Bitcoin Vault: Oro electrónico antirrobo de igual a igual

Eyal Avramovich
github.com/bitcoinvault

Resumen. La visión original de Satoshi Nakamoto para Bitcoin era crear una versión de igual a igual de dinero electrónico. La mayoría de las bifurcaciones exitosas del protocolo intentan mejorar aún más esta visión y proporcionan un sistema de pagos más escalable y eficiente. Tenemos la percepción de la mayor promesa de Bitcoin no como un medio de intercambio, sino como una reserva de valor: una mejor forma de oro, no dinero en efectivo. A fin de cumplir esa promesa, proponemos un conjunto de modificaciones al protocolo original creando la mejor tienda electrónica de valor. Al aumentar el tiempo efectivo de confirmación de transacciones de Bitcoin de 10 minutos a 24 horas, podemos combatir el mayor defecto de Bitcoin como una forma de oro: la susceptibilidad al robo. Un sistema menos orientado a tener calderilla y más a mantener los ahorros de la vida con total tranquilidad, donde cada transacción se alerta en cadena para144 bloques y se puede cancelar en caso de emergencia con una clave de recuperación invulnerable que nunca se haya usado antes. El arranque de este sistema no es a través de la bifurcación dura sino a través de un mecanismo más justo de minería acelerada, lo que permite que el sistema recupere el Bitcoin en un corto período de tiempo. Nos gustaría dar todo el crédito al creador del documento técnico de Bitcoin Royale [1] que creó la visión del oro electrónico sin robo. Como equipo, nos gustaría avanzar con esa idea y comenzar a implementar todas las características esenciales que se mencionan a continuación y hacerla aún más avanzada con la tercera solución de clave privada que se revela como una característica adicional en el párrafo 6.2.

1. Introducción

Bitcoin [2] es un innovador sistema de pago descentralizado lanzado en 2009 que permite a las partes realizar transacciones directamente sin pasar por una institución financiera de confianza. El sistema se basa en la evidencia de trabajo para mantener un libro de contabilidad distribuido sin un operador confiable, que sea seguro siempre que los nodos honestos controlen más potencia de CPU que cualquier grupo cooperante de nodos atacantes. Satoshi Nakamoto, su creador, describió el Bitcoin originalmente como un «sistema de efectivo electrónico».

A lo largo de los años, se han lanzado múltiples modificaciones exitosas del protocolo original en forma de bifurcaciones de la base de código de Bitcoin, que incluyen Litecoin [3] lanzada en 2011 para reducir el tiempo de confirmación de la transacción y cambiar el algoritmo de prueba de trabajo para favorecer el hardware de nivel de consumidor como GPU; Bitcoin Cash [4] lanzada en 2017 para escalar el rendimiento de las transacciones del protocolo original al aumentar el tamaño del bloque; y Bitcoin Gold [5] lanzada también en 2017 para hacer obsoletos los equipos de minería especializados al cambiar el algoritmo de hash.

Fiel a la visión original, el enfoque principal en estas bifurcaciones y otros es hacer de Bitcoin un mejor sistema de efectivo. Las limitaciones del protocolo original, como las altas tarifas de transacción, los tiempos de confirmación de 10 minutos y el rendimiento aproximado de solo 4 transacciones por segundo, obstaculizan la capacidad de Bitcoin de competir con los sistemas de pago centralizados en línea dominantes en la actualidad.

2. Dinero electrónico u oro electrónico

Aunque Bitcoin no tuvo mucho éxito a la hora de ser adoptado por el consumidor como efectivo electrónico, sí que ha tenido más éxito como una forma de oro electrónico. Existe un largo debate en la industria sobre si Bitcoin es superior como medio de intercambio o como una reserva de valor. El oro no es un medio efectivo de pago para los bienes y servicios del día a día. Los consumidores invierten principalmente en oro para protegerse contra la inflación y preservar el poder adquisitivo futuro. A diferencia de las monedas nacionales, la política monetaria fija de Bitcoin y el suministro limitado lo hacen particularmente atractivo a este respecto.

La historia muestra que los sistemas rara vez se pueden diseñar para cumplir varios objetivos competitivos a la vez, de forma que la optimización de Bitcoin para convertirse en un mejor medio de intercambio disminuye su potencial como depósito de valor. En el mismo sentido, podemos mejorar de forma considerable su utilidad como oro electrónico si sacrificamos aún más las propiedades requeridas para efectivo electrónico útil. En este documento, proponemos una serie de modificaciones al protocolo original de Bitcoin centrado en un solo objetivo: crear el depósito de valor definitivo.

Si ya no damos prioridad a competir como un sistema de pago en línea, no necesitamos centrarnos en las tarifas de transacción o el rendimiento de la transacción. Después de todo, el oro es costoso de transportar y normalmente se adquiere para inversiones a largo plazo. Una propiedad que es particularmente relevante para nuestros esfuerzos es el tiempo de confirmación de la transacción. Las compensaciones en este frente, como el aumento sustancial del tiempo promedio de confirmación de 10 minutos de Bitcoin, pueden generar ventajas esenciales. Como no esperaríamos cargar un envío de oro a través de ubicaciones en menos de 10 minutos, este sacrificio parece natural.

3. El problema del robo

El requisito clave de una reserva de valor es ser imperecedera. El robo es uno de los principales riesgos de pérdida cuando se trata de algo de valor y el oro funciona bastante bien en este sentido. El robo físico de oro es significativamente más arriesgado de ejecutar que cualquier ataque virtual a un activo electrónico. Además, a un ladrón le resultaría difícil esconder una carga considerable de oro robado de las autoridades, especialmente a través de las fronteras. El lavado y liquidación de oro robado en grandes cantidades mientras permanece anónimo tampoco es una tarea sencilla.

Desafortunadamente, a Bitcoin en este sentido está en desventaja. Los fondos están protegidos por el protocolo con conjuntos de claves privadas criptográficas. Obtener acceso electrónico a estas claves le permite al atacante confiscar todos los fondos de forma remota, inmediata e irrevocable. El lavado de fondos robados también es significativamente más fácil ya que las transacciones son seudónimas,

la trazabilidad puede verse interrumpida por el uso de mezcladores [6] y se pueden crear identidades de Sybil en masa. Como resultado, el robo de criptomonedas está aumentando con más de mil millones de dólares robados en 2018 [7]. Las listas de incidentes importantes reportadas por la comunidad [8] muestran que incluso las instituciones profesionales bien informadas sobre las últimas prácticas de seguridad son propensas a los ataques.

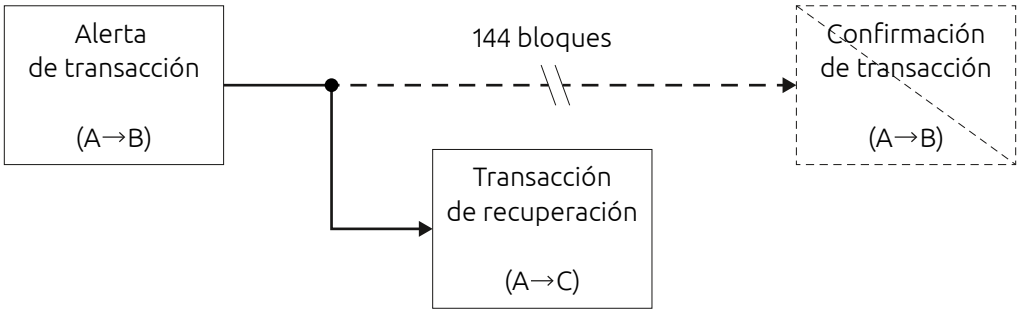
La gestión segura de las claves privadas por parte de los usuarios finales está demostrando ser uno de los principales desafíos de Bitcoin. Dado que las claves deben usarse regularmente para interactuar con los fondos y las transacciones firmadas deben transmitirse a través de Internet, finalmente cada clave se vuelve vulnerable. Las prácticas conscientes de la seguridad, como dividir los fondos entre monederos «calientes» y «fríos» son engorrosas y no resuelven el problema de raíz. Los incidentes muestran que los monederos calientes inevitablemente contienen cantidades significativas [9, 10] y el uso de monederos fríos solo reduce la interacción con las claves pero no las elimina por completo [11].

4. Solución antirrobo

Proponemos una solución para evitar el robo basada en una nueva y sofisticada secuencia de comandos de bloqueo y modificación del protocolo. Por defecto, una transacción realizada con el nuevo script de bloqueo se retrasará 24 horas. Cuando un minero agrega una transacción a un nuevo bloque, la transacción ya no se confirmará de inmediato. En cambio, se agregará en la cadena como una alerta por la duración de 144 bloques (suponiendo un tiempo de bloque de 10 minutos). Si no se altera durante 144 bloques, la transacción cambiará del estado de alerta a «confirmado».

El beneficio de las alertas en cadena es que los propietarios de monedas recibirán notificaciones anticipadas sin censura cada vez que muevan sus monedas. El propietario tendrá 24 horas para actuar sobre la alerta y podrá anular la transferencia si no está autorizada. Las retiradas retrasadas son un estándar probado de la industria antirrobo en monederos de custodia y el sistema bancario tradicional. Coinbase Vault [12], por ejemplo, tiene un tiempo de espera de 48 horas. Nuestra solución propuesta proporciona la misma protección sin un tercero de confianza.

La anulación de emergencia de una transacción en estado de alerta requiere una transacción de recuperación especial y se lleva a cabo de inmediato sin estar sujeta al retraso de 24 horas. La transacción de recuperación requiere una clave de recuperación especial que debe incorporarse al script de bloqueo durante la creación del monedero. Una vez que se ha registrado una clave de recuperación para un monedero determinado, no se puede cambiar.



La clave de recuperación privada utilizada para la anulación de emergencia está destinada a ser una clave nueva que nunca se ha utilizado antes. Esta clave se puede generar sin conexión y nunca se debe conectar a Internet ni a ningún dispositivo. El proceso de registro solo requiere la parte pública de esta clave, asegurando que la clave privada pueda permanecer sin usar. A diferencia de las claves de monederos frío que deben usarse ocasionalmente y, por lo tanto, son vulnerables al robo, la clave de recuperación se usará por primera vez solo en la anulación de emergencia y, por lo tanto, puede ser completamente resistente al robo. Una vez que se ha utilizado la clave de recuperación, debe considerarse comprometida y todos los fondos deben transferirse inmediatamente a un nuevo monedero protegido por una nueva clave de recuperación no utilizada.

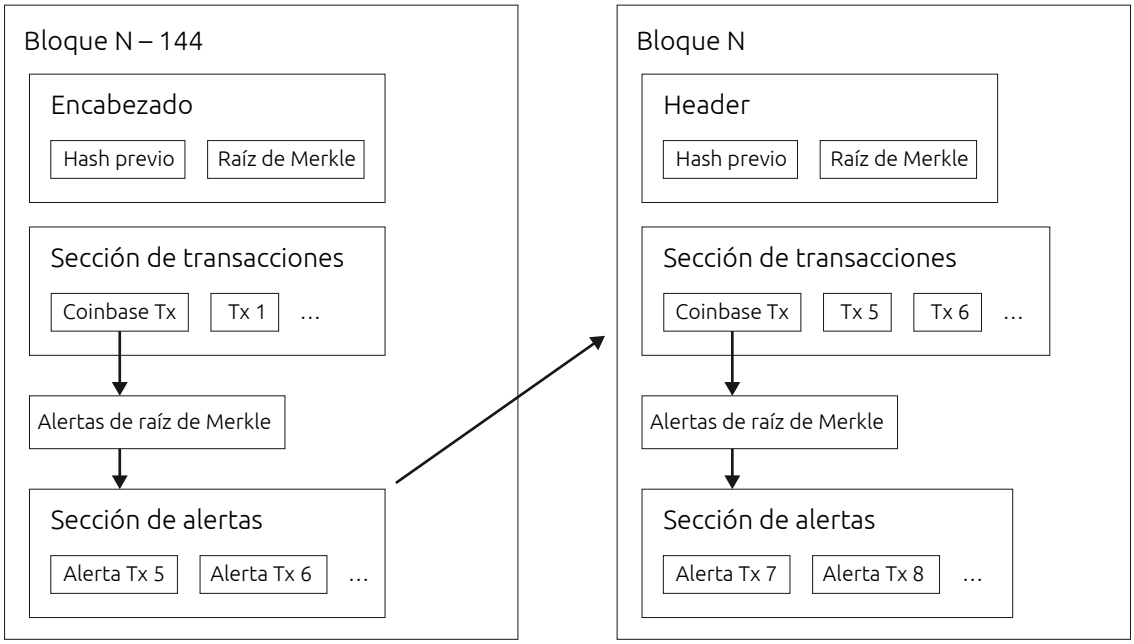
El concepto original de Bitcoin Royale de oro digital suponía retrasar todas las transacciones en el sistema durante 24 horas, haciendo que la moneda sea un depósito de valor seguro y de movimiento lento. Nos gustaría ampliar este concepto para aprovechar lo mejor de dos mundos: el oro digital y el efectivo digital, sin comprometer la seguridad.

Junto con las alertas de movimiento lento, condicionalmente mantenemos las transacciones rápidas e «instantáneas». Para proporcionar la máxima seguridad, el envío de dicha transacción requerirá que un usuario realice una 2FA basada en blockchain, utilizando la tercera clave proporcionada durante la creación del monedero.

5. Bloques

Al igual que el protocolo original de Bitcoin, cada bloque contiene una lista de transacciones confirmadas y contiene el hash raíz de Merkle de estas transacciones en su encabezado. Dado que algunas transacciones deben esperar 24 horas en la cadena, no se pueden agregar de inmediato a la sección de transacciones de un bloque. En cambio, se agregan a una nueva sección especial que no existe en el protocolo original de Bitcoin: la sección de alertas. El hash de raíz de Merkle para la sección de alertas se almacena en la entrada de la transacción de Coinbase manteniendo la compatibilidad del encabezado de bloque con el Bitcoin original.

Cuando se extrae un nuevo bloque, el minero mira hacia atrás 144 bloques y examina la sección de alerta del bloque N-144. Todas las alertas para transacciones que aún son válidas se confirman y llenan la sección de transacciones del nuevo bloque.



Los pasos para minar el bloque N son los siguientes:

1) Agregue nuevas transacciones regulares para bloquear la sección N alertas (no confirmado).
2) Agregue nuevas transacciones instantáneas para bloquear la sección de transacciones N (confirmado)
3) Agregue nuevas transacciones de recuperación a la sección de transacciones del bloque N (confirmado).
4) Vaya a la sección de alertas del bloque N-144 y agregue las transacciones válidas para bloquear la sección de transacciones N (confirmado).

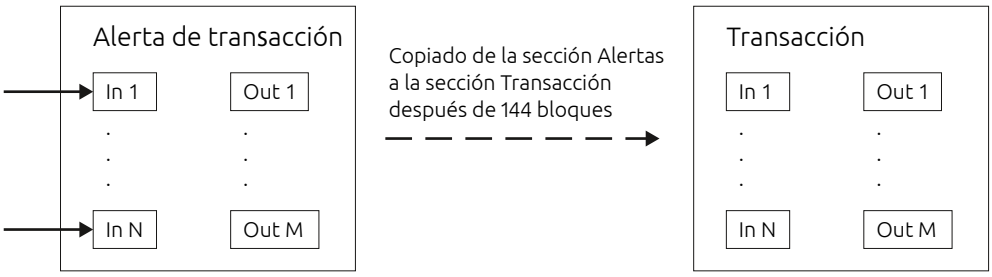
6. Scripts

La funcionalidad principal de Bitcoin Vault está disponible a través del sofisticado script de bloqueo, que se comporta de manera diferente en función del número de firmas presentadas en el script de desbloqueo. Hay dos variantes disponibles:

1. Script de bloqueo de alertas: requiere una o dos firmas. Si se presenta una firma, se genera una transacción de alerta. Si se presentan dos firmas, se genera una transacción de recuperación.
2. Alerta + secuencia de comandos de bloqueo instantáneo: requiere una, dos o tres firmas. Si se presenta una firma, se genera una transacción de alerta. Si se presentan dos firmas, se genera una transacción instantánea. Si se presentan las tres firmas, se genera una transacción de recuperación.

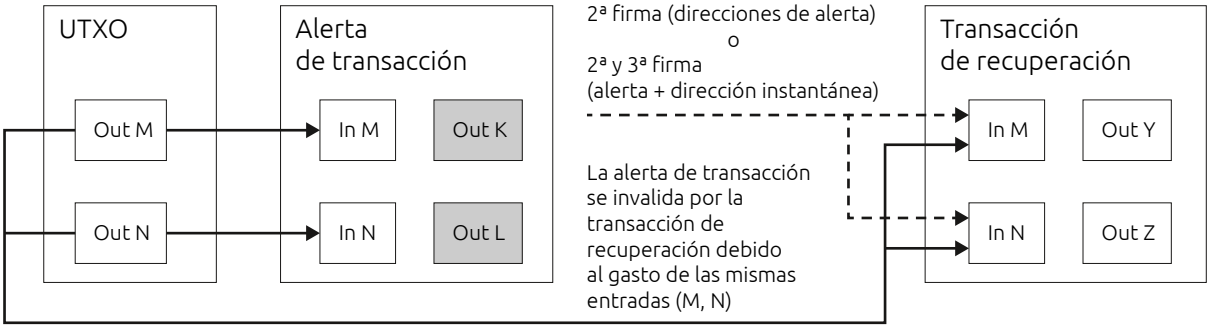
7. Transacciones

Las transferencias de monedas se realizan utilizando transacciones regulares idénticas a las del protocolo Bitcoin. Su formato no cambia a medida que pasan de la sección de alertas a la sección de transacciones.



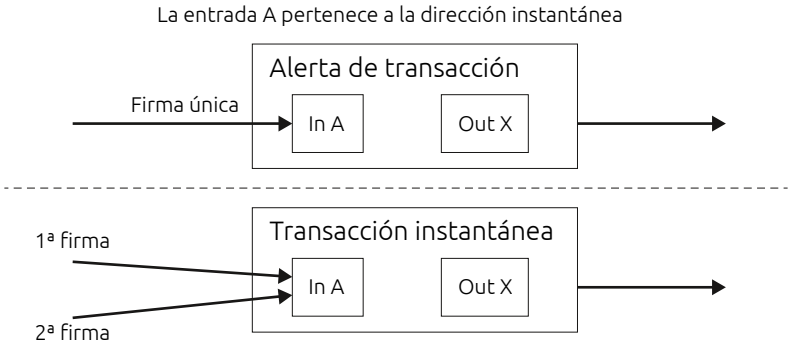
7.1. Transacciones de recuperación

Una transacción de recuperación gasta el mismo UTXO que la alerta recuperada. La diferencia es que presenta más firmas para el mismo UTXO: 2 en caso de script de bloqueo de alerta o 3 en caso de script de alerta + bloqueo instantáneo. Cuando se procesa una transacción de recuperación, se gasta el UTXO recuperado, lo que invalida las alertas existentes que dependen de este UTXO y evita que se confirmen después de su retraso de 24 horas.



7.2. Transacciones instantáneas

Una transacción instantánea permite omitir el retraso predeterminado de 24 horas para la confirmación de la transacción y acelerar la confirmación de la transacción a unos 10 minutos. Su mecanismo es similar a los monederos protegidos por tecnología multisig. Requiere una firma adicional de una clave privada separada que debe almacenarse de forma segura en una ubicación separada. Es por eso que las transacciones instantáneas solo se pueden enviar desde direcciones P2SH especiales: direcciones instantáneas, generadas a partir de la secuencia de comandos de alerta + bloqueo instantáneo.



8. Compatibilidad

Nuestro diseño intenta hacer que el protocolo sea lo más compatible posible con el protocolo estándar de Bitcoin. El objetivo subyacente es minimizar los cambios de código necesarios en los nodos completos, billeteras, pools y mineros de Bitcoin existentes. Sin embargo, si los cambios se realizan en una cadena de bloques ya existente, requieren una bifurcación dura.

Para evitar cambiar el formato del encabezado del bloque, lo que hace que la moneda sea incompatible con los mineros ASIC de bitcoin, el hash de raíz de Merkle para la sección de alertas se almacena en la entrada de la transacción estándar de Coinbase.

Si se requierela bifurcación dura, nuestro objetivo es hacer que la transición sea lo más fácil posible para los usuarios de monedas existentes. No todos los tipos de script existentes cambian su comportamiento, por lo que todas las monedas existentes antes de la bifurcación dura se pueden gastar de la manera habitual. Sin embargo, le recomendamos encarecidamente que cambie a los nuevos scripts más seguros.

9. Incentivo

El sistema toma prestado el modelo de incentivos de Bitcoin que ha demostrado tener éxito en la última década. La incorporación de alertas requiere modificaciones menores a este modelo. Los mineros están incentivados para incluir las alertas de transacciones en un bloque mediante la promesa de una tarifa calculada a partir de la diferencia entre el valor de los productos y los insumos. Las tarifas se calculan a partir de las futuras transacciones en bloque y se distribuyen al minero original, el que incluye alertas de transacciones.

El futuro minero seguirá recibiendo recompensa de bloque por extraer un nuevo bloque, todas las tarifas del nuevo instante, las transacciones de registro y recuperación y la promesa de una tarifa futura de las alertas de transacciones. Las reglas de consenso obligan al futuro minero a incluir todas las alertas del bloque N-144 a las secciones de transacciones, excluyendo las que se recuperaron.

En caso de cancelación de la alerta, las tarifas para el minero original de la alerta son irrecuperables y el costo total es la tarifa de la alerta original más la tarifa por la transacción de recuperación.

10. Trabajo relacionado

Estamos particularmente impresionados con el trabajo de Malte Möser et al. sobre los convenios de Bitcoin [13]. Su extensión del lenguaje de script de Bitcoin permite restricciones en el uso futuro de monedas, que pueden usarse para implementar una variedad de medidas de seguridad. El principal de dichos lenguajes son las transacciones de bóveda, que se asemejan a nuestro mecanismo de retiros retrasados propuesto.

Hemos optado por una implementación más simple que no requiere una matriz recursiva de scripts personalizados para ser implementados por billeteras. Nuestra propuesta es más que una extensión opcional, es un cambio fundamental en el protocolo con un amplio efecto obligatorio en las transacciones. Transmitir la carga de la implementación a los mineros y dejar la experiencia de transacción del usuario final idéntica a la predeterminada, nos permite llevar a cabo mejor nuestra misión de crear oro electrónico verdadero.

Referencias

1. Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
2. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://www.bitcoin.org/bitcoin.pdf, 2008.
3. Litecoin Project, “Litecoin, open source P2P digital currency”, https://litecoin.org, 2014.
4. “Bitcoin Cash”, https://www.bitcoincash.org, 2018.
5. bitcoingold.org, “Bitcoin Gold”, https://bitcoingold.org, 2018.
6. J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, “Coinparty: Secure multi-party mixing of bitcoins”, In: *CODASPY ’15*, 2015.
7. CipherTrace, “Cryptocurrency Anti-Money Laundering Report, 2018 Q4”, https://ciphertrace.com/crypto-aml-report-2018q4, 2019.
8. “BLOCKCHAIN GRAVEYARD”, https://magoo.github.io/Blockchain-Graveyard, 2019.
9. C. Zhao, “Binance Security Breach Update (May 7 2019)”, https://binance.zendesk.com/hc/en-us/articles/360028031711, 2019.
10. J. Buck, “Coincheck: Stolen $534M ln NEM Were Stored On Low Security Hot Wallet“, https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet, 2018.
11. J. Preissler, “Important Notice: Only trade TIO on trade.io”, https://medium.com/@trade.io/important-notice-only-trade-tio-on-trade-io-823d59fd7104, 2018.
12. KM. Cutler, “Coinbase Launches A More Secure Bitcoin Storage Option Called ‘Vault’”, https://techcrunch.com/2014/07/02/coinbase-vault, 2014.
13. M. Möser, I. Eyal, E. Gün Sirer, “Bitcoin Covenants”, In: *Financial Cryptography and Data Security, FC 2016, Lecture Notes in Computer Science*, Vol. 9604. Springer, Berlin, Heidelberg.