

# What a Change Address Is and Why Wallets Create One

October 15, 2026 · Document #355 · [bip39-pharse.com](https://bip39-pharse.com)



Photo by [Erik Mclean](#) on [Unsplash](#)

A change address receives the leftover balance from a spent UTXO using an internal derivation path to preserve user privacy.

## Contents

|                                               |   |
|-----------------------------------------------|---|
| How the UTXO Model Generates Change           | 2 |
| The Internal Derivation Path in BIP44         | 2 |
| Why Wallets Avoid Reusing the Sending Address | 2 |
| How Change Shows Up in a Wallet               | 3 |
| FAQ                                           | 3 |
| Sources                                       | 4 |
| Example sequences from the BIP39 wordlist     | 4 |
| Reading a BIP39 phrase                        | 5 |
| See also                                      | 6 |

In UTXO-based blockchains like Bitcoin, balances do not exist as static account ledgers. Funds are stored as discrete records called **Unspent Transaction Outputs** (UTXOs). When a transaction occurs, the software cannot carve out a partial amount from an existing UTXO. It must consume the selected UTXO in its entirety as an input, allocate the payment amount to the recipient's output, assign a portion to transaction fees, and route any remaining value to a change address.

## How the UTXO Model Generates Change

Operating a UTXO wallet resembles paying with physical currency. If you hold a single paper bill worth 50 dollars and purchase an item worth 30 dollars, you cannot tear the bill to pay the exact total. You hand the 50-dollar bill to the merchant and receive 20 dollars back.

In Bitcoin and similar networks, transaction inputs and outputs balance according to a strict mathematical relationship:

$$\text{Total Input Value} = \text{Recipient Output} + \text{Change Output} + \text{Miner Fee}$$

If an address contains a UTXO worth 0.05 BTC and you send 0.01 BTC, the wallet creates a transaction with:

- 1 One input consuming the 0.05 BTC UTXO completely.
- 2 One payment output of 0.01 BTC assigned to the recipient's address.
- 3 One miner fee deduction (for example, 0.0001 BTC).
- 4 One change output of 0.0399 BTC directed to a new address controlled by your wallet.

If the wallet omitted the change output, the remaining 0.0399 BTC would be treated as an unallocated remainder and claimed entirely by the miner validating the block.

## The Internal Derivation Path in BIP44

Modern HD (Hierarchical Deterministic) wallets generate change addresses automatically using a standardized tree structure derived from a single BIP39 seed phrase. Standards like BIP44, BIP49, and BIP84 formalize how these keys are derived.

The BIP44 standard defines the derivation path syntax:

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

The change level contains a constant index that separates public payment addresses from private operational addresses:

- `0` defines the external chain. Addresses generated under `.../0/index` appear in your wallet's "Receive" screen and are meant to be shared with third parties.
- `1` defines the internal chain. Addresses generated under `.../1/index` are reserved for internal wallet operations, specifically change outputs.

For Native SegWit transactions conforming to BIP84, the first receiving address uses the path `m/84'/0'/0'/0/0`, while the first change address uses `m/84'/0'/0'/1/0`. Each time a transaction requires change, the wallet increments the `address_index` on branch `1`, generating a fresh address automatically without altering the master seed.

## Why Wallets Avoid Reusing the Sending Address

Early wallet software sometimes routed change back to the address that funded the input. Modern wallets deliberately avoid this behavior to mitigate privacy and security risks.

- **Preventing Common-Input Clustering:** Blockchain surveillance firms analyze transaction graphs using the common-input ownership heuristic, which assumes all inputs in a multi-input transaction belong to the same entity. Reusing addresses across multiple spends links separate transactions together, revealing the user's total holdings and payment habits.
- **Obfuscating Transaction Flow:** When a transaction has two outputs—one going to the merchant and one going to a fresh change address—an external observer cannot immediately determine which output represents the payment and which represents the returned funds.
- **Cryptographic Hygiene:** Bitcoin addresses often represent the hash of a public key. When you spend from an address, you reveal the public key itself on-chain. Generating a fresh change address keeps the public key for the remaining funds unexposed until those funds are spent in a subsequent transaction.

## How Change Shows Up in a Wallet

Most mobile and consumer-oriented wallets hide change addresses to simplify the user interface. The interface calculates your aggregate balance across all derived addresses, presenting a single total.

Advanced desktop wallets (such as Sparrow Wallet or Electrum) provide full visibility into the derivation structure:

- In Electrum, enabling the Addresses tab displays two collapsible trees: "Receiving" (derived from branch 0) and "Change" (derived from branch 1).
- In Sparrow, navigating to Addresses reveals distinct tables for external and internal paths, showing the derivation index, balance, and number of transactions associated with each.
- Through **coin control** settings, advanced users can inspect individual UTXOs residing on internal change addresses, freeze specific change outputs, or manually choose which change UTXOs to spend in future transactions.

## FAQ

### Can you spend from a change address immediately?

In most modern wallets, yes. Once the parent transaction containing the change output is broadcast to the network's mempool, your wallet can generally spend that unconfirmed change UTXO in a child transaction (using Child-Pays-For-Parent mechanics), provided standard node mempool limits and policy rules allow chained transactions.

### What happens if the change amount is smaller than the miner fee?

If the change amount falls below the network's **dust limit** (the threshold where creating and spending the output costs more in transaction fees than the output itself is worth), the wallet typically drops the change output entirely and adds that remainder to the miner fee to avoid generating uneconomic UTXOs that nodes would reject under standard relay rules.

## Do account-based blockchains like Ethereum use change addresses?

No. Ethereum and similar networks use an account-based model rather than the UTXO model. Balances update directly as global state adjustments, meaning partial spends simply deduct from the sender's account without generating change outputs.

## Sources

- [BIP 44: Multi-Account Hierarchy for Deterministic Wallets \(github.com\)](#)
- [BIP 84: Derivation scheme for P2WPKH based accounts \(github.com\)](#)

Continue reading on bip39-phrase.com: [What Is Bitcoin Address & How It Works](#)

More on this topic: [Keys & Addresses](#)

## 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 | frog  | 2  | about    | 3  | wrestle | 4  | aunt    |
| 5 | tone  | 6  | convince | 7  | kitten  | 8  | rack    |
| 9 | order | 10 | toss     | 11 | basic   | 12 | outdoor |

### Example 2

|   |         |    |          |    |          |    |       |
|---|---------|----|----------|----|----------|----|-------|
| 1 | sponsor | 2  | truth    | 3  | cherry   | 4  | earth |
| 5 | salad   | 6  | ginger   | 7  | holiday  | 8  | logic |
| 9 | stone   | 10 | announce | 11 | acoustic | 12 | old   |

### Example 3

|   |        |    |          |    |       |    |       |
|---|--------|----|----------|----|-------|----|-------|
| 1 | garlic | 2  | negative | 3  | rely  | 4  | guide |
| 5 | style  | 6  | comfort  | 7  | alley | 8  | use   |
| 9 | right  | 10 | pattern  | 11 | fatal | 12 | shy   |

### Example 4

|   |         |    |         |    |        |    |        |
|---|---------|----|---------|----|--------|----|--------|
| 1 | guard   | 2  | budget  | 3  | lava   | 4  | pen    |
| 5 | one     | 6  | north   | 7  | order  | 8  | demand |
| 9 | disease | 10 | peasant | 11 | island | 12 | hello  |

### Example 5

|   |        |    |         |    |          |    |         |
|---|--------|----|---------|----|----------|----|---------|
| 1 | race   | 2  | chat    | 3  | canal    | 4  | hire    |
| 5 | finger | 6  | genuine | 7  | solution | 8  | sibling |
| 9 | eager  | 10 | battle  | 11 | supreme  | 12 | ostrich |

**Example 6**

|          |             |            |           |
|----------|-------------|------------|-----------|
| 1 subway | 2 exact     | 3 favorite | 4 erupt   |
| 5 govern | 6 diagram   | 7 visit    | 8 present |
| 9 agree  | 10 surround | 11 quiz    | 12 melt   |

**Example 7**

|          |            |           |           |
|----------|------------|-----------|-----------|
| 1 enrich | 2 wild     | 3 wink    | 4 slam    |
| 5 target | 6 mansion  | 7 ask     | 8 enforce |
| 9 deny   | 10 deposit | 11 minute | 12 length |

**Example 8**

|          |          |          |           |
|----------|----------|----------|-----------|
| 1 emerge | 2 glue   | 3 lumber | 4 number  |
| 5 notice | 6 ivory  | 7 total  | 8 clump   |
| 9 poem   | 10 alien | 11 rare  | 12 spirit |

**Example 9**

|          |             |           |            |
|----------|-------------|-----------|------------|
| 1 unfair | 2 merit     | 3 child   | 4 hybrid   |
| 5 hurdle | 6 snap      | 7 pattern | 8 scan     |
| 9 test   | 10 language | 11 fatal  | 12 kitchen |

**Example 10**

|            |           |          |            |
|------------|-----------|----------|------------|
| 1 ramp     | 2 fiscal  | 3 essay  | 4 nurse    |
| 5 busy     | 6 benefit | 7 echo   | 8 whale    |
| 9 electric | 10 silk   | 11 raven | 12 tonight |

## 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](https://bip39-phrase.com), where the list is numbered from 1.

| # | Word                     | Index (0-2047) | Word no. | 11 bits     |
|---|--------------------------|----------------|----------|-------------|
| 1 | <a href="#">frog</a>     | 745            | 746      | 01011101001 |
| 2 | <a href="#">about</a>    | 3              | 4        | 00000000011 |
| 3 | <a href="#">wrestle</a>  | 2034           | 2035     | 11111110010 |
| 4 | <a href="#">aunt</a>     | 122            | 123      | 00001111010 |
| 5 | <a href="#">tone</a>     | 1826           | 1827     | 11100100010 |
| 6 | <a href="#">convince</a> | 380            | 381      | 00101111100 |
| 7 | <a href="#">kitten</a>   | 986            | 987      | 01111011010 |
| 8 | <a href="#">rack</a>     | 1412           | 1413     | 10110000100 |

| #  | Word    | Index (0-2047) | Word no. | 11 bits     |
|----|---------|----------------|----------|-------------|
| 9  | order   | 1249           | 1250     | 10011100001 |
| 10 | toss    | 1837           | 1838     | 11100101101 |
| 11 | basic   | 152            | 153      | 00010011000 |
| 12 | outdoor | 1257           | 1258     | 10011101001 |

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): 5d200ff907ae445f1ed5849c3cb44c4e

This sequence ends in the checksum bits 1001, but SHA-256 of its entropy starts with 0110, 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

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/](https://bip39-phrase.com/security/)