MONERO

PROTOCOL GUIDE

Monero

The principles, in plain language

What it is, why it exists and how it protects your privacy.

01

What is Monero

Monero is digital money that works like cash: you pay another person directly, with no bank in between, and nobody else needs to find out who paid, to whom or how much. Its unit is called XMR and it was born in 2014.

NO MIDDLEMEN

No company, bank or government controls it. Thousands of computers around the world keep the network running.

PRIVATE BY DEFAULT

Privacy is not switched on with a button: every transaction has it.

OPEN SOURCE

Anyone can read the code, review it and propose improvements.

02

Five prior ideas

If you already know how a cryptocurrency works, jump straight to section 4.

1. **The shared ledger.** At a bank, a single entity records who owns how much. Here the ledger is public and thousands of computers keep it at the same time. Transactions are grouped into blocks chained to one another: the *blockchain*.
2. **Keys.** You have two linked numbers. The public key is like your mailbox number: you can give it to anyone. The private key is the key that opens it, and it is never shared.
3. **The digital signature.** It is a seal that only you can apply with your private key. It proves you authorized a payment without revealing the key.
4. **Miners.** They are the ones who add new blocks to the ledger by solving a problem that takes a lot of computation. In return they collect new coins. Cheating would cost more than it earns.
5. **Outputs.** You do not have a balance, but loose coins, like banknotes. To pay you spend one or several whole banknotes and receive the change as a new banknote. A spent banknote cannot be spent again.

03

The problem: almost all digital money is public

In Bitcoin and most cryptocurrencies, the ledger is open: anyone can see which address paid which and how much. Your name does not appear, but it is enough for an address to be linked to you just once (a purchase, an exchange) for its whole history to be followed. It is as if your bank statement were public with the name blacked out.

> **Fungibility.** If every coin carries its history in plain view, a coin with a "bad reputation" can be worth less than an identical one. Money should be interchangeable unit for unit. Monero was designed so that it is.

04

The three privacy principles

Monero hides three things at once in every payment, each with its own technique.

HIDDEN RECEIVER

Stealth addresses

A new mailbox for every letter.

HIDDEN SENDER

Ring signatures

Signing inside a crowd.

HIDDEN AMOUNT

Confidential amounts

Sealed envelopes that can be added up.

Who receives: stealth addresses

Your Monero address is public and reusable, but it never appears on the chain. For each payment, whoever pays you uses your address to build a new, one-time destination that only you can recognize as yours. It is as if every letter arrived at a different mailbox that only you know how to open: from the outside, two payments to you do not seem to be related.

Who pays: ring signatures

When you spend a coin, your wallet mixes it with 15 other coins from the chain that belong to other people and signs in a special way. The signature proves that one of the 16 is yours, but not which. It is like signing a document in the middle of a crowd that signs at the same time: it is known that one of them signed, not who.

In addition, each spent coin leaves a unique tag that prevents it from being spent twice, without revealing which one it is.

How much: confidential amounts

Amounts travel in sealed envelopes. The network does not open any of them, but it can add up the incoming and outgoing ones and check that they match, that is, that nobody has created money out of nothing. An extra proof guarantees that no envelope contains a negative amount.

> The three mechanisms work together: nobody knows who receives, who sends or how much, and yet anyone can verify that everything is valid.

05

A payment, step by step

1. The person about to pay you uses your address, which is long and reusable.
2. Their wallet creates a one-time destination for you. Your address does not appear on the chain.
3. To spend their coins, the wallet mixes them with 15 others and signs. Nobody knows which one is the real one.
4. The amounts go in sealed envelopes that the network checks without opening.
5. Miners include the payment in a block, in about 2 minutes, and thousands of nodes verify it.
6. Your wallet recognizes the payment as yours with your view key. After about 20 minutes (10 blocks) you can spend it.

06

What keeps the network secure

MINING FOR EVERYONE

It uses RandomX, an algorithm designed for ordinary computers and unfavourable to specialized machines.

PERMANENT REWARD

After the main issuance, each block keeps paying 0.6 XMR to miners, so that they always have an incentive.

Each node checks all the rules on its own, so there is no need to trust anyone. No network is invulnerable: in 2025 one group concentrated a lot of mining power and managed to reorganize up to 18 recent blocks, the largest episode of this kind in Monero's history. That is why, for large payments, it is wise to wait for several confirmations.

REFERENCE

Quick glossary

TERM	IN ONE SENTENCE
Blockchain	Public ledger made of chained blocks
Node	Computer that stores the ledger and checks all the rules
Miner	Whoever adds new blocks and collects coins for it
Wallet	Program that stores your keys and creates your payments
Public and private key	Your mailbox, which is shared, and its key, which is not
Stealth address	One-time destination derived from your address
Ring signature	Signature that proves one of several signed, without saying who
Key image	Unique tag of each spent coin that prevents double spending
XMR	The unit of Monero

> **Next step.** The complete guide, "Monero in depth", explains each of these pieces in more detail and with their maths, chapter by chapter.

Sources: The Block and Cointelegraph (2025 reorganizations).