



UTN.BA

UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES



ciie

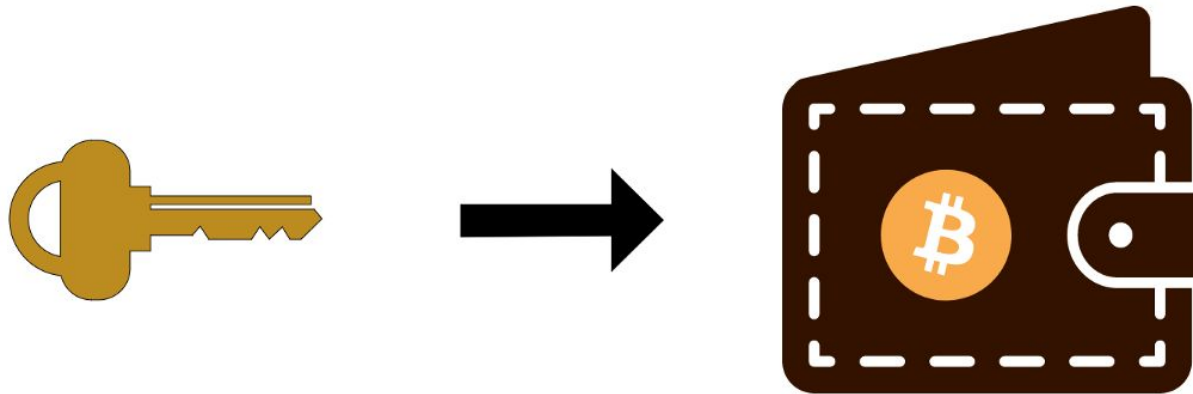
Centro de Investigación
e Innovación Educativa

Direcciones y billeteras Bitcoin

4.3 Billeteras Bitcoin

Una Billetera Bitcoin o simplemente Wallet

Una billetera Bitcoin o Wallet es un software contenedor de claves privadas, usualmente implementadas como archivos estructurados o simples bases de datos.



Billeteras no deterministas (Aleatorias)

Los primeros clientes Bitcoin, las carteras eran simplemente colecciones de claves privadas generadas aleatoriamente. Este tipo de cartera se conoce como cartera no determinista de Tipo-0. Por ejemplo, el cliente Bitcoin Core genera previamente 100 claves privadas aleatorias cuando se inicia

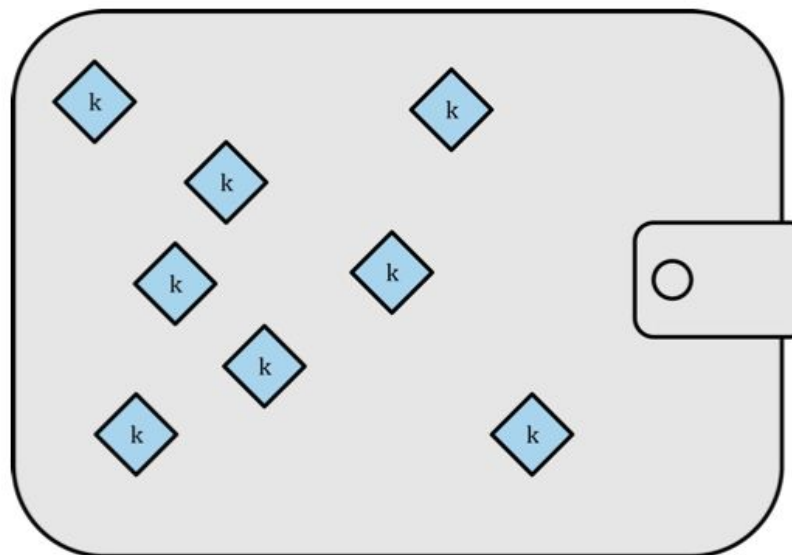


Figure 8. Cartera no determinista (aleatoria) Tipo-0: una colección de claves generadas aleatoriamente

“Mastering Bitcoin by Andreas M. Antonopoulos (O’Reilly). CC-BY-NC 2017 Andreas M. Antonopoulos, 978-1-491-95438-6.”

Bitcoin Core

Bitcoin Core – Wallet




File Settings Help



Overview Send Receive Transactions

Balances

Available:	0.00000000 BTC
Pending:	0.00000000 BTC
Total:	0.00000000 BTC

Recent transactions

	2/18/15 00:49 Marcus	-3.34896127 BTC
	2/13/15 10:08 Paul	+3.34896127 BTC
	2/6/15 05:58 Amanda	-0.23000000 BTC

BTC  

Billeteras deterministas a partir de semilla

Las Billeteras deterministas o "con semilla" contienen claves privadas que surgen a partir de una semilla común. La semilla es un número generado aleatoriamente que sirve para derivar las claves privadas y es suficiente para recuperar todas las claves derivadas, y por lo tanto una única copia de seguridad en el momento de la creación es suficiente.

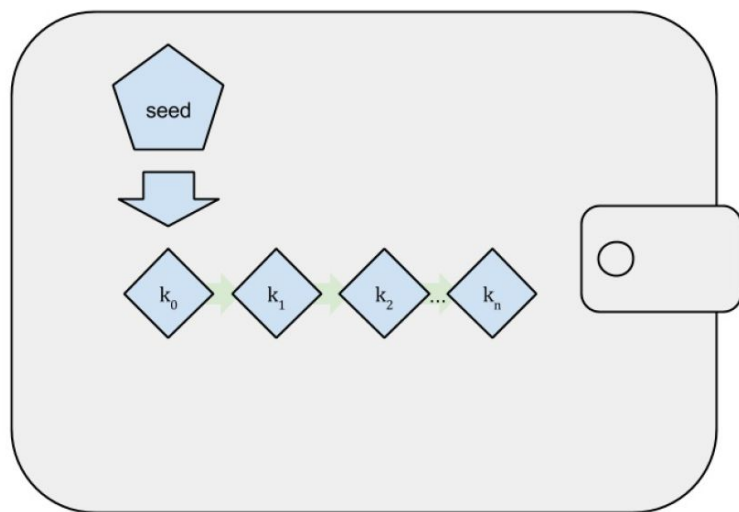


Figure 5-2. Type-1 deterministic (seeded) wallet: a deterministic sequence of keys derived from a seed

“Mastering Bitcoin by Andreas M. Antonopoulos (O’Reilly). CC-BY-NC 2017 Andreas M. Antonopoulos, 978-1-491-95438-6.”

Palabras o código Mnemotécnico

Los códigos mnemotécnicos son palabras en inglés o español que codifican un número aleatorio utilizado como semilla para obtener una billetera determinista. La secuencia de palabras es suficiente para volver a crear la semilla y desde allí volver a recrear la billetera y todas las claves derivadas. Una aplicación que implementa un código mnemotécnico le mostrará al usuario una secuencia de 12 a 24 palabras al crear la billetera por primera vez.

Ejemplo palabras o código Mnemotécnico

Table 6. Código mnemónico de entropía de 128 bits y su semilla resultante

Entropía de entrada (128 bits)	0c1e24e5917779d297e14d45f14e1a1a
Mnemónico (12 palabras)	army van defense carry jealous true garbage claim echo media make crunch
Semilla (512 bits)	3338a6d2ee71c7f28eb5b882159634cd46a898463e9 d2d0980f8e80dfbba5b0fa0291e5fb88 8a599b44b93187be6ee3ab5fd3ead7dd646341b2cd b8d08d13bf7

Table 7. Código mnemónico de entropía de 256 bits y su semilla resultante

Entropía de entrada (256 bits)	2041546864449caff939d32d574753fe684d3c947c33 46713dd8423e74abcf8c
Mnemónico (24 palabras)	cake apple borrow silk endorse fitness top denial coil riot stay wolf luggage oxygen faint major edit measure invite love trap field dilemma oblige
Semilla (512 bits)	3972e432e99040f75ebe13a660110c3e29d131a2c80 8c7ee5f1631d0a977fcf473bee22 fce540af281bf7cdeade0dd2c1c795bd02f1e4049e20 5a0158906c343

Billeteras deterministas jerárquicas

Las carteras deterministas jerárquicas contienen claves derivadas en una estructura de árbol, de tal manera que de una clave padre puede derivarse una secuencia de claves hijas, de cada una de las cuales puede derivarse una secuencia de claves nietos, y así sucesivamente, a una profundidad infinita.

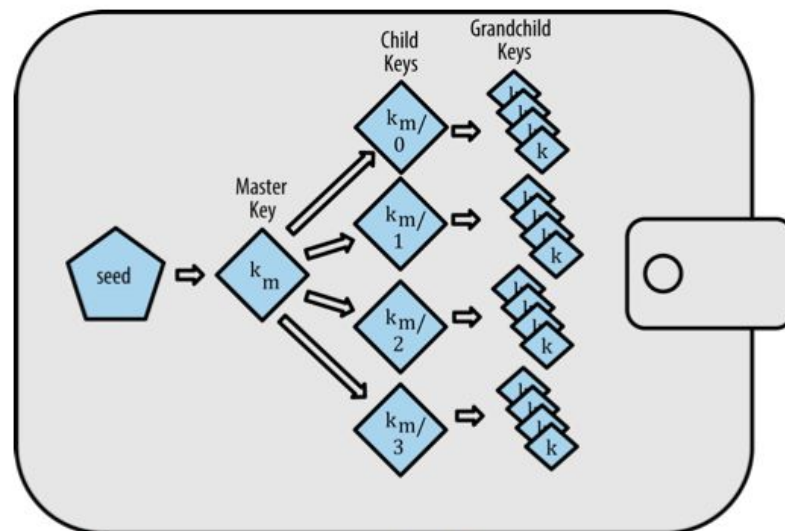
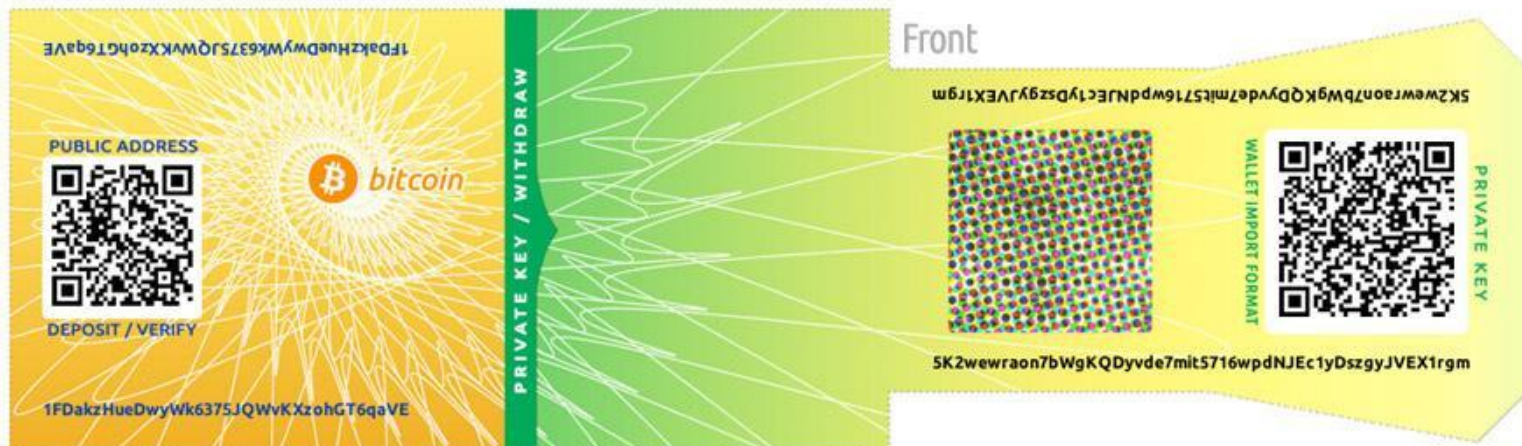


Figure 9. Cartera determinista jerárquica de Tipo-2: un árbol de claves generadas a partir de una única semilla

“Mastering Bitcoin by Andreas M. Antonopoulos (O’Reilly). CC-BY-NC 2017 Andreas M. Antonopoulos, 978-1-491-95438-6.”

https://bitcoinpaperwallet.com/



Hardware Wallet - <https://trezor.io/>



Hardware Wallet - <https://www.ledger.com/>

