Whitepaper

Fundy: custodia avanzada con TimeLocks y Miniscript

Juan Carlos De La Torre, Miguel Fortes, Diego García

Bitcoin, custody, timelocks, miniscript

En el ámbito de las criptomonedas, la seguridad en la custodia de los activos es esencial. Sin embargo, la complejidad técnica y la falta de mecanismos de seguridad avanzados en la gestión de fondos de Bitcoin han limitado su adopción por parte de usuarios menos técnicos. Este WhitePaper aborda dicho desafío mediante la presentación de una prueba de concepto como solución de custodia avanzada para Bitcoin, basado en los conceptos de Miniscript y Timelocks. Se presenta un caso de uso específico que ilustra cómo un padre y un hijo podrían compartir la custodia de los fondos de una manera segura, permitiendo que el hijo libere fondos bajo circunstancias excepcionales.

Introducción

La custodia avanzada es una solución de seguridad que implementa medidas adicionales para salvaguardar los fondos en una transacción, al establecer condiciones específicas para la liberación de los fondos, sólo en circunstancias determinadas.

En la actualidad, las wallets tradicionales de Bitcoin carecen de funcionalidades de custodia avanzada en relación con las transacciones, limitándose únicamente a operaciones básicas sin bloqueos temporales ni condiciones específicas para acceder a los fondos. Estas wallets, debido a su diseño y arquitectura, no admiten este tipo de custodia, lo que las hace primitivas y poco flexibles.

La solución para ello, ha surgido con el desarrollo de una wallet de nueva generación como prueba de concepto, de la cuál se ha puesto un fuerte enfoque en la implementación de la custodia avanzada en cuestión de control condicional de fondos. Se ha centrado en la liberación de los fondos mediante transacciones tipo *Pay-to-Witness-Script Hash* [1] (P2WSH), una mejora de las existentes *Pay-to-Script-Hash* [2] (P2SH) que permite añadir un script con una condición a cumplir dentro de una transacción con mejores premisas. En este caso incluye un script de bloqueo mucho más completo con ayuda del lenguaje y tecnología Miniscript. Este script incluye uso de *Timelocks* [3] (añadidos en BIP-65,BIP-68, BIP-112 y BIP-113) que permiten liberar los fondos en un bloque especificado como una condición temporal.

Marco teórico

Una wallet en el dominio Bitcoin, es un programa o dispositivo que permite a los usuarios almacenar, enviar y recibir criptomonedas como el Bitcoin. Funciona mediante la generación de un par de claves criptográficas: una clave pública, que se utiliza para recibir fondos, y una clave privada, que se utiliza para acceder y gastar los fondos. La wallet mantiene un registro de las transacciones, y firma digitalmente las operaciones salientes con la clave privada correspondiente. La importancia de una wallet radica, en que es el medio para gestionar de forma segura las criptomonedas, puesto que proporciona control sobre los activos digitales y protege contra el acceso no autorizado.

Con la reciente inclusión de miniscript y descriptores, se ha presenciado cómo el paradigma de las billeteras, tal como se conoce, irán experimentando cambios significativos.

Miniscript es un lenguaje de scripting utilizado en Bitcoin que simplifica y mejora la legibilidad de los scripts de transacciones [5]. Fue desarrollado para facilitar la creación de scripts complejos al tiempo que mantiene la seguridad y la flexibilidad de Bitcoin. La principal característica de Miniscript es su enfoque en la composición modular, permite a los desarrolladores combinar una serie de operaciones y condiciones comunes para crear scripts de manera más intuitiva. Asimismo, Miniscript se basa en políticas (policy language), que especifican qué condiciones deben cumplirse para que una transacción sea válida.

Un ejemplo de Miniscript con una política simple: los fondos solo pueden ser gastados si el propietario presenta una firma válida y otra condición basada en el tiempo (tras 1000 bloques):

```
and_v(v:pk(K),older(1000))
```

- *pk(K)*. Clave pública del propietario
- *older(1000)*. 1000 bloques deben de ser minados para que los fondos puedan ser desbloqueados.

Esta tecnología, se usa en Bitcoin para crear scripts de transacción más simples y seguros, facilitando la construcción de contratos inteligentes y escenarios de gasto condicional. Al utilizar Miniscript, los desarrolladores pueden reducir errores y mejorar la legibilidad de los scripts, lo que a su vez, contribuye a una mayor seguridad y facilidad de uso en la gestión de transacciones en la red Bitcoin.

Por otro lado, los descriptores son una característica introducida en la biblioteca de Bitcoin Core para simplificar y mejorar la gestión de claves y scripts en transacciones. Los **descriptores** son una representación en forma de normas de cómo los scripts y direcciones deberían ser generadas, como si se trataran de un manual de instrucciones [4]. Un descriptor es una cadena de texto que describe una estructura de clave o script, puede incluir información sobre el tipo de clave - pública o privada -, condiciones de gasto - firmas múltiples o límites de tiempo - y otras propiedades relevantes.

```
wpkh([d34db33f/44'/0'/0'/0]xpub6ERApfZwUNrhLCkDtc
HTcxd75RbzS1ed54G1LkBUHQVHQKqhMkhgbmJbZRkrgZw4kox
b5JaHWkY4ALHY2grBgd9JU1jR5e3GK4Piz3fqzyzm)
```

Este descriptor representa una cartera de Pay-to-Witness-Public-Key-Hash (P2WPKH) que sigue el estándar BIP44 para la jerarquía de claves.

Siendo los componentes de este descriptor los siguientes:

- *wpkh*: Es la función que genera un script de gasto P2WPKH. P2WPKH es el formato de dirección SegWit nativo que utiliza hashes de claves públicas para las direcciones.
- *[d34db33f/44'/0'/0'/0']*: Es el prefijo del derivado de la clave. La cadena d34db33f es el "fingerprint" de la clave maestra y /44'/0'/0'/0' es el camino de derivación BIP44 que identifica la cuenta específica.
- *xpub...zyzm*: Es la clave pública extendida (xpub) que se utilizará como semilla para derivar las claves públicas de las direcciones de la cartera.

El uso de estos simplifica la creación de scripts de transacción al permitir una especificación más clara y concisa de los requisitos de gasto. Asimismo, facilita la construcción de contratos inteligentes y escenarios de gasto condicional, ya que los descriptores encapsulan la lógica compleja en una estructura legible.

Falta destacar la inclusión de Timelocks en este nuevo modelo de wallets:

Los **timelocks** mencionados anteriormente, son una característica de Bitcoin que permite establecer restricciones temporales en las transacciones. Se utilizan para la gestión avanzada de fondos y ofrecen control adicional sobre cuándo se pueden gastar los fondos. Cuando se aplica un timelock a una transacción, se especifica un período de tiempo durante el cual los fondos estarán bloqueados y no se podrán gastar. En términos técnicos, los timelocks se implementan mediante el uso de scripts en las transacciones de Bitcoin.

Para concluir, los timelocks son reglas especiales que dicen cuándo se puede usar el dinero, es decir, son como un temporizador que permite hacer cosas en ciertos momentos. Y, los descriptores son instrucciones especiales que ayudan a organizar y manejar el dinero de forma más fácil, y por lo tanto, a alto nivel se vería como un manual de cómo gastar el dinero de manera inteligente.

En los próximos años, se efectuará una transformación de las wallets en formas totalmente innovadoras, gracias a la implementación de estas nuevas tecnologías.

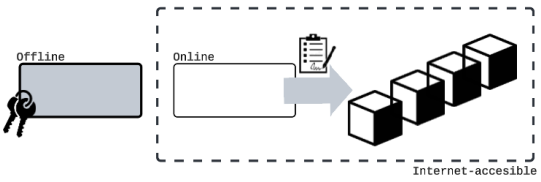
Wallet de custodia avanzada

Nuestra prueba de concepto de wallet creada está estructurada en dos partes:

Por un lado, la parte online que se encuentra conectada a internet y hace toda la funcionalidad que no necesita de claves privadas, como la información de todas las addresses, creación de la PSBT y la inclusión de la transacción a la blockchain. Esto protege las claves de una posible brecha de seguridad.

Por otro lado, en la parte offline, que a su vez se divide en la parte para el padre y la del hijo. La funcionalidad que se observa, utiliza información delicada que debe estar protegida. Si eres el hijo, podrás generar el mnemonic, la clave pública y firmar la PSBT cuando se active la condición de tiempo. Mientras que, en la parte del padre, se podrá generar el mnemonic, el descriptor de la wallet y firmar la PSTB en cualquier momento.

Por último, para el desbloqueo de fondos se ha diseñado un script en el cual el dueño de la wallet - padre -, será capaz de desbloquearlos en cualquier momento. Sin embargo, el heredero de los fondos tendrá acceso a partir de una fecha concreta, elegida por el dueño. Todo ello, es posible gracias a que se ha introducido un timelock a la hora de generar el descriptor.



- Para realizar la prueba de concepto entre las tecnologías que se han utilizado para la implementación cabe remarcar el modelo server-client gracias a Node.Js. La interfaz gráfica con ayuda de Javascript y Bootstrap.

  Importante enmarcar la utilización de las librerías de **bitcoin core** y la de **bitcoinerlab** para la generación de descriptores y direcciones compatibles a Miniscript.

  A la hora de convertir esta prueba de concepto en una solución de uso particular es imprescindible desacoplar la lógica del

servidor y adaptarla a una solución cliente, mediante Electron o React.Js.

Caso de uso

Padre e Hijo (Regalo de cumpleaños)

Respecto a lo mencionado anteriormente, se lleva en práctica un caso dónde un padre pretende hacer un regalo a su hijo por su 18 cumpleaños.

1. El hijo generará el mnemonic y su clave pública. Este guardará el mnemonic y pasará la pública a su padre.

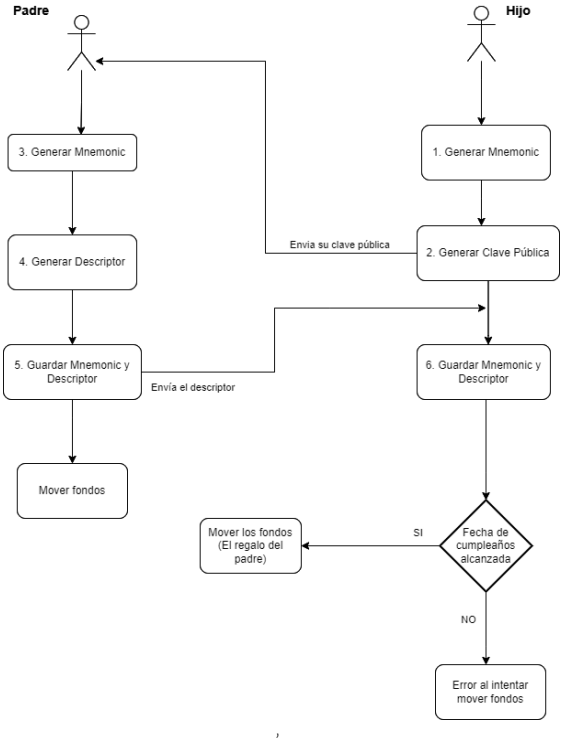
2. El padre recibirá la clave pública del hijo, creará su propio mnemonic y generará un descriptor usando la fecha de cumpleaños y la clave de hijo.

3. El padre le pasará el descriptor generado al hijo

4. Tanto el padre como el hijo, guardarán su propio mnemonic y el descriptor en común.

5. Con estos datos, el padre ya puede mover los fondos sin ningún problema. El hijo aún no tiene acceso a los fondos.

6. Una vez llegue la fecha de cumpleaños del hijo, éste será capaz de mover los fondos y recibir su regalo.



Beneficios de la solución

Este novedoso modelo de wallet permite compartir los mismos fondos entre dos personas distintas sin necesidad de compartir el mnemonic o clave privada. Además, su característica de bloqueo temporal (timelock) lo hace aún más interesante que las wallets existentes con multifirma.

Esta solución revolucionaria resuelve de manera efectiva los desafíos relacionados con la herencia de Bitcoin y la pérdida de fondos, debido al extravío de las claves. Un aspecto crucial, es el bloqueo temporal que se aplica a los fondos, lo cual habilita a una segunda persona - el hijo - poder rescatar los fondos utilizando sus propias claves, siendo completamente distintas de las claves que el padre ha perdido. De esta manera, se garantiza la seguridad y la accesibilidad a los fondos, incluso en situaciones de pérdida de claves.

Revelaciones importantes sobre la seguridad

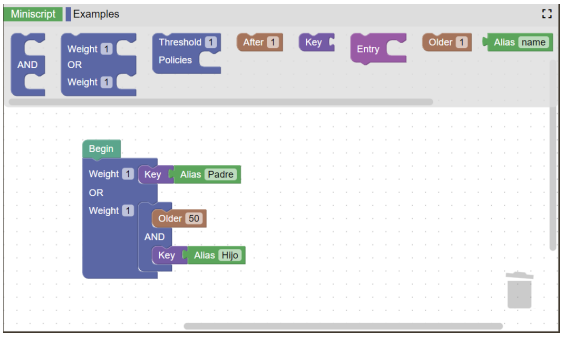
En el ámbito de bitcoin, es crucial seguir unas pautas de seguridad y custodia para proteger el mnemonic. Para ello, el usuario debería seguir los siguientes mecanismos para mantenerse totalmente seguro:

- Guardar su seed en un lugar seguro y offline .
- Realizar copias de seguridad de su seed y almacenarlas en múltiples ubicaciones seguras.
- Mantener la seed bajo secreto, nadie debe conocerla.
- Utilizar opciones de almacenamiento que protejan la seed de daños físicos, como el fuego o el agua.

Además, sería interesante usar técnicas para mantener a salvo toda la información crítica del usuario. Para ello, se cifra su seed utilizando algoritmos criptográficos confiables. Asimismo, se recomienda utilizar contraseñas fuertes y únicas para proteger la seed cifrada.

Mejoras y aplicaciones futuras

En el futuro, se prevé una mejora significativa al proporcionar a los usuarios un cliente flexible tal y como comentamos en la sección de tecnologías, mediante React o Electron. Un componente les permitirá crear y establecer sus propias condiciones de bloqueo (ver figura abajo). Esta innovadora funcionalidad, facilitará a cada usuario para diseñar y personalizar su propia wallet según sus necesidades y preferencias individuales, brindándoles la capacidad de programar su dinero de manera completamente flexible y autónoma.



Dicho enfoque, permitirá a los usuarios tener un control sin precedentes sobre sus activos financieros, abriendo un mundo de posibilidades y creando un ecosistema donde la creatividad y la personalización sean los pilares fundamentales.

Conclusión

Respecto a lo expuesto, se plantea cómo un intento de solucionar el problema que se encuentra actualmente con la custodia avanzada de fondos. Gracias a la nueva tecnología que ha surgido recientemente, como miniscript, timelocks, descriptores...etc, permite crear un nuevo paradigma de wallets.

Asimismo, los beneficios de usar dicha wallet son inmensos. En primer lugar, se hace hincapié en la posibilidad de compartir los mismos fondos entre varias personas, como en el caso de la herencia de padre e hijo. Pero se puede aplicar a cualquier casuística, ya que permite que la programación de Bitcoin, que, hasta ahora se había usado como una simple moneda de cambio que no es "inteligente", ahora sí lo sea.

Bibliografía

[1] Eric Lombrozo, Johnson Lau, Pieter Wuille. Segregated Witness (Consensus layer) BIP-141.
https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[2] Gavin Andresen. Pay to Script hash (BIP-16).
https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki

[3] Bit2Me Academy. Timelock's explanation.
https://academy.bit2me.com/que-es-timelock/

[4] BitcoinDevKit Documentation. Descriptors.
https://bitcoindevkit.org/descriptors

[5] Pieter Wuille. Miniscript: practical composability for Bitcoin script.
https://prezi.com/view/KH7AXjnse7gIXNoqCxPH