GUÍA ESPECIAL

¿CÓMO NACEN REALMENTE TUS CLAVES PRIVADAS?

Lo que el caso Coldcard le enseñó a toda la industria y cómo D’CENT protege el origen de las claves desde el primer instante.

UNA GUÍA PARA INVERSORES

Entropía · Frase semilla · Secure Element · D’CENT S × R3covery

por Hernán Coronel

ANTES DE EMPEZAR

El titular habló de una billetera fría. El problema nació mucho antes.

A fines de julio de 2026, una serie de barridos de Bitcoin fue vinculada con semillas generadas por versiones vulnerables del firmware de Coldcard. El total observado fue creciendo a medida que aparecieron nuevas tandas: primero unos USD 70,2 millones en 41 minutos y luego cerca de USD 89 millones, según análisis de blockchain citados por distintos medios.

01 **2021**

El error de integración habría estado presente desde marzo de 2021.

02 **41 MINUTOS**

1.196 direcciones fueron barridas en la primera gran ola analizada.

03 **≈ USD 89 M**

Cifra preliminar acumulada tras nuevas olas vinculadas al caso.

La pregunta útil no es “¿fallaron todas las billeteras frías?”. La pregunta útil es: ¿cómo se creó la información secreta que daba origen a esas billeteras?

Este documento parte de ese caso para explicar el mecanismo de manera simple. Cuando se describa el diseño de D’CENT, se indicará expresamente que se trata de documentación técnica publicada por la propia compañía.

CAPÍTULO 1

Tus criptomonedas no están dentro de la billetera

Una hardware wallet no es un pendrive lleno de XRP, Bitcoin o XLM. Los activos permanecen registrados en sus respectivas blockchains. Lo que la billetera protege es la información que permite autorizar un movimiento: la clave privada.

Por eso perder el aparato no necesariamente significa perder los activos. Si existe un respaldo válido, la billetera puede reconstruirse. El verdadero peligro aparece cuando otra persona obtiene o puede reconstruir la clave privada: desde ese momento puede firmar como si fuera el propietario.

La billetera no guarda las monedas.

Guarda el poder de moverlas.

Ese poder nace en el momento exacto en que se genera la clave.

CAPÍTULO 2

Todo comienza con algo que nadie debería poder predecir

Antes de las palabras, de las direcciones y de las cuentas, existe una fuente de aleatoriedad. En criptografía se la llama entropía. Su trabajo es producir un punto de partida imposible de adivinar.

256

bits de entropía declarados por D’CENT para su generación estándar.

2^{256}

posibles valores teóricos: un espacio astronómico.

0

datos que deberían venir del teléfono, la nube o un servidor.

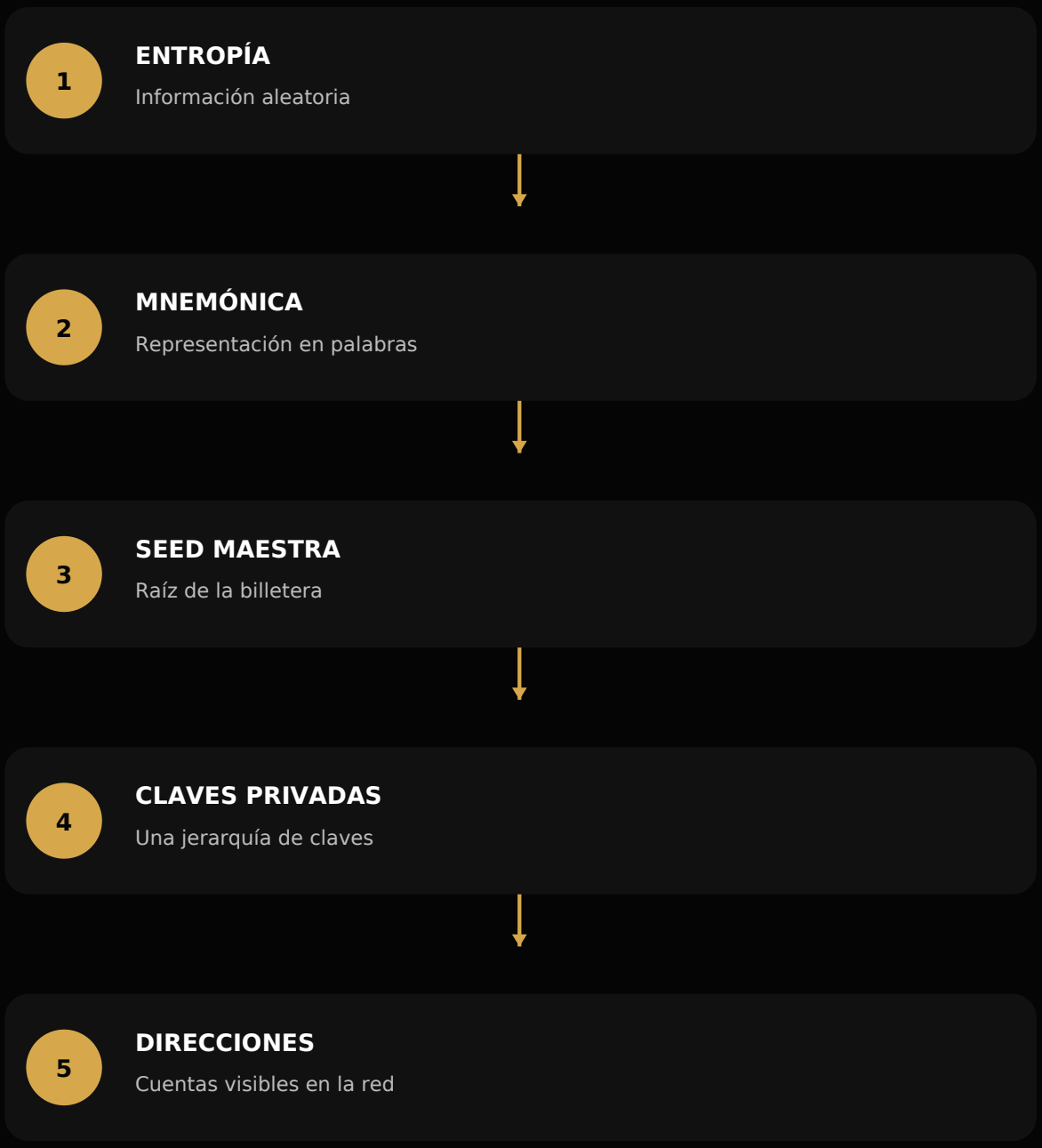
LA METÁFORA DE LA CERRADURA

Imaginá una cerradura con una combinación gigantesca. Si cada número fue elegido de verdad al azar, probar todas las combinaciones resulta inviable. Pero si alguien descubre que la fábrica usó la hora, un número de serie o una fórmula predecible, la cerradura sigue pareciendo compleja aunque el conjunto real de opciones sea mucho menor.

La seguridad no empieza cuando escondés la llave. Empieza cuando esa llave nace.

CAPÍTULO 3

De la entropía a una dirección: el mapa completo



La frase de recuperación es fundamental, pero no debe confundirse con una sola clave privada. Funciona como una raíz capaz de reconstruir una familia completa de claves y direcciones.

CAPÍTULO 3 · CONTINUACIÓN

¿Qué son realmente las 24 palabras?

Las palabras existen para que una persona pueda copiar y recuperar información criptográfica sin transcribir una larga cadena de bits. En el estándar BIP39, la entropía se combina con una suma de verificación y se divide en grupos que se traducen mediante una lista de 2.048 palabras.

01 **oro**	02 **puerta**	03 **noche**
04 **código**	05 **puente**	06 **calma**
07 **valor**	08 **nodo**	09 **futuro**
10 **clave**	11 **red**	12 **origen**

Estas palabras son solo una ilustración y no forman una frase válida.

! SI ALGUIEN LAS OBTIENE

Puede reconstruir la billetera sin tener el dispositivo.

! SI EL ORIGEN FUE DÉBIL

Moverlas a otro aparato no corrige la debilidad original.

CAPÍTULO 4

Coldcard: qué falló exactamente

Según el análisis técnico publicado tras el incidente, una integración de firmware de marzo de 2021 encaminó la generación de semillas hacia un generador seudoaleatorio determinista de software, en lugar del generador físico de números aleatorios previsto en el hardware.

✓ **LO QUE DEBÍA OCURRIR**

Hardware RNG → entropía impredecible → seed segura

✕ **LO QUE OCURRIÓ**

Fallback de software → valores condicionados → espacio reducible

El programa de respaldo se inicializaba con datos como el identificador único del chip y registros de tiempo, sin incorporar nueva entropía después de iniciarse. Bajo ciertas condiciones, un atacante podía reconstruir candidatos fuera del dispositivo, derivar sus direcciones y compararlas con la información pública de la blockchain.

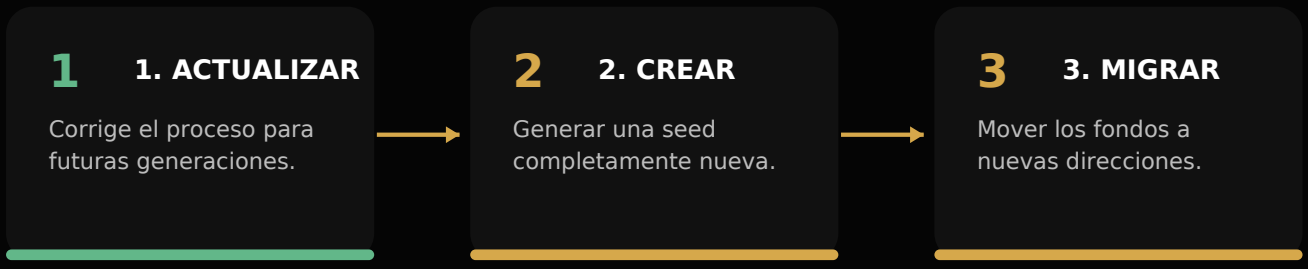
No rompieron Bitcoin.

Redujeron el misterio con el que había nacido la llave.

CAPÍTULO 4 · CONSECUENCIA

Una actualización no repara una seed que ya nació débil

El firmware corregido puede evitar que nuevas semillas se generen por el camino vulnerable. Pero no puede transformar retroactivamente una seed ya creada. La debilidad acompaña a esa frase, aunque después se importe en otro dispositivo.



Copiar la misma frase vulnerable en otra billetera equivale a cambiar la caja fuerte, pero seguir usando la misma llave defectuosa.

PREGUNTA DE LA COMUNIDAD: ¿Y SI HABÍA PASSPHRASE?

Una passphrase BIP39 robusta y desconocida deriva una billetera distinta. En teoría, puede impedir el acceso si el atacante solo reconstruyó las palabras originales. No hay un desglose público completo que permita saber cuántas de las billeteras afectadas la utilizaban.

CAPÍTULO 5

La respuesta de D’CENT: separar el origen de la clave del firmware general

D’CENT publicó una explicación específica a raíz del caso Coldcard. La compañía afirma que sus claves se generan fuera de línea mediante un TRNG —generador físico de números verdaderamente aleatorios— integrado dentro de un Secure Element certificado.

✕ NO DEL TELÉFONO

La app no origina la aleatoriedad.

✕ NO DE INTERNET

No depende de una conexión o servidor.

✕ NO DEL FIRMWARE

La función crítica vive dentro del chip seguro.

Según D’CENT, la clave se crea, se almacena y se utiliza dentro del Secure Element. Para firmar una transacción, el chip devuelve la firma, no la clave privada.

CAPÍTULO 5 · EL PROCESO

Cómo genera D’CENT una clave, paso a paso

01 **Ruido físico**
El TRNG del chip obtiene aleatoriedad física.

↓

02 **256 bits**
El Secure Element produce el material secreto.

↓

03 **Clave y respaldo**
Se crea la estructura de la billetera dentro del chip.

↓

04 **Firma interna**
Las operaciones se firman sin exponer la clave.

↓

05 **Resultado público**
Solo sale la firma necesaria para la blockchain.

En la D’CENT Biometric, la compañía describe un proceso BIP39 de 256 bits que se representa en 24 palabras. En la D’CENT S, el respaldo se maneja mediante la tarjeta R3covery y la frase no se muestra al usuario.

¿Qué significa EAL5+ o EAL6+?

EAL significa Evaluation Assurance Level. Es parte del estándar internacional Common Criteria, utilizado para evaluar productos de seguridad. El número expresa la profundidad y rigurosidad de la evaluación realizada sobre el diseño y sus controles.

5+ D’CENT BIOMETRIC

Secure Element con certificación Common Criteria EAL5+.

6+ D’CENT S

Secure Element con certificación Common Criteria EAL6+.

En la práctica, el Secure Element es un microprocesador dedicado a operaciones sensibles. Está diseñado para generar y custodiar secretos, resistir intentos de extracción y ejecutar la firma dentro de un entorno separado del teléfono.

LO IMPORTANTE PARA ENTENDER ESTE CASO

D’CENT afirma que el generador físico y el manejo de claves se ejecutan dentro de ese chip, no en el firmware general del dispositivo. Esa separación arquitectónica es la diferencia central que la marca plantea frente al fallo de entropía de Coldcard.

CAPÍTULO 6

Dos arquitecturas, dos caminos de generación

A **CASO COLDCARD**

Firmware vulnerable

↓

PRNG determinista de software

↓

Semillas potencialmente predecibles

B **DISEÑO DECLARADO POR D’CENT**

TRNG físico en Secure Element

↓

256 bits de entropía

↓

Clave creada y usada dentro del chip

La comparación no consiste en decir “una genera semillas y la otra no”. Ambas necesitan un origen secreto. La diferencia está en dónde se produce la aleatoriedad, qué componente la controla y si valores externos predecibles pueden condicionarla.

Una clave privada debe ser privada antes de existir.

Esa es la idea técnica central del artículo enviado por D’CENT.

CAPÍTULO 7

D’CENT S × R3covery: dos tarjetas, dos funciones

La nueva D’CENT S utiliza formato de tarjeta, conexión NFC y un Secure Element EAL6+. El kit incorpora una segunda tarjeta dedicada exclusivamente a la recuperación.

S D’CENT S · PRINCIPAL

Se lleva con vos.

Guarda la clave privada.

Firma transacciones por NFC.

No tiene batería ni cable.

R R3COVERY · RESPALDO

Se guarda separada.

Conserva el respaldo dentro de su Secure Element.

No puede firmar transacciones.

✓ EAL6+

Secure Element certificado.

✓ IP69

Resistencia declarada a polvo y agua.

✓ NFC

Sin batería y fuera de línea por defecto.

Según la guía oficial: compatible con más de 100 blockchains y más de 4.900 tokens.

CAPÍTULO 7 · RECUPERACIÓN

La mini tarjeta no es una copia para gastar

R3covery tiene una sola misión: conservar el material de recuperación. La tarjeta principal es la que firma. La tarjeta de respaldo no funciona como una segunda billetera cotidiana ni permite gastar fondos por sí sola.

1

CONFIGURACIÓN

Emparejás D’CENT S con R3covery.

2

RESGUARDO

La principal va con vos; R3covery queda en la caja fuerte.

3

INCIDENTE

La principal se pierde, se daña o es robada.

4

RESTAURACIÓN

R3covery permite recuperar en una nueva D’CENT S.

Una en tu billetera. La otra en tu caja fuerte.

¿Qué pasa si se pierde una de las tarjetas?

1 PERDÉS LA D’CENT S PRINCIPAL

La R3covery puede utilizarse para restaurar el acceso en una nueva D’CENT S siguiendo el procedimiento de la aplicación. La tarjeta de respaldo no firma por sí sola.

2 PERDÉS LA R3COVERY

Mientras la principal siga intacta, los activos continúan accesibles. La recomendación oficial es crear un nuevo respaldo cuanto antes.

3 CAMBIÁS DE TELÉFONO

La clave no depende del teléfono. La aplicación es la interfaz; la tarjeta conserva el secreto y autoriza mediante NFC y PIN.

La separación física reduce el riesgo de que el dispositivo de uso diario y su respaldo se pierdan en el mismo incidente.

CAPÍTULO 8

Cinco preguntas que deberías hacer antes de elegir una hardware wallet

01

¿Dónde se genera la aleatoriedad?

Dentro de un chip dedicado, en el teléfono, en el firmware o en un servidor.

02

¿Qué componente guarda la clave?

Y si la clave puede salir de ese entorno durante una firma.

03

¿Cómo se crea el respaldo?

Palabras visibles, tarjeta cifrada, nube o combinación de métodos.

04

¿Cómo verificás lo que firmás?

Dirección, monto, red y permisos antes de aprobar.

05

¿Qué ocurre si perdés el dispositivo?

Qué necesitás para restaurar y dónde está guardado.

La marca importa. Pero la arquitectura importa más.

CAPÍTULO 9

Errores cotidianos que ningún chip puede corregir por vos

✓

NO FOTOGRAFÍES UNA SEED

Una imagen puede terminar sincronizada en la nube.

✓

NO LA ESCRIBAS EN UN CHAT

Mensajería, correo y notas digitales amplían la superficie de exposición.

✓

REVISÁ ANTES DE FIRMAR

Dirección, red, monto y permisos deben coincidir con tu intención.

✓

USÁ FUENTES OFICIALES

Aplicaciones y actualizaciones deben provenir del fabricante.

✓

SEPARÁ USO Y RESPALDO

No guardes la billetera principal y su recuperación en el mismo lugar.

La autocustodia no es comprar un aparato. Es asumir un proceso.

CONCLUSIÓN

La verdadera seguridad empieza antes de la primera transacción

El caso Coldcard mostró que una billetera puede permanecer fuera de línea y, aun así, quedar expuesta si su clave nació de una fuente predecible. El punto crítico no fue la blockchain: fue el origen del secreto.

La respuesta técnica publicada por D’CENT se apoya en otra arquitectura: generación física de aleatoriedad dentro de un Secure Element certificado, custodia y firma dentro del mismo chip, y ausencia de dependencia del teléfono o de servidores para crear la clave.

En la nueva D’CENT S, esa lógica se combina con una separación sencilla de entender: una tarjeta para usar y firmar; otra tarjeta para recuperar y guardar.

NO PROTEGÉS UNA BILLETERA.

PROTEGÉS EL ACCESO A TU PATRIMONIO.

Y para protegerlo, primero tenés que entender cómo nació la llave.

CONOCÉ D’CENT S × R3COVERY →

Enlace de acceso compartido por Hernán Coronel

FUENTES

Documentación consultada

D’CENT Wallet Team · 3 ago 2026

How D’CENT Generates and Protects Your Private Keys

https://store.dcentwallet.com/blogs/post/how-dcent-generates-private-keys

D’CENT · Guía oficial

DCENT S Card Wallet: introducción y especificaciones

https://support.dcentwallet.com/dcent-scard-wallet/intro

D’CENT · Producto

DCENT S × R3covery: información y acceso al producto

https://store.dcentwallet.com/products/dcent-s-r3covery-card-kit-affiliates?bg_ref=IAFOQ2N11Y

The Hacker News · 1 ago 2026

Coldcard Hardware Wallet Flaw Linked to $70 Million Bitcoin Theft

https://thehackernews.com/2026/08/coldcard-hardware-wallet-flaw-linked-to.html

New York Post · 3 ago 2026

Actualización de pérdidas preliminares cercanas a USD 89 millones

https://nypost.com/2026/08/03/business/coldcard-software-flaw-linked-to-millions-in-crypto-hacks-fro

Las cifras del incidente eran preliminares al 4 de agosto de 2026 y pueden cambiar con nuevos análisis. Las características técnicas de D’CENT se presentan conforme a documentación publicada por el fabricante. Material educativo; no constituye asesoramiento financiero.