

Using Bitcoin



Using Bitcoin

from first transaction

Learn bitcoin by using bitcoin

Ryan Wold

Copyright © 2025 Ryan Wold

First edition, 2025.

ISBN: *[pending]*

BSBN: *[pending]*

Typeset in Palatino and Helvetica Neue.

Illustrations by the author.

Printed in the United States of America.

Some details in this space change quickly: wallet recommendations, fee levels, and regulations. Treat those as dated snapshots. The enduring parts of this book are the mental models, workflows, and habits.

Draft 2026-10-12 · 3b255ee-dirty (v040)

Text and illustrations © Ryan Wold, licensed CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>). Code MIT. Title, cover and the LiveWallet name reserved.

Contents

Quick Facts	vi
How to Read This Book	viii
1 Start Here	1
1.1 Why I Wrote This	2
1.2 The Path	3
2 Why Direct Payments	4
2.1 You Already Know The Problem	4
2.2 Money Solves A Coordination Problem	4
2.3 Online Money Still Uses Middlemen	6
2.4 Why Electronic Cash Matters	7
3 What Bitcoin Is	9
3.1 Bitcoin Is A Protocol	9
3.2 Sending Information, Not Coins	9
3.3 More Than A Payment	10
3.4 Peer To Peer Means Direct	11
3.5 The Record Is Shared—And Checkable	12
4 Wallets	14
4.1 Where Your Bitcoin Actually Lives	14
4.2 Choosing Your First Wallet	15
4.3 What You Actually See	16
4.4 Getting A Small Amount	17
5 Seed And Recovery	19
5.1 Why The Backup Looks Like Words	19
5.2 What To Do The Moment The Words Appear	19
5.3 Recovery Is Part Of Setup	20
5.4 If You Lose The Phone	21
5.5 The Rule You Must Not Break	21
5.6 What Losing The Backup Looks Like	22

6	First Transaction	23
6.1	Receiving Comes First	23
6.2	Before You Send: Check The Network	23
6.3	Sending Is Signing A Message	24
6.4	The Sender Pays For Delivery	25
6.5	What It Actually Looks Like	26
6.6	Pending Is Not The Same As Broken	28
6.7	When Things Go Wrong	28
6.8	Mistakes To Avoid On The First Send	29
7	Network Reference	31
7.1	Why There Are Multiple Networks	31
7.2	How To Tell Them Apart	31
8	After The First Send	33
8.1	What Good Progress Looks Like	33
8.2	What Good Tools Feel Like	33
8.3	Look It Up Yourself	34
8.4	What To Do This Week	35
8.5	What You Should Be Able To Say Now	35
8.6	A Glimpse Ahead: Payments That Carry Meaning	36
8.7	What Changes When Money Moves Like Information	37
9	Quick Words	39
	How This Started	42
	Where To Go From Here	43
	About the Author	44

Quick Facts

Three numbers to carry through the book.

100,000,000

satoshis (sats) in one bitcoin



one dollar = **100** cents

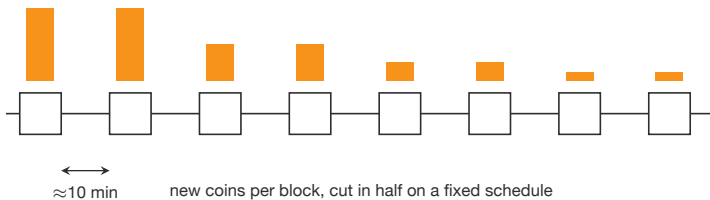


one bitcoin = **100,000,000** sats

A first transaction is a few thousand sats: cents, not coins. Wallets show both, so read the unit before the number.

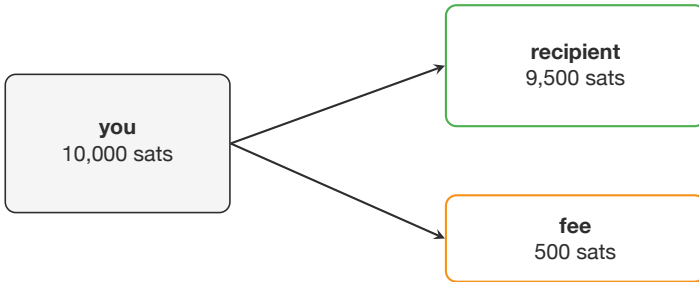
21,000,000

coins, ever, released one block at a time



A block lands about every ten minutes. The last sliver arrives around 2140.

Every transaction sends some sats, pays some sats



The sender pays the fee, like postage on a letter. It is usually a few hundred sats, and the receiver never pays it. What is not sent to the recipient or kept as fee comes back to you as change.

Three sentences to keep

- A wallet holds keys, not coins.
- The seed phrase restores everything. Never share it.
- Pending is not broken. Wait, then check an explorer.

Each one gets its own chapter. Come back to this page when a number in the wild looks strange.

How to Read This Book

This book uses a small set of visual cues to help you navigate.

Concept Box

Key ideas explained in context.

Warning: Warning

Honest notes about current pain points. Bitcoin is not always easy—yet.

Key points are highlighted with an orange bar for quick scanning.

Try It boxes (green border) walk you through practical steps.

Action Checklists (orange border) appear at chapter ends with things to do.

Numbered steps (1) show sequences that should be followed in order.

The line that runs through this book and the notebooks at `livewallet.app` is the same: learn bitcoin by using bitcoin.

If you want to try Bitcoin before reading the theory, skip to Chapter 4 (Wallets) and follow the path from there through your first transaction. If you want to understand the problem first, start at the beginning. Either path works. The notebooks start on testnet. Real coins are a switch you make later, on a Livebook you run yourself, and the amount should stay under one dollar while you learn.

Chapter 1

Start Here

This book is about making your first careful Bitcoin transaction.

Not a trading strategy. Not a grand theory. Just enough understanding to set up a wallet, protect the backup, receive a small amount, and send a small amount without doing anything careless.

Use a tiny amount while learning. The goal is competence, not commitment.

If you only remember four things, remember these:

- 1 Set up a wallet you can understand.
- 2 Write down the seed phrase on paper.
- 3 Receive a small amount.
- 4 Send a small test payment.

That is enough to turn Bitcoin from a topic into a tool.

You do not need to settle every argument about Bitcoin before you can learn to use it. You need a working mental model and a cautious first experience.

Think of a newcomer named Maya. She does not want hype. She wants to know what Bitcoin is, how to avoid obvious mistakes, and what actually happens when money moves.

Try It: What Success Looks Like

- set up a wallet on a phone
- write down the backup words before funding it
- receive a very small amount
- send a test payment and understand what happened

That is the path this book follows.

Why I Wrote This

Most of the systems you use every day—to send messages, share photos, read news—were built when moving information became cheap. But moving *value* is still expensive. Not because the technology does not exist, but because the old infrastructure is still in the way.

When you sent your first email, you did not realize you were participating in a shift from postal mail to digital communication. You were just sending a message. Bitcoin is a similar shift—not from paper money to digital money (that already happened), but from *middleman money* to *direct money*.

The systems we have work. They also take a cut, add delay, and decide who gets to participate. Those are not bugs—they were necessary when the systems were built. But they are becoming relative inefficiencies as information moves faster and people expect to transact as easily as they communicate.

This book will not ask you to believe Bitcoin is the future. It will show you how to use it once, carefully, and let you decide for yourself whether the directness matters.

The Path

You can think of the rest of the pages as answers to four beginner questions:

- What problem is Bitcoin trying to solve?
- What does a wallet actually do?
- Why is the seed phrase such a big deal?
- What happens when I send a transaction?

Action Checklist

- ☐ keep the amount tiny
- ☐ move slowly when the wallet shows backup words
- ☐ treat the first send as practice, not performance
- ☐ stop and check instead of guessing

By the end, you should be able to make a first transaction, explain the wallet-seed-transaction model in plain language, and keep learning from experience instead of headlines alone.

Chapter 2

Why Direct Payments

Bitcoin makes more sense when you start with a question you have probably already asked: why is it so hard to just send someone the money?

You Already Know The Problem

You want to send \$50 to a relative in another country. Western Union charges \$12. A bank wire costs \$30 and takes three days. Even Venmo only works if both people live in the same country and have accounts.

Or maybe the problem is smaller. You read a good article and would pay a dime for it, but the site wants \$12 a month. A street musician posts a video you love and you would tip a dollar, but the platform takes a third of it and the rest does not arrive for weeks.

These are not edge cases. They are everyday friction that most people have learned to accept.

The internet lets you send a photo to anyone on earth in seconds, for free. Sending five dollars to the same person still requires a company in the middle, a fee, and sometimes days of waiting.

| We solved this problem for information decades ago. We still have not solved it for money.

Money Solves A Coordination Problem

Stepping back: money itself is just a coordination tool.

You have fish. You need shoes. The shoemaker does not want fish. Money gives people a shared middle step so that any two people can trade, even if neither wants what the other has.

Good money helps people do three ordinary things:

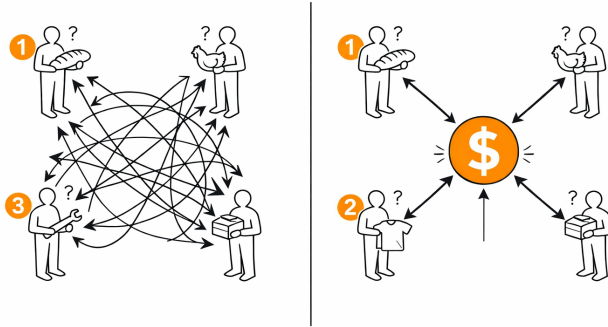


Figure 2.1: *Barter is messy. Money becomes the shared hub.*

- It helps you trade for what you need.
- It holds value long enough to save and plan.
- It gives people a common way to quote prices.

For a beginner, the main point is simpler: money is a coordination tool. Better money reduces friction.

A Good Beginner Filter

When a payment system feels abstract, ask three plain questions:

- does it help two people exchange more directly
- does it make small payments easier or harder
- who gets to delay, reverse, or refuse the payment

Online Money Still Uses Middlemen

Most money today is not cash in your pocket. It is a record in somebody else's database.

When you pay online, a surprising number of parties may sit between you and the person receiving the money: banks, card networks, processors, and merchants' banks. The flow usually works, but it is not direct.

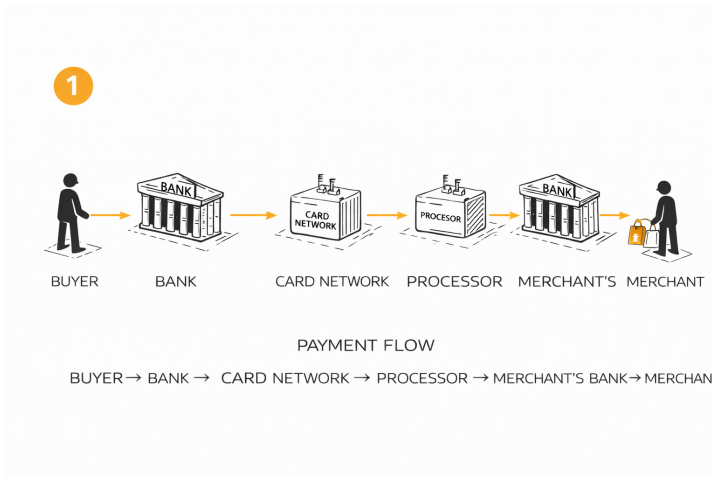


Figure 2.2: Most online payments pass through several intermediaries before they settle.

That arrangement creates trade-offs:

- payments can be reversed later
- small payments become uneconomical
- some people are excluded from the system entirely
- cross-border payments can be slow and expensive

These trade-offs were necessary when the systems were designed. Banks needed intermediaries because trust had to be established between strangers who could not verify each other directly. Card networks needed proces-

sors because merchants could not connect to every bank on their own. Each layer solved a real problem.

But the layers add up. And as information technology accelerates, the overhead of those older layers becomes a relative inefficiency—not a flaw in the original design, but a cost that no longer needs to be this high.

The internet moves information fast. Money still often moves through older rails, older business models, and other people's permission systems.

Why Electronic Cash Matters

Cash has useful properties that many digital payments lost.

Cash is direct. Cash is final. Cash can work for small amounts. And cash does not require every payment to pass through an account relationship first.

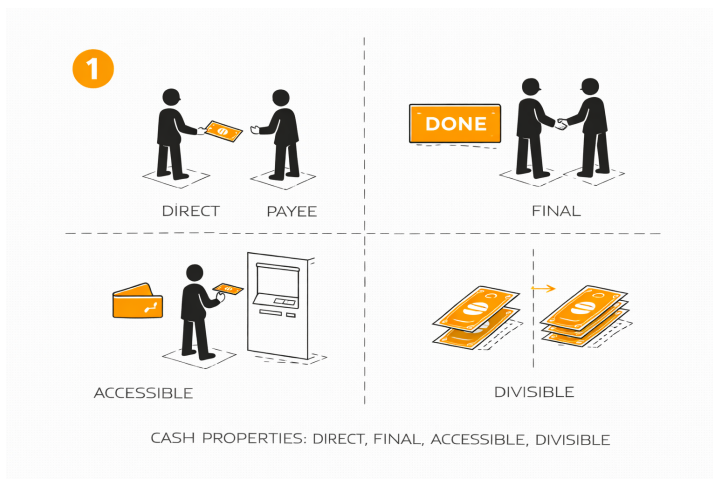


Figure 2.3: *Cash is direct, final, accessible, and easy to divide into small amounts.*

That is why the phrase *electronic cash* matters. The goal is not to replace every bank or card. The goal is to make direct digital payments possible

when direct payment is the better fit.

If every digital payment requires an account relationship, a gatekeeper, and a meaningful fee, some uses of money simply never show up. The local newspaper that could charge five cents per article instead charges twelve dollars a month or runs ads. The musician who could earn a penny per play instead gets a fraction of a cent from a platform that takes the rest. The freelancer who could be paid instantly across a border instead waits a week and pays a wire fee.

These are not hypotheticals. They are business models and livelihoods that do not exist because the payment infrastructure prices them out.

Bitcoin only matters if it helps digital money feel more direct, more final, and more usable at small scale.

Chapter 3

What Bitcoin Is

Bitcoin is easier to understand when you stop treating the wallet app as the whole system.

Bitcoin Is A Protocol

Bitcoin is not a company with a CEO. It is not a share of ownership in a business. And it is not just the wallet app on your phone.

Bitcoin is a protocol: a shared set of rules that computers follow to keep a record of who can spend what.

That means two useful things for a beginner:

- the app you use is only an interface
- the money does not live inside the app itself

Try It: The Beginner Mental Model

- the wallet app is the interface
- the shared ledger is the record
- the key is what lets you authorize spending

People often say they “bought Bitcoin” when what they really gained was the ability to control value on the network with a key.

Sending Information, Not Coins

Here is the shift that makes everything else click: a Bitcoin transaction is not shipping a coin through the internet. It is sending a *message*.

Think of it as a sealed letter.

You write instructions inside: pay this much, to this address. That is the content.

You seal the envelope. In the physical world, sealing means folding the flap so the contents cannot be changed without tearing the paper. In Bitcoin, sealing means *signing*—your wallet uses your private key to create a mathematical stamp that proves you authorized this message.

Think of a wax seal on a letter. Anyone who receives the letter can look at the seal and verify it came from you. But only you have the signet ring that makes the seal. If someone tampers with the contents, the seal breaks. That is what a digital signature does: it proves who sent the message and that nothing was changed along the way.

Then you address the envelope and drop it in the mailbox. The network carries it. The computers that process transactions check the seal, confirm the instructions make sense, and deliver it.

Nobody opens the envelope and changes the amount. Nobody redirects it to a different address. The signature guarantees integrity. The address sets the destination. The network processes the delivery—though it may take minutes, and a malformed or underfunded transaction can be rejected.

A transaction is a signed message. The signature proves it is yours. The network processes and confirms it.

More Than A Payment

The envelope analogy goes further than payment.

You can write on the outside of the envelope. Not just the address—you can add a note, a reference number, a label that other systems can read without opening the seal. In Bitcoin, this means a transaction can carry small amounts of data alongside the payment: a timestamp, a document hash, a short message.

You can also put an envelope inside an envelope. A transaction can reference other transactions, or carry structured information that another application knows how to read.

And here is the part that surprises most people: an envelope does not have to go in the mail to be useful. You can prepare a signed transaction, use it as a receipt or a template, and never broadcast it. Systems can benefit from the transaction format—the structure, the signature, the clear fields—without every message needing to be posted to the public ledger.

When a transaction *does* get posted, the network adds something no private system can: a timestamp and a permanent public record. That is the postmark. But the container is useful with or without it.

For a beginner, the practical takeaway is simpler: a Bitcoin transaction is not just a way to move money. It is a signed, structured container. That is why people keep finding new uses for it.

Peer To Peer Means Direct

Peer to peer sounds technical, but the beginner idea is simple: one person can pay another person on the network without asking a bank or card network to route the payment first.

- 1 Maya decides to pay Rosa.
- 2 Her wallet creates a message: “pay this much to Rosa.”
- 3 Her wallet seals the message with her signature.
- 4 The network checks the seal and confirms the payment.
- 5 Rosa can now treat that payment as received.

No bank has to approve the transfer first. No card network has to route it. No processor has to decide whether the transaction fits its business model.

That does not make Bitcoin magical. It makes it a different kind of payment system—one where the message goes directly from sender to recipient, and the math does the work that a middleman used to do.

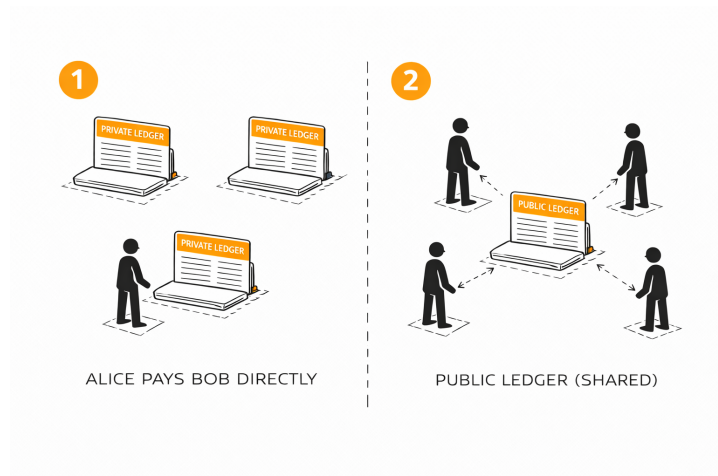


Figure 3.1: Bitcoin allows a direct payment path instead of routing every payment through a processor.

The Record Is Shared—And Checkable

Traditional ledgers are private. Your bank has one. A merchant has another. A payment company may keep a third. If those records disagree, the parties have to work it out.

Bitcoin uses a shared ledger instead. Many computers keep copies of the same history. No single machine is the whole system. No single office is “the place” where Bitcoin lives.

This is why people call Bitcoin distributed. Copies of the ledger exist in many places, under many operators, at the same time.

There is something else unusual about this ledger: it is public. When Maya looks up her transaction on a block explorer later, she is seeing something most financial systems do not offer—a record that anyone can verify independently. Not because the system is broken, but because it was designed that way.

Traditional payments are private by default, which means you trust the bank’s version of the record. Bitcoin payments are public by default,

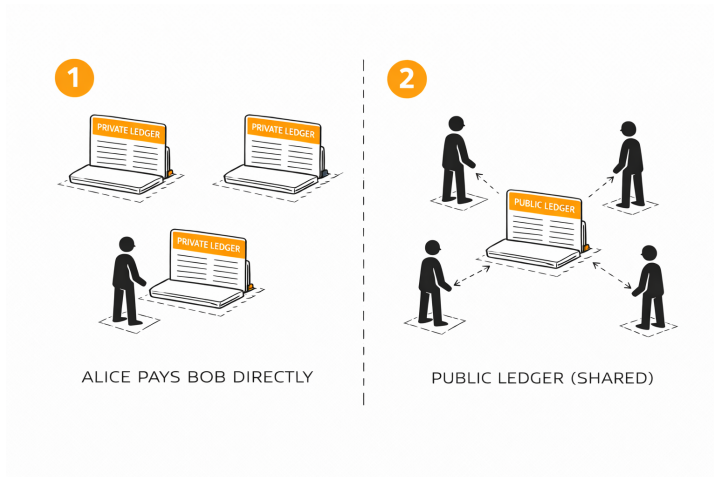


Figure 3.2: *Private ledgers stay separate. A public ledger gives many participants the same record.*

which means you can check. That transparency is not an accident. It is a design choice, and it has consequences—some empowering, some worth thinking carefully about—that we will return to later.

Bitcoin is a shared public record, and a wallet gives you keys that let you sign messages authorizing changes to your part of that record.

Try it. Look up a real transaction on the shared record: [transactions/verify-on-chain.livemd](https://transactions.verify-on-chain.livemd).

Most users do not need the full history on their phones. A lightweight wallet can still be useful because it talks to the network without carrying the whole chain itself.

Chapter 4

Wallets

The first mental shift is simple but important:

A wallet holds keys, not coins. The coins live on the ledger.

Where Your Bitcoin Actually Lives

When newcomers hear “digital money,” they often imagine the money sitting inside an app, a phone, or a cloud account.

Bitcoin does not work like that.

The money is recorded on the shared ledger. Your wallet gives you the keys that let you prove which part of that record you control. Lose the phone and the ledger does not disappear. Lose the backup to the keys and you may lose access.

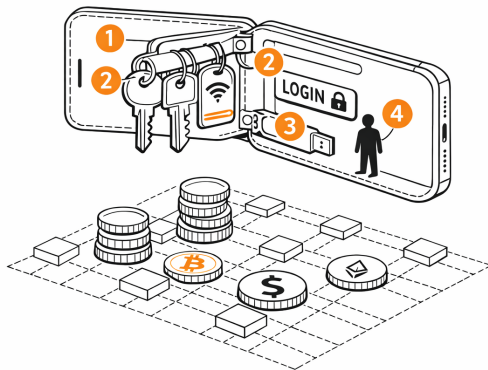


Figure 4.1: *A wallet is closer to a key organizer than a purse full of coins.*

That is why wallets matter so much. They are not just nice-looking interfaces. They are the tools that stand between you and the part of the ledger you can spend from.

Choosing Your First Wallet

Maya's first decision is not "Which app is coolest?" It is "Who controls the keys?"

Custodial wallet:

- A company holds the keys for you.
- Recovery is easier.
- You are trusting that company not to freeze, lose, or misuse access.

Non-custodial wallet:

- You hold the keys.
- You get real control.
- You also take on the backup responsibility yourself.

For learning, the beginner-safe path is usually:

- use a non-custodial wallet
- keep the amount small
- test backup and recovery before trusting the wallet with more

The first goal is not the perfect wallet. It is a wallet you can understand. If the responsibility feels heavy, lower the amount while learning. Do not lower the backup standard.

Warning: Custody changes the failure mode

A custodial wallet may feel familiar because it behaves like an ordinary account. That familiarity usually means a company can freeze access, delay withdrawals, or decide how recovery works.

A non-custodial wallet asks more from you, but it is also the first time the ownership model becomes real. Start small enough that you can afford to learn carefully.

Then choose a form factor:

- **Mobile wallet** for small everyday amounts and fast learning
- **Desktop wallet** if you want a larger screen or more controls
- **Hardware wallet** when the amount starts to feel important

If you are new, a mobile wallet is usually enough for the first pass.

Try It: A Good First Wallet**Look for:**

- backup instructions before you fund it
- receive and send screens that are easy to read
- a clear restore or import path
- a setup flow you can test with a tiny amount

Be cautious if:

- it is hard to tell who controls the keys
- the backup path feels hidden or optional
- the app feels confusing before you even try a first receive

What You Actually See

Most wallets hide the cryptography on purpose.

You usually do not see a raw public key. You see:

- a receive address
- a QR code
- a send screen
- a confirmation prompt

The useful beginner rule is this:

- an address or QR code is safe to share for receiving
- a private key or seed phrase is never safe to share

Two facts about addresses save a lot of confusion later.

First, one seed phrase makes as many addresses as you will ever need. The wallet derives them from the seed in order, so a backup of the words is a backup of every address the wallet has shown you or ever will. Many wallets show a fresh address each time you tap Receive. That is normal, and the old ones keep working.

Second, an address is not the key. The wallet computes an address from the public half of a key, and there is no way to run that computation backwards. Handing someone an address tells them where to pay you and nothing else.

Test before trust. A wallet is not real to you until you have received, restored, and sent with a small amount.

Getting A Small Amount

Once the wallet is ready, Maya needs a tiny amount to learn with. Five to ten dollars is plenty. The goal is not investment. It is practice material.

There are a few common paths:

- **An exchange or app.** Services like Cash App, Coinbase, or a local equivalent let you buy a small amount with a bank account or card. The important beginner step is the *withdrawal*: once you buy, send the Bitcoin to your own wallet. If it stays on the exchange, you are using a custodial account, not your own keys.

- **A Bitcoin ATM.** These exist in many cities. They accept cash and send Bitcoin to an address you provide. Fees are often higher than online exchanges (sometimes 5–10%), but the process is fast and does not always require an account.
- **From another person.** If you know someone who already uses Bitcoin, ask them to send you a small amount. You give them the receive address or QR code from your wallet. This is the simplest path and the one that feels most like the rest of the book.
- **Earn some.** Ask to be paid a small amount for a task, a product, or a favor.

Warning: Most on-ramps require identity verification

Exchanges and ATMs in most countries require some form of identity check (called KYC—know your customer) before you can buy. This usually means a government ID and sometimes a photo. It is a legal requirement, not a scam. But it does mean your purchase is tied to your identity. If that matters to you, buying from another person or earning Bitcoin avoids this step.

Do not optimize for price, ideology, or long-term storage yet. Optimize for a safe first experience.

Your first wallet should hold a learning amount, not a life-changing amount.

Try it. Make a seed and a wallet, then derive an address, in LiveWallet: [wallet/seed-and-wallet.livemd](#).

Try it. See how keys become an address: [wallet/keys-and-addresses.livemd](#).

Chapter 5

Seed And Recovery

This chapter has one main job:

Treat the seed phrase as the backup to your wallet, not as a password you type casually into random places.

Why The Backup Looks Like Words

A private key is far too awkward to memorize or write down as a giant string of numbers. Wallets solve that by turning the backup into 12 or 24 simple words.

Those words are the root backup for the wallet. If you still have them, you can usually recover access even if the original phone is gone.

If somebody else gets them, they can usually recover access too.

That is why the seed phrase is better understood as master backup material than as a login secret.

What To Do The Moment The Words Appear

When the wallet shows the seed phrase, stop and slow down.

Try It: When The Words Appear**Do this immediately:**

- write the words down on paper
- keep them in the right order
- check the spelling carefully
- store the paper somewhere safer than your phone

Do not do this:

- do not screenshot it
- do not photograph it
- do not drop it into Notes, email, or cloud storage
- do not send it to a friend “just in case”

That one pause is one of the most important moments in the entire beginner journey.

| If a seed phrase becomes easy to copy, it becomes easy to steal.

The only normal place to type those words later is the restore or import screen of a wallet you trust.

Recovery Is Part Of Setup

A lot of people treat recovery as a future problem. It is not. Recovery is part of setup.

Maya should assume the phone will eventually be lost, replaced, broken, or wiped. A wallet is not really ready until she knows the backup works.

That means testing recovery while the amount is still small:

- 1 Create the wallet.
- 2 Write down the seed phrase.
- 3 Restore the wallet from the written words.

- 4 Make sure the same wallet comes back.

Only after that test should the wallet start holding more than an experiment. An untested backup is hope, not recovery.

If You Lose The Phone

Losing the phone is not the disaster. Losing both the phone and the seed phrase is the disaster.

If Maya loses the phone but still has the backup words, the normal path is:

- get a new device
- install the wallet again or use a compatible wallet
- choose restore or import
- enter the words in order
- wait for the balance and history to reappear

The exact screens vary by wallet, but the principle does not.

The Rule You Must Not Break

No legitimate support person, giveaway, verification page, or friend ever needs your seed phrase.

If anyone asks for it, they are asking for control.

Warning: A request for your seed phrase is a theft request

It does not matter whether the message says support, recovery, verification, or prize claim. The words are the backup. Anyone who gets them can usually restore the wallet and move the funds.

What Losing The Backup Looks Like

Here is what Maya does not want to happen.

She sets up a wallet. She skips the backup because the amount is small. Six months later she has added more over time. One day the phone breaks.

She gets a new phone and installs the wallet. It asks for her recovery words. She does not have them.

There is no support number to call. There is no “forgot my password” link. The money is still on the ledger, but nobody can sign for it anymore. It is like a locked safe with no key—the contents still exist, but no one can reach them.

This is not a rare disaster story. It is the most common way people lose access to Bitcoin. The amount was small when they skipped the backup. It was not small when they needed it.

Write it down. Store it carefully. Test it once. Share it with no one.

Try it. Practice the backup words on testnet, not with real coins: [wallet/seed-and-wallet.livemd](https://wallet.seed-and-wallet.livemd.com).

Chapter 6

First Transaction

You have a wallet and a backup. Now the part you came for.

Maya wants to receive a small amount and send a small payment without doing anything reckless.

Receiving Comes First

Before sending, you usually receive.

The wallet will normally show a receive screen with:

- an address—a long string of letters and numbers, like `bc1qxy2k gdygjrsqtzq2...`
- a QR code that encodes the same address
- maybe a local-currency estimate beside the Bitcoin amount

The practical move is simple: if someone is paying you in person, let them scan the QR code. If they are paying you remotely, copy the address carefully.

If you paste an address, glance at the beginning and end before confirming. Small checks prevent boring mistakes.

Sharing a receive address is normal. Sharing a seed phrase is never normal.

Before You Send: Check The Network

This book uses Bitcoin as the default for your first transaction. The addresses, fees, and confirmation times in these examples all assume the Bitcoin network.

There are other networks with similar names—you may encounter them as you explore further. Chapter 7 has a short reference if you need it. For now, the only thing that matters is this: make sure you and the recipient are on the same network before you send.

Warning: Sending on the wrong network

Sending to an address on a different network can mean lost funds or a confusing rescue attempt. When in doubt, stop and check. A tiny test send is always cheaper than a mistake.

Sending Is Signing A Message

Remember the sealed letter from earlier. A Bitcoin transaction is not shipping a coin through the internet. It is composing a message—“pay this much to this address”—and signing it with your key.

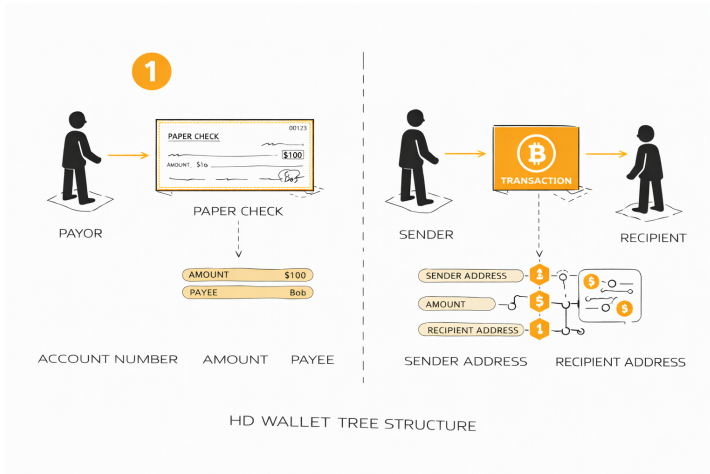


Figure 6.1: A transaction is an instruction to move value, similar in spirit to a signed check.

Your wallet helps you fill in the practical parts:

- who is getting paid (the address)
- how much to send (the amount)
- what fee to attach (the postage)
- whether the final review looks right

When you tap confirm, the wallet seals the message with your signature and sends it to the network. The network checks the seal, confirms you have the funds, and delivers the payment.

That is why losing your key is different from losing a password. A password can be reset by whoever runs the system. A signature key is yours alone—nobody else can reset it, and nobody else can forge it.

The Sender Pays For Delivery

Transactions also work like sending a letter with postage.

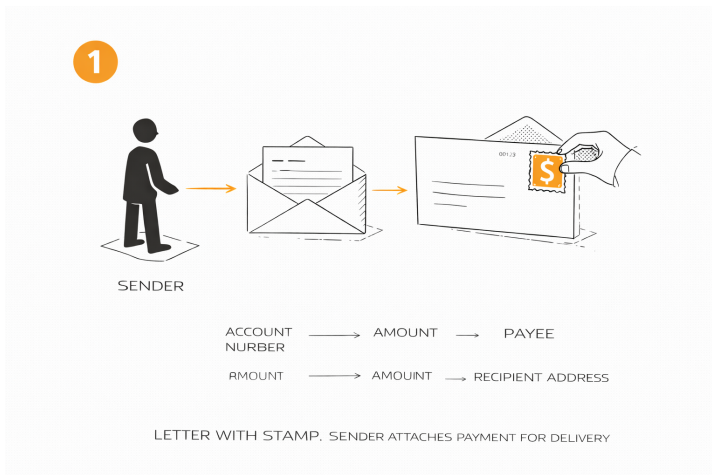


Figure 6.2: *The sender attaches the fee, much like attaching postage to a letter.*

You attach a fee because the network needs a reason to process the trans-

action. The receiver does not pay that delivery cost. The sender does.

There is one more line on the receipt that surprises people the first time. Your wallet does not draw four dollars out of a balance. It spends whole chunks of earlier payments, the way you hand over a twenty-dollar bill for a four-dollar coffee. Whatever is not going to the recipient comes back to you as change, at an address inside your own wallet. The wallet handles this on its own. The fee is what is left after the payment and the change: the part of the bill nobody claimed, which the network keeps for delivering the transaction.

So when you look the transaction up later, expect two destinations, one for the recipient and one back to you. That second line is not a mistake and not a double payment.

For a first transaction, that means:

- accept the wallet's default fee unless you have a reason not to
- send a very small test payment first
- do not rush the confirmation screen

What It Actually Looks Like

Here is what Maya's first send looks like in practice.

She opens her wallet and taps Send. She pastes Rosa's address—it starts with bc1q and looks like a long string of random characters. She enters 50,000 satoshis, which her wallet shows as about \$4. The suggested fee is around 500 satoshis—a few cents. She reviews: right address, right amount, small fee. She taps Confirm.

The wallet shows "Pending." About twelve minutes later, it changes to "1 confirmation." The money has arrived. Rosa's wallet now shows the same amount.

Total time: under fifteen minutes. Total cost: a few cents in fees.

Try It: A Safe First Send**Before you start:**

- make sure the wallet is backed up
- have the recipient's address or QR code ready
- confirm you are both on the same network
- keep the amount small enough to treat as practice

Then do this:

- get the address or QR code from the recipient
- open the wallet's send screen
- enter the amount
- review the fee and final details
- confirm the transaction

If you are nervous: do the first send to another address you control.

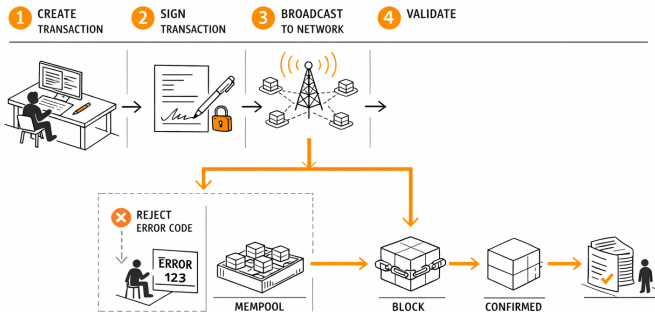


Figure 6.3: A transaction is created, broadcast, checked, and then either confirmed or rejected.

Most wallets will show the transaction in history immediately, even before it is confirmed in a block.

If Maya is nervous, the safest first send is often to herself: one address in the wallet paying another address in the same wallet.

Pending Is Not The Same As Broken

After you send, the usual first status is something like:

- pending
- unconfirmed
- broadcasting

That does not usually mean failure. It means the transaction has been created and is waiting to be included in a block. A first confirmation typically takes around ten minutes, but it can be faster or slower depending on network traffic.

Then, once it is confirmed, the payment becomes much harder to unwind. That is why Bitcoin can feel both empowering and unforgiving.

Pending is normal. Reversed by customer support is not. If the wallet gives you a transaction ID, that is your receipt for checking the payment later.

When Things Go Wrong

Maya sends a payment and twenty minutes later it still says “Pending.” She wonders if she made a mistake.

Usually, this just means the network is busy. The transaction is waiting its turn. If she attached a typical fee, it will almost always confirm within an hour.

What she should do: nothing. Wait. Check the transaction ID on a block explorer if she wants reassurance. The explorer will show whether the network has seen the transaction and how close it is to being confirmed.

What she should *not* do: send the same payment again. That is how beginners accidentally pay twice.

Warning: Bitcoin does not have an undo button

If Maya sends to the wrong address, there is no customer support line to call. The payment is a signed message, and once the network confirms it, it is final.

This is why the book keeps saying: check the address, keep the amount small, and treat the first sends as practice. The finality that makes Bitcoin powerful also makes carelessness expensive.

Mistakes To Avoid On The First Send

Most beginner mistakes are not exotic. They are ordinary rushed mistakes.

- sending too much on the first try
- mixing up the amount or units (satoshis vs. whole bitcoin)
- not checking the address beginning and end
- panicking when the transaction is still pending
- assuming Bitcoin works like a credit card and can be reversed later
- sending on the wrong network without checking the ticker first

Action Checklist

- ☐ confirm the ticker and network match
- ☐ receive a small amount first
- ☐ send a small test payment to yourself or a trusted recipient
- ☐ watch it move from pending to confirmed
- ☐ check the transaction ID on an explorer
- ☐ only then increase the amount

| The best first transaction is boring: small amount, careful check, ordinary fee, patient wait.

The LiveWallet notebooks start on testnet. That is play money on a copy of the network. Real coins are a deliberate switch, made only on a Livebook you run yourself. Keep the amount under one dollar while you learn.

Try it. Receive a small test payment: `transactions/receive.livemd`.

Try it. Send a small test payment: `transactions/send.livemd`.

Chapter 7

Network Reference

This chapter is a short reference for the ticker and address checks mentioned in the First Transaction chapter. The walkthrough in this book uses Bitcoin. If you are on a different network, the same habits apply—just confirm the ticker and address format match before you send.

Why There Are Multiple Networks

Bitcoin launched as a single network in 2009. Over the following decade, disagreements about how the system should scale led to splits—called forks—that created separate networks with shared history but different rules.

You do not need to master the politics. You do need to know which network you are on and which network your recipient is on.

The three main labels to recognize:

- **BTC** (Bitcoin) — the most widely listed on exchanges and apps
- **BCH** (Bitcoin Cash) — forked from BTC in 2017, larger blocks
- **BSV** (Bitcoin SV) — forked from BCH in 2018, focused on scaling and protocol stability

Each network has its own ledger. Coins on one network cannot be spent on another.

How To Tell Them Apart

Check the label first:

- if the wallet or exchange says BTC, you are on the BTC network
- if it says BCH or Bitcoin Cash, you are on BCH
- if it says BSV or Bitcoin SV, you are on BSV

Then check the receive address format:

- BTC often uses addresses starting with bc1, 1, or 3
- BCH often uses the bitcoincash:q... style, though legacy formats also exist
- BSV often uses addresses starting with 1

If a service simply says “Bitcoin” with no variant, do not guess. Check the ticker, address format, or deposit instructions before sending.

Action Checklist

- ☐ confirm the ticker
- ☐ confirm the address format
- ☐ send a small test amount first when unsure

| When in doubt, stop and check. A tiny test send is cheaper than a confusing rescue attempt.

Chapter 8

After The First Send

If you have read this far and completed the basic flow, you do not need more hype. You need repetition.

What Good Progress Looks Like

Progress in Bitcoin is not memorizing jargon. It is making a few careful habits feel ordinary.

A useful beginner can do a handful of things calmly and reliably:

- explain what a wallet does
- protect the seed phrase
- receive and send a small amount
- stay calm while a payment is pending
- check what network a service actually supports

The real beginner advantage is not buying low. It is learning good habits while the stakes are still small.

What Good Tools Feel Like

Good tools do not try to impress you with complexity. They make the important things obvious.

Good wallet design usually does three things well:

- it makes backup hard to ignore
- it makes receive and send easy to understand
- it reveals deeper controls only when you need them

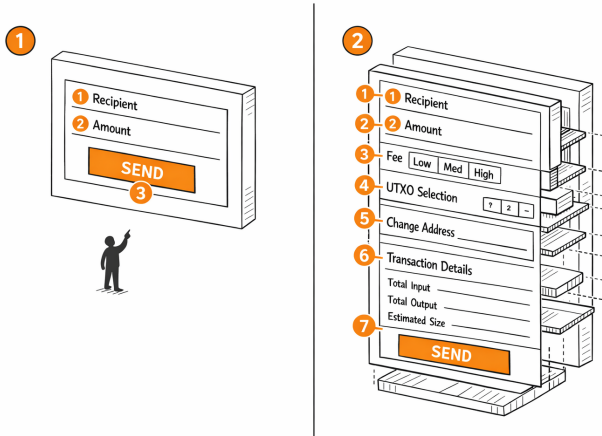


Figure 8.1: *A good wallet keeps the first-use flow simple and reveals extra detail only when the user needs it.*

If a wallet makes you feel lost before you even receive a small amount, switch while the amount is still trivial.

Look It Up Yourself

A block explorer is a read-only window into the network. It lets you check what the network sees instead of relying only on what the wallet UI tells you.

If your wallet gives you a transaction ID, paste it into an explorer for the same chain and look for the basic facts:

- whether the transaction exists
- whether it is pending or confirmed
- the amount that moved
- the change that came back to you
- the fee that was attached

Try It: Check Your Last Transaction

Use an explorer that matches the chain you are on.

If you are using BTC, use a BTC explorer. If you are using BCH or BSV, use an explorer for that chain.

Look up:

- the transaction ID from your wallet, or
- the receive address you used

Then answer three questions:

- did the network see the transaction
- is it still pending or already confirmed
- do the amount and destination match what you intended

What To Do This Week

Keep the next steps boring and practical:

Action Checklist

- ☐ keep only a small learning amount in the wallet
- ☐ back up the seed phrase carefully
- ☐ send one more small transaction—try adding a memo if your wallet supports it
- ☐ look up the transaction on an explorer and check whether the memo appears
- ☐ explain the wallet, seed, and transaction model to one other person without jargon

If you can explain those basics clearly, your understanding is already getting more solid.

What You Should Be Able To Say Now

If this book worked, you should now be able to say:

- I know what problem Bitcoin is trying to solve.
- I know that a wallet holds keys, not coins.
- I know why the seed phrase matters.
- I know how a first transaction feels.
- I have sent at least one transaction—ideally one with a memo attached.
- I know enough to keep learning without pretending I know everything.

A Glimpse Ahead: Payments That Carry Meaning

You just sent value. But a transaction can carry more than an amount.

Some wallets let you attach a short memo to a transaction—a note that travels with the payment and gets written into the public record. It might be a receipt reference, a thank-you, or just a label so you remember what the payment was for six months from now.

Try It: Send a Transaction With a Memo

If your wallet supports it, send a small amount to yourself or a friend and include a short message—even just “test.”

Look for:

- a “memo,” “message,” or “note” field on the send screen
- the option may appear under advanced or optional settings

After the transaction confirms, look it up on an explorer. You should see your memo stored alongside the payment.

This is a small example of a bigger idea. Bitcoin transactions are not just IOUs—they are programmable messages. The network can enforce simple rules automatically: release a payment only after a certain date, require two people to sign off, or lock funds until a condition is met.

These rules are sometimes called *smart contracts*, but the name makes them sound more exotic than they are. Think of them as instructions baked into the payment itself—no phone call to a bank, no manual approval step, no intermediary deciding whether to follow through.

You do not need to understand how these work under the hood right now. What matters is the user-facing implication: as wallets improve, payments will do more than move money. They will carry context, enforce agreements, and reduce the back-and-forth that makes transactions slow and expensive today.

A transaction that carries a memo is your first step past “just sending money.” The same machinery that attaches a note can attach rules, conditions, and context.

What Changes When Money Moves Like Information

You have now done something most people have not: sent value directly to another person over the internet, without asking a company to do it for you.

That may seem small. It is small, on purpose—this book kept the amount tiny so you could focus on learning. But the underlying shift is not small at all.

For most of the internet’s history, information and money have moved on different rails. Information got fast, free, and global. Money stayed slow, expensive, and gated. When you send someone a photo, you do not think about which country they live in or whether an intermediary will approve the delivery. When you send someone ten dollars, you think about all of those things.

That gap is not permanent. The systems that make money expensive to move were necessary when they were built—they solved real trust problems between strangers. But the overhead they add is becoming a structural inefficiency. Not a flaw in the original design. A cost that the technology now exists to reduce.

Bitcoin is one attempt to close that gap. Whether it becomes the domi-

nant one is an open question. But the first transaction you just completed is proof that direct digital payment works: a signed message, verified by math, settled in minutes, for a few cents, across any distance.

There is also something worth sitting with about the transparency of what you just did. Your transaction is on a public ledger. Anyone with the transaction ID can verify that it happened. That is unusual. Most financial records are private—controlled by the institution that holds them. A public ledger means the record belongs to nobody and is checkable by everybody.

That transparency creates both opportunities and challenges. It makes fraud harder to hide. It makes audit easier. It also means that privacy requires thoughtful design, not just default obscurity. These are real trade-offs, and they are worth understanding as you go deeper.

For now, you have done the important thing: you have used the tool. The theory will make more sense with experience behind it.

The notebooks at `livewallet.app` start on testnet. When you are ready for real coins, that is a switch you make yourself, on a Livebook running on your own machine, with an amount under one dollar.

Try it. Check a transaction the network has already seen: `transactions/verify-on-chain.livemd`.

| The best next step is simple: use Bitcoin carefully, keep the stakes low, and let experience sharpen the theory.

Chapter 9

Quick Words

You do not need much jargon to use Bitcoin, but a few words are worth keeping straight. Some of these appeared in the book. Others you will encounter on explorers, in wallet settings, and in conversations as you keep learning.

Wallet

The app or device that manages the keys you use to receive and send Bitcoin.

Seed phrase

The backup words (usually 12 or 24) that can restore the wallet if the phone or device is lost. Sometimes called a recovery phrase or mnemonic.

Private key

The secret that lets you sign transactions. The seed phrase generates this. Never share it.

Signature

The mathematical proof that a transaction was authorized by the holder of the private key. Like a wax seal: anyone can verify it, but only the key holder can create it.

Address

A receive destination. Safe to share for getting paid. Generated from the public key.

Transaction

A signed message that instructs the network to move value from one address to another.

Fee

The small amount attached to a transaction to pay for processing. Paid by the sender, like postage.

Confirmation

The stage where a transaction has been included in a block and is much

harder to unwind. One confirmation means it is in the most recent block. More confirmations mean more blocks have been added on top.

Block

A batch of transactions that has been verified and added to the ledger. New blocks are added regularly.

Mempool

The waiting room. Transactions sit here after being broadcast and before being included in a block. When your wallet says “pending,” this is usually where the transaction is.

Memo (OP_RETURN)

A short message attached to a transaction. It is stored on the public ledger alongside the payment. Sometimes called an OP_RETURN output. Useful for receipts, labels, or lightweight records.

Smart contract

A set of rules embedded in a transaction that the network enforces automatically—for example, requiring multiple signatures or releasing funds after a certain date. No intermediary needed.

Satoshi (sat)

The smallest unit of Bitcoin. One bitcoin equals 100,000,000 satoshis. Most beginner transactions are measured in satoshis, not whole coins.

UTXO

Unspent transaction output. You may see this in wallet settings. It is the technical name for a chunk of value you can spend—think of it as an unbroken bill in your wallet.

Change address

When you spend part of a UTXO, the leftover goes back to you at a new address. This is automatic. It is like paying with a \$20 bill and getting change.

Ticker

The short label for a network or asset, such as BTC, BCH, or BSV.

Explorer

A read-only website or tool for checking what the network sees. Paste a transaction ID or address to look up details.

Custodial

Someone else holds the keys for you.

Non-custodial

You hold the keys and the backup responsibility yourself.

Ledger

The shared record of all transactions. Public and distributed across many computers.

| If you can explain these words in plain language, you are already past the beginner fog.

How This Started

You just sent a first transaction. So did I.

Mine did not start with a book. It started with an online friend.

I wanted to send a payment myself, not through an app I did not understand. He sat with me, over the internet, and we built a transaction using a small JavaScript library called `bsv.js`. Line by line. A destination. An amount. A signature. Then we sent it.

That was the door.

After that I bought a few books and read up on bitcoin. I read a lot of documentation and source code too. I made prototype interactions and test payments, first with that JavaScript library, then with Elixir and the `bsv-ex` library. Small amounts. Test networks. The same loop you just did, over and over.

I kept reaching for patterns that did not really exist yet: ways to send, receive, and read payments that the tools did not offer. So I kept going.

Eventually I ran a node—a computer that keeps a copy of the shared record and talks to the others. I used it to receive transactions, process them, move them, and read them.

This book is the front door I wish someone had handed me. When you are ready to do more of the how, the notebooks at livewallet.app are the next room. The book itself lives at livewallet.app/bitcoin-book.

I started the same way you just did: one careful send, with someone willing to sit with me.

Where To Go From Here

If you want to keep learning, these are worth your time.

Bitcoin: A Peer-to-Peer Electronic Cash System (Satoshi Nakamoto, 2008)

The original nine-page paper that started it all. Shorter and more readable than most people expect. It will make more sense now that you have made a transaction.

Mastering Bitcoin (Andreas M. Antonopoulos)

The standard technical reference. If you want to understand how transactions, scripts, and the network actually work under the hood, this is where to go next.

The Bitcoin Standard (Saifedean Ammous)

An economic argument for why Bitcoin matters as money. Useful for understanding the “why” behind the technology, even if you do not agree with every claim.

Block explorers

Practice reading the public ledger. Pick an explorer that matches the network you use and look up your own transactions. This is the fastest way to build intuition about how the system works.

Your own wallet

The best reference is continued use. Keep the stakes small, keep experimenting, and let experience fill in what no book can.

About the Author

Ryan Wold is a software engineer and writer based in the United States. He has worked on digital infrastructure, open-source systems, and public interest technology. He wrote this book because direct digital payments matter, and because the front door was harder to find than it needed to be.

For updates, corrections, and current wallet recommendations:
usingbitcoin.org

If this book helped, the best thing you can do is hand it to someone else.

Colophon

This book was typeset in Palatino (body), Helvetica Neue (headings), and Menlo (code) using XeLaTeX. The trim size is 5.5" × 8.5".

Illustrations were created in an isometric line-art style with a two-color palette: black line work with Bitcoin orange (#F7931A) accent.

The callout system uses three signal colors: orange for actions and emphasis, green for safe operations, and red for warnings.

The text was written, revised, and tested with real beginners.