Restored Wallet Still Syncing: Wait or Worry?

October 31, 2026 · Document #414 · bip39-phrase.com



Photo by Jorien Loman on Unsplash

Learn how restored wallets find transactions, why scans take time, and which signs distinguish sync problems from incorrect recovery settings.

Contents

What a restored wallet is doing 1

Why light wallets and full nodes differ 2

Check progress before changing recovery settings 2

FAQ 3

Sources 3

Example sequences from the BIP39 wordlist 4

Reading a BIP39 phrase 5

See also 5

A restored wallet can show a zero balance while it is still finding addresses and checking their transaction history. Importing a recovery phrase recreates keys; the wallet must then discover which keys have been used. A zero balance during that process does not establish that the phrase is wrong. The useful clues are scan progress, the latest block checked, server connectivity, and whether familiar receiving addresses reappear.

What a restored wallet is doing

For a typical BIP39 wallet, the recovery phrase and optional passphrase produce a seed. The wallet derives keys using its supported derivation paths and address types, then searches for transactions involving those addresses. The blockchain does not store your recovery phrase or a single record representing your entire wallet.

Discovery often means checking consecutive addresses until the wallet reaches a limit of unused addresses. BIP44 specifies an external address gap limit of `20`: discovery stops after 20 consecutive receiving addresses with no transaction history. An address with a zero balance is not necessarily unused. Implementations can offer different limits or recovery options. A wallet may also need to examine multiple accounts and change addresses, which receive funds left over from spending.

A full-node wallet can perform two separate jobs: synchronize its local blockchain and rescan historical blocks for wallet transactions. A node can be fully synchronized while a newly restored wallet is still rescanning. Conversely, importing keys cannot make an unfinished node immediately know the latest wallet balance.

Why light wallets and full nodes differ

A server-based light wallet usually asks a remote service for transaction histories associated with its derived addresses or scripts. Because the server has already indexed the blockchain, discovery can finish in seconds or minutes for a modest wallet. Large histories, many accounts, server limits, and connection problems can extend that time.

Some light wallets use compact block filters, such as those defined by BIP157 and BIP158, to find potentially relevant blocks. Their recovery work differs from querying an address-history server, so light wallets do not all have the same timing or progress indicators.

A full node downloads and validates blocks locally. Initial synchronization can take hours, days, or longer depending on storage speed, processor performance, network throughput, and how much history remains. A wallet rescan reads relevant historical blocks to find wallet transactions; its duration depends on the scan range, available hardware, and the wallet's scanning optimizations.

Pruning adds another constraint: old blocks needed for a historical rescan may no longer be stored locally. Recovery may require downloading those blocks again through a supported workflow, potentially including a full blockchain download. Entering the phrase repeatedly will not resolve missing block data.

Check progress before changing recovery settings

1. Identify what is unfinished. Look for separate indicators for network synchronization, wallet scanning, and server connection. Record the block height or scan percentage, then compare it again after several minutes. Advancing progress is a reason to wait; there is no universal recovery deadline.
2. Check the chain tip. Compare the wallet's reported height with an independent source for the same network. A height that remains behind while new blocks appear elsewhere points toward synchronization or server trouble. A small temporary difference can occur because blocks propagate between peers at different times. Matching heights alone do not prove that wallet discovery is complete.

3. Compare a known receiving address. Use an address from your own earlier records and check whether the restored wallet derives it. A match strongly supports the recovery settings for that address, although other accounts or address types may still need discovery. Never enter your phrase into a block explorer.
4. Inspect connectivity and errors. Repeated disconnects, timeouts, unavailable servers, disk errors, or an unchanged scan position suggest an operational problem. In Bitcoin Core, `getblockchaininfo` reports fields including `blocks`, `headers`, and `initialblockdownload`; `getwalletinfo` can report wallet scanning progress. Call these through your own node's interface.
5. For a server-based wallet, try another supported server if progress has stopped. A server that reports an old chain tip or returns incomplete history can leave the wallet showing zero. Changing servers carries privacy implications because the replacement may learn which scripts or addresses you query.

If scanning finishes at the current chain tip and the balance remains zero, investigate recovery settings. Confirm the intended network, original wallet's phrase format, BIP39 passphrase, account, derivation path, address type, and discovery limits. A different BIP39 passphrase normally produces a different valid seed without an incorrect-passphrase error. A valid phrase checksum also cannot prove that you restored the intended wallet: it detects many input errors, but not all.

Avoid sending funds merely to test an uncertain recovery. Preserve the original backup and recovery details while diagnosing the problem.

FAQ

How long should I wait before worrying?

Watch measurable progress rather than elapsed time alone. An advancing scan can justify waiting for hours or longer; repeated errors or a stationary height justify investigation sooner.

Does a zero balance mean my phrase is wrong?

No. Incomplete discovery, a lagging server, or incorrect account settings can produce zero. A familiar derived address is useful evidence that part of the recovery matches.

Should I restart a stalled wallet?

Save diagnostic details first, then close it normally. Restarting may fix a connection problem, but scan continuation depends on the wallet. Never delete wallet files or backups as a troubleshooting shortcut.

Sources

- BIP44: Multi-Account Hierarchy for Deterministic Wallets (github.com)
- Electrum Documentation: Frequently Asked Questions (electrum.readthedocs.io)
- Bitcoin Core RPC Reference: rescanblockchain (bitcoincore.org)

Continue reading on bip39-phrase.com: Derivation Path Explained: What m/44'/0'/0'/0/0 Means
More on this topic: Recovery

Example sequences from the BIP39 wordlist

Randomly generated sequences of words from the BIP39 English wordlist. None of them passes the BIP39 checksum, so no wallet will accept them: they show the format only. Never store funds with a phrase you found in a document.

Example 1			
1 error	2 example	3 congress	4 creek
5 evidence	6 model	7 rebuild	8 hidden
9 throw	10 sausage	11 chunk	12 private

Example 2			
1 hotel	2 potato	3 vocal	4 february
5 kitchen	6 wrap	7 autumn	8 stumble
9 brave	10 elevator	11 work	12 typical

Example 3			
1 faint	2 inspire	3 color	4 salon
5 trim	6 runway	7 seek	8 march
9 expose	10 slot	11 maid	12 media

Example 4			
1 pumpkin	2 betray	3 route	4 emerge
5 observe	6 auction	7 glass	8 glue
9 monster	10 prefer	11 already	12 barely

Example 5			
1 account	2 floor	3 south	4 frame
5 funny	6 grow	7 hope	8 taxi
9 frozen	10 tip	11 defense	12 million

Example 6			
1 fee	2 arena	3 security	4 stone
5 purpose	6 thunder	7 pony	8 sort
9 destroy	10 treat	11 ritual	12 motor

Example 7			
1 tuition	2 endless	3 rich	4 tortoise
5 express	6 palace	7 stuff	8 lion
9 news	10 napkin	11 mail	12 young

Example 8			
1 spin	2 wave	3 oppose	4 ski
5 have	6 jealous	7 wet	8 miss
9 rookie	10 ridge	11 custom	12 claw

Reading a BIP39 phrase

Every word stands for an 11-bit number: its position in the 2048-word list, counted from 0. Here is Example 1 decoded word by word. Each word links to its page on bip39-phrase.com, where the list is numbered from 1.

#	Word	Index (0-2047)	Word no.	11 bits
1	error	614	615	01001100110
2	example	627	628	01001110011
3	congress	376	377	00101111000
4	creek	409	410	00110011001
5	evidence	622	623	01001101110
6	model	1140	1141	10001110100
7	rebuild	1434	1435	10110011010
8	hidden	859	860	01101011011
9	throw	1802	1803	11100001010
10	sausage	1533	1534	10111111101
11	chunk	325	326	00101000101
12	private	1369	1370	10101011001

The 12 words carry 132 bits: 128 bits of entropy followed by a 4-bit checksum. The checksum must equal the first 4 bits of the SHA-256 hash of the entropy.

`Entropy (hex): 4cc9ccbc1994dd1d2cd35be157f4a2d5`

This sequence ends in the checksum bits 1001, but SHA-256 of its entropy starts with 1111, so wallets reject it as an invalid phrase. That is the point of the checksum: about 15 of every 16 random or mistyped sequences fail it.

See also

- Coins Sent to Mistyped or Wrongly Restored Wallets · October 15, 2026

- Mnemonic Keys to the Kingdom: Why BIP-39 Still Matters in 2025 · June 15, 2025

Educational document. The example sequences are random and fail the BIP39 checksum: they are not wallets and must never hold funds. Security notes: bip39-phrase.com/security/