



Billeteras determinísticas jerárquicas y semillas

BILLETAS HD (DETERMINÍSTICAS JERÁRQUICAS)

BIP-32

Billeteras HD (determinísticas jerárquicas)

- Las billeteras determinísticas jerárquicas pueden respaldarse fácilmente mediante listas de palabras semilla.
- Si pierde el dispositivo que contiene su billetera, puede recrearla usando sus palabras semilla y recuperar el acceso a sus fondos.
- Puede utilizar las palabras semilla para crear la misma billetera en varios dispositivos diferentes.
- **La mayoría de las billeteras modernas son determinísticas jerárquicas.**

Billeteras HD (determinísticas jerárquicas)

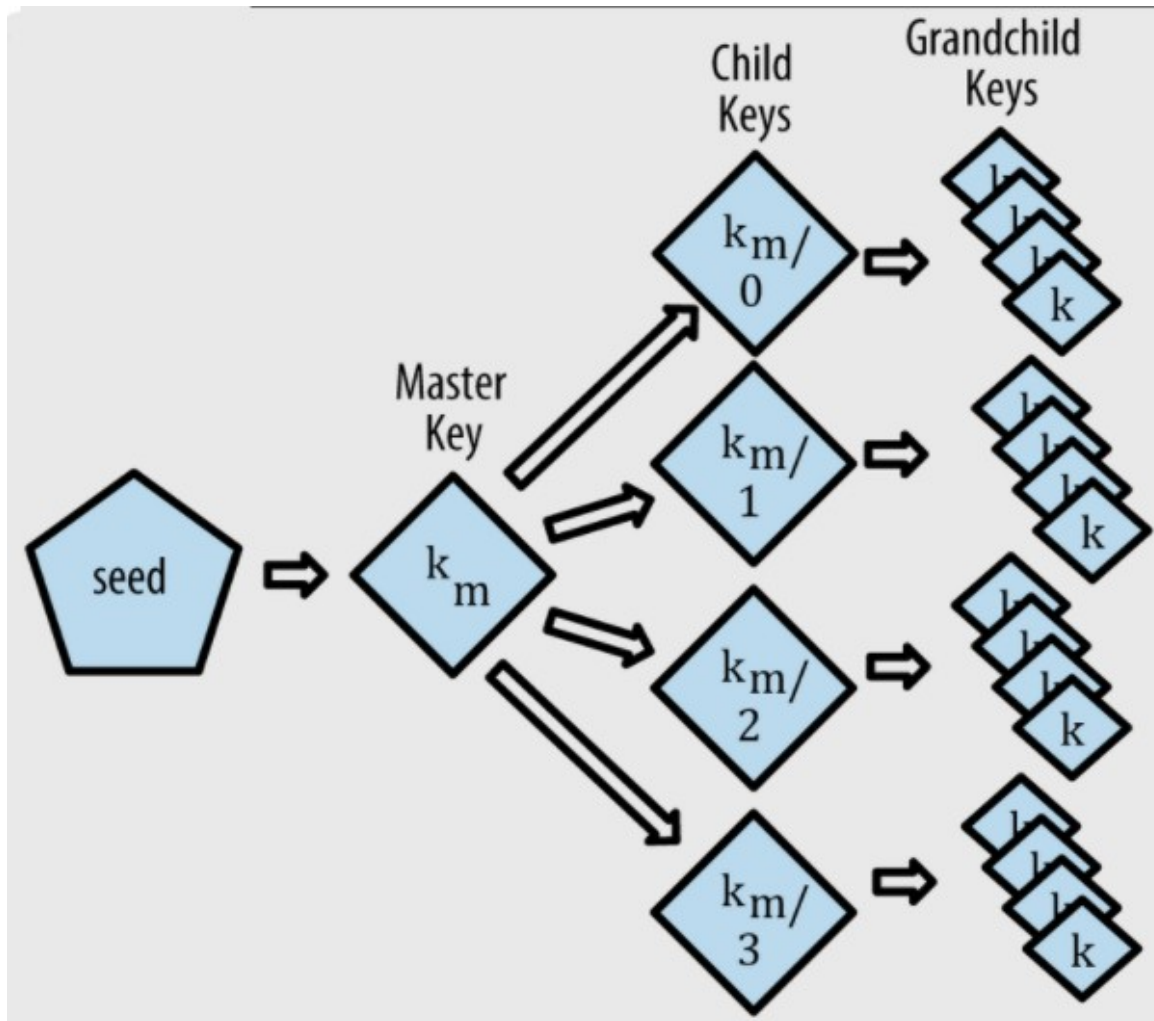
- **Jerárquicas:** porque todas las claves y direcciones de la billetera se derivan de una “**semilla maestra**” inicial (es decir, un número muy grande).
 - **La semilla maestra se utiliza para generar la clave inicial.**
 - **A partir de esta clave inicial se generan subclaves** (por ejemplo, claves hijas, nietas, etc.).
- **Determinísticas:** si se parte de la misma semilla inicial al instalar una billetera, la clave maestra y las subclaves derivadas serán idénticas.

Semilla maestra = número = lista de palabras semilla

UNCLASSIFIED - NON CLASSIFIÉ

- **Las semillas maestras son un número aleatorio.**
- **Ese número se representa mediante una lista de palabras.**
 - Es más fácil para las personas recordar una lista de palabras que un número grande.
- **Las billeteras suelen utilizar 12 o 24 palabras para representar una semilla maestra.**
 - 12 palabras se utilizan principalmente en billeteras para teléfonos móviles y computadoras.
 - 24 palabras se utilizan principalmente en billeteras de hardware.
- Algunas billeteras permiten utilizar una frase de contraseña además de las palabras semilla para generar la semilla maestra.

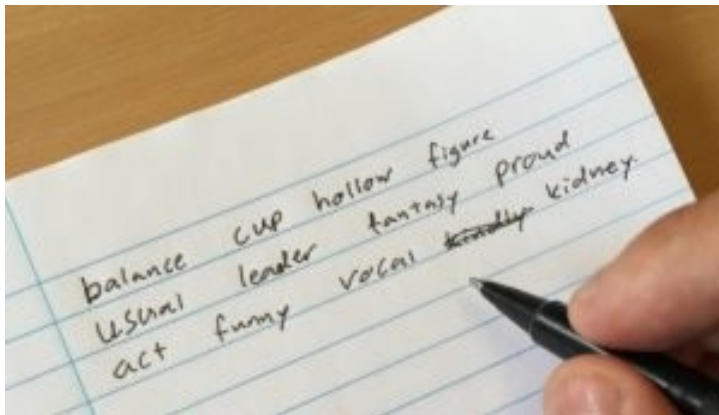
Semillas y claves



LISTAS DE PALABRAS SEMILLA

Listas de palabras semilla

- Listas de palabras que funcionan como respaldo de la billetera.



Billeteras y semillas

- Las listas de palabras semilla se usan para respaldar la mayoría de las billeteras digitales:

Billeteras para teléfonos móviles

Billeteras para computadoras

Billeteras de hardware

Billeteras como extensiones o complementos de navegador

- Las listas de palabras semilla no se utilizan para respaldar algunas billeteras:

Billeteras en papel

Billeteras con custodia

Cuando se configura una billetera

- **El software de la billetera le proporcionará una lista de palabras si está creando una billetera nueva.**
 - Las billeteras no vienen con listas de palabras semilla precargadas.
 - Las billeteras utilizan una serie de “factores ambientales” para generar un número aleatorio.
 - Ese número aleatorio determina qué palabras te entregará el sistema.
- Tanto las billeteras de hardware como las billeteras de software generan una lista de palabras semilla cuando se configuran.

Cómo se generan las listas de palabras semilla (versión corta)

- Durante la instalación de la billetera se genera un número aleatorio.
- Se le aplican operaciones matemáticas a ese número.
- El número resultante se divide en 12 números más pequeños.
- Cada uno de esos números más pequeños corresponde a una de las 2048 palabras específicas.

Cómo se generan las listas de palabras semilla (explicación un poco más larga...)

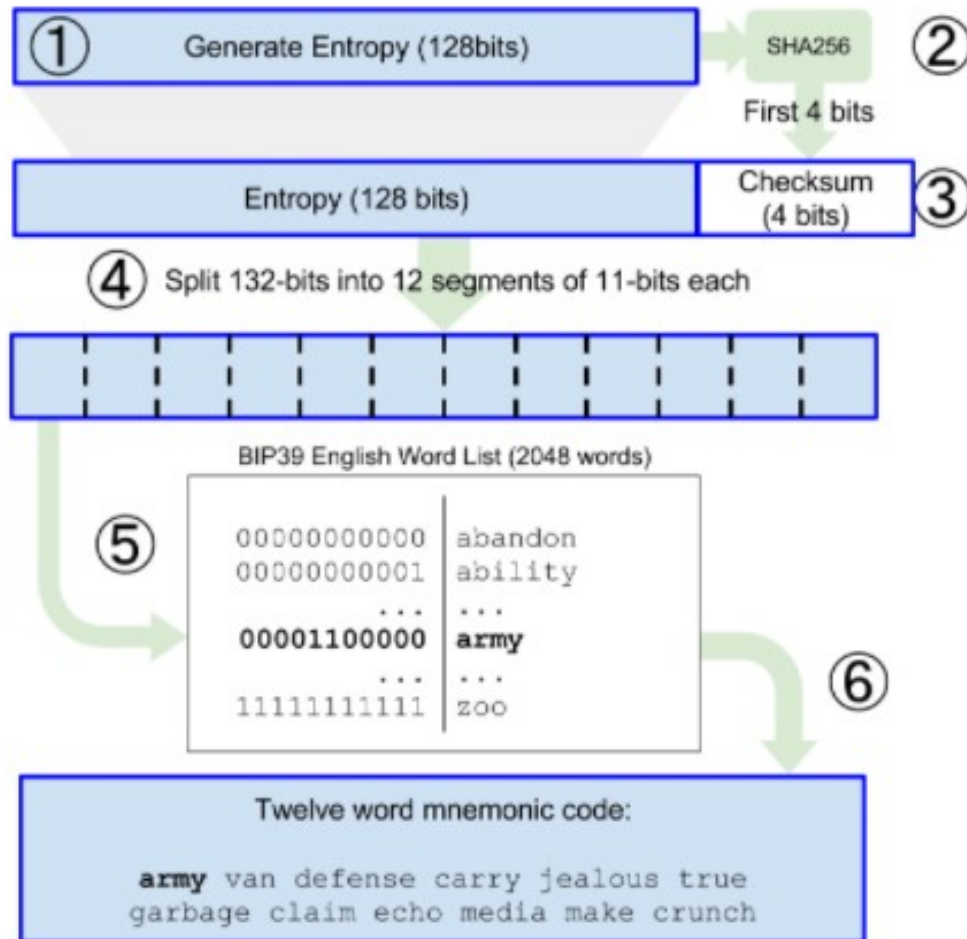
1. Durante la instalación, la billetera genera un número aleatorio de 128 bits (es decir, la semilla).
2. Ese número aleatorio se somete a un hash (SHA-256).
3. Se añaden los primeros 4 bits del hash al final del número aleatorio.
4. El número resultante, de 132 bits, se divide en doce números de 11 bits.
5. Cada palabra de la lista de palabras BIP-39 corresponde a un número específico.
6. La secuencia ordenada de palabras representa el número de la semilla inicial.

12 palabras semilla = número de 132 bits

110010001000100010001101110101000110001100010110
100000110100111111001101110101100001110011000
0011011010110011110011100011110100111110101

Cada grupo de 11 bits se representa mediante una palabra diferente

Mnemonic Words 128-bit entropy/12-word example



Antonopoulos, A. y G.
Wood (2018). Mastering
Ethereum. Implementing
Smart Contracts, O'Reilly.

Las semillas pueden generar claves para distintos tipos de criptomonedas.

Registered coin types

These are the registered coin types for usage in level 2 of BIP44 described in chapter "Coin type".

All these constants are used as hardened derivation.

index	hexa	symbol	coin
0	0x80000000	BTC	Bitcoin
1	0x80000001		Testnet (all coins)
2	0x80000002	LTC	Litecoin
3	0x80000003	DOGE	Dogecoin
4	0x80000004	RDD	Reddcoin
5	0x80000005	DASH	Dash (ex Darkcoin)
6	0x80000006	PPC	Peercoin

ESTÁNDAR DE LISTAS DE PALABRAS SEMILLA

BIP-39

Estándar BIP-39

- Los cambios que se realizan en Bitcoin se proponen y adoptan a través de documentos llamados Propuestas de Mejora de Bitcoin (Bitcoin Improvement Proposals, BIP).
- BIP-39 es un estándar propuesto y aceptado para crear respaldos de billeteras mediante listas de palabras semilla.
- BIP-39 incluye listas de palabras semilla en 10 idiomas diferentes.
- La mayoría de las billeteras siguen el estándar BIP-39, aunque algunas no lo hacen.

Listas de palabras (BIP-39)

Diez idiomas

2048 palabras en cada idioma

- Inglés
- Japonés
- Coreano
- Español
- Portugués
- Chino (simplificado)
- Chino (tradicional)
- Francés
- Italiano
- Checo

1	abandon		
2	ability	2041	yellow
3	able	2042	you
4	about	2043	young
5	above	2044	youth
6	absent	2045	zebra
7	absorb	2046	zero
8	abstract	2047	zone
9	absurd	2048	zoo

1	的	2040	嘗
2	一	2041	卿
3	是	2042	妨
4	在	2043	艇
5	不	2044	吞
6	了	2045	韋
7	有	2046	怨
8	和	2047	矮
9	人	2048	歇

2048 lines (2048 sloc)	2048 lines (2048 sloc)	2048 lines (2048 sloc)	2048 lines
1 abandon	1 abaisser	1 abaco	1 的
2 ability	2 abandon	2 abbaglio	2 一
3 able	3 abdiquer	3 abbinato	3 是
4 about	4 abeille	4 abete	4 在
5 above	5 abolir	5 abisso	5 不
6 absent	6 aborder	6 abolire	6 了
7 absorb	7 aboutir	7 abrasivo	7 有
8 abstract	8 aboyer	8 abrogato	8 和
9 absurd	9 abrasif	9 accadere	9 人
10 abuse	10 abreuver	10 accenno	10 这
11 access	11 abriter	11 accusato	11 中
12 accident	12 abroger	12 acetone	12 大
13 account	13 abrupt	13 achille	13 为
14 accuse	14 absence	14 acido	14 上
15 achieve	15 absolu	15 acqua	15 个
16 acid	16 absurde	16 acre	16 国

<https://github.com/bitcoin/bips/tree/master/bip-0039>

Algunas consideraciones sobre las listas de palabras (BIP-39)

- **Selección inteligente de palabras**
 - La lista de palabras se diseña de forma tal que basta con escribir las primeras cuatro letras para identificar de manera unívoca cada palabra.
- **Se evitan palabras similares**
 - Pares de palabras como “build” y “built”, “woman” y “women”, o “quick” y “quickly” no solo dificultan la memorización de la frase, sino que también aumentan la probabilidad de errores y hacen más difícil adivinarla.

Nota: Algunas billeteras no utilizan BIP-39.

- La **billetera Electrum** no utiliza BIP-39.
 - Se creó dos años antes de que se propusiera el estándar BIP-39.
 - Electrum genera sus claves privadas y direcciones a partir de una frase semilla compuesta por palabras del lenguaje natural.
 - Electrum utiliza un algoritmo diferente para derivar la semilla.
 - Las nuevas instalaciones de Electrum ahora utilizan las listas de palabras estándar de BIP-39.

RUTAS DE DERIVACIÓN

Rutas de derivación

- Existen diferentes rutas que se pueden utilizar para derivar claves a partir de la clave maestra.
- La ruta de derivación predeterminada para Bitcoin es `m / 44' / 0' / 0' / 0`.
- Cada número en esa ruta representa un determinado nivel y posición dentro del árbol jerárquico.

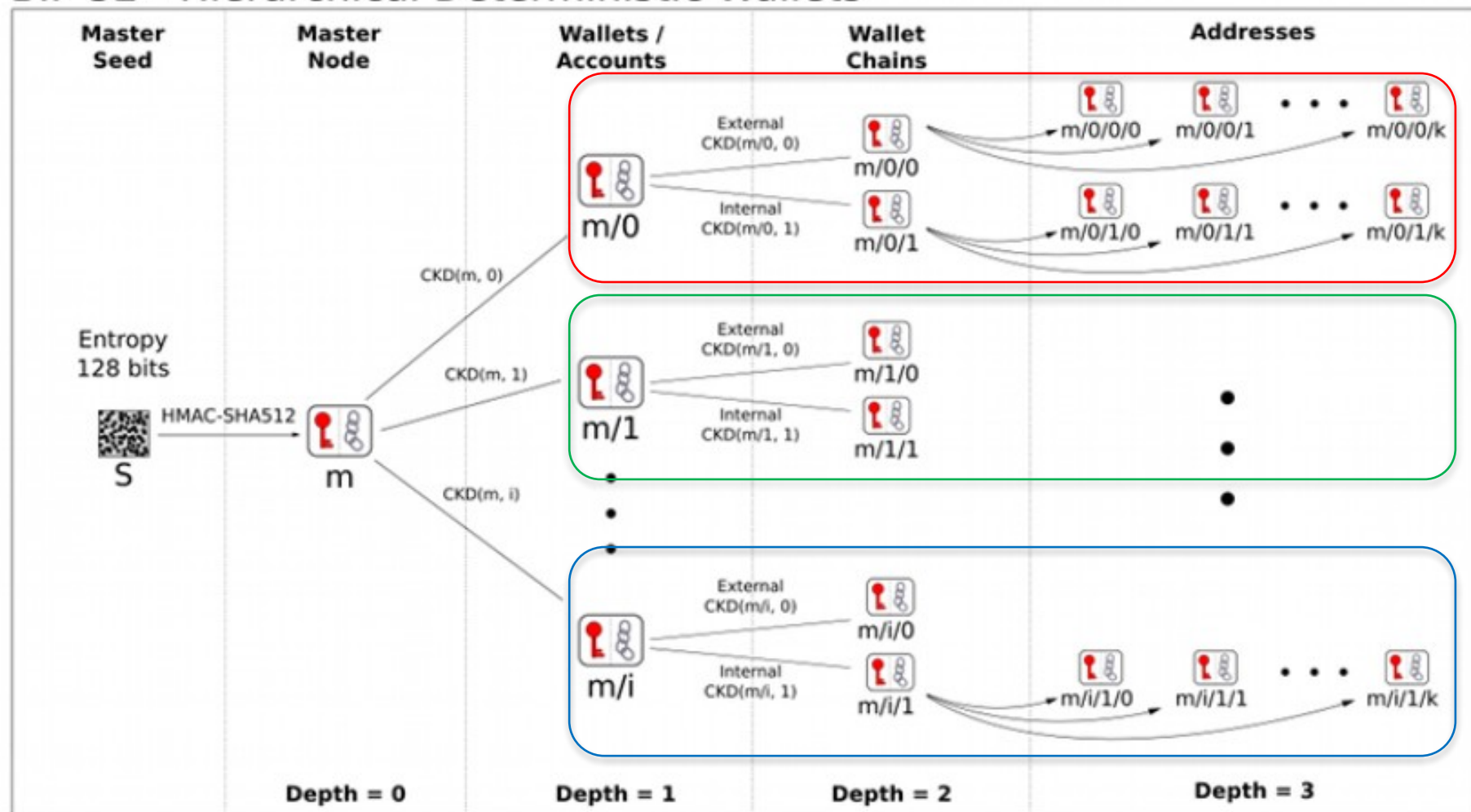
```
m / purpose' / coin_type' / account' / chain /  
address_index
```

Distintas billeteras utilizan distintas rutas de derivación.

Cuando se utiliza una lista de palabras semilla para recrear una billetera, es necesario usar el tipo de billetera adecuado.

Rutas de derivación

BIP 32 - Hierarchical Deterministic Wallets



Child Key Derivation Function ~ $CKD(x,n) = \text{HMAC-SHA512}(x_{\text{Chain}}, x_{\text{PubKey}} || n)$

Qué significan las listas de palabras semilla y las rutas de derivación para un investigador

- **Si se conoce la lista de palabras semilla de una persona:**
 1. Es posible generar todas sus claves y direcciones
 2. Se puede tomar control del uso de sus criptomonedas
 3. Se pueden rastrear todas sus transacciones.
- **Pero es necesario conocer el tipo de billetera:**
 - Cuando se recrea la billetera del sospechoso, debe utilizarse una billetera que emplee las mismas rutas de derivación.
- **No es necesario conocer la contraseña:**
 - La contraseña se utiliza para cifrar la billetera una vez que ha sido creada.

Recursos – Videos en YouTube

(Andreas Antonopoulos)

- [Preguntas frecuentes sobre Bitcoin: How do mnemonic seeds work? \(¿Cómo funcionan las semillas mnemotécnicas?\)](#)
- [Preguntas frecuentes sobre Bitcoin: Passphrases and seed storage \(Frases de contraseña y almacenamiento de semillas\)](#)

Propuestas de Mejora de Bitcoin (BIP)

- **BIP-32:** Hierarchical Deterministic Wallets (Billeteras determinísticas jerárquicas)
- **BIP-39:** Mnemonic code for generating deterministic keys (Código mnemotécnico para generar claves determinísticas)
- **BIP-44:** Multi-Account Hierarchy for Deterministic Wallets (Jerarquía de múltiples cuentas para billeteras determinísticas)
- **BIP-49:** Derivation scheme for P2WPKH-nested-in-P2SH based accounts (Esquema de derivación para cuentas basadas en P2WPKH anidadas en P2SH)