Bitcoin Private

PAPEL BLANCO

La revolución de la Privacidad

Cumpliendo la Vision de Satoshi desde 2018 en adelante

Febrero 2018

Par Revisado

Autores:
Bitcoin Private Community Jacob Brutman, Ph.D. Jon Layton
Christopher Sulmone
Giuseppe Stuto Geoff Hopkins Rhett Creighton

Traducido por:
Por la comunidad España

Telegram:
t.me/bitcoinprivateespanol

Twitter Oficial España:
https://twitter.com/btcprivate_es?lang=es

Grupo Oficial Facebook España:
https://www.facebook.com/groups/BitcoinPrivateEspana/

Sinopsis

Internet creó el mayor punto de inflexión de intercambio de información en la historia. Si bien hay innumerables ventajas para el fácil acceso de la vasta información, los seres humanos han sido obligados a renunciar a su privacidad a cambio. Con demasiada frecuencia, y sin culpa del usuario final, un tercero con seguridad inadecuada es hackeado y la información sensible se ve comprometida o robada. Se necesita un sistema mejor que elimine intermediarios de confianza y faculte a dos personas para que realicen transacciones libremente y de forma segura. Una nueva criptomoneda, Bitcoin Private, se presenta aquí como una red transaccional privada, rápida y de bajo costo, un verdadero cumplimiento de la hoja de ruta del creador de Bitcoin, Satoshi Nakamoto. Bitcoin Private es el producto de una combinación de bits (Fork) de Bitcoin con Zclassic. La cadena privada resultante de Bitcoin tiene tarifas significativamente más bajas que Bitcoin, junto con velocidades de transacción de cuatro a seis veces más rápidas. Lo que es más importante, se incorpora zk-SNARKs, una tecnología de privacidad revisada por pares implementada originalmente por la Fundación Zcash. zk-SNARKs permite transacciones potencialmente anónimas y privadas, un logro que ninguna otra tecnología de privacidad puede reclamar. Los conjuntos UTXO de Zclassic y Bitcoin comprenderán las monedas iniciales en este nuevo libro mayor. Esto significa que aproximadamente 20.4 millones de 21 millones de monedas existirán al momento de la bifurcación, asegurando que Bitcoin Private tendrá la inflación más baja que jamás haya existido en el universo de la criptomoneda. En conclusión, este documento técnico trata sobre Bitcoin Private, sus ventajas tecnológicas, la aplicabilidad comercial y el potencial de la cadena para el desarrollo futuro, así como su enfoque impulsado por la comunidad.

1. Introducion

Durante la mayor parte de la historia , las transacciones han sido privadas y bastante anónimas. La información de una transacción solo se divulgó al remitente y al destinatario. Actualmente, la gran mayoría de las transacciones financieras se realizan utlizando la tecnología, lo que hace cada vez más difícil mantener la privacidad financiera. Los métodos de pago más comunes (por ejemplo, tarjeta de crédito / débito, ApplePay, etc.) dan como resultado que toda la información de una transacción se almacene digitalmente. Si bien existen beneficios inmensos gracias al uso de estas metodologías de transacción, no deberían excluir el derecho de la privacidad financiera para el consumidor medio. Teniendo en cuenta la frecuencia con que ocurren las infracciones dentro de las grandes instituciones financieras y se producen filtraciones importantes de información personal y financiera, es evidente la necesidad de opciones de privacidad financiera. Además, varias instituciones financieras han sido sorprendidas vendiendo datos de clientes, ademas de haber bloqueado transacciones legales sin una base legal válida.

En octubre de 2008, Satoshi Nakamoto publicó el artículo académico titulado “Bitcoin: A Peer-to-Peer Electronic Cash System” en el que se detallaba la base de la primera criptomoneda.5 La visión de Satoshi era crear una divisa que permitiera eliminar entidades institucionales de terceros. control de transacciones, inflación limitada y libertad monetaria a través del anonimato. Desde el lanzamiento de Bitcoin en 2009, se han creado más de 1000 criptomonedas diferentes y se ha logrado un progreso inmenso.6 De hecho, muchas nuevas criptomonedas superan ampliamente a Bitcoin en términos de velocidad de transacción y recargos. En cualquier caso, Bitcoin sigue siendo la criptomoneda más popular debido a su ventaja de primer jugador y una cantidad significativa de pares de bases disponibles para el comercio.

A medida que la cadena de bloques de Bitcoin creció a través de los años, empezaron a surgir problemas notables que incluían un tamaño de bloque pequeño y fijo (que dio lugar a recargos más altos e inpracticos), tiempo de creación de bloques lento (promedio de 10 minutos), período de ajuste de dificultad largo (cada 2 semanas), y el desarrollo / producción masiva de dispositivos de minería con circuitos integrados de aplicación avanzada (ASIC) (para el cálculo rápido de SHA-256, este algoritmo es un parámetro de consenso clave) que conduce a una mayor centralización. Para que Bitcoin aborde estos elementos, la migración de más del 50% de sus mineros tendría que dar su consentimiento para cambiar el código que están ejecutando; hasta la fecha, tal evento no ha sucedido. Esto ha impulsado la creación de “Hard Forks”de Bitcoin (como Bitcoin Cash y Bitcoin Gold), para permitir algunas de estas mejoras tecnológicas. Por ejemplo, Bitcoin Cash remodelado para permitir tamaños de bloque más grandes (≥8 MB frente a 1 MB),

lo cual disminuye las tarifas y aumenta el rendimiento de la transacción. Sin embargo, esto no vino sin concesiones - su potencial de precio fue dañado debido a su carencia de un tamaño de bloque fijo y el "mercado de tarifas." El mercado de honorarios en “mempool” de Bitcoin desafía transacciones grandes y pequeñas para competir contra el recargo de oportunidad el uno del otro; esto hace que la importancia de su propiedad sea aún más urgente, lo que provoca una mayor demanda. Bitcoin Gold tomó otra ruta, reduciendo el tiempo de bloqueo (2.5 min), cambiando el algoritmo PoW a Equihash (resistente ASIC) e introduciendo un algoritmo de ajuste de dificultad mejorado, que ocurre cada bloque (Bitcoin Cash más tarde instituyó un ajuste de dificultad de cada bloque en noviembre de 2017). Cumplió en gran medida su objetivo como una “Fork” de Bitcoin compatible con GPU, pero carece de la adopción generalizada de Bitcoin, y los desarrolladores realizaron una captura de efectivo preminado que muchos argumentan es menos que ética dado que ocurrió detrás de puertas cerradas.[7] A pesar de lo mejor de intenciones, las “Forks” de Bitcoin se han mantenido indiscutiblemente detrás de Bitcoin en los mercados de criptomonedas a partir del cuarto trimestre de 2017.

En el centro de la visión de Satoshi, muchos se sienten atraídos por la capacidad de la tecnología para manifestar una unidad deflacionaria de valor financiero que también nos permite disfrutar y aprovechar el anonimato. El "Derecho a la Privacidad" es una libertad suprema en el mundo libre, y es esencial para los principios establecidos por Satoshi y la comunidad de criptomonedas. La privacidad financiera es un principio crítico en la visión de Satoshi de un nuevo mundo de divisas digital, sin embargo, muchas personas todavía están atrapadas en una encrucijada con transacciones pseudo anónimas en blockchains. Además, hay organizaciones gubernamentales y del sector privado que aprovechan los conjuntos de datos masivos y el aprendizaje automático para identificar a las personas asociadas con dicha transacción. De hecho, BitFury es capaz de desanonimizar hasta el 15% de las transacciones de Bitcoin a partir de enero de 2018, una cifra que aumenta diariamente y alterará notablemente el hemisferio de criptomoneda en los años venideros. Esta falta de privacidad en relación con Bitcoin es irónica dado el intento original de su creador, aunque, existe una solución.

Varias criptomonedas han intentado resolver este problema de privacidad. Desafortunadamente, muchos de ellos aún pueden verse comprometidos a través de diversas técnicas, debido a sus sistemas de transacción en cadena que prometen el anonimato a través de la ofuscación o los nodos TOR. En 2014, un documento de investigación innovador de los investigadores del MIT discutió "argumentos de conocimiento no interactivos de conocimiento cero", o zk-SNARKs. Sorprendentemente, las criptomonedas que implementan zk-SNARK permiten transacciones blindadas: los fondos son completamente anónimos sin que la transacción o el saldo de la dirección aparezca en el libro de contabilidad. En 2016, los autores de esta investigación desarrollaron y lanzaron Zcash, la primera criptomoneda que incorporar zk-SNARKs. Se incorporó un "impuesto al fundador" en el código de Zcash, que permite que el equipo de desarrollo y los primeros inversores obtengan el 20% de las monedas extraídas por la comunidad minera. Después de escuchar atentamente a la comunidad minera, Rhett Creighton decidió bifurcar Zcash

solo 8 días después, eliminando los impuestos del fundador y creando Zclassic, una plataforma Zcash basada en la transparencia a través del desarrollo de la comunidad. Desafortunadamente, Zclassic sufría de las mismas ideas que derivaron en su grandeza: la ausencia de un impuesto de fundador llevó a una falta de desarrollo activo. Sin embargo, existen varios métodos de gobernanza que pueden prevenir este desarrollo obsoleto.

Bitcoin Private, un supuesto "fork-merge" de Bitcoin y Zclassic, tiene la intención de agregar privacidad y capacidad de almacenamiento a la cadena de bloques de Bitcoin sin dejar de ser consciente de los desafíos, las elecciones y los fallos de las bifurcaciones anteriores. Para lograr esto, Bitcoin Private usará un tamaño de bloque más grande (2 MB), un tiempo de bloque más corto (2.5 min) y un algoritmo de prueba de trabajo (PoW) resistente a ASIC (GPU) para minería - Equihash. Además, debido a la naturaleza dual de este fork-merge, una mayor parte de la criptocomunidad se verá involucrada. Después del "snapshot" , las direcciones ZCL (t & z) y BTC (segwit y normal) recibirán BTCP (1: 1 para ambos) en la misma dirección. Este es el primer fork de su clase y la comunidad de cadena de bloques de código abierto finalmente a comenzando a explorar completamente la maleabilidad de los conjuntos UTXO.

Tabla 1: Comparación de Bitcoin Private, Bitcoin, Bitcoin Cash y Bitcoin Gold.

	BitcoinPrivate	Bitcoin	Bitcoin Cash	Bitcoin Gold
Oferta total	21 million	21 million	21 million	21 million
Privacidad	zk-SNARKs	x	x	x
Tiempo de bloque	2.5 min	10 min	10 min	2.5 min
Tamaño de bloque	2 MB	1 MB	8 MB	1 MB
PoW Algoritmo	Equihash	SHA256	SHA256	Equihash
Ajuste de dificultad	Every Block	2 Weeks	Every Block	Every Block
Preminado	x	x	x	Si
Impulsado por la comunidad	Si	x	x	x
Gobernabilidad	Si	x	x	x

2. Metodologia de la bifurcacion.

Para Bitcoin Private, se propone un "fork-merge", por el cual los UTXO de dos criptomonedas se combinan en una cadena de bloques. Esto pasará formalmente fuera de la cadena de bloques Zclassic, ya que zk-SNARKs y las transacciones JoinSplit son fundamentalmente parte de esta nueva cadena de bloques. Se puede comparar la resolución de una cadena de bloques con un mecanismo de polimerización de crecimiento de cadena: cuando se resuelve el siguiente bloque, la cadena de bloques crece, del mismo modo que un polímero crece tras la adición reactiva de monómero al extremo de la cadena del polímero. Sin embargo, aunque las cadenas de polímero más largas son generalmente deseables ya que imparten una mayor tenacidad en el plástico resultante, el aumento del tamaño de la cadena de bloques da como resultado un mayor consumo de almacenamiento, así como tiempos de sincronización de nodos significativamente más largos. Afortunadamente, esta instantánea solo necesitará recuperar el estado de la dirección de Bitcoin y Zclassic en un solo punto en el tiempo, que será llevado a la nueva cadena. Este enfoque es efectivo y da como resultado una reducción significativa en el almacenamiento requerido por la cadena de bloques, en este caso reduciéndolo de 157 GB a solo 10 GB (en el lanzamiento). Además, los clientes privados de Bitcoin apoyarán la poda de la blockchain y las técnicas SPV como Electrum para reducir la carga de blockchain en los dispositivos de los usuarios.

Un problema importante que cualquier fork debe manejar es el llamado "ataque de repetición", en el que una transacción post-fork en la cadena de bloques original se vuelve válida en la nueva cadena de bloques. Todas las bifurcaciones de monedas deben tener protección de repetición para garantizar la legitimidad e independencia de la cadena de bloques original. Para salvaguardar contra los ataques de reproducción de Bitcoin y Zclassic, Bitcoin Private contará con protección de repetición bidireccional. Este es un problema estudiado, y estamos utilizando el enfoque estándar de la industria que se incorporará de una manera bidireccional como se indicó anteriormente. Esto ya está implementado, y estamos utilizando el enfoque estándar de la industria (SIGHASH_FORKID), que está bien estudiado y ha funcionado con éxito para Bitcoin Gold.

La instantánea de Bitcoin y Zclassic está configurada para los primeros bloques marcados con fecha posterior a las 5 PM UTC del 28 de febrero de 2018, y el lanzamiento de la bifurcación / red principal ocurre aproximadamente 2 días después. Después del lanzamiento, habrá aproximadamente 700,000 Bitcoinprivate minables. Se ha seleccionado una recompensa de bloque inicial de

1.5625 Bitcoin Private junto con una reducción a la mitad cada 210,000 bloques (~ 1 año). Sin embargo, si este experimento no tiene éxito, se puede implementar un plan alternativo, que se describe en la Sección 7.

3. Prueba de trabajo: Equihash

Como se discutió en la introducción, la minería de Bitcoin es realizada principalmente por ASIC, instrumentos especializados capaces de superar significativamente a las GPU. A diferencia de las GPU, los ASIC son mucho más difíciles de adquirir y han llevado a una centralización significativa de la minería Bitcoin. De hecho, Igor Homakov ha sugerido que más del 60% de la tasa de hash de la red Bitcoin se encuentra en China.

Mientras tanto, es mucho más probable que los algoritmos resistentes a ASIC se descentralicen, ya que las GPU están más disponibles en todo el mundo. La descentralización del hash de red permite una democratización significativamente mayor de la cadena de bloques, una susceptibilidad disminuida a un ataque del 51% y garantiza que la criptomoneda generada a través de la minería, así como los aranceles asociados recaudados, se distribuyan por la comunidad de la manera más equitativa posible. Esto impide aún más la capacidad de unos pocos mineros de influir en el desarrollo de la cadena de bloques, así como de manipular el mercado mediante la minería de cantidades significativamente grandes de la criptomoneda.

Bitcoin Private utilizará el altamente reconocido algoritmo Equihash PoW, que fue desarrollado por Alex Biryukov y Dmitry Khovratovich en la Universidad de Luxemburgo como un mecanismo de prueba de trabajo asimétrico (PoW). A diferencia de otros algoritmos PoW resistentes a ASIC, Equihash esta basado en el "Problema de cumpleaños" y el algoritmo mejorado de Wagner utilizado para resolverlo. Además, Equihash presenta una "dureza de memoria" por la cual una penalización computacional pronunciada se asocia con una reducción en el uso y la velocidad de la memoria. Esta característica aumenta la resistencia a ASIC de Equihash debido al costo de implementar más memoria en los ASIC para que sean competitivos con las GPU o incluso las CPU. Los autores del documento original discuten que aunque la dureza de la memoria no protege contra la minería de CPU basada en botnets, la gran cantidad de consumo de memoria sería extrema, de modo que la base de usuarios de PC infectadas notaría una diferencia significativa en el rendimiento y tomaría las medidas necesarias para eliminar la infección

4. Transacciones transparentes vs. blindadas

Bitcoin Private es un amalgama de dos sistemas de transacción: transacciones transparentes y blindadas. Las transacciones transparentes operan con los mismos principios que Bitcoin: entrada, salida, cantidad y firma. Las fuentes de todos los fondos, destinos y cantidades se almacenan de forma transparente en la blockchain. Las transacciones blindadas, a la inversa, encriptan estos detalles en una sección especial de un bloque llamado JoinSplit. Estas transacciones son verificables pero indescifrables para observadores de terceras partes. Cuando se gastan notas blindadas, la integridad de la cadena de bloques se mantiene a través de un algoritmo

especializado de cero conocimiento llamado zk-SNARKs. Este algoritmo ejecuta una serie de cálculos para mostrar los valores de entrada sumados a los valores de salida para cada transferencia blindada. Entonces, el remitente prueba que tienen las claves de gasto privado de las notas de entrada, lo que le da la autoridad para gastar. Finalmente, las claves de gasto privado de las notas de entrada se vinculan criptográficamente a una firma a lo largo de toda la transacción, de tal forma que la transacción no puede ser modificada por una parte que no conocía estas claves privadas. Toda esta metodología se basa en la configuración confiable de Zcash: en el lanzamiento de Zcash, las claves necesarias para pruebas de conocimiento cero y las transacciones privadas se generaron y posteriormente se destruyeron; esto se llamó "La Ceremonia". Al hacer esto, el sistema puede garantizar "una fuerte e inolvidable capacidad de respuesta contra los ataques de mensajes elegidos".

5. Programa voluntario de contribución de mineros

Para crear una tesorería para el mantenimiento y desarrollo de Bitcoin Private, se lanzó un programa voluntario de contribución de mineros. En este programa, 62,500 Bitcoin Private se subastan a mineros hasta un total de 50,000 Zclassic donados al fondo de tesorería privado de Bitcoin mediante hash power. El pago para cualquier minero alistado en el programa se puede determinar mediante la siguiente ecuación:

$$P = Zm * 62,500 / Zp$$

Donde P es el pago para el minero, Zm es el Zclassic extraído por el minero, y Zp es el Zclassic total extraído por todo el grupo. Los 62,500 Bitcoin Private se generan en la bifurcación y se depositan en las direcciones de billetera correspondientes proporcionadas por cada minero. El monedero multi-sig ZCL pre-fork que se estableció para este programa contendrá hasta 50,000 Zclassic y posteriormente se bifurcará en BTCP para establecer un tesoro para el desarrollo, bonificaciones, marketing continuo y el desarrollo general de Bitcoin Private por parte de la comunidad. Este es uno de varios métodos para abordar el problema original de desarrollo obsoleto de Zclassic.

En algunos aspectos, este programa podría verse como un "preminado", concepto al que el equipo de contribución de Bitcoin Private se opone vehementemente. Sin embargo, el preminado generalmente ha sido realizado por y directamente para el grupo central y ese no es el caso aquí. En este caso, la comunidad minera puede voluntariamente optar por donar fondos a cambio de un acceso temprano incentivado a la minería de Bitcoin Private. Además, debido al estilo de subasta del

programa, la comunidad minera puede elegir cuánto valdrá cada colectivo de ZCL como colectivo (véase la ecuación anterior): este tipo de metodología de libre mercado está en el centro de Satoshi. visión original para Bitcoin. Estos fondos se utilizarán para listados de intercambio (50%), desarrollo (25%), marketing (15%) y general / administrativo (10%).

6. Gobernanza del Fondo del Tesoro

Se ha creado un consejo de gobierno de fondos del tesoro formado por tres miembros de la comunidad y dos miembros de la comunidad minera, incorporado como BTCP Developer Community, LLC. En el momento de esta publicación, Jacob Brutman, Ph.D. (Líder de Operaciones), Giuseppe Stuto (Responsable de Marketing) y Peter Hatzipetros (Asesor General) representan a la comunidad, mientras que Adib Alami y Evan Darby representan a la comunidad minera. También se preparó un documento de estatutos para el consejo.15

7. El futuro de Bitcoin Private

Mejorar la privacidad en todos los ámbitos es una parte importante del proyecto Bitcoin Private. Actualmente, zk-SNARKs consume bastante RAM y CPU durante la firma de la transacción, lo que puede llevar unos minutos. Una de las primeras mejoras implementadas después de la “fork” es el nuevo “sapling”, denominado "Jubjub", actualmente en desarrollo por el equipo de desarrollo central Zcash.16 Este nuevo árbol permitirá una mejora significativa en la velocidad y la facilidad de uso de transacciones blindadas para las monedas de privacidad zk-SNARKs. Otra metodología para mejorar la privacidad de Bitcoin Private es utilizar el proyecto de privacidad "Dandelion" actualmente en desarrollo.17 Esta técnica implica el "tallo" (las transacciones) y la "pelusa" (ofuscación). Si bien cualquier procedimiento de ofuscación es inherentemente menos seguro que zk-SNARK, la ofuscación de diente de león podría agregarse a las transacciones transparentes y protegidas de Bitcoin Private, mejorando la privacidad en general.

Permitir mejoras de Blockchain en Bitcoin Private es de gran importancia para el proyecto. BIP9 se ha incorporado a la cadena de bloques para permitir “softforks” y, por lo tanto, mejoras.18 Después de que se haya completado la codificación adecuada para las mejoras, se les pide a los mineros que indiquen que están listos para aceptar el cambio de la cadena de códigos. Cuando el 95% de los mineros acepta el cambio, se convierte en

"Bloqueado" y el “softfork” está completo. Sin embargo, si los mineros no indican la preparación dentro del tiempo especificado, el tenedor blando fallará, y no habrá cambios. El apoyo y el desarrollo del proyecto Bitcoin Private se basarán en la recolección continua de fondos del tesoro de una manera diferente a las donaciones de fondos mineros. Sin embargo, el equipo de contribución de Bitcoin Private se

opone firmemente a cualquier tipo de imposición de impuestos sobre su comunidad sin un voto democrático a favor de tal. Por lo tanto, uno de los primeros cambios propuestos a través de BIP9 involucrará los parámetros de recaudación de fondos del tesoro. De esta forma, los mineros pueden elegir cuál es la cantidad adecuada que están dispuestos a donar colectivamente para garantizar el exitoso futuro del programa.

Como se establece en la Sección 2, la baja cantidad de Bitcoin Private minable que queda después de la horquilla podría causar algunos problemas, incluida una tasa de hash de red extremadamente baja. Una posible solución es ofrecer la eliminación de las monedas que permanecen inamovibles antes de la “fork”. Si se elige esta implementación, aproximadamente el 0.14% de todas las monedas privadas Bitcoin no movidas del fork se eliminarán diariamente en el transcurso de dos años. En este escenario, las monedas de Bitcoin Private se eliminarían por igual en todas las carteras: cada billetera con Bitcoin Private sin reclamar perderá ca. 0.14% de sus monedas por día durante 2 años. Esta metodología liberaría una porción significativa de monedas para los mineros, mientras que les daría tiempo suficiente para que los usuarios reclamen sus monedas bifurcadas. Además, el bajo porcentaje de eliminación diaria debería evitar cualquier impacto en la capitalización del mercado.

Como medida de respaldo, se ha implementado una "bomba de dificultad" en Bitcoin Private para permitir un desarrollo en el futuro significativo, de forma similar a como ocurre con Ethereum.19 Cuando se utiliza, la bomba de dificultad se aplicará al antiguo código blockchain, recordando a los mineros de adoptar una nueva base de código para mejoras continuas. Este método se considera un último recurso y solo se usará en circunstancias extremas. Potencialmente, la bomba podría implementarse para introducir un nuevo sistema de gobernanza, como, por ejemplo, el sistema presentado por Decred.20 Esto permitirá una mayor democratización y descentralización del blockchain de Bitcoin Private. Actualmente, la fecha de la bomba de dificultad está establecida para el 2 de marzo, 2019, sin embargo, los “hardforks” se pueden utilizar para extender esta fecha indefinidamente. No por casualidad, la primera division se producirá alrededor de la fecha de la bomba de dificultad; esto permitirá que se realicen cambios en caso de que el experimento de baja inflación no sea exitoso.

8. Aplicaciones comerciales

El procesamiento de pagos sigue siendo uno de los casos de uso más profundos de Bitcoin en la actualidad. Es probable que los comerciantes hayan tramitado más de 1 billon de $ equivalente a Bitcoin para el año 2017 utilizando las empresas de procesamiento de pagos de Bitcoin, como BitPay. Los usuarios de Wallet de esta misma empresa obtienen más de 1 billon de $ en activos por mes y envían más de 1,500 millones de $ de billetera a billetera por mes.21 Al igual que internet trajo un nuevo y revolucionario método de pago, la criptomoneda está haciendo lo mismo.

Los consumidores esperan un cierto nivel de conveniencia cuando se trata de transferir valor a cambio de bienes y servicios, y esta es la razón por la que el procesamiento de pagos en la web se ha vuelto un lugar común. Junto con esta expectativa de conveniencia, existe un nivel supuesto de privacidad que viene con tal transacción. Desafortunadamente, en las últimas dos décadas ha habido entidades que se beneficiaron de la creación de un "perfil" en línea de un consumidor mediante el seguimiento de las transacciones con tarjeta de crédito en línea.22 Esto es increíblemente invasivo y sirve como una gran premisa de apoyo de por qué un consumidor querría realizar transacciones en línea con criptomonedas. A pesar del diseño técnico de la criptomoneda más popular, esta privacidad ya no se puede esperar en el blockchain.14 Sin embargo, Bitcoin Private podría satisfacer las necesidades de privacidad de los consumidores a través de las transacciones zk-SNARKs.

Bitcoin Private jugará un papel importante en la transferencia de activos digitales entre pares y comerciantes. Ofrece a los proveedores una tecnología de criptomoneda probada, segura y ampliamente adoptada con el beneficio adicional de anonimato y privacidad comprobables. Potencialmente, cientos de miles de casos de uso natural provendrán de Bitcoin Private en uso comercial. Mientras que otras monedas con z-protocolo podrían ser capaces de cumplir este papel, generalmente ninguno ha optado o tenido éxito. Esto es probablemente debido a los altos requisitos de CPU y memoria de las transacciones blindadas; sin embargo, el lanzamiento del “sapling” "Jubjub" permitirá transacciones blindadas móviles. El equipo de contribución de Bitcoin Private tiene un fuerte deseo de llevar la criptomoneda a la aceptación general, lo que permite un uso generalizado. Por lo tanto, se lanzará un servicio de transacción blindada amigable con el proveedor poco después del “sapling”. Además del caso del uso de proveedor web estándar, las plataformas de monedero móvil podrían utilizarse para almacenar y transferir Bitcoin Private a través de transacciones transparentes y blindadas en aplicaciones de “ brick” y “mortar”. Además, esta misma plataforma podría ser utilizada por cualquier usuario y no estaría limitada a las tiendas. A partir de ahora, Bitcoin Private ya ha sido contactado por varios vendedores y comerciantes para utilizarlo como una opción de pago para sus productos. Un porcentaje de estas transacciones comerciales podría ser recaudado para el tesoro privado de Bitcoin, lo que podría anular la necesidad de una recaudación de tesorería a través de la minería.

9. Proyecto impulsado por la comunidad

Muchos proyectos de criptomonedas, ya sean utilidades o monedas, pretenden ser impulsados por la comunidad y de código abierto. Si bien esto es cierto hasta cierto punto, normalmente existe un equipo de desarrollo central que controla todo el futuro del proyecto. Existen pocas excepciones (por ejemplo, Decors) según las cuales la comunidad tenga el control real del futuro; sin embargo, los equipos de desarrollo todavía suelen estar cerrados. Si bien los miembros de la comunidad pueden sugerir modificaciones en el código correspondiente, estas solicitudes

pueden pasar desapercibidas. El proyecto Bitcoin Private representa un verdadero esfuerzo de la comunidad, con más de 100 colaboradores actualmente (6 de febrero de 2018) y está creciendo a diario.

Se han implementado varias iniciativas que separan Bitcoin Private de otras monedas comunitarias. Por ejemplo, se ha lanzado un programa de embajadores multilingüe en todo el mundo por el cual los miembros de la comunidad pueden participar activamente para ayudar a promover Bitcoin Private y aumentar la comunidad. Además, Bitcoin Private ha abierto una "convocatoria de desarrolladores" en la que cualquiera puede postularse, incluso aquellos nuevos en la tecnología de blockchain, y contribuir de manera significativa al proyecto. Quienes no tienen experiencia previa pueden aprender de este programa de desarrollo y dominar la tecnología / ingeniería de blockchain. Estos dos programas combinados han agregado más de cien nuevos contribuyentes en un lapso de pocos días, ampliando nuestro equipo contribuyente diario a más de 300 miembros. El tamaño del equipo de contribución de Bitcoin Private muestra la dedicación del proyecto a su inspiración impulsada por la comunidad y es una hazaña que ninguna otra criptomoneda ha logrado según el mejor conocimiento del equipo. Esto muestra la naturaleza verdaderamente descentralizada del desarrollo de Bitcoin Private

10. Conclusión

Bitcoin Private es una criptomoneda desarrollada y mantenida por una diversa comunidad . Miembros del equipo de todo el mundo colaboran a diario para que este proyecto sea un éxito. Lo hacen porque creen que el proyecto cumple con la visión original de libertad financiera de Satoshi a través de transacciones rápidas, de bajo costo, descentralizadas y privadas. La inclusión con visión de futuro de Bitcoin Private de la propuesta de bipedestación BIP9 permitirá desarrollos futuros, y una bomba de dificultad incluida avanzará metodologías de gobernanza alternativas si BIP9 resulta ineficaz. Las aplicaciones comerciales de Bitcoin Private son numerosas: desde transacciones globales rápidas hasta compras en tiendas locales. Esta fusión de la vasta y dedicada tecnología de transacciones dedicadas y blindadas de Bitcoin de Zclassic marcará el comienzo de una nueva era de privacidad blockchain demostrable y sin confianza.

11. Agradecimientos

Queremos agradecer a la comunidad minera por sus generosas donaciones a través del Programa voluntario de contribución de mineros. También nos gustaría agradecer a la molécula de cafeína por ayudar al equipo a pasar muchos días y noches largos; sin café, este proyecto no podría haber sido posible. Muchas gracias también se requieren a nuestro increíble equipo de desarrollo: ustedes son la base sobre la cual confiamos. Finalmente, nos gustaría agradecer a toda la comunidad de BitcoinPrivate

- usted es la columna vertebral de este proyecto y no estaríamos aquí sin usted.

12. Referencias

[1] *Dutch Banks Tax Agency Under DdoS Attacks a Week after Big Russian Hack Reveal*. https://www.bleepingcomputer.com/news/security/dutch-banks-tax-agency-under-ddos- attacks-a-week-after-big-russian-hack-reveal/ (Accessed Feb. 5, 2018).

[2] The Biggest Data Breaches of the 21st Century. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html (Accessed Feb. 6, 2018).

[3] *What Chase and Other Banks won't Tell you about Selling your Data*. https://www.forbes.com/sites/adamtanner/2013/10/17/what-chase-and-other-banks-wont-tell- you-about-selling-your-data/#5eacaaf62c41 (Accessed Feb. 5, 2018).

[4] *Santander Totta has no Known Legal Basis to Block Bitcoin Related Transactions says Portuguese Consume Watchdog*. https://www.ccn.com/santander-totta-has-no-known-legal-basis-to-block-bitcoin-related-transactions-says-portuguese-consumer-watchdog/ (Accessed Feb. 5, 2018).

[5] Nakamoto S.; (2008) *Bitcoin: A peer-to-peer electronic cash system.*

[6] *List of Cryptocurrencies.* https://cryptocurrencyfacts.com/list-of-cryptocurrencies/ (Accessed Feb. 5, 2018).

[7] *Premine Endowment*. https://bitcoingold.org/premine-endowment/ (Accessed Feb. 2, 2018)

[8] Brandeis, L.; Warren, S.; (1890) *The Right to Privacy*.

[9] "BitFury Group De-Anonymizes Over 15% of the Bitcoin ... - The Merkle." 11 Jan. 2018, https://themerkle.com/bitfury-group-de-anonymizes-over-15-of-the-bitcoin-network-with-new-blockchain-analysis-tool/ (Accessed Jan. 30, 2018).

[10] Ben-Sasson, E; Chiesa, A; Garman, C.; Green, M,; Miers, I.; Tromer, E.; Virza, M. (2014) *Zerocash: Decentralized Anonymous Payments from Bitcoin*.

[11] *Interpreter.*cpp. https://github.com/BTCPrivate/BitcoinPrivate/blob/6b6abb3d121ba5231e5d775e9e2287dbbf7687f6/src/script/interpreter.cpp#L1089 (Accessed Feb. 9, 2018)

[12] Homakov, I. (2017) *Stop. Calling. Bitcoin. Decentralized*. https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27 (Accessed Feb. 4, 2018)

[13] Biryukov, A.; Khovratovich, D.; (2016) *Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem.*

[14] *Zcash - How zk-SNARKs works in Zcash.* https://z.cash/technology/zksnarks.html (Accessed Feb. 3, 2018).

[15] *BTCP Developer Community, LLC Bylaws.* https://btcpfoundation.org/bylaws.pdf

[16] *What is Jubjub?* https://z.cash/technology/jubjub.html (accessed Feb. 1, 2018).

[17] *Bitcoin Developers Reveal Roadmap for 'Dandelion' Privacy Project* https://www.coindesk.com/bitcoin-developers-reveal-roadmap-dandelion-privacy-project/ (accessed Feb. 5, 2018).

[18] *BIP9*. https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki (Accessed Feb. 7, 2018)

[19] *What is the Ethereum Difficult Bomb*. https://themerkle.com/what-is-the-ethereum-difficulty- bomb/ (accessed Feb. 5, 2018)

[20] *Decred Documentation.* https://docs.decred.org/ (Feb. 1, 2018)

[21] *Bitcoin Transactions aren't as Anonymous as Everyone Hoped*. https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/ (Accessed Feb. 5, 2018).

[22] *Google Now Tracks Your Credit Card Purchases and Connects them to its Online Profile of you.*

https://www.technologyreview.com/s/607938/google-now-tracks-your-credit-card-purchases- and-connects-them-to-its-online-profile-of-you/ (Accessed Feb. 5, 2018).

13. Informacion relevante.

Todo el contenido es original y ha sido investigado y producido por Bitcoin Private a menos que se indique lo contrario en este documento. Ninguna parte de este contenido puede reproducirse de ninguna forma, ni mencionarse en ninguna otra publicación, sin el consentimiento expreso de Bitcoin Private.

Este documento tiene únicamente fines informativos y no constituye una oferta de venta ni un intento de solicitar una oferta para comprar o vender ningún valor en ninguna jurisdicción donde dicha oferta o solicitud sea ilegal. No hay suficiente información en este documento para tomar una decisión financiera y cualquier información contenida en este documento no debe usarse como base para este propósito. Este documento no constituye una recomendación personal ni tiene en cuenta los objetivos particulares de inversión, las situaciones financieras o las necesidades de los lectores. Los lectores deben considerar si algún consejo o recomendación en este documento es adecuado para sus circunstancias particulares y, si corresponde, buscar asesoramiento profesional, incluido asesoramiento fiscal. El precio y el valor de la criptomoneda a los que se hace referencia en esta investigación, y los ingresos derivados de ellos, pueden fluctuar. El rendimiento pasado no es una guía para el rendimiento futuro, los retornos futuros no están garantizados y puede ocurrir una pérdida de capital original. Las fluctuaciones en las tasas de cambio podrían tener efectos adversos sobre el valor o el precio de, o los ingresos derivados de, ciertas inversiones. La información proporcionada sobre Bitcoin Private no pretende ser, ni debe interpretarse ni utilizarse como asesoramiento de inversión, fiscal o legal, una recomendación o una oferta de venta, ni una solicitud de una oferta para comprar monedas privadas de Bitcoin.

Algunas declaraciones contenidas en este documento pueden ser declaraciones de expectativas futuras y otras declaraciones prospectivas basadas en las opiniones y suposiciones de Bitcoin Private e implican riesgos e incertidumbres conocidos y desconocidos que podrían causar que los resultados, el desempeño o los eventos reales difieran materialmente de los expresados o implícitos. en tales declaraciones. Además de las declaraciones que son prospectivas por razones de contexto, las palabras "puede, quiere, debería, podría, puede, espera, planea, pretende, anticipa, cree, estima, predice, potencial, proyectado o continúa" y similares las expresiones identifican las declaraciones prospectivas. Bitcoin Private no asume la obligación de actualizar ninguna información prospectiva contenida en este documento. Si bien Bitcoin Private ha tomado las medidas razonables para garantizar que la información contenida en este documento sea precisa, Bitcoin Private no

garantiza ni garantiza (incluyendo la responsabilidad frente a terceros), expresa o implícita, su precisión, fiabilidad o integridad.