



UTXO Label Card

Coin control and label convention: which coin speaks when you pay · belongs to Chapter 8 · Date: _____

Bitcoin has no account balance, only individual coins (UTXOs), and every coin has an origin. Exchange, trading partner, customer or swap service: someone knows this coin belongs to you. The blockchain never forgets that, your wallet does not show it. The label is the only reminder and stays local on your device. If two coins enter one transaction as inputs, chain analysis treats them as owned by the same person (common-input heuristic): once combined, linked forever, retroactively for the entire history of both coins. Coin control means you choose yourself, before every payment, which coins go in. Without labels, that choice is blind.

1 · THE ORIGIN CLASSES

Code	Class	Who knows about this coin	Rule
K	KYC purchase at a regulated exchange (Chapter 4)	The exchange with your full identity record, subject to reporting, chain analysis firms via the exchange data.	Tagged sats. Acceptable for saving, and the documented route for selling via the exchange.
P	No-KYC purchase peer-to-peer (Chapter 5)	Only the trading partner, depending on the payment method also their bank. No record at any exchange.	The premium paid for this separation. Never with K in one transaction, or it is lost retroactively.
E	Income: wages, sales, invoices, mining	The payer knows the address and usually your name.	Own class. Combined with K or P, you link the payer to the other observer.
L	Lightning swap back to the chain (Chapters 8/9)	The swap service sees both sides. In the transaction graph the coin no longer hangs on its old history.	Own class. Do not move almost the same amount shortly afterwards: amount correlation links even across a broken path.
M	Mixed (CoinJoin output)	No outsider can clearly assign the output to an input. Only you know which class it came from.	Never spend with unmixed coins, never send directly to a KYC exchange. Saving, paying directly, Lightning, P2P: all fine.
W	Change	Anyone who knows the parent coin. Analysis spots change by round amounts and address formats.	Inherits the parent coin's class, no exception. Set the label the moment you send.
U	Unknown (found without a label)	You no longer know. That is exactly the problem.	Treat like a foreign coin: spend alone or leave it, never combine with a clean class.

2 · THE LABEL CONVENTION

Fixed format: **CLASS-SOURCE-YYYY-MM-PURPOSE**. Source is your private code for the exchange, trading partner or customer (A1, HP, KD3). For change, the W is followed by the parent coin's label, for mixed coins by the class of the input.

Label	Read as
K-A1-2026-03-Savings	KYC purchase at exchange A1 in March 2026 via savings plan. Exchange and authorities can link the coin to your name.
P-HP-2026-04-Cash	P2P trade in April 2026, paid in cash. Only the trading partner knows the coin, no bank in the chain.
E-KD3-2026-05-Invoice	Invoice paid by customer KD3 in May 2026. Customer knows address and name, the invoice is in the origin documentation.
L-SW-2026-06-Swap	Lightning balance swapped back to the chain in June 2026. The swap service knows both sides.
M-K-2026-08-CoinJoin	CoinJoin output from August 2026, input from class K. For tax purposes the mix is, by common reading, not a disposal and the purchase date keeps running, but this is not expressly regulated (Chapter 18).
W-P-HP-2026-04-Cash	Change from a payment with P-HP-2026-04-Cash. Class P, stays in the P wallet.

3 · RULES FOR SPENDING (COIN CONTROL)

Rule	Why
One transaction, one class.	Joint inputs weld the history of every coin involved into one cluster. Never K with P, never M with unmixed coins, never U with anything. Two exchanges within K know your name anyway: defensible, but deliberate.
Change inherits the class and gets a label at once.	The sender's trail runs on through the change from transaction to transaction. Change without a label is class U within weeks.
Every receipt to a fresh address.	Receiving to the same address links all related transactions by itself. Good wallets generate one automatically, never bypass that.
Consolidate small coins only within one class.	Many small inputs cost proportionally high network fees, and mixing small amounts is uneconomical. Consolidation is itself a transaction with joint inputs, so only within one class.
Withdrawals to a KYC exchange only from class K, unmixed.	The exchange links every incoming coin to your name at once. Some reject freshly mixed coins or demand proof of origin. The holdings meant for sale stay on their documented route.
A label is no substitute for origin documentation.	Every coin needs a record: purchase receipt, trade data, invoice, date, price. When a bank, exchange or authority asks, the document you can present is what counts. Tax obligations apply equally to every class (Chapter 18).

⚠ **Three mistakes that destroy privacy retroactively.** **First:** a KYC coin and a No-KYC coin as joint inputs. The premium paid for the No-KYC coins is lost, irrevocably. **Second:** sending mixed coins directly to a KYC exchange or spending them with unmixed ones. The same state as before the mix, only with a detour. **Third:** using an address twice. Even the mixed wallet becomes traceable. None of these mistakes can be fixed afterwards.

4 · YOUR WALLET STRUCTURE (FILL-IN SHEET)

Separate wallets does not mean a second hardware wallet: with the optional passphrase (Chapter 6), the same hardware wallet creates any number of separate wallets with their own keys, addresses and history. Each needs its own passphrase backup, not a new seed. At minimum, separate accounts that never form joint transactions.

Cl.	What may go in	Wallet code	Backup code	Coin control	Labels complete
K	Only K and W from K. Holdings meant for sale stay here, unmixed.				
P	Only P and W from P. No contact with exchanges.				
M	Only mixed outputs, back into cold storage on fresh addresses.				
L	Swap returns. After a waiting period, spend individually or mix.				
E	Income with records. Own account, own addresses.				
U	Finds without a label. Quarantine until the origin is documented.				

Wallets, backup locations, exchanges and trading partners only as codes that only you can decode. No addresses, amounts, seeds or passphrases on this sheet: it may be found without giving anything away.