



## **BIP-39: Herramienta de frase mnemotécnica**

**Determinación del software de billetera adecuado**

# BIP-39: Herramienta de frase mnemotécnica

Herramientas para autoridades de aplicación.


1. Genera una semilla a partir de la lista de palabras mnemotécnicas proporcionada.
2. Deriva claves y direcciones según distintas rutas de derivación.
3. Verifica en la blockchain si las direcciones derivadas han sido utilizadas.
4. A partir de los resultados, la herramienta proporciona una lista de posibles billeteras con sus respectivas rutas de derivación.

# BIP-39: Herramienta de frase mnemotécnica

- La herramienta puede utilizarse desde una página web (menos segura).
- También puede descargarse (más segura).
- Puede emplearse con listas de palabras semilla en distintos idiomas.
- La versión descargable ofrece opciones avanzadas.
- Solo sugiere billeteras: puede que no coincidan exactamente con la utilizada por el sospechoso.
- Algunas billeteras pueden utilizar la ruta de derivación correcta para BTC, pero no para ETH.


# Versión en línea


## BIP39 Mnemonic phrase tool

 Settings


Enter the mnemonic phrase

Mnemonic Phrase


Passphrase (optional) 

Index severity 

1

Account severity 

1

Check addresses online 

☒

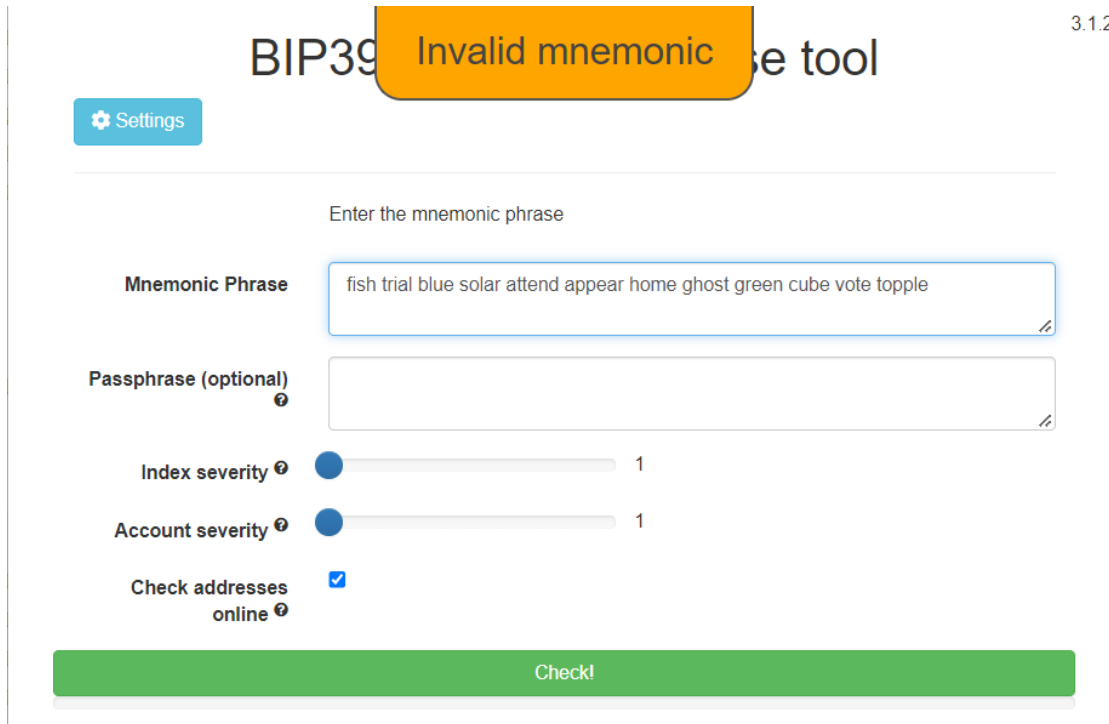
Check!

<https://cryptotools.nl/4ce35eb2e285eceaf0ef20f1b68aa4f8/tool/>

# Uso

- Ingrese la frase mnemotécnica, es decir, la lista de palabras semilla correspondiente a la billetera del sospechoso.
- No es necesario preocuparse por las frases de contraseña, la severidad del índice ni la de la cuenta.
- Asegúrese de que la opción **Check addresses online** esté marcada si desea que la herramienta verifique en línea si las billeteras sugeridas contienen criptomonedas.
  - La herramienta consultará exploradores de blockchain e intentará identificar los activos asociados a las direcciones que genere.
- Haga clic en el botón verde CHECK.

# Recibirá un mensaje de error si introduce una lista de palabras semilla no válida.



The screenshot shows the 'BIP39 Invalid mnemonic tool' interface. At the top right, the version '3.1.2' is displayed. A blue 'Settings' button is in the top left. The main heading is 'Enter the mnemonic phrase'. Below this, the 'Mnemonic Phrase' field contains the text 'fish trial blue solar attend appear home ghost green cube vote topple'. The 'Passphrase (optional)' field is empty. Below the passphrase field are two sliders: 'Index severity' and 'Account severity', both set to 1. The 'Check addresses online' checkbox is checked. A large green 'Check!' button is at the bottom.

























## Invalid mnemonic!

Possible reasons for this are:

- It is an Electrum mnemonic phrase, this is not a BIP39 mnemonic, works differently and is not supported right now
- The words are incorrect, for this look at [Github](#) for the wordlists
- The order of words are incorrect
- The words belong to another type of mnemonic phrase, for instance Monero (Monero requires the rescan of the blockchain and uses a different list of words)

# Busque las marcas de verificación verdes.

## Results


Coin	Type	Derivation path	Address	Used by	Is used?	Full Wallet 
BTC	BIP32	m/44'/0'/0'/0	1CbZ1Kpu7NcjMsaVuT95snvr8YaPbetiDJ	Blockchain.info (legacy), Bitcoin.com (app), MultiBit HD, BRD, Coinomi (old legacy), Ledger (legacy)		
BTC	BIP44	m/44'/0'/0'/0/0	1DV3jDfd6qfTtnvZ7HjBDFcmavTEsNjeDP	Exodus, Bitpay (app), Mycelium, Copay, Jaxx, Coinomi (current legacy), Enjin, KeepKey, Blockchain.info		
BTCTEST	BIP44	m/44'/1'/0'/0/0	miY4xTAJ8u75MmB3qeQzCEDX7b5AYGRsgb	KeepKey		
BTC	BIP49	m/49'/0'/0'/0/0	392CPSHFqWhLM82q9DJGdPW2Krx57khK7	Trezor, Ledger, edge, Coinomi (Compatibility)		
BTCTEST	BIP49	m/49'/1'/0'/0/0	2N7F1irDpZ28iXVBmAFRh4L5tuTFF663MQr	Trezor, Ledger		
BTC	BIP84	m/84'/0'/0'/0/0	bc1qa6pya3pxqja795uh73xa8qlvuj0g5hfsy7czkz	Coinomi, Wasabi Wallet (password mandatory)		
ETH	BIP44	m/44'/60'/0'/0/0'	0x436B93CeC3872750dCd527379045d3D31baaaC3e	Ledger		
ETH	BIP44	m/44'/60'/0'/0/0	0xCFeb408c1dD76587Dd241136582432EB52e521C1	Jaxx, Metamask, Exodus, imToken, Trezor, KeepKey		
LTC	BIP44	m/44'/2'/0'/0/0	LfEzFu6yNjLDDKVEe2DRiJkr314xXcfnzB	Coinomi (legacy), KeepKey, Ledger		
LTC	BIP49	m/49'/2'/0'/0/0	MSsaRVmwzUvD8YdJsHWG3CCugxgfQ6TVX3	Coinomi (compatibility), Trezor		
LTC	BIP84	m/84'/2'/0'/0/0	ltc1qvpexu95gs3f4prk5j0trl8gnq99yvp66rvva58	Coinomi (default)		
DASH	BIP44	m/44'/5'/0'/0/0	XbBE3SkMarCoCrtzndNNSUzgnULw4axwaf	Trezor, Ledger, KeepKey		
DOGE	BIP44	m/44'/3'/0'/0/0	DLa3AZJw1TJeAJk9haPvA1QSVfDguwcsvc	Trezor, Ledger, KeepKey		

# Resultados

- **Coin** identifica las criptomonedas que se hayan detectado.
- **Type** indica el tipo de dirección (P2PKH, SegWit, etc.).
- **Derivation path** señala la ruta utilizada para derivar las subclaves.
- **Address** identifica la primera dirección que se generó al crear la billetera.
- **Used by** indica las billeteras que podrían utilizarse para recrear la billetera del sospechoso.



# Resultados (cont.)

- **Is used** indica si ese tipo de billetera fue efectivamente utilizado y contiene fondos.
  - Un **círculo verde** con una marca de verificación indica que fue utilizado.
- **Full wallet** indica q  y detalles disponibles sobre la cantidad de criptomonedas en la billetera.
- Identifique la marca de verificación verde y haga clic en el ícono de billetera junto a ella para obtener y exportar los detalles.
  - Luego deberá hacer clic en el botón azul *Generate all addresses* para visualizar la información disponible.

# Intento de recrear la billetera del sospechoso utilizando el software sugerido.

- Si se detecta más de una criptomoneda, puede ser conveniente seleccionar una billetera que figure para ambas.

BTC	BIP44	m/44'/0'/0'/0/0	1DV3jDfd6qfTtnvZ7HjbDFcmavTEsNjeDP	Exodus, Bitpay (app), Mycelium, Copay, Jaxx, Coinomi (current legacy), Enjin, KeepKey, Blockchain.info	✓	
ETH	BIP44	m/44'/60'/0'/0/0	0xCFeb408c1dD76587Dd241136582432EB52e521C1	Jaxx, Metamask, imToken, Trezor, KeepKey, Exodus	✓	

# Calculate entire wallet

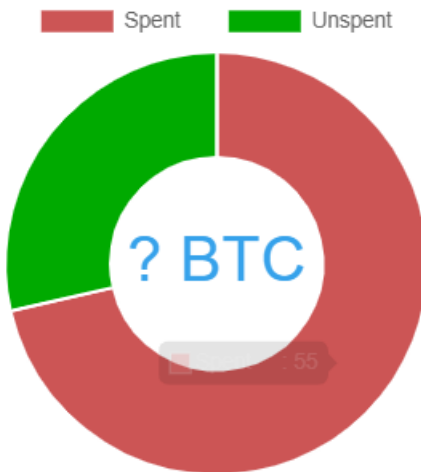
Generates all addresses associated with this type of wallet

## Status



In progress

## Statistics



## Exports

Chainalysis custom cluster

All addresses

All receive addresses

All private keys

Generate all addresses!

Account

Index

Address

Type

# Datos exportables

- **Chainalysis custom cluster:** archivo JSON con el clúster detectado. Puede importarse directamente en Chainalysis Reactor para rastreo y análisis.
- **All addresses:** archivo .txt con todas las direcciones receptoras descubiertas.
- **All receive addresses:** archivo .txt que contiene todas las direcciones receptoras descubiertas.
- **All private keys:** archivo .txt que contiene las claves privadas de las direcciones identificadas.

```
cluster.json - Notepad
File Edit View

{"id":"8f3ff69d-84ea-4143-bfe1-341309d5b032","name":"cluster","depositAddresses":[{"asset":"BTC","address":"392CPSHfqWhLM82q9DJGfdPW2Krx57khK7"}, {"asset":"BTC","address":"3EcGChfwTRp4NoPFHm7uTHJHciHgqTx3c3"}],"receivedTransfers":[],"sentTransfers":[]}
```

Ln 1, Col 1 | 100% | Unix (LF) | UTF-8

```
private_keys (2) - Notepad
File Edit View

undefined:L1STSa1UeQNu6BWvAqgU7bgo7yHssxQBpR9LeLFX4HC3LMSUEj72
undefined:L4wgySttuP5rimZ8mn4o7qdnETotGqimTsJJ1CULLW58wcAyrICz
undefined:L1STSa1UeQNu6BWvAqgU7bgo7yHssxQBpR9LeLFX4HC3LMSUEj72
```

Ln 1, Col 1 | 100% | Unix (LF) | UTF-8

```
all_addresses (2) - Notepad
File Edit View

1DV3jDfd6qfTtnvZ7HjbDFcmavTEsNjeDP
```

Ln 1, Col 1 | 100% | Unix (LF) | UTF-8

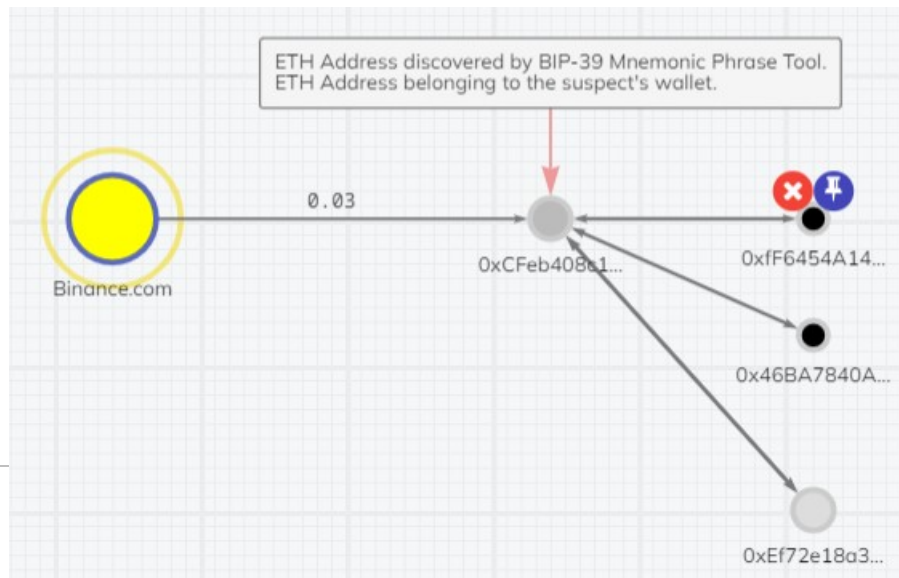
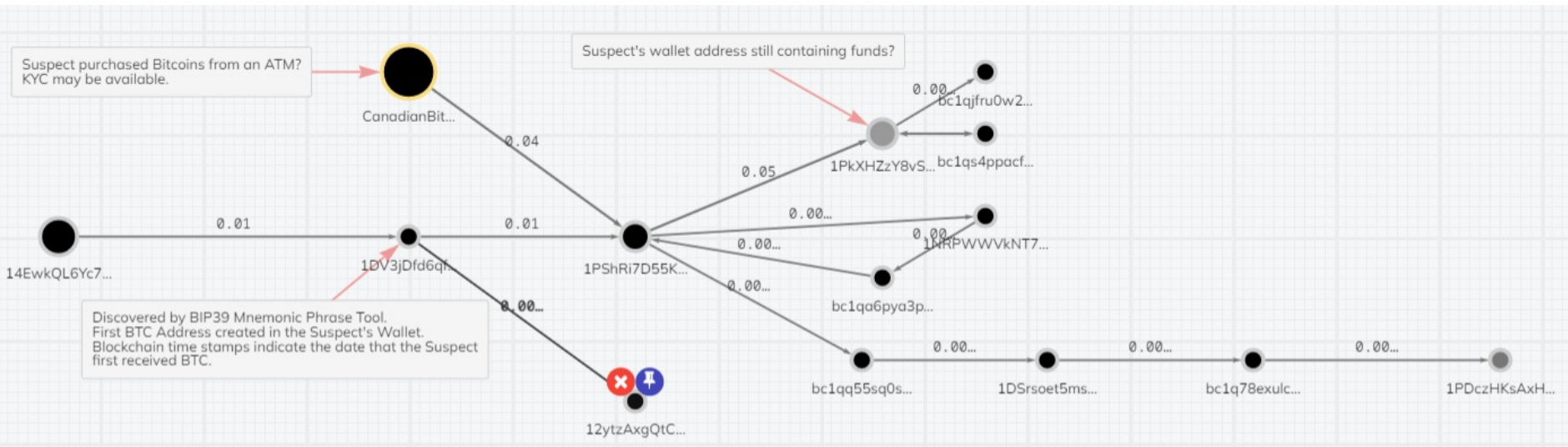
```
receive_addresses (1) - ...
File Edit View

1DV3jDfd6qfTtnvZ7HjbDFcmavTEsNjeDP
```

Ln 1, Col 1 | 100% | Unix (LF) | UTF-8

# personalizado generado por Chainalysis

UNCLASSIFIED - NON CLASSIFIÉ



# Advertencia

- **No confíe ciegamente en la herramienta** con respecto a los archivos exportables que contienen direcciones y claves (no siempre los genera correctamente).
- **Recree la billetera del sospechoso probando con las distintas billeteras sugeridas.** Una vez hecho esto, podrá incautar los fondos disponibles y/o exportar los archivos de registro generados por la billetera.
- **Es posible que la billetera sugerida no coincida con la que efectivamente utilizó el sospechoso.**









# Ejercicio - BIP39: Herramienta de frase mnemotécnica

- Durante un registro, usted encuentra la siguiente lista de palabras semilla.
- Identifique las billeteras que podría utilizar para acceder a los fondos del sospechoso.

1. regret
2. earn
3. clerk
4. ginger
5. future
6. cook
7. million
8. sudden
9. bag
10. bird
11. prefer
12. spot



# Results

Coin	Type	Derivation path	Address	Used by	Is used?	Full Wallet ?
BTC	BIP32	m/44'/0'/0'/0	1MeemYzXLzRjdFvYZxoKETGDkGoimSnB2A	Blockchain.info (legacy), Bitcoin.com (app), MultiBit HD, BRD, Coinomi (old legacy), Ledger (legacy)	✗	
BTC	BIP44	m/44'/0'/0'/0/0	1PkXHZzY8vS8xUYZ8rEKwEGpqYX7vpFzZP	Exodus, Bitpay (app), Mycelium, Copay, Jaxx, Coinomi (current legacy), Enjin, KeepKey, Blockchain.info	✓	
BTCTEST	BIP44	m/44'/1'/0'/0/0	mv2e7tGapD4d1aDdQG4Jo2shVwNMzBR6Pj	KeepKey	✗	
BTC	BIP49	m/49'/0'/0'/0/0	3PPiAFhNaU7XubbGDLNSA2uzfctwf2tnBi	Trezor, Ledger, edge, Coinomi (Compatibility)	✗	
BTCTEST	BIP49	m/49'/1'/0'/0/0	2NFvthrEimwrT8z3qzNaPNQyGGf3wWKWSMb	Trezor, Ledger	✗	
BTC	BIP84	m/84'/0'/0'/0/0	bc1qmtP36dqeekz3gcjeu3sjldty5sdd3gy3ewlkdw	Coinomi, Wasabi Wallet (password mandatory)	✗	
ETH	BIP44	m/44'/60'/0'/0/0	0x4BD27acA1759c7c4f228b2bC948d91Eb7aE81AFE	Ledger	✗	
ETH	BIP44	m/44'/60'/0'/0/0	0x5DD2602A2DE363D6Edd258116468Ac08415b9B22	Jaxx, Metamask, Exodus, imToken, Trezor, KeepKey	✗	
LTC	BIP44	m/44'/2'/0'/0/0	LKrACYcCFoJZNvNEkArqM3nJWr8bUGo2rB	Coinomi (legacy), KeepKey, Ledger	✗	
LTC	BIP49	m/49'/2'/0'/0/0	MC666mSAJa8K4eUvGPpt3sEDE9zqF9WgDF	Coinomi (compatibility), Trezor	✗	
LTC	BIP84	m/84'/2'/0'/0/0	ltc1qxerhmt2l692g4d4eu9lencvzmw8tvm57q8p55	Coinomi (default)	✗	
DASH	BIP44	m/44'/5'/0'/0/0	Xeofw4bfoxLsbhj4nP9EhXNnKH6YQVkgmt	Trezor, Ledger, KeepKey	✗	