



Libro Blanco de Bitcoin Vault

Eyal Avramovich, Kacper Wiśniewski, Piotr Kozłowski, Radek Popiel et Anon
Whitepaper v1.0

Resumen

En 2009, una persona anónima o un equipo de desarrolladores anónimos creó la primera red entre pares basada en la tecnología de blockchain que permitía a los usuarios transferir fondos entre direcciones de hash anónimas. La revolución de Bitcoin había comenzado. Resultó en una serie de bifurcaciones del concepto original.

Uno de ellos ha llevado al concepto de Bitcoin Vault.

Nuestro objetivo como desarrolladores era mejorar la blockchain existente con características únicas que dieran a los usuarios más control y aumentaran su nivel de seguridad con la forma en que se gestionan las direcciones de los monederos, se almacenan las claves privadas y públicas y se transfieren los activos entre individuos. Queríamos crear una moneda que ofreciera todas las ventajas de Bitcoin con características adicionales para que los usuarios tuvieran el máximo control de sus activos de forma fácil y cómoda sin comprometer la flexibilidad que ofrecen las criptomonedas.

Con la inmutabilidad de la blockchain como característica clave detrás de los libros de contabilidad distribuidos, vimos no sólo ventajas sino también, por nuestra propia experiencia, peligros relacionados con los fondos perdidos, extraviados o robados. Con varios cambios en el código y la forma en que se utilizan las claves públicas y privadas en el ecosistema de la blockchain, se nos ocurrió la idea de hacer reversibles las transacciones irreversibles sin comprometer la inmutabilidad de la blockchain.

Contenido

Introducción	3
Declaración del problema	3
Misión y Visión	3
Acercamiento de BTCV	4
Solución de Seguridad de 3 Claves	4
Ecosistema de Bitcoin Vault	4
Gold Wallet	4
Key Generator	5
Electrum Vault	5
Perspectiva Técnica	6
Prueba de Trabajo	8
Minería Combinada	8
Recompensas por Bloque	9
Desarrollo de Bitcoin Vault	11
Etapas de desarrollo de BTCV:	11
Mainnet	11
Hoja de ruta	11
Línea de trabajo nº 1: Mejoras de desarrollo	11
Línea de trabajo nº 2: Mejoras de seguridad	12
Línea de trabajo nº 3: Actualizaciones de la experiencia del usuario	12
Línea de trabajo nº 4: Productos	12
Línea de trabajo nº 5: Actividades de marketing	13
Línea de trabajo nº 6: Otras actualizaciones.	13
Computación Cuántica y DLT: Nuestra vision	14
Amenaza de la computación cuántica	14
Oportunidad de la computación cuántica	14
Fundador de Bitcoin Vault	15
Trabajos relacionados	15
Fuentes de BTCV:	15
Referencias	15

Introducción

Bitcoin Vault (BTCV) fue lanzado en 2019 como cadena alfa. Se desarrolló intensamente entre diciembre de 2019 y noviembre de 2020, cuando se lanzó una funcionalidad clave que permite realizar en la blockchain transacciones reversibles.

Bitcoin Vault es la primera criptomoneda del mundo que permite a los usuarios cancelar las transacciones después de que se hayan publicado en la blockchain. Este revolucionario enfoque es posible con un protocolo de blockchain personalizado que confirma los pagos dentro de 144 bloques (o dentro de unas 24 horas). Esta funcionalidad protege a los usuarios contra la pérdida de sus fondos en caso de robos comunes de claves, equivocaciones del usuario o errores y fallos.

Bitcoin Vault es una bifurcación dura de Bitcoin Royale, que añade al proceso una clave privada, lo que da un total de tres claves. Desde su lanzamiento a finales de 2019, hemos ampliado los fundamentos técnicos y de mercado en línea con una ambiciosa hoja de ruta que se extiende hasta 2022 y más allá.

Declaración del problema

Según el informe de CipherTrace sobre crímenes de criptografía y lavado de dinero de la primavera de 2020, en los primeros cinco meses de ese año, los robos, hackeos y fraudes de criptografía ascendieron a un total de 1,36 mil millones de dólares.

Las bolsas de criptomonedas deben recuperar diariamente los fondos de los usuarios que fueron enviados por error a las direcciones equivocadas. Esto les cuesta tiempo y dinero y no garantiza que los fondos de esos usuarios sean recuperados.

No hay fuentes fiables sobre cuántos activos criptográficos, monedas, fichas se transfieren cada día a direcciones conocidas de estafas, hackeos o se pierden debido a ataques del tipo “hombre en el medio”.

Creemos que una parte importante de lo anterior podría evitarse si el usuario tuviera la simple posibilidad de cancelar y revertir las transacciones salientes tan pronto como se diera cuenta de que cometió un error, que se robaron bienes o que alguien obtuvo acceso no autorizado a su monedero de criptomonedas.

Misión y Visión

BTCV fue desarrollado para proporcionar un nivel extra de seguridad basado en la Solución de Seguridad de 3 Claves que permite a los usuarios revertir ciertos tipos de transacciones en la blockchain. Cuenta con toda la comodidad de Bitcoin, mientras que añade importantes funcionalidades que permiten la transparencia y la libertad del usuario. Bitcoin Vault es nuestra respuesta a los problemas a los que se ha enfrentado la comunidad criptográfica durante la última década, los cuales son principalmente:

1. Acceso no autorizado a los monederos debido a los hackeos o al acceso a las claves privadas de los usuarios,
2. Errores humanos con el envío de activos criptográficos a direcciones de monedero equivocadas u otro tipo de errores relacionados con la introducción errónea de cantidades de transferencia o con la equivocación de la cantidad de transferencia con la cantidad de gas,
3. Errores, fallos y otras cuestiones relacionadas con el software de criptomonedas.

El desarrollo del BTCV se centra en las funcionalidades de seguridad y protección, la comodidad y la experiencia del usuario, ya que también creemos que éstos son los desafíos clave que impiden que una parte significativa de la sociedad forme parte de la comunidad mundial de criptografía.

Acercamiento de BTCV

Las criptomonedas dieron a los usuarios libertad y responsabilidad sobre la forma en que almacenan, administran y transfieren fondos a través de las redes P2P. En este libro blanco, asumimos que todo usuario de las criptomonedas debe estar familiarizado con el concepto de clave pública y privada y saber cómo almacenar y asegurar las claves de forma segura. Sobre la base de este supuesto, hemos desarrollado un nuevo enfoque relativo a la gestión de las claves y su utilización para diversos tipos de transacciones.

Solución de Seguridad de 3 Claves

Bitcoin Vault desarrolló una solución de seguridad de 3 claves que requiere que los usuarios generen tres claves de algoritmo de firma digital de curva elíptica (ECDSA), donde una se almacena automáticamente dentro de la aplicación y las otras dos deben ser gestionadas por el usuario. La configuración actual de Bitcoin Vault permite a los usuarios cancelar la transacción iniciada y revertirla a una dirección de un monedero existente o nuevo.

La solución soporta tres claves de ECDSA con diferentes roles en el ecosistema:

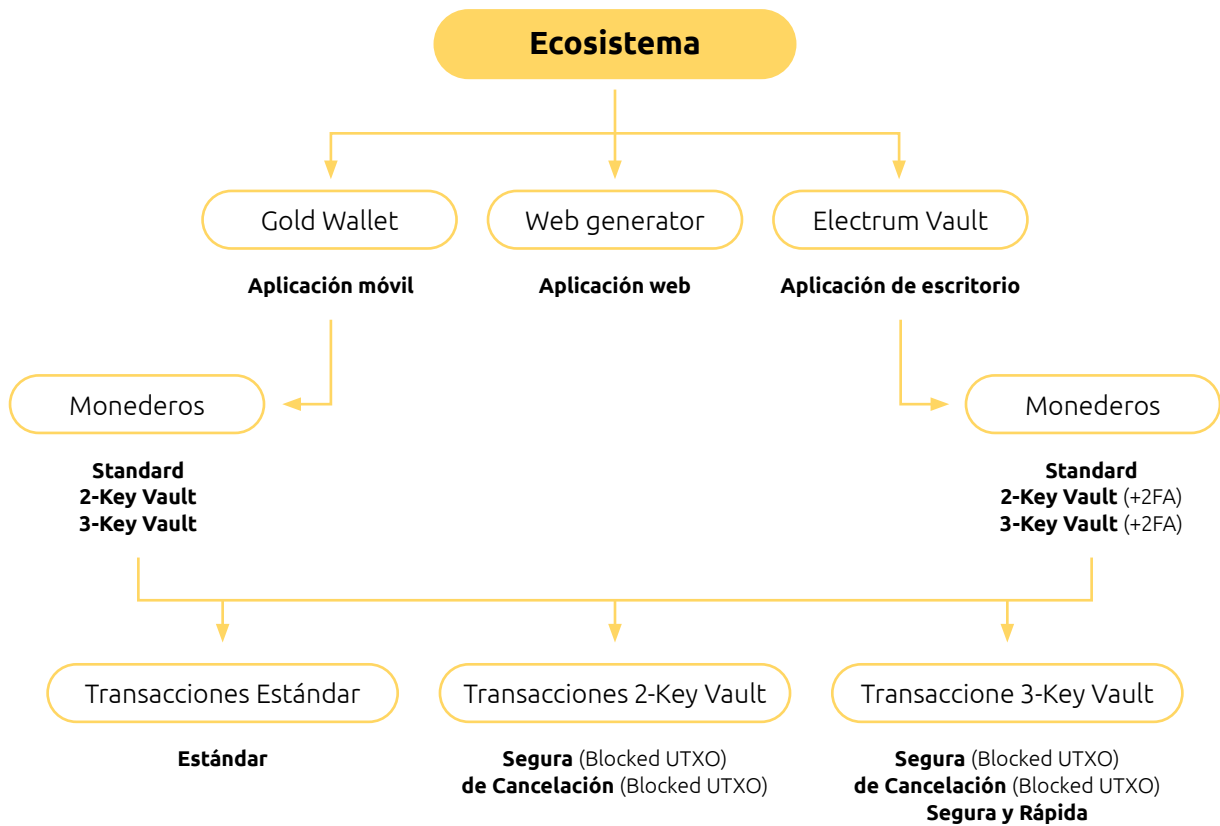
- La clave de transacción estándar se genera automáticamente y funciona en segundo plano. Es necesaria para iniciar todas las transacciones y para recuperar el monedero en caso de hackeo informático o problema técnico.
- La Clave de Transacción de Cancelación permite a los usuarios realizar transacciones de cancelación en un plazo aproximado de 24 horas, después de que se generen 144 bloques.
- La Clave de Transacción Rápida les da a los usuarios la posibilidad de hacer transacciones rápidas seguras y transferir BTCV en cuestión de minutos.

Ecosistema de Bitcoin Vault

El ecosistema de Bitcoin Vault incluye tres aplicaciones creadas internamente con el único propósito de almacenar y gestionar el BTCV. Juntas, forman una poderosa herramienta que garantiza un mayor estándar de seguridad, transparencia y libertad.

Gold Wallet

Gold Wallet es una aplicación para dispositivos móviles diseñada para almacenar, enviar y recibir BTCV. Permite a los usuarios crear tres tipos de monederos y realizar varios tipos de transacciones, entre las que se incluyen las Transacciones Seguras y Rápidas, Seguras y de Cancelación. Gold Wallet también puede ser utilizado como un autenticador para la autenticación de dos factores (2FA) para la aplicación de escritorio Electrum Vault.



Key Generator

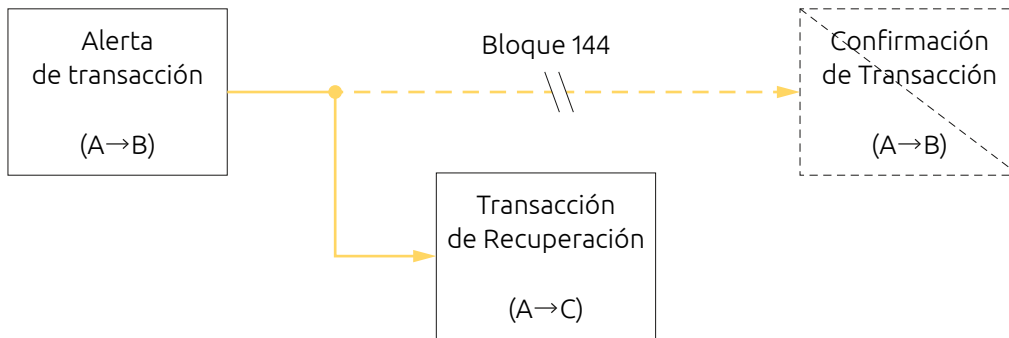
Key Generator es una aplicación basada en la web que genera las claves públicas y privadas individuales necesarias para configurar monederos y realizar transacciones. Utiliza sólo recursos locales, lo que significa que el proceso de generación de claves, así como las propias claves, nunca salen del dispositivo del usuario. No se almacenan en ningún lugar y no se puede acceder a ellas en línea. Las claves se almacenan fuera de línea, proporcionando el máximo nivel de seguridad.

Electrum Vault

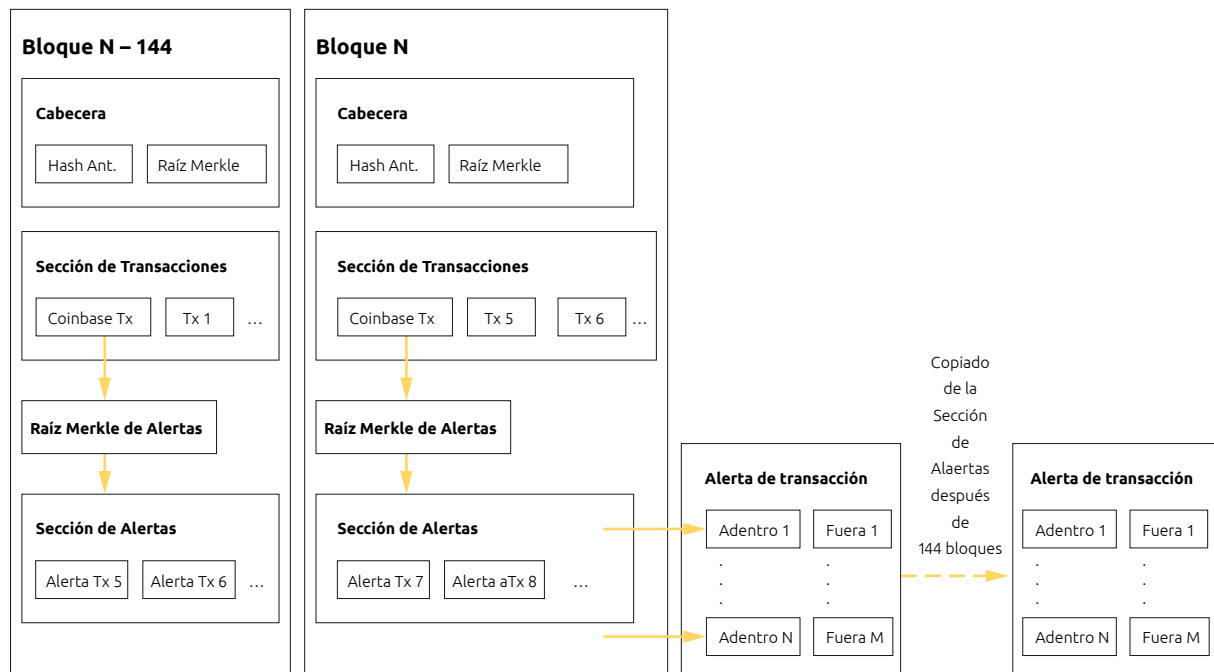
Electrum Vault es una aplicación de escritorio basada en el monedero Electrum de código abierto. Tiene todas las funcionalidades de Gold Wallet, lo que significa que puede ser utilizada para almacenar, enviar o recibir BTCV, crear monederos y realizar transacciones, incluyendo las Transacciones Seguras y Rápido, Seguras y de Cancelación.

Perspectiva Técnica

Guión de bloqueo, retraso por defecto de 144 bloques, transacciones de alerta en la cadena:



Estructura de bloque de BTCV con sección de alerta (cómo se almacena, qué sucede cuando la transacción cambia de estado de alerta a confirmado, cómo los mineros verifican cuando la transacción cambia de estado).



Las Alertas de Transacciones cambian el ciclo de vida de las UTXOs.

En la versión estándar, UTXO tiene dos estados: no gastado y gastado (lo que básicamente significa que se elimina). La nueva versión de Bitcoin Vault introduce un nuevo estado: confirmado. Esto cambia la forma en que los UTXO se almacenan en la base de datos. A partir de ahora, el estado "confirmado" es el momento en que se elimina la UTXO de la base de datos y el estado "gastado" bloquea la UTXO y

almacena la información sobre la altura del bloque en el que se ha gastado. De esta manera, el sistema espera a que se confirme la Alerta de Transacción antes de eliminar la UTXO.

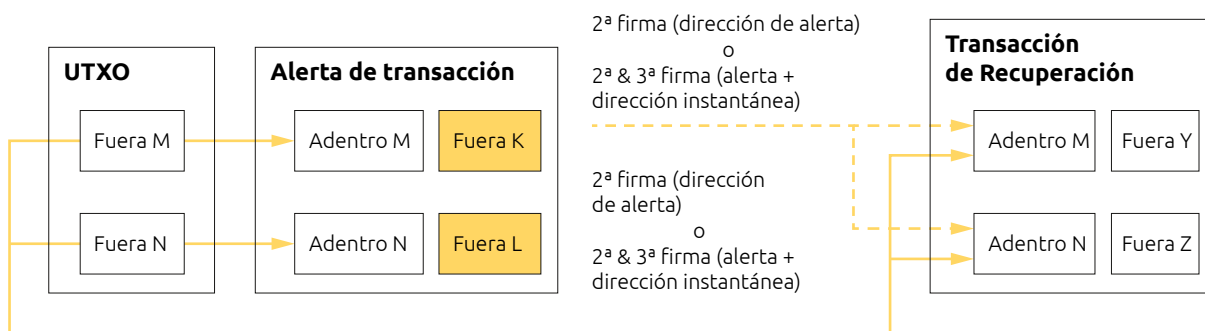
Es un enfoque necesario porque, hasta que se reciba la confirmación, la Alerta de Transacción podría recuperarse con la Transacción de Recuperación (utiliza sólo UTXO bloqueada como entrada). La mejor manera de alterar el ciclo de vida de UTXO en la aplicación sería almacenar información sobre la altura en la que se ha gastado: altura gastada. Esta nueva información determinará en qué estado se encuentra la UTXO:

- 0 cuando no se ha gastado,
- >0 cuando se ha gastado.

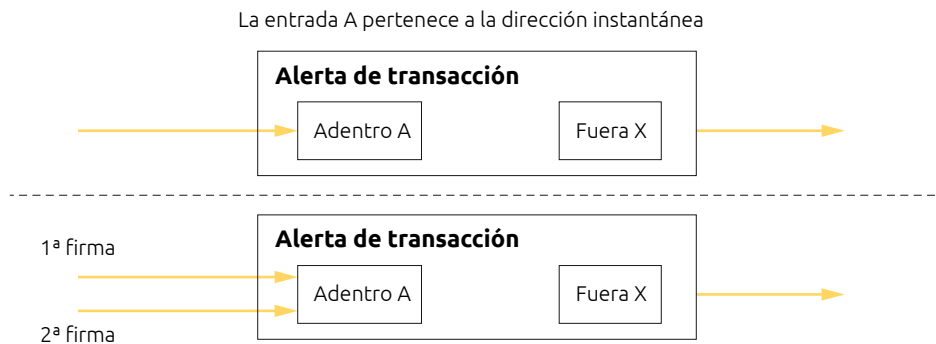
Además, la misma información debe considerarse en la estructura Deshacer. La lista Deshacer almacena la información de estados previos de UTXO a diferentes alturas y utiliza dicha información cuando se produce una reorganización de la cadena.

Los nuevos estados y tipos de transacciones de UTXO también tienen un impacto en los saldos visibles para los usuarios. Las UTXO que están en estado de gasto deben contarse como un nuevo saldo que será visible en el saldo confirmado. No pueden contarse como saldo no confirmado porque ese saldo está relacionado con transacciones no minadas y gastables. La idea es crear saldos no gastables pero informativos:

- alertas salientes: contadas a partir las UTXOs en estado gastado, que son bloqueadas por Alertas de Transacciones,
- alertas entrantes: contadas a partir de las UTXOs que van a estar disponibles después de la confirmación de las Alertas de Transacciones.



Cómo funciona la Transacción Rápida (explicación de la desviación de la demora de 24 h; lo que la hace posible: multi-firmas):



Prueba de Trabajo

Bitcoin Vault es una moneda de prueba de trabajo basada en el código fuente abierto de Bitcoin Royale. Con la bifurcación realizada el 17 de noviembre de 2020, se implementó una minería combinada con Bitcoin (BTCV).

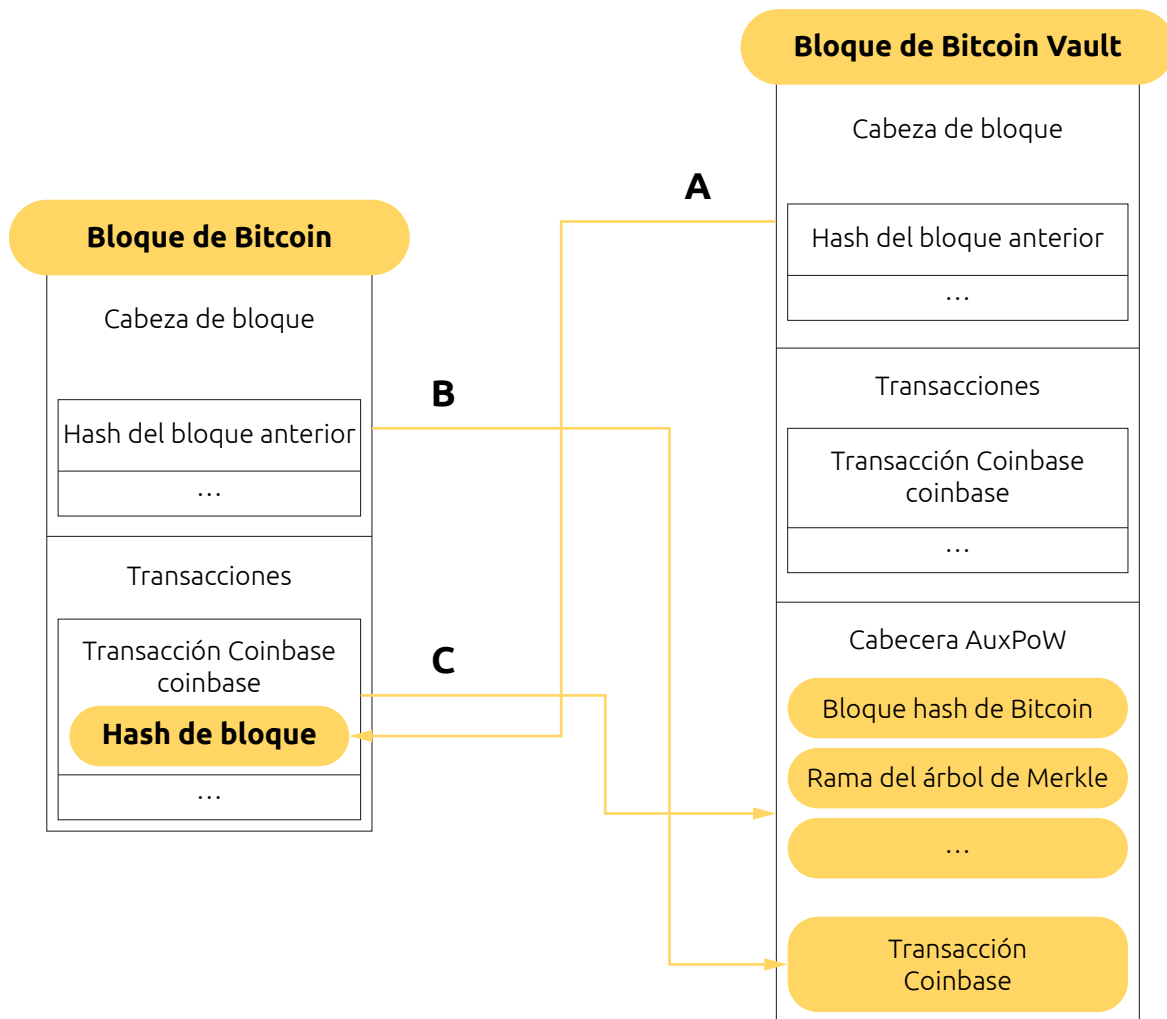
Minería Combinada

Junto con la importante actualización del protocolo BTCV en el bloque número 58 420, Bitcoin Vault también fue ajustado para admitir la minería combinada. La minería combinada, también conocida como Prueba de Trabajo Auxiliar, es un proceso en el que los mineros buscan simultáneamente el PoW de al menos dos criptomonedas separadas con la misma potencia de cálculo. Sin embargo, para construir esa relación entre las blockchains, la matriz y la auxiliar, es más fácil cuando la cadena auxiliar está preparada para el cambio.

En Bitcoin Vault, se implementó la minería combinada con Bitcoin, ya que ambas criptomonedas utilizan la función hash SHA-256. En este caso, BTC es la cadena matriz y BTCV la cadena auxiliar.

Como resultado, las soluciones de prueba de trabajo (matriz) de Bitcoin se pueden utilizar para validar Bitcoin Vault (cadena auxiliar) como un mecanismo de consenso de prueba de trabajo (AuxPoW).

Explicación técnica con ejemplo gráfico de la estructura de bloques y la relación entre los bloques BTC y BTCV:



Con la implementación de la minería combinada al protocolo, los mineros del BTCV se ven incentivados por la posibilidad de obtener dos recompensas de bloque tanto del BTC como del BTCV. Un incentivo adicional consiste en que gracias a la potencia de hash adicional añadida a la red por el piggybacking de la red Bitcoin con una tasa de hash más alta, se aumenta la seguridad de la red.

Recompensas por Bloque

Bitcoin Vault tiene un suministro total de 21 millones de monedas y un tiempo estimado de minería de un bloque de 10 minutos.

La recompensa por bloque de Bitcoin Vault se diseñó para eliminar ciertos problemas que surgen en las primeras etapas del desarrollo de la criptomoneda. Se identificaron dos problemas principales:

El período inicial para conseguir nuevos participantes es demasiado corto para alcanzar el número adecuado de miembros de la comunidad necesarios para el desarrollo sostenible del proyecto.

Las recompensas por bloque después del período inicial disminuyen drásticamente. Esto podría desalentar a los mineros a seguir participando en el proceso de minería y dar lugar a importantes caídas en la potencia de hash.

Para prevenir tales amenazas, Bitcoin Vault propuso las siguientes soluciones:

- Extender el período con mayores recompensas de bloque a 46 meses.
- Dividir este período en nueve subperíodos más cortos, cada seis meses, con una reducción más gradual de la recompensa por bloque.

Esto permite al equipo que está detrás del proyecto tener suficiente tiempo para el desarrollo. La comunidad tiene la oportunidad de crecer hasta alcanzar números significativos, se incentiva a los mineros a participar en la red desde los primeros días por un período más largo y hay suficiente tiempo para que el número de monedas alcance a Bitcoin sin causar una reducción drástica de las recompensas por bloque.

Durante ese período, la reducción de las recompensas por bloque está programada de la siguiente manera:

Fecha	Reducción de la Recompensa de BTCV	Número de subperíodo	Recompensa por bloque	Tiempo de subperíodo	Bloques de subperíodo
Mayo 2020	175 a 150	1	175	6 months	29850
Nov. 2020	150 a 125	2	150	6 months	26600
Mayo 2021	125 a 100	3	125	6 months	26600
Nov. 2021	100 a 75	4	100	6 months	26600
Mayo 2022	75 a 50	5	75	6 months	26600
Nov. 2022	50 a 25	6	50	6 months	26600
Mayo 2023	25 a 12,5	7	25	6 months	26600
Nov. 2023	12,5 a 6,25	8	12.5	6 months	26600
Mayo 2024	6,25 a 3,125	9	6.25	6 months	26600

Como resultado, se van a distribuir 19 687 500 monedas durante este período, alcanzando el número de Bitcoins del 4º halving (estimado para el 11 de marzo de 2024). Después de eso, la recompensa por bloque de BTCV seguirá el programa de halving de Bitcoin.

Desarrollo de Bitcoin Vault

Etapas de desarrollo de BTCV:

Mayo 2019 – Diciembre 2019	Pre-Alpha
Diciembre 2019 – Septiembre 2020	Alpha
Septiembre 2020 – Noviembre 2020	Beta
Nov. – 2020	Mainnet

Mainnet

Mainnet fue lanzada con éxito el 17 de noviembre de 2020 con el número 58 420 de altura de bloque.

Hoja de ruta

En diciembre de 2020, el equipo de desarrollo de BTCV lanzó un nuevo plan de trabajo que abarca los años 2021-2022. El desarrollo posterior del BTCV se dividió en seis líneas de trabajo:

Línea de trabajo nº 1: Mejoras de desarrollo

La línea de trabajo de desarrollo se refiere a todas las actualizaciones de la blockchain que se añadirán a Bitcoin Vault. El objetivo principal de esta línea de trabajo es participar en el ecosistema Dapp alrededor de Ethereum 2.0 con BTCV envuelto (wBTCV) hasta finales de 2021.

- 1er trimestre 2021
 - wBTCV ERC-20 token – análisis y tokenómicos detrás wBTCV
- 2º trimestre 2021
 - Integración del libro mayor (ledger)
- 3er trimestre 2021
 - wBTCV ERC-20 token, fase de pruebas beta
- 4º trimestre de 2021
 - Lanzamiento de BTCV
 - Inicio de integración con DeFI ecosystem
- 1er trimestre 2022
 - Integración total con el ecosistema DeFI
 - Desarrollo de Dapps (aplicaciones descentralizadas)
- 2º trimestre 2022+
 - Desarrollo de Dapps (aplicaciones descentralizadas)

Línea de trabajo nº 2: Mejoras de seguridad

Bitcoin Vault tiene un equipo interno de expertos en seguridad de blockchain. La integridad de la blockchain de Mainnet ha sido verificada en numerosas ocasiones y en 2021 nuestro principal objetivo será reforzar el código e identificar cualquier error y agujeros dejados, también con el apoyo de socios externos. Después de las pruebas de penetración internas y externas, ejecutaremos un programa de premios abierto para los desarrolladores y trabajaremos estrechamente con la comunidad de “sombrero blanco”.

- 1er trimestre 2021
 - Auditoria de código completa (interna y externa)
- 2º trimestre 2021
 - Pruebas de penetración (internas)
- 3er 2021
 - Pruebas de penetración (externas)
- 4º trimestre 2021
 - Auditoría de seguridad CIS/20
 - Matriz de Seguridad en la Nube
- 2022+
 - Más mejoras de seguridad y auditorías
 - Hackathons
 - Programa de recompensas

Línea de trabajo nº 3: Actualizaciones de la experiencia del usuario

La experiencia de los usuarios es uno de los factores más importantes para el uso y la adopción del producto. Nuestro objetivo es seguir desarrollando y actualizando las aplicaciones y adaptarlas a las necesidades de una gran variedad de usuarios en base a las opiniones recibidas de la comunidad.

- 1er y 2º trimestre 2021
 - mejoras UX de la aplicación móvil GoldWallet
 - Electric Vault: aplicación móvil con opción de modo fácil y modo experto
- 3er trimestre 2021
 - GoldWallet: notificaciones para usuarios
- 4º trimestre 2021
 - Integración de GoldWallet con aplicaciones de terceros
- 2022+
 - Otras mejoras UX

Línea de trabajo nº 4: Productos

Junto con el desarrollo de la tecnología de información, nos estamos centrando fuertemente en la adopción de mercado con nuevos productos en preparación. En 2021, queremos lanzar productos de staking con el apoyo de los socios de BTCV y conectar el ecosistema de BTCV con las monedas FIAT.

- 1er trimestre 2021
 - Nuevos productos del staking a través de terceros
 - Nuevos productos de comercialización

- 2º trimestre 2021
 - Nuevas pasarelas de pago
 - integraciones FIAT
- 3er trimestre 2021
 - Plataforma de análisis de datos (Big Data)
- 4º trimestre 2021
 - Productos relacionados con el token de wBTCV
- 2022+
 - Nuevas funcionalidades 3Keys
 - productos dApps (aplicaciones descentralizadas)

Línea de trabajo nº 5: Actividades de marketing

En 2021, planeamos lanzar una campaña mundial de concienciación y compromiso dirigida a los usuarios actuales y futuros de BTCV, así como a toda la comunidad criptográfica del mundo. Buscaremos nuevas asociaciones que fortalezcan la seguridad de la blockchain de BTCV y que permitan al BTCV estar a la vanguardia de la investigación cuántica.

- 1er trimestre 2021
 - Lanzamiento de una nueva página web
- 2º y 3er trimestre 2021
 - Campaña mundial de sensibilización y compromiso
- 4º trimestre 2021
 - Asociación estratégica de seguridad
- 2022+
 - Asociación científica estratégica

Línea de trabajo nº 6: Otras actualizaciones

Con algunas mejoras adicionales al ecosistema del BTCV, queremos conectar y colaborar con nuestra comunidad y ofrecer nuevas opciones para los hodlers a través de un nuevo mecanismo de airdrops que se lanzará en su totalidad a principios del segundo trimestre de 2021. Nuestro enfoque a largo plazo estará también en torno a la computación cuántica y su potencial para influir en la criptografía de la blockchain.

- 1er trimestre 2021
 - Desarrollo y lanzamiento del nuevo mecanismo de airdrops
 - Lock del monedero de airdrops
- 2º trimestre 2021
 - Plataforma / aplicación de airdrops
- 3er trimestre de 2021
 - Plataforma de análisis de Blockchain
- 4º trimestre 2021+
 - Investigación Cuántica
 - Programa de subvención con asociación científica

Computación Cuántica y DLT: Nuestra vision

Como la mayoría de los desarrolladores de blockchain estamos realmente interesados en el progreso de las tecnologías cuánticas. Los investigadores y desarrolladores que trabajan en las tecnologías de libro mayor distribuido (DLT) como Blockchain dependen de la criptografía de clave pública y de las funciones de hash que son esenciales para todas las soluciones de blockchain.

La blockchain de Bitcoin Vault está asegurada por potentes algoritmos criptográficos como ECDSA y SHA-256, también utilizados en Bitcoin, así como en muchas otras criptomonedas. Los algoritmos de cifrado utilizados actualmente son lo suficientemente potentes para los métodos computacionales tradicionales.

Amenaza de la computación cuántica

En teoría, la mejora exponencial de la potencia de cálculo con la tecnología cuántica puede llevar al punto en que puede ser posible descifrar una clave pública para calcular el hash de la clave privada o romper el algoritmo SHA-256 para obtener el bloque de valor de hash de una sola vez requerido en la blockchain. De acuerdo con muchos expertos en el campo, todavía estamos a años de investigación del desarrollo de computadoras cuánticas estables. Incluso entonces, esas computadoras necesitarían estar adecuadamente codificadas con el propósito de romper ciertos algoritmos criptográficos.

Oportunidad de la computación cuántica

En lugar de centrarnos en las amenazas, nos gustaría centrarnos en las oportunidades.

Una vez más, en teoría, cuando las computadoras cuánticas sean capaces de alcanzar la suficiente estabilidad para realizar cálculos fiables, sería posible utilizarlas para mejorar los algoritmos criptográficos. Ésta es la oportunidad que vemos para el futuro de la blockchain.

En la actualidad, podemos considerar diferentes enfoques para lograr el objetivo de una moneda resistente a lo cuántico, es decir:

- criptosistemas basados en retículos,
- criptosistemas de clave pública de base multivariante,
- criptosistemas de isogenias de curvas elípticas supersingulares,
- criptosistemas de firma digital basados en hash,
- soluciones híbridas como las probadas por Google (CECPQ1 y CECPQ2)
- y algunos otros.

Para encontrar una solución anticuántica adecuada y preparar la moneda BTCV para una era post-cuántica, nuestro equipo de desarrollo necesita hacer más investigación en términos de las técnicas necesarias de compresión de clave y del uso de ciertos tipos de códigos y técnicas de codificación.

Sin embargo, hoy en día, no hay algoritmos de blockchain post-cuánticos que proporcionen un tamaño de clave pequeño, tamaños de firma/hash cortos, ejecución rápida, baja complejidad computacional y bajo consumo de energía, todo al mismo tiempo. Estos factores son especialmente críticos para los dispositivos incorporados con recursos limitados, como los utilizados en la Internet de las cosas.

Durante los próximos 3 a 5 años, nosotros, los desarrolladores de BTCV, nos centraremos en alcanzar la preparación operativa en la resistencia cuántica a través de nuevas asociaciones, especialmente con expertos de diversas empresas, empresas de nueva creación y universidades técnicas.

Fundador de Bitcoin Vault

Bitcoin Vault fue fundada por Eyal Avramovich, CEO de Minebest, uno de los principales operadores mundiales de instalaciones de minería criptográfica situadas en Asia y Europa.

Más información sobre Minebest se puede encontrar aquí: <https://minebest.com/>

Más información sobre el equipo detrás de Bitcoin Vault se puede encontrar en el sitio web oficial: <https://bitcoinvault.global/>

Trabajos relacionados

Nos gustaría dar crédito a los creadores de Bitcoin Royale por la idea conceptual que llevó al desarrollo de Bitcoin Vault.

Libro Blanco de Bitcoin Royale: <https://bitcoinroyale.org/bitcoinroyale.pdf>

Fuentes de BTCV:

Se puede encontrar información adicional sobre el proyecto:

<https://bitcoinvault.global/>

<https://twitter.com/vaultbitcoin>

<https://medium.com/bitcoin-vault-btcv>

https://t.me/Bitcoin_Vault

<https://www.facebook.com/bitcoinvaultofficial>

<https://www.instagram.com/bitcoinvaultofficial>

<https://www.youtube.com/c/BitcoinVault>

Referencias

1. Bitcoin Whitepaper, Satoshi Nakamoto, <https://bitcoin.org/bitcoin.pdf>
2. Bitcoin Royale: Peer-to-Peer No-Theft Electronic Gold, Ian Duoteli Fleming, <https://bitcoinroyale.org/bitcoinroyale.pdf>
3. Cryptocurrency Anti-Money Laundering and Crime Report, Spring 2020, <https://ciphertrace.com/cryptocurrency-anti-money-laundering-and-crime-report-spring-2020/>
4. The Chainalysis 2020 Crypto Crime Report, <https://go.chainalysis.com/2020-Crypto-Crime-Report.html>

5. Bitcoin, crypto-coins, and global anti-money laundering governance, Malcolm Campbell-Verduyn, https://www.researchgate.net/publication/322596368_Bitcoin_crypto-coins_and_global_anti-money_laundering_governance
6. Namecoin project, <https://www.namecoin.org/>
7. Bitcoin Wiki, Merged Mining Specifications, https://en.bitcoin.it/wiki/Merged_mining_specification
8. Adam Back, Hashcash – A Denial of Service Counter-Measure, <http://www.hashcash.org/papers/hashcash.pdf>
9. Phil Daian, Rafael Pass, Elaine Shi; Snow White: Robustly Reconfigurable Consensus and Applications, <https://eprint.iacr.org/2016/919.pdf>
10. Wrapped Tokens A multi-institutional framework for tokenizing any asset <https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf>
11. Smart Contract Extensibility with Wrapped Tokens <https://yos.io/2019/07/13/smart-contract-extensibility-wrapped-tokens/#:~:text=Wrapped%20Tokens%20is%20a%20design,two%20versions%20at%20any%20time.>
12. Aleksei Pupyshev, Ilya Sapranidi, Elshan Dzhabarov, Shamil Khalilov, Ilya Teterin, Graviton: interchain swaps and wrapped tokens liquidity incentivisation solution, <https://arxiv.org/ftp/arxiv/papers/2009/2009.05540.pdf>