el conjunto de aplicaciones estará restringido al desarrollo interno por razones de seguridad, pero el objetivo futuro es abrir la plataforma a desarrolladores de aplicaciones descentralizadas (dApps) externos para que cualquiera pueda contribuir al ecosistema directamente.

Todo esto es una gran mejora en la funcionalidad del sistema y la propuesta de valor. Para soportar esta funcionalidad, los requisitos de Super Nodos serán mucho más altos:

- Al menos 500 ZEN congelados en una dirección t.
- Múltiples núcleos de CPU.
- 8GB de RAM o más.
- 100GB de almacenamiento o más.
- 96% de tiempo de actividad del nodo por día.

PAGOS, AJUSTE Y OBJETIVOS DE LA RED

Un aspecto importante en el ecosistema de ZenCash es que deseamos crear descentralización máxima para la resistencia a la censura. Entendemos que al establecer un número significativamente más grande de fondos congelados (staking) que va de 42 a 500 corremos el riesgo de centralizar la arquitectura de los Super Nodos. Una manera de prevenir la centralización es la de aumentar el grupo de pagos para incentivar la creación de nodos. Esta es la motivación principal detrás de aumentar los pagos del operador de nodos de 3,5% de las recompensas mineras a un total de 20%, con un 10% destinado a operadores de Nodos Seguros y un grupo de 10% dedicado a operadores de Super Nodos.

La segregación de los grupos debe crear un equilibrio conjunto de modo que la red crezca hasta el punto de que el costo marginal sea igual a los ingresos marginales. Los Super Nodos tendrán un costo marginal significativamente más alto y por lo tanto, esperamos menos, pero el flujo de ingresos será independiente del grupo de Nodos Seguros para que el crecimiento de un segmento no canibalice indebidamente el estado del otro. Nuestro número meta de Super Nodos y Nodos Seguros están entre 2,000-2,500 Super Nodos y 20,000-25,000 Nodos Seguros, respectivamente.

Las principales desviaciones de ese objetivo podrían inducir pagos futuros o ajustes de los fondos congelados.

TIEMPO DE IMPLEMENTACIÓN

Se espera que la implementación total de este sistema de aplicación de Super Nodos sea en el cuarto trimestre de 2018 con un prototipo disponible para probarlo al final del tercer cuarto. La construcción de la red comenzará mucho antes. Los ajustes de la recompensa del bloque se implementarán con la próxima actualización del sistema de hard fork programada para ser lanzada a testnet a mediados de abril y a finales del mes de mayo.

Para fomentar la expansión temprana y sin problemas de la red de Super Nodos, proponemos el siguiente cronograma:

- El sistema de congelación de fondos (staking) de los Super Nodos será implementado en Mayo en el hard fork (bifurcación).
- Los prospectos a operadores de Super Nodos registran una dirección t con al menos 500 ZEN.
- Los operadores de Super Nodos ejecutarán una versión modificada del software de los Nodos Seguros.
- El 10% de las recompensas en bloque se acumularán a las direcciones tipo multi firma (multisig) dedicadas a los Super Nodos.
- Los operadores de Super Nodos se compensarán de manera similar al sistema actual de Nodos Seguros hasta que el software de nivel de producción esté disponible en el cuarto trimestre del año.

El mecanismo propuesto proporciona un incentivo parcial para comenzar a planificar los Super Nodos rápidos en etapa temprana y también para seguir con la configuración de los nodos cuando el sistema entre en funcionamiento. Dado que el número esperado de Super Nodos requerirá entre 1 y 1.25 millones de ZEN para comprometerse con las direcciones de nodos congelados (mantener los ZEN en el nodo), es mejor que este proceso de acumulación se inicie temprano y se extienda durante un período más prolongado que comenzar repentinamente en el Q4 del año. Creemos también que este sistema de recompensa híbrido incentiva la acumulación temprana y el seguimiento en la configuración de Super Nodos cuando el sistema se active.

CONCLUSIÓN

Lo que proponemos en este documento es una importante actualización del sistema en múltiples niveles. El sistema de los Super Nodos traerá seguimiento y pagos de Nodos Seguros en la cadena y automatizará el proceso para lograr grandes mejoras de eficiencia y confiabilidad. La economía del sistema cambiará de una manera que incentiva en gran medida a los usuarios a establecer más Nodos Seguros y Super Nodos. Un aumento de casi 3 veces en los pagos aumentará en gran medida la cantidad de nodos operativos y la introducción de Super Nodos aumenta la calidad de los sistemas que componen la red. Sin embargo, el cambio más notable es que esta grande red en crecimiento (posiblemente la más grande de la industria) migrará a una plataforma en la que las aplicaciones distribuidas residirán a través de cadenas laterales multinivel. Las aplicaciones que ya están en nuestra cartera aportan gran utilidad a la comunidad, pero esto es solo un punto de partida. El futuro objetivo es abrir la plataforma a desarrolladores de aplicaciones descentralizadas (dApps) externas para que cualquier persona en el mundo pueda contribuir al ecosistema. Nuestra misión siempre ha sido integrar sociedades y hacer del mundo un lugar mejor. ¡Estas actualizaciones del sistema crearán una red mucho más poderosa sobre la cual la verdadera diversión puede comenzar!

Referencias:

[1] - https://github.com/ZencashOffical/
[2] -https://zencash.com/
[3] -https://securenodes.eu.zensystem.io/

zencash