VELES

whitepaper

Veles: Un ecosistema para VPNs abiertas descentralizadas y anonimato en red

9 de diciembre 2018,
Versión 1.01

Autores:
@AltcoinBaggins
@mdfkbtc

Resumen

Veles es un proyecto de software open-source que apunta a ayudar a la comunidad de Internet a mejorar la libertad de acceso a la información, a prevenir la censura en Internet, y a aumentar el anonimato de las comunicaciones sobre la red. Creemos que la tecnología blockchain, introducida por Satoshi Nakamoto y luego avanzada por muchos otros desarrolladores, tales como el equipo de Dash los cuales introdujeron el sistema de nodos maestros (masternodes), pueden ayudarnos a construir redes más robustas, fiables y distribuidas de forma más justa. Las tecnologías open-source existentes para proveer conexiones anónimas basadas en ruteo onion (onion-networking) son construidas sobre el concepto de simples redes voluntarias (volunteer networks). Uno de los pilares más importantes detrás de la tecnología blockchain es el uso de modelos de teoría de juegos para construir redes autosustentables, donde los participantes son incentivados económicamente para soportar la red. Creemos que integrar las ventajas de estos nuevos conceptos tecnológicos y económicos con fundamentos ya establecidos por miles de hackers y cypherpunks en las áreas de anonimato de comunicaciones sobre redes, cuyas bases han sido probadas una y otra vez a lo largo de estos años, es la forma correcta de alcanzar la visión establecida para el proyecto Veles y para avanzar un poco más la tecnología que brinda soluciones a la comunidad de Internet.

1. Introducción

La hipótesis y la tecnología detrás de Bitcoin y blockchain ya ha probado su validez por más de 10 años y, si bien ha enfrentado muchos retos en el proceso, y nuevos surgen asiduamente, nuevas soluciones aparecen para los mismos a un paso acelerado. Mediante el uso de las mejores prácticas en la industria, y una administración de proyecto y procesos de desarrollo adecuados, el ecosistema Veles puede proveer un ecosistema entre pares para blockchain y de cryptomonedas seguro, resistente a amenazas comunes como ataques 51 % o futuras como la presentada por la computación cuántica, al tiempo que asegura transacciones rápidas con comisiones mínimas. Para proveer el incentivo a la red y soportar su micro-economía, la cryptomoneda VLS se convierte en la piedra fundamental del ecosistema Veles.

Para prevenir la censura y mejorar el anonimato de las comunicaciones en Internet, una de las áreas principales del foco en el desarrollo del proyecto Veles es la utilización de protocolos de tunelización y técnicas de redes privadas virtuales (virtual private network - VPN) para crear conexiones punto-a-punto seguras, utilizando SSL/TLS, esquemas de llave pública y certificados digitales.

2. Mejoras en el Consenso

Nuestra estrategia para un mejoramiento de las funcionalidades de blockchain se basa en una mejora en el sistema de recompensas, la seguridad y la utilidad práctica del concepto de Proof-of-Work. Para lograrlo hemos recurrido a las siguientes tecnologías:

El uso de múltiples algoritmos combinado con recompensas por bloque dinámicas y protección contra el minado instantáneo (insta-mine), el sistema mejorado de recompensas de Veles y la resistencia a ataques de 51 %. Esta mejora además minimiza los intentos de minado especulativo y previene el recompensar a los mineros con "monedas baratas" en tales situaciones.

Las recompensas dinámicas por bloque son calculadas de forma individual en base al hashrate de cada algoritmo. Por ejemplo, si el algoritmo X11 tiene un hashrate de 200 GS/s mientras que Scrypt tiene uno de 5 MH/s, las recompensas para los bloques X11 será de aproximadamente 0.2 VLS, mientras que los de Scrypt serán de aproximadamente 0.003 VLS por bloque. Es por lo tanto imposible el favorecer a un algoritmo particular en comparación con aquellos menos usados.

El minado multi-algorítmico le brinda a un gran número de mineros la oportunidad de minar, lo cual en nuestra opinión mejora la descentralización de la red y la distribución de recompensas. Esto permite que tanto mineros GPU como ASIC se unan en la red Veles en armonía. La distribución de recompensas por algoritmo es consistente en la totalidad de la red, por ejemplo si X11 acumulo un hashrate de 200 GH/s, las recompensas serán comparables a las de Lyra2z conun hashrate de 30 MH/s. Para realizar un ataque 51 % de manera exitosa, un atacante necesitará tener el control del 51 % del hashrate *de cada algoritmo*. La protección contra insta-mine funciona de la siguiente manera: si el hashrate de un algoritmo en particular de repente se incrementara más de un 50 %, la dificultad de minada se incrementará significativamente para los siguientes bloques, con un decremento de dificultad lento. Esto elimina las distorsiones de tiempos de bloque especulativos. Una parte integral de ese sistema multi-algorítmico es la manera en que cada algoritmo recalcula y cambia individualmente una dificultad. La configuración de dificultad son controlados por una protección contra abrazo mortal (dead-lock), lo que protege contra el congelamiento y efectivamente reaclcula la dificultad tanto ante incrementos como decrementos repentinos del hashrate. Esto hace que el minado especulativo de monedas sea dificultoso, ya que transacciones previas deben ser confirmadas primero.

3. Provisión de anonimato, tunelización y VPN

La tecnología de red privada virtual (virtual private netwotk - VPN) permite a los usuarios de Internet evitar restricciones geográficas y censura, o conectarse a servidores proxy para proteger su identidad y que sus datos de geolocalización permanezcan anónimos en Inernet. Sin embargo, algunos sitios de Internet bloquean el accesso a soluciones populares de VPN para prevenir la evasión de restricciones geográficas. Incluso cuando algunos proveedores de VPN se encuentran en búsqueda de soluciones a ésto, ellos no necesariamente proveen de soluciones permanentes y confiables a todos los usuarios de Internet.

Hay estrategias exitosas para salvar estas restricciones y mejorar el anonimato en la comunicación. Una de las soluciones eficietes es el uso de saltos múltiples en ruteo onion (multi-hop onion routing). Para transferir la información en redes onion clásicas, el originante selecciona un conjunto de nodos de una lista. ¿Se establece un camino en base a los nodos elegidos, denominado cadena o circuito, a través del cual el mensaje será transmitido. Para preservar el anonimato del emisor, ningún nodo en el circuito puede establecer si el nodo anterior del cual recibió el paquete es el emisor original u otro intermediario como él. De la misma forma, ningún nodo sabe cual es la cantidad de nodos en el circuito y solamente el nodo final, llamado nodo de salida, puede determinar su propia ubicación dentro del circuito.

Redes voluntarias actuales como Tor pueden todavia sufrir de diversas debilidades que nosotros creemos que pueden ser atacadas mediante la implementación de tecnología masternada basada en blockchain, la cual toma conceptos de los modelos de teoría de juegos para construir redes autosustentables y autoreguladas, donde servicios de VPN y ruteo onion puedan ser provistos de manera justa, robusta, segura y fiable. El concepto de masternodes extiende blockchain con una red secundaria, llamada la red de masternodes. Estos nodos tendrán una alta disponibilidad y proveerán un nivel de servicio requerido a la red y tendrán un colateral para participar, para ganarse su pago en la moneda de Veles. Estos masternodes pueden proveer un sinnúmero de servicios extra a la red. Por el otro lado, tanto el colateral como el requerimiento de una gran disponibilidad desalentarán a actores malos a participar. El concepto de red de masternodes fue introducido en el whitepaper de Dash, y como una prueba de concepto, sy primer implementación incluyó PrivateSend e InstaSend.

La red Veles avanzará sobre el concepto de Proof-Of-Service y el sistema de redes de masternodes introducido por el equipo de Dash mediante su integración con robustas tecnologías de código abierto tales como OpenVPN, el cual es un servidor SSL VPN open source y cliente software/librería soportado por un amplio rango de clientes, incluyendo iPhone, Android, Windows, Linux, FreeBSD o macOS. El modelo de seguridad OpenVPN está basado en SSL, el estándar de la industria para comunicaciones vía Internet. OpenVPN implementa extensiones de seguridad de redes en las capas 2 y 3 del modelo OSI utilizando el protocolo SSL/TLS, soporta métodos para autenticación de cliente flexible basado en certificados de cliente digitales y usa un modelo de seguridad de nivel industrial diseñado para proteger tanto contra ataques pasivos como activos.

El sistema de masternodes de Veles también introduce la red de masternodes de nivel II para proveer la función de nodos de salida. Estos nodos requerirán sólo la mitad del colateral del nodo completo de nivel I pero también requerirán un poder de cómputo y recursos de memoria sustancialmente menores, sólo proveyendo ancho de banda y funcionando como enrutadores de multi-salto o nodos de salida para construir circuitos similares a los de la red onion. Estos nodos podrán ser ejecutados en un gran número de dispositivos incluyendo aquellos con pocos recursos tales como los Raspberry Pi. Usuarios dispuestos a incrementar el nivel de anonimato en sus comunicaciones podrán escoger el número que deseen de saltos para enrutar su tráfico.

Para asegurar la mejor disponibilidad, velocidad, ecuanimidad del servicio y desalentar ataques del estilo de DDoS cada usuario de VPN deberá pagar una pequeña comisión en la cryptomoneda del ecosistema Veles para de esta formaacceder al servicio de VPN, de forma que la red no sea fácilmente usada incorrectamente.

Para conseguir el suficiente anonimato en el pago del servicio VPN la transacción no será enviada directamente a los nodos operadores sino a una dirección especial de destrucción de monedas (burn address). Los operadores de nodos reciben regularmente su proporción ecuánime de recompensas por proveer el nivel de servicio requerido de forma consistente, independientemente de las comisiones pagadas por los usuarios. Nuestro objetivo es mantener estas comisiones tan bajas como sea posible solo para mantener su rol como sistema anti-span y de desaliento de uso incorrecto de la red.

Esta estrategia puede también ayudar a prevenir la centralización ya que la red desalentará a los participantes a crear unos pocos nodos muy poderosos, y en lugar de esto alentará a los mismos a incrementar el número de nodos aumentando la diversidad y la descentralización del ecosistema. El plan de destruir las comisiones VLS pagadas para obtener servicio VPN ayudará a su vez a la micro-economía del ecosistema ya sea mediante un decremento de la tasa de emisión de VLS o incluso posiblemente decrementando el número de VLS en circulación, ayudando a la cryptomoneda a mantener su valor a través del tiempo.

4. La Visión

Nuestra visión es la de construir e impulsar redes y ecosistemas descentralizados auto-incentivados, auto-soportados y auto-gobernados proveyendo servicios de VPN y anonimato robustos, confiables y seguros a los usuarios de Internet., aprovechando tecnologías de punta y mejores prácticas, para construir un ecosistema abierto gobernado por la comunidad, resistente a la censura, los que creemos que serán más eficientes que las soluciones convencionales de redes de voluntarios o propietarias mencionadas anteriormente. La idea del presente whitepaper es solamente mostrar la dirección del proyecto y explicar nuestros objetivos. Es el propósito del equipo Veles el de impulsar y salvaguardar todos los procesos involucrados en el desarrollo y administración del ecosistema Veles

hasta que la red sea lo suficientemente madura y haya alcanzado la fase final donde el gobierno abierto, administración de proyecto y procesos de desarrollo estarán bien establecidos y testeados al punto que el ecosistema pueda ser dejado definitivamente en las manos de la comunidad, guiado por contratos inteligentes y algoritmos.