REVUO MONERO

Edición 2, 4T 2017

Rincón del Equipo Central

Al revisar las actividades del Proyecto de Monero durante el 2017, lo más significativo es el grado del progreso del mismo. Voy a cubrir lo más destacado; sin embargo, de ninguna manera pretende ser comprensible.

En el 2017 vimos la adición de las Transacciones Confidenciales de Círculo (Ring Confidential Transactions) a la cadena principal de Monero, primero como opción y a partir de septiembre obligatorias en cada transaccion. En la bifurcación de septiembre también se incremento el tamaño de los círculos a mínimo 5. Ahora damos por hecho que el ocultamiento de las cantidades de las transacciones es parte de la experiencia de Monero, pero hace menos de un año este no era el caso. Un gran desafío fue el descubrimiento de un error critico por parte un miembro del Laboratorio de Investigación de Monero que afecto a todas las monedas basadas en CryptoNote. Esto no solo requirió un parche en el código de Monero, sino además de la divulgación responsable hacia otras monedas basadas en el mismo protocolo. Esto se llevó a cabo de manera ejemplar en la cadena de bloques de Monero sin causar ningún tipo de daño. Otros eventos significativos incluyen el rediseño de la url https://getmonero.org/ y la salida de la versión beta de la GUI. ¿Que traerá el futuro? El 2017 ha visto la investigación y el desarrollo de algunas de las actualizaciones más importantes para el futuro del proyecto, incluidas las pruebas de bala (bulletproofs), transacciones con multifirmas (multi-signature) y el continuo desarrollo del proyecto Kovri.

Por el lado de la comunidad, ha habido un crecimiento significativo. Este crecimiento se ha extendido a través de las comunidades de Monero de una manera admirable, con la celebración de reuniones regulares y el Monero Coffe Chat. Un aspecto importante del crecimiento de la comunidad, han sido las reuniones (meet-ups) que se celebran a nivel mundial.

Debo expresar mi más sincera gratitud y agradecimiento a los desarrolladores, investigadores, colaboradores, miembros de la comunidad, donantes y por último pero no menos importantes, los miembros del equipo central (core). Sin ustedes el extraordinario progreso que hemos visto en el 2017 simplemente no hubiera ocurrido. Ha sido un placer y un honor haber trabajado con todos ustedes este año.

Francisco “ArticMine” Cabañas

En esta publicación...

ACTUALIZACIÓN DEL DESARROLLO

Bajo la superficie, Monero es una fuente de tecnología y de código. El trabajo en la base del código se realiza de diferentes formas, desde la corrección de errores hasta la implementación de innovaciones. Quienes trabajan en el código subyacente son solo parte de la ecuación. El ritmo de trabajo en la interfaz gráfica para el usuario (GUI) avanza de manera constante, con un diseño simple e intuitivo para que los usuarios la puedan trabajar. Monero tiene decenas de personas trabajando en todos los aspectos de la base del código. Nos tomamos el tiempo para ver algunos de los aspectos destacados del desarrollo del último periodo.

Multfirmas (Multisig)

Uno de los mayores logros del último período es la implementación de las multifirmas al monedero CLI, que permite que los Monero solo puedan ser gastados si un número predeterminado de firmantes firman la transacción. En los últimos 3 meses, las multifirmas N/N y el N-1/N, se han implementado y fusionado completamente en la base del código.

Al ser un cambio en el monedero, no hay necesidad de esperar hasta el próximo fork para utilizar esta característica. Simplemente se construye desde el código actual desde el código fuente para hacer uso de ella.

Pruebas de Bala (BulletProofs)

En esta edición, un tema en común entre el desarrollo y el Laboratorio de investigación (MRL) son las pruebas de bala. El equipo de desarrollo no desperdicio tiempo en traer esta tecnología al código una vez recibió el guiño del equipo MRL para realizar el cambio de las pruebas de rango a las pruebas de bala.

Al momento de escribir esta edición, las pruebas de bala de salida simple (single output bulletproofs) están activas en la red de pruebas (testnet), y las salidas múltiples (multi output bulletproof) están en desarrollo. Aún sigue la discusión de si activar en la próxima bifurcación las pruebas de bala de salida simple (pese que las salidas múltiples son un poco más eficientes, además de producir una mayor reducción en el tamaño de la transacción comparada con las pruebas de rango) o darle un mayor tiempo a esta tecnología en la red de pruebas.

Subdirecciones (Subadresses)

Las subdirecciones han sido otra característica largamente esperada. Permitirán generar múltiples direcciones de un mismo monedero. En otras palabras, un individuo será capaz de entregar diferentes direcciones a propósitos diferentes y tener acceso a los fondos utilizando una sola semilla mnemotécnica. Esto incrementa la privacidad, ya que, aunque las direcciones secretas (stealth adresses) esconden la dirección de destino en la cadena de bloques, el elemento humano de postear la misma dirección en múltiples sitios podría atar esa dirección a un usuario causándole algunas consecuencias.

El trabajo de las subdirecciones ha finalizado y al igual que las multifirmas, es una característica del monedero, por ende no requiere de una bifurcación y puede ser utilizada construyendo desde el código fuente.

GUI Actualizado

Hacia finales del 2017 la comunidad financio a **dsc** para la implementación del tema oscuro para el diseño de la GUI creado por **knufflebund**. En vez de contentarse con solo agregar el nuevo tema y poderlo cambiar entre si, el equipo GUI decidió optimizar el nuevo diseño al hacerlo más accesible y amigable para el usuario.

Adicional a esto, el trabajo para agregar las subdirecciones al monedero GUI está en camino, aunque no hay una fecha disponible de lanzamiento de la característica.

Respuesta de Vulnerabilidad

Este equipo de trabjo es nuevo y aunque técnicamente es un grupo que trabaja para sí mismo, lo incluímos en está edición ya que no genera suficiente contenido para su propia sección, pero su trabajo es invaluable para el continuo desarrollo y la seguridad de Monero. El proyecto de Monero esta comprometido en proporcionar software privado y seguro, que incluye reportes de caza recompensas para mitigar potenciales vulnerabilidades de Monero y Kovri. Puedes conocer y aprender el gran trabajo realizado por **anonimal**, **luigi1111**, **fluffypony** y **moneromooo** en hackerone.com/monero.

ACTUALIZACIÓN DEL LABORATORIO DE INVESTIGACIÓN DE MONERO

Mantenerse al día con los avances, examinar e implementar mejoras, dar recomendaciones de privacidad, hacer investigación propia y estar en línea de defensa en contra de ataques, son solo parte de las tareas del Laboratorio de Investigación de Monero: asegurando que Monero se mantenga a la vanguardia de las tecnologías de privacidad y la tecnología blockchain. En esta sección, haremos un recorrido de lo que fue el final del 2017 para nuestros dos investigadores académicos de tiempo completo financiados por la comunidad.

Pruebas de Bala

Una de las mayores emociones del último periodo fue el trabajo realizado por el MRL para implementar pruebas de rango más eficientes (las pruebas de bala) en la base del código. Analizando las transacciones de Monero, las prueba de rango son la mayor parte de cada transacción, al implementar las pruebas de bala se reducirá el tamaño de las transacciones en más de un 80%, lo que a su vez disminuirá las comisiones que se calculan en XMR/byte. Se espera que las pruebas de bala estén activas en la cadena de bloques para el 2018.

RuffCT

Corrección: Antes de continuar, nos gustaría corregir un error que tuvimos en la anterior edición. Expresamos que **Shi-Feng**, **Sun**, **Man Au**, **Joseph Liu** y **Tsz Hon Yuen** contactaron el Laboratorio de investigación de Monero (MRL) sobre las RingCT 2.0. Esto es un malentendido de cómo llego el papel blanco a manos del MRL describiendo las RingCT 2.0.

Aunque la prioridad fueron las pruebas de bala, el MRL ha continuado su incursión en la viabilidad sobre la implementación de las RuffCT en Monero. De hecho, viendo como las RuffCT incrementan drásticamente el número de anillos con la desventaja en los tiempos de verificación, se ha buscado combinar las pruebas de bala con las RuffCT, para así permitir el incremento del tamaño de círculos sin exceder el uso de la red. Esto reducirá aún más la posibilidad de encontrar las salidas (outputs) de las transacciones e incrementar la privacidad.

Protocolo SPECTRE

El MRL inicio el análisis de un whitepaper publicado a finales del 2016 esbozando un protocolo a base de DAG llamado SPECTRE. Mientras que SPECTRE ordena las transacciones y continua acomodando los bloques al DAG, al momento de escribir esta edición, existen varias criptomonedas que utilizan la estructura DAG pero lo hacen solo a escala de transacciones. Un potencial cambio a una estructura sin la cadena de bloques genera una gran emoción, pero antes de determinar si Monero puede beneficiarse, los investigadores manifestaron que se requiere una mayor investigación de los posibles ataques de este nuevo protocolo.

Multifirmas & Estándares de Monero

A **Brandon** le tomo tiempo ordenar la propuesta informal de multifirmas, en un proyecto formal criptográfico listo para publicar. El trabajo incluyo repasar pruebas preliminares en Java como también el análisis final del código C++.

Este trabajo fue escrito para su inclusión en lo que hoy conocemos como el documento 'Estándares de Monero', en el que cada estándar (un ejemplo de estándar seria las funciones hash, los algoritmos PoW, los esquemas RingCT, las pruebas de rango, etc.) es elaborado según las razones de su elección y sus alternativas con los pros y sus contras. De esta manera aquellos miembros del MRL y desarrolladores que integren el equipo conozcan el documento y puedan fácilmente iniciar futuras investigaciones.

NIPoPoW

Los hermanos Noether examinan la posibilidad de utilizar las Pruebas No-Interactivas de Prueba de trabajo (NIPoPoW) como una manera segura de iniciar los nodos livianos. Esto permitirá a los nodos remotos conectarse a nodos completos y recibir solamente algunos bloques seleccionados y confiar en que los bloques son los correctos. Esto será útil para los nodos remotos recien iniciados, pero no podrán recuperar los registros de transacciones previas. Debido a su uso limitado, en el momento no hay planes para incorporarlo pero es necesario tener planes alternativos si surgiera la necesidad.

ACTUALIZACIÓN KOVRI

La batalla por la privacidad de Monero y del mundo se desata en muchos frentes y el equipo Kovri está atrincherado asegurando que este protegida para el futuro.

Para aquellos que no sepan, Kovri es un enrutador privado que se integrará a Monero. Una vez integrado, se tendrá la opción de enrutar las transacciones a través de Kovri, escondiendo la ubicación geográfica y las direcciones IP. Esto incrementará la privacidad en cada transacción.

Asistente para el Proyecto Kovri

En el último periodo del año pudimos apreciar el ingreso al proyecto de **rehrar** el colaborador de la página web, como director asistente. Financiado por el Forum Funding System - FFS (Sistema de financión colectivo - SFC), **rehrar** es el responsable del mantenimiento de la página web (una actualizada página web para Kovri viene en camino y debe estar en funcionamiento para inicios del 2018), las extensiones de desarrollo, educación y el apoyo al grupo de traductores. **Rehrar** paso de trabajar un cuarto de tiempo, a medio tiempo en el 2018.

Las extensiones de desarrollo se iniciaron al final del año contactando a varias universidades. Desafortunadamente, era muy tarde semestralmente para que los estudiantes consideraran tomar en serio nuevos proyectos. Con los primeros acercamientos ya hechos, se retomarán las extensiones en el 2018.

Desarrollo

A medida que avanza el lanzamiento de la versión Alpha, Kovri continua desarrollandose. Resumiremos algunos avances a continuación:

En este 4P (cuarto periodo), vimos no una, sino dos dias0 en el código de i2pd; los dias0 son errores graves en el código que amenazan el software y pueden ser explotados, tal como paso con Heartbleed en OpenSSL. **Anonimal** dijo, "perdí la noción después de encontrar 7", dias0 en el código de i2pd, reafirmando su posición en que todo el código de i2pd debe ser removido del proyecto Kovri. Tomará tiempo, pero esto asegura la calidad del código y minimiza ataques.

Una red de pruebas está disponible en la que los contribuyentes pueden probar fugas y errores sin la necesidad de conectarse a la red principal de I2P (Proyecto Invisible de Internet) o tener acceso a internet, además de alojar su propia mini red local. Esta red proporciona un banco de pruebas donde los cambios pueden ser examinados y hacer pruebas de seguridad sin interferir paralelamente en la ejecución de la red principal de I2P. El trabajo offline es otro beneficio que trae la red para los contribuyentes quienes estén interesados en hacer pruebas.

Otra área de desarrollo es la construcción preliminar de una API (Interfaz de Programación para Aplicaciones). Esto es esencial para aplicaciones como Monero que buscan conectarse a la red de I2P, utilizando el enrutador Kovri. Con la creación de la API, ahora más que nunca, se dan los primeros pasos hacia un futuro brillante en la privacidad de Monero.

Este resumen es lo que resalta del trabajo del último periodo. Para mayor información dirigirse al repositorio de Kovri en Github.

Investigación / Revisión / Colaboración

Desde su creación, el proyecto Kovri decidió estar al frente de todos los avances sobre tecnología de anonimato. El tiempo para revisar nuevos desarrollos, documentos y otras investigaciones relacionadas con le tecnología de redes mixtas se apartan. Así mismo, por seguridad, toda solicitud de cambios, en particular la de los nuevos contribuyentes, deben ser examinados con gran precisión. Kovri ha colaborado en diferentes ramas del proyecto de Monero, incluyendo el grupo de trabajo de traducciones, el Laboratorio de Investigación y el equipo de desarrollo, sin mencionar algunas colaboraciones cercanas con las dependencias de software como Crypto++.

Contribuyentes

Al proyecto le gustaría agradecer a todos los involucrados que han entregado su tiempo, energía, recursos y dinero en el último periodo. En particular, queremos resaltar a **anonimal** por estar siempre presente y más, a **rehrar** por su continuo soporte y entusiasmo y a **MoroccanMalinois** por sus contribuciones. Nos gustaría extender una cordial bienvenida a los nuevos reclutas **selsta** y **oneiric**. Esperamos sus contribuciones y estamos muy agradecidos de tenerlos en la familia.

ACTUALIZACIÓN DE LA COMUNIDAD

El equipo de trabajo de la Comunidad inicio en el 2017 y ha continuado sin parar. Su principal objetivo es identificar y satisfacer las necesidades dentro de la comunidad, esto puede puede hacer de varias maneras, tales como la creación de materiales educativos, acompañar en iniciativas, generar guías u otras. La comunidad es un grupo abierto y cualquier interesado en ver su crecimiento puede unirse visitando el reddit /r/monerocommunity o participando en las reuniones que se organizan cada dos semanas (ver detalles en Github).

Reuniones y el Coffee Chat

Un logro pequeño pero destacable, son las reuniones que se realizan en el canal #monero-community de IRC cada dos meses. Estas son reuniones abiertas donde se discuten aspectos relacionados a la comunidad y cualquiera puede participar.

Una segunda reunión del mismo tipo llamada el Monero Coffee Chat comenzó gracias a **Justin 'sgp' Ehrenhofer**, donde los colaboradores se reunen cada mes en una transmisión en vivo a conversar temas sobre el desarrollo, proyectos, filosofía e información importante. Estos chats tienen la intención de hacer más accesibles a los colaboradores y que las personas puedan participar de una manera personal.

Taiga & Mattermost

Como Monero es una iniciativa dirigida por individuos (grassroot), sin un liderazgo estructural central, todo el desarrollo, el código y demás, dependen de equipos de trabajo que se completamentan entre si dentro de sus campos de experticie y pasiones. El equipo central encontró la manera de invertir y proveer los recursos necesarios para que estos equipos de trabajo orgánicamente lleven a cabo su visión de Monero. Estos recursos son Mattermost (una alternativa a Slack de fuentes abiertas auto hospedado) y Taiga (una plataforma de desarrollo ágil de fuentes abiertas auto hospedada), entre otros que están siendo examinados para el futuro. Para acceder a estos recursos pueden dirigirse a la página de 'Hangouts' de getmonero.org para mayores detalles

Integraciones

Serhack y **cryptochangements** continuan trabajando en la creación de complementos (plugins) de fuentes abiertas para varias plataformas y que los comerciantes puedan integrar a Monero como una opción de pago para sus bienes y servicios. En el último periodo vimos el lanzamiento de los complementos para WCHMS y Magneto sumándolos a los ya existentes de Woocommerce y Prestashop. Un complemento para OpenCart se prevee para el 2018.

Videos Educativos

Savandra continua trabajando con miembros de la comunidad para que crear videos fáciles de entender y accesibles para los recién llegados. El video de Kovri se lanzó hace muy poco, después de meses de trabajo, y el guión para involucrarse a Monero está en camino. Estos videos se suman a los ya existentes de Monero basics, direcciones secretas, firmas círculares y RingCT.

Kit de reuniones para Monero

En una reunión, en el espacio de lluvia de ideas, **serhack** sugirió la creación de un "kit de reuniones" para dar a grupos interesados que quisieran conocer más sobre Monero. Esto resultó en el trabajo de todo un mes concluyendo con los materiales necesarios. Incluye monederos de papel y actividades que muestran el uso de los monederos, cubiertas para cámaras web, stickers, infografías y folletos de mano. El proyecto fue financiado por donantes a través del Sistema de financiación colectivo (FFS síglas en inglés). Uno de los colaboradores, **Justin**, distribuyó estos kits a varias organizaciones alrededor de los Estados Unidos.

Traducciones

El equipo de trabajo se formó a finales del 2017 con el único propósito de localizar todos los materiales de Monero, pasando por la página web, después a la GUI, hasta panfletos impresos. Desde su comienzo, **ErCiccione** ha liderado el equipo para traducir la GUI en más de 5 lenguajes, traducir la página web de Kovri, corregir traducciones existentes y traducir el deamon de Monero. Si estás interesado en ayudar, puedes visitarlos en el canal #monero-translations de IRC o ver la petición del proyecto en Taiga para traducir guías, wiki's y, un rastreador de tareas.

ACTUALIZACIÓN DE KASTELO

Kastelo es un proyecto iniciado por **msvb-lab** *cuyo objetivo principal es el de crear las especificaciones de un monedero físico (hardware) de fuentes abiertas. Siendo un equipo nuevo, con tres meses de trabajo, el progreso en el desarrollo ha sido asombroso.*

Financiamiento & Taiga

En agosto 19 del 2017, **micheal**, posteo una propuesta para la fabricación de un monedero físico en el Sistema de financiación colectivo (FFS). Hasta este punto, pese al desarrollo que le han hecho grandes proveedores al monedero físico, Monero no ha tenido ningun soporte de parte de ellos. Sin embargo, el tener un monedero físico completamente de fuentes abiertas fue tan atractivo que la propuesta fue financiada en muy corto tiempo.

Micheal aprovecho los recursos de Monero para los equipos de trabajo y estableció un sitio para el monedero en Taiga, que al momento de escribir esta edición, ha atraído a 33 colaboradores en los que se aprecian desde mecánicos, diseñadores, hasta quienes realizan las pruebas. Todas las actualizaciones del proyecto pueden ser vistas en las peticiones de Taiga de Monero.

Prototipos para las Vacaciones

Después de varios meses de trabajo, el equipo y **msvb-lab** desarrollaron varios prototipos funcionales e hicieron un gran progreso. Después de un pequeño proceso de suscripción, se enviaron alrededor de 30 prototipos a prueba.

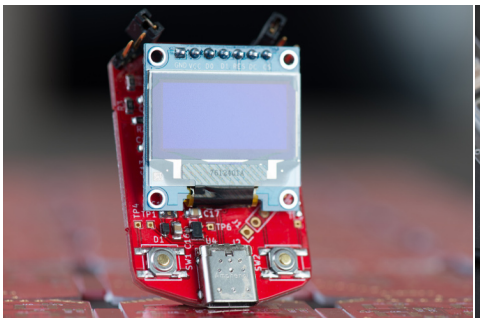
Cabe mencionar que se le advirtió a quienes probaran los prototipos el no mantener sus monedas en ellos porque solo se enviaron con los programas de comunicación interna (firmware) más básicos. Las fotos de los prototipos se muestra en la parte inferior de esta página.

Conferencia 34C3

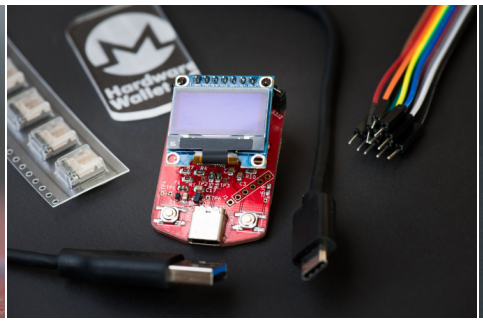
Micheal se unió al equipo que asistió a la conferencia 34C4 y presentó el progreso del monedero a los diferentes asistentes. Llevaba consigo otros prototipos para repartir entre los participantes interesados.

Reuniones de los Equipos de Trabajo

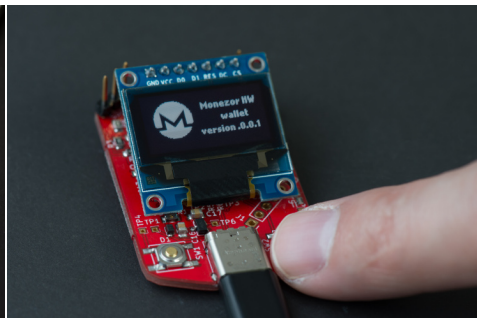
Para hacer esto una realidad, Kastelo requiere de equipos pequeños trabajando simultáneamente. A la fecha, estos grupos incluyen equipos de pruebas de calidad (QA), equipos de programación de comunicación interna (firmware), mecánica, diseño de matrices de puertas programables (FPGA) y de logo y mercadeo. Mensualmente se reúnen en un solo grupo y luego se dividen en sus respectivas áreas para discutir los temas correspondientes. El calendario de éstas reuniones se publican en seguida de otros registros en la página web de getmonero.org.



Prototipo del monedero físico



Toma glamour



Arranque básico del firmware

ACTUALIZACIÓN DE MONERUJO

Monerujo es un equipo recién conformado, liderado por m2049r y su banda de piratas renegados. Mantienen el logro de haber sido el primer grupo en hacer un monedero para teléfonos Android con una Validación de Pago Simplificado (SPV). Buscan expandirse en otras áreas y su éxito es un ejemplo para los equipos de trabajo venideros.

Monedero Liviano para Android

Monerujo empezó cuando un miembro relativamente nuevo, **m2049r**, posteó en reddit sobre querer trabajar en un monedero para Android en agosto. En los meses siguientes, sin ayuda alguna, tuvo éxito en colocar una versión beta lista en Google Play Store de un monedero SPV funcional.

No tardó mucho tiempo en que un equipo se conformara alrededor de Monerujo, incluyendo diseñadores UX/UI, diseñadores gráficos, redactores y administradores de proyectos que hicieron del siguiente lanzamiento no solo funcional, sino accesible y estéticamente agradable.

El monedero puede ser descargado desde la tienda de Google Play Store y los usuarios pueden visitar **monerujo.io** para mayor información.

Integración de XMR.to

En noviembre del 2017, el administrador de XMR.to contacto a **m2049r** para integrar XMR.to al monedero (XMR.to es un servicio de confianza de la comunidad que paga a direcciones Bitcoin después de enviar una cantidad de Monero a ellas). Al no encontrar ningún tipo de inconveniente, lo integraron al monedero.

En el momento, los usuarios pueden pegar una dirección de XMR o de BTC en el campo de envío, o escanear el código QR obteniendo la conversión de BTC directamente de la aplicación API de XMR.to. Esto quiere decir que Monerujo se puede utilizar en cualquier parte donde Bitcoin o Monero sean aceptados.

Programación de Comunicación Interna (Firmware) del Monedero Físico

Como se señaló, la comunidad financio con éxito el desarrollo del monedero físico para depositar los Moneroj de una manera segura. Dado qué el progreso del monedero físico tuvo un progreso rápido y emocionante, cabe anotar que la propuesta en el Forum Funding System solo cubrió el desarrollo de las especificaciones del monedero fisico y no de la programación de la comunicación interna.

El equipo de Monerujo vio la oportunidad de involucrarse en el éxito de Monero y cerca del final del 2017, decidieron iniciar el desarrollo de una opción de firmware que los usuarios podrán utilizar en los monederos de Kastelo.

SE BUSCA AYUDA

El equipo se encuentra en la búsqueda de individuos apasionados y con los conocimientos que estén dispuestos a colaborar a desarrollar Monerujo para los sistemas F-Droid y iOS. Si alguien quiere ayudar, únanse al chat público de Monerujo en Mattermost (mattermost.getmonero.org) y pregunten por **m2049r**.