LESSONS

← Back to Course Home

BITCOIN SECURITY MASTERY · MODULE 1

Bitcoin Basics

This foundational module builds the mental model you need before touching any software or hardware. By the end of Module 1, you will understand exactly how Bitcoin works — and why that knowledge is essential to securing it.

5	~5h	3
LESSONS	READING	EXERCISES

MODULE LEARNING OBJECTIVES

- ✓ Explain what Bitcoin is and how it differs from traditional financial systems
- ✓ Describe the role of the blockchain and why it is immutable
- ✓ Define wallets, private keys, public keys, and Bitcoin addresses
- ✓ Understand what a transaction is and how it gets confirmed
- ✓ Read a basic block explorer and interpret transaction data
- ✓ Understand UTXOs and why they matter for your security and privacy

LESSON 1.1

What Is Bitcoin?

An introduction to Bitcoin as a decentralised, peer-to-peer electronic cash system — covering the origin of Bitcoin's creation, Satoshi Nakamoto's whitepaper, and the core problem Bitcoin solves.

The History of Money

Satoshi Nakamoto & the 2008 Whitepaper

Trustless vs. Trust-Based Systems

Bitcoin vs. Banks

Hey, welcome to Bitcoin Security Mastery. I want to start this course with the most important question of all — one that sounds simple but that most people have never actually had answered properly.

What is Bitcoin?

Not the price. Not whether you should buy it. Not whether it’s going up or down. I mean: what actually IS it? How does it work? And why does any of this matter?

Because here’s the truth — you cannot protect something you don’t understand. And this entire course is about protecting your Bitcoin. So we are going to build the foundation right now, in plain English, before we touch a single piece of hardware.

The History of Money (Why This Matters)

To understand Bitcoin, you first have to understand money — specifically, what goes wrong with it.

For most of human history, money was something physical. Gold. Silver. Shells. Things you could hold, that were scarce, that couldn’t just be conjured out of thin air. If you had gold, you had value. Nobody could print more of it.

Then we moved to paper money — and paper money started out as a receipt. You hand over your gold, the bank gives you a piece of paper saying ‘we owe you this gold.’ Convenient. Fine.

But over time, something shifted. Governments and banks started printing more receipts than they had gold to back them. In 1971, the United States formally disconnected the dollar from gold entirely. From that moment on, the dollar — and every major currency in the world — became what’s called fiat money. It’s worth something because the government says it is. Not because it’s backed by anything real.

And the consequence of that? Inflation. The purchasing power of your savings erodes, year after year, because more money is constantly being created. The people at the top of the system benefit. Everyone else slowly loses.

Bitcoin was built as the answer to that problem.

Satoshi Nakamoto and the 2008 Whitepaper

In October 2008, right in the middle of the worst financial crisis in living memory — banks collapsing, governments bailing them out with freshly printed money — a person using the name Satoshi Nakamoto published a nine-page document called ‘Bitcoin: A Peer-to-Peer Electronic Cash System.’

We don’t know who Satoshi is. Could be one person, could be a group. They disappeared from the internet in 2011 and have never been identified. And that anonymity — as we’ll see later in this course — turns out to be one of Bitcoin’s most important features.

But the idea in that whitepaper was radical. Satoshi proposed a form of digital money that didn’t require a bank, a government, or any company to operate. A system where you could send value to anyone in the world, directly, without asking anyone’s permission.

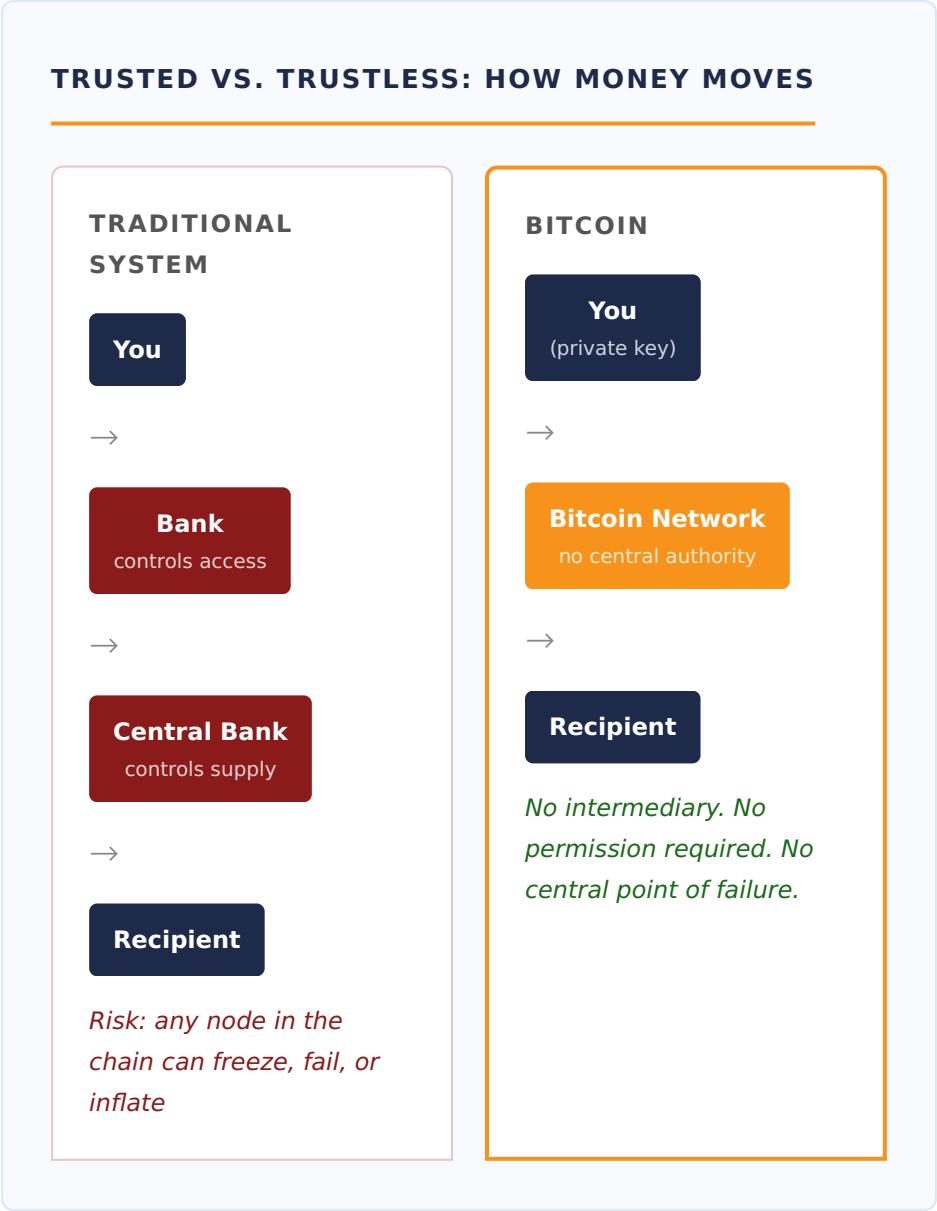
No middleman. No third party. No one who could freeze your account, reverse your transaction, or print more of it to devalue what you already held.

That’s the idea. Now let’s look at how it actually works.

Trust vs. Trustless Systems

Every financial system in the world today is built on trust. You trust your bank to hold your money. You trust your government not to inflate it away. You trust the payment processor when you swipe your card. You trust a dozen

different companies and institutions every single day just to use your own money.



And most of the time, that trust holds. But sometimes it doesn’t. Banks fail. Governments freeze accounts. Payment processors block transactions for political reasons. In some countries, people wake up one morning and their savings have been seized or inflated into worthlessness overnight. This isn’t hypothetical — it has happened, repeatedly, across history.

Bitcoin replaces trust with mathematics.

Instead of relying on a bank to keep a ledger of who owns what, Bitcoin uses a public ledger called the blockchain — a record of every transaction ever made, stored simultaneously on thousands of computers all over the world. Nobody owns it. Nobody controls it. And everyone can verify it independently.

To change the history on this ledger, you would have to redo an enormous amount of computational work — work that would cost more money than it's worth to attack. The system is secured not by laws, not by guards, but by mathematics and energy.

When we say Bitcoin is 'trustless,' we don't mean you blindly trust nothing. We mean you don't have to trust any specific person or institution. You can verify everything yourself.

Bitcoin vs. Banks: Who Controls Your Money?

Here's a question worth sitting with: do you actually own the money in your bank account?

Legally? Not exactly. When you deposit money in a bank, you become an unsecured creditor of that bank. They owe you the money — but they're also lending most of it out, investing it, and using it as they see fit. You have a claim on it. That's not the same as owning it.

Your bank can freeze your account. They can block certain transactions. They can be forced by a government to hand over your funds. They can go insolvent. These aren't paranoid fantasies — they're things that happen.

Bitcoin works differently. When you hold Bitcoin properly — meaning you hold the private keys yourself, which is what

this entire course is about — nobody can freeze it, seize it, or block you from using it. There is no customer service line to call and no account to close. The Bitcoin simply exists on the network, and you control it with a cryptographic key that only you possess.

Now, that power comes with responsibility. And that's exactly why this course exists. Self-custody — the act of truly owning your Bitcoin — requires knowledge. It requires the right setup. And it requires the security habits we're going to build together over the coming modules.

KEY TAKEAWAYS

So: Bitcoin is a decentralised, mathematically-secured, fixed-supply form of digital money that nobody controls and anybody can verify. It was created in 2008 as a direct response to the failures of the trust-based financial system. And it puts you — not a bank, not a government — in control of your own wealth.

That's the foundation. In the next lesson, we're going to look under the hood and understand how the blockchain actually works — how transactions get confirmed, why the ledger can't be faked, and what 'mining' really means.

LESSON 1.2

How the Blockchain Works

A plain-English walkthrough of how blocks are chained together and why this structure makes Bitcoin transactions virtually impossible to reverse or tamper with.

In the last lesson we covered what Bitcoin is — a decentralised, trustless form of digital money secured by mathematics rather than institutions. But I used one word without fully unpacking it: the blockchain. You need to understand what it actually is, how it is built, and why it makes Bitcoin transactions effectively impossible to reverse. That is what this lesson is about. Let's get into it.

What a Block Is and What It Contains

Let's start with the word itself. Blockchain. Take it apart: you have blocks, and they form a chain. A block is simply a batch of Bitcoin transactions — like a single page in a ledger. Every ten minutes or so, the Bitcoin network collects all the recent transactions people have broadcast, bundles them together, and seals them into a new block.

ANATOMY OF A BITCOIN BLOCK

BLOCK HEADER

Previous Block Hash	`00000000000000000abc...f7d2`
Merkle Root	`a3f8c9e2...7b4d`
Timestamp	2024-04-19 · 18:09 UTC
Nonce	2,083,236,893
Difficulty Target	000000000000000000...

TRANSACTIONS

Coinbase TX (miner reward)

TX: Alice → Bob 0.05 BTC

TX: Carol → Dave 0.12 BTC

+ ~2,500 more transactions

The block header's "Previous Block Hash" is what chains blocks together — changing any transaction in a past block changes its hash, which breaks every block that follows it.

Each block contains roughly two thousand transactions on average, a timestamp recording when it was created, and something critical: a digital fingerprint of the block that came before it. That fingerprint is called a hash. A hash is a unique string of letters and numbers produced by running data through a mathematical function. Change even a single character in the original data and you get a completely different output.

So when Block 2 contains the hash of Block 1, it is permanently linked to it. If anyone tried to alter Block 1 — even changing a single transaction — its hash would change entirely, and Block 2's reference would no longer match. The chain breaks. This is why the blockchain is immutable: every block is cryptographically locked to the one before it, all the way back to the very first block — the Genesis Block — mined by Satoshi in January 2009.

Proof of Work: How Miners Compete to Add Blocks

Here is where it gets interesting — and where most explanations start losing people. Who decides which

transactions go into each block? And who actually adds the block to the chain? The answer is miners. And they earn the right to add a block through a process called Proof of Work.

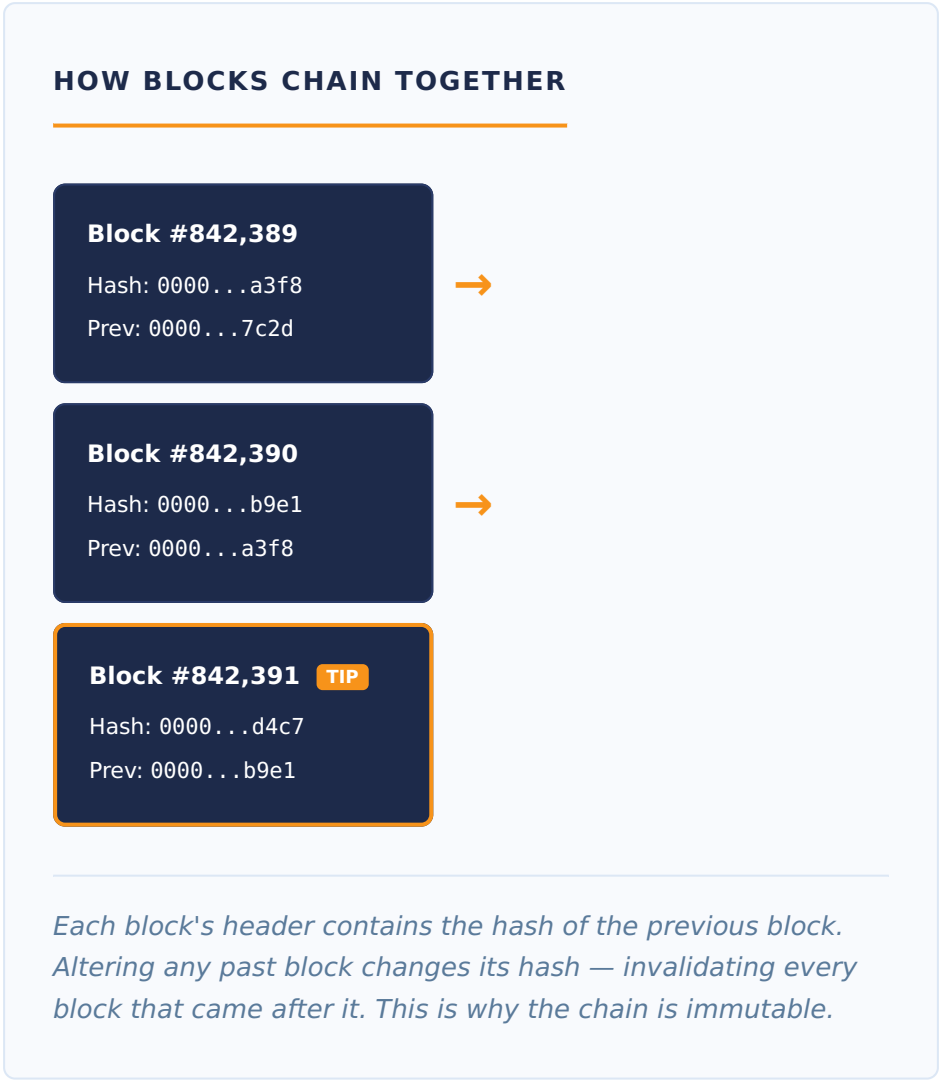
Here is the simplest way to explain it. Imagine a combination lock with trillions of possible combinations, and the only way to open it is to try one combination after another, as fast as you possibly can. There is no shortcut. No clever trick that skips ahead. Just raw, repeated computational effort. Miners are doing something mathematically equivalent. They race to find a number — called a nonce — that, combined with the block's data, produces a hash meeting the network's specific requirements. The first miner to find it wins.

The winning miner broadcasts the new block to the entire network. Every other node independently verifies that the transactions are valid and the Proof of Work is correct, then adds it to their copy of the blockchain. The winner receives two things: newly created Bitcoin called the block subsidy, and every transaction fee included in that block. This is the only way new Bitcoin enters circulation — not printed by a central authority, but earned through verifiable, expendable work.

Why the Longest Chain Wins

Here is a question you might be wondering about: what happens if two miners find a valid block at almost exactly the same moment? For a brief period, there are two competing versions of the blockchain. The network temporarily splits. This is where one of Bitcoin's most elegant rules resolves everything: the longest chain wins. Not longest by number of blocks — by accumulated Proof of Work. The chain with the

most total computational effort behind it is the canonical chain.



When nodes detect a competing chain that has accumulated more Proof of Work, they switch to it automatically. The shorter chain’s blocks become orphaned — technically valid but not part of the main chain. Any transactions in those orphaned blocks simply re-enter the mempool and get picked up in future blocks. The conflict resolves itself, without any central authority making a call.

This is also what makes Bitcoin extraordinarily resistant to attack. To rewrite any part of the blockchain — to reverse a confirmed transaction — you would need to redo all the Proof of Work from that point forward, faster than the rest of the

network is building ahead. With Bitcoin's current hash rate, executing such an attack would require more computing power than exists on Earth. It is not merely difficult. It is economically irrational.

Confirmations and Transaction Finality

When you broadcast a Bitcoin transaction, it first lands in what is called the mempool — a waiting room of unconfirmed transactions. Miners select transactions from the mempool when assembling their next block. Once your transaction is included in a mined block, it has one confirmation. Think of each confirmation as a new layer of mathematical cement poured on top of your transaction.

Each additional block added to the chain after yours is one more confirmation. Every confirmation makes it exponentially harder to reverse that transaction, because an attacker would need to redo the work for your block and every block stacked on top of it. Six confirmations is the widely accepted standard for considering a transaction final. At current block times, that is roughly one hour.

For small everyday payments, one or two confirmations is typically sufficient. For significant transactions — a large purchase, a major transfer — waiting for six or more is standard practice. The higher the value at stake, the more confirmations you should require before treating it as settled.

KEY TAKEAWAYS

So: the blockchain is a chain of blocks, each containing a batch of transactions and a cryptographic fingerprint of the

block before it. Miners compete through Proof of Work to add new blocks, earning Bitcoin for their effort. The longest chain — the one with the most accumulated work — is the truth. And confirmations tell you how deeply buried, and therefore how final, your transaction is.

In the next lesson we are going to take this foundation in the most practically important direction: wallets, private keys, and Bitcoin addresses. This is where self-custody begins — and where most people make their most critical mistakes. Understanding keys is the difference between truly owning your Bitcoin and just hoping someone else doesn't take it. Don't skip this one.

LESSON 1.3

Wallets, Keys, and Addresses

Your wallet does not hold Bitcoin — it holds keys. Understanding the difference between private keys, public keys, and addresses is the foundation of self-custody.

Private Keys **Public Keys & Addresses**

The Seed Phrase **HD Wallets**

In the last lesson we took apart the blockchain — how blocks chain together through cryptographic hashes, and how Proof of Work makes the ledger immutable. Now we move to something even more personal: wallets, private keys, and Bitcoin addresses. Most people think a wallet holds their Bitcoin. That single misunderstanding is the source of more

lost money, more confusion, and more security mistakes than almost anything else in this space. So let's get this right.

Private Keys: What They Are, Why They Are Everything

A private key is a number. Specifically, it is a 256-bit number — that is a number so astronomically large that if every atom in the observable universe were a computer trying combinations, they could not guess it in the lifetime of the universe. Your private key is generated randomly when you create a Bitcoin wallet. Nobody else has it. Nobody can derive it. It exists only where you have stored it.

BITCOIN ADDRESS

`bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh`

Share this freely to receive Bitcoin
Cannot reveal your private key

These derivation steps only work in one direction. You can always go from private key → address, but you cannot reverse-engineer a private key from an address or public key.

This number — this key — is your proof of ownership. When you want to send Bitcoin, your wallet uses your private key to create a cryptographic signature that proves you authorised the transaction, without ever revealing the key itself. The Bitcoin network verifies the signature and processes the transaction. No bank authorises it. No company approves it. The key is the authority. And this is why the phrase “not your keys, not your coins” is not just a slogan — it is a literal technical fact. If someone else holds your private key, they own your Bitcoin.

When you hold Bitcoin on an exchange, the exchange holds the private keys. You have a number in a database that says how much Bitcoin they owe you. That is not the same thing as holding Bitcoin. As the industry learned from Mt. Gox, from FTX, from Celsius, and from dozens of others — if the exchange fails, freezes, or simply decides to stop operating, your access to that number disappears with it. Self-custody means you hold the key. Nobody can take your Bitcoin unless they take your key.

Public Keys and Bitcoin Addresses

Your private key never travels anywhere. But Bitcoin needs a way to receive funds — a destination address you can share publicly. Here is how that works. From your private key, your wallet performs a one-way mathematical operation called elliptic curve multiplication to produce a public key. From the public key, it applies two hashing functions to produce a Bitcoin address. The critical property: these operations work in only one direction. You can go from private key to address, but you cannot reverse-engineer the private key from the address or even from the public key.

Your Bitcoin address is what you share when someone wants to pay you. Think of it like an email address — sharing it with the world does not put you at risk. Nobody can extract your private key from your address. You can publish your Bitcoin address openly. You can print it on a business card. You can post it online. None of that endangers your funds. What endangers your funds is exposing your private key — or your seed phrase, which we will cover next.

One more important detail: modern Bitcoin wallets generate a new address for every transaction. This is not a bug or an inconvenience — it is a privacy feature. When you reuse an address, anyone can see all the transactions associated with that address by looking at the blockchain. A new address per transaction breaks that trail. Your wallet handles this automatically; you do not have to manage it manually.

The Seed Phrase: Your Master Backup

Here is the problem with private keys: a raw 256-bit private key looks like this. [PAUSE] That is not something any human can memorise or safely write down by hand. So the Bitcoin community developed a standard called BIP-39 — a way to encode a private key as a sequence of 12 or 24 ordinary English words. This is your seed phrase. Your wallet generates it when you set up a new wallet, and you must write it down immediately on paper, in order, and store it somewhere physically secure.

YOUR SEED PHRASE — WHAT IT IS AND WHY IT MATTERS

1 abandon	2 ability	3 able
4 about	5 above	6 absent
7 absorb	8 abstract	9 absurd
10 abuse	11 access	12 accident

12 or 24 ordinary English words — encodes your entire master private key

- ✓ Write on paper, in ink, right now
- ✓ Verify each word carefully
- ✓ Store physically — fireproof safe, off-site copy
- ✓ Consider a steel backup for long-term storage

✗ Never photograph it

✗ Never type it into any device

✗ Never store digitally or in cloud

✗ Never share it with anyone, ever

This is the most important thing I will tell you in this entire lesson. Your seed phrase is your master key. Every private key your wallet will ever generate — every address, every transaction, every coin — can be derived from that seed phrase. Which means that whoever has your seed phrase has your Bitcoin. All of it. There is no reset button, no customer service line, no recovery process. If someone photographs your seed phrase, they can drain your wallet. If you lose your seed phrase and your hardware wallet breaks, your Bitcoin is gone forever.

Write your seed phrase on paper — never type it into any device, never photograph it, never store it digitally in any form. For serious holdings, consider stamping or engraving it

onto a steel plate. Products like Cryptosteel, Blockplate, and SeedPlate are designed specifically for this. They survive fire, water, and decades of time. Your seed phrase needs to outlast every digital device you own. Paper is a reasonable start. Steel is the standard. We cover backup strategies in detail in Module 4.

HD Wallets and Derivation Paths

One seed phrase, thousands of addresses. How? This is the purpose of HD wallets — Hierarchical Deterministic wallets. HD is the standard used by virtually every modern Bitcoin wallet. Here is how it works: your 12 or 24 seed words are converted into a master private key. That master key can deterministically derive billions of child keys, each producing its own address. Every time your wallet generates a new receive address for you, it is creating the next child key in the sequence.

What this means in practice is remarkable: your seed phrase is your entire wallet, forever, on any device. If your hardware wallet fails tomorrow, you buy a new one, enter your seed phrase, and your wallet is completely restored — every address, every transaction history, every balance. This is not a feature of the device. It is a feature of the mathematical relationship between your seed phrase and every key it can generate. The device is just a tool. The seed phrase is the wallet.

You may encounter the phrase derivation path — notation like m/84 prime/0 prime/0 prime/0/0. This tells your wallet which child keys to generate and in what order. Different wallet standards use different paths, which is why it is important to note which type of wallet you created — Legacy, SegWit, or

Native SegWit — when you back up your seed phrase. Your wallet software handles all of this automatically; you do not need to memorise the numbers. But if you ever need to recover your wallet in an unfamiliar application, knowing the derivation path ensures you find all your funds.

KEY TAKEAWAYS

Let’s bring this together. Your private key is a unique number that proves you own your Bitcoin and authorises every transaction. From it, your wallet derives a public key and then a Bitcoin address — which you can share freely. Your seed phrase — 12 or 24 words — encodes your master private key in a form you can write down and recover from. And your HD wallet uses that one seed phrase to generate every address you will ever need. The key principle running through all of this: if you do not hold the key, you do not own the Bitcoin.

In the next lesson we go deeper into how Bitcoin actually moves — transactions, inputs, outputs, and a concept called UTXOs that most people never learn but that becomes critical when you start thinking seriously about privacy and security. See you there.

LESSON 1.4

Transactions and UTXOs

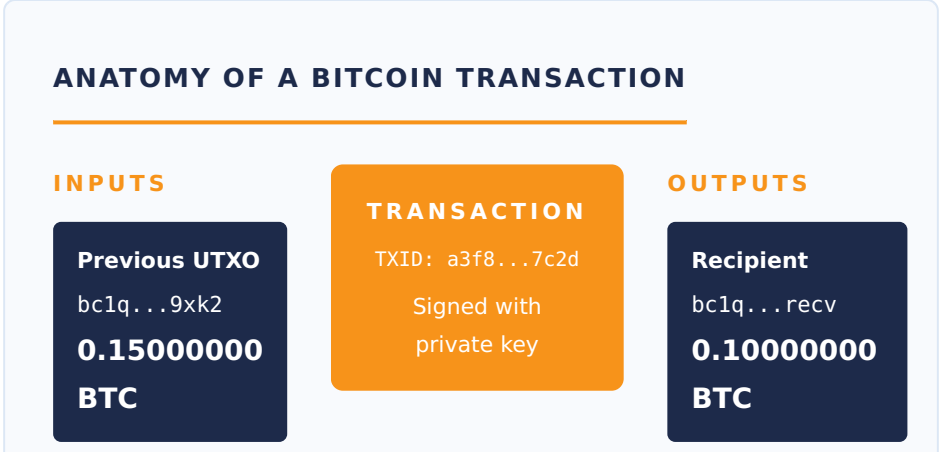
How value actually moves on the Bitcoin network — and why understanding UTXOs is critical for both security and privacy.

Anatomy of a Transaction | Inputs, Outputs & Change | Fees & the Mempool | Reading a Block Explorer

In the last lesson we covered wallets, private keys, public keys, and how your seed phrase is your master backup. Now we go one level deeper: how does Bitcoin actually move? When you send Bitcoin, what exactly is happening on the network? And why is a concept called the Unspent Transaction Output — the UTXO — something every serious Bitcoin holder needs to understand? Let's dig in.

Anatomy of a Bitcoin Transaction

Every Bitcoin transaction has the same basic anatomy: inputs and outputs. Inputs are the funds you're spending — they point back to previous transactions where Bitcoin was sent to you. Outputs are where the Bitcoin goes next — either to the recipient or back to yourself as change. Think of it like using a $50 bill to pay a $30 tab. You hand over the $50 as the input. The restaurant takes $30 as one output. You receive $20 in change as a second output. Bitcoin works exactly the same way, except it all happens cryptographically on a public ledger.



Funds being spent (consumed in full)

Change (back to you)
`bc1q...chng`
0.04900000 BTC

Miner fee: 0.001 BTC (input − outputs)

Every satoshi is accounted for. Input amounts must equal output amounts plus the miner fee. If you spend a 0.15 BTC UTXO to send 0.10 BTC, your wallet creates a change output for the remainder minus the fee.

Here's how a real transaction looks: someone wants to send 0.1 BTC. Their wallet finds a previous output — let's say 0.15 BTC — that was sent to their address. It creates a new transaction with two outputs: 0.1 BTC to the recipient's address, and 0.049 BTC back to a change address the sender's own wallet controls. The difference — 0.001 BTC — goes to miners as the transaction fee. Nothing is wasted, nothing is created. Every satoshi is accounted for.

Inputs, Outputs, and Change Addresses

Now let's talk about UTXOs — Unspent Transaction Outputs. A UTXO is simply a chunk of Bitcoin you've received that hasn't been spent yet. Your Bitcoin balance isn't one big number sitting in a bucket. It's a collection of specific outputs from

previous transactions — each a distinct amount, linked to a specific address you control. When you send Bitcoin, your wallet selects one or more UTXOs as inputs, spends them in full, and creates new outputs for the recipient and for your change.

Why does this matter for security? A few reasons. First, your wallet has to manage UTXO selection carefully. If you have twenty small UTXOs and you want to send Bitcoin, your wallet may need to combine several of them — and that combination reveals to the blockchain that all those UTXOs likely belong to the same wallet. Second, each UTXO is tied to a specific address, which is why using a new address for each transaction protects your privacy. We'll go much deeper into this in Module 5 when we cover chain analysis and privacy strategies.

Change addresses are something most beginners never think about. When your wallet spends a UTXO, it creates a new output for your change — and it sends that change to a brand-new address inside your own wallet. This is automatic and correct behavior in any reputable wallet. But here is the security implication: if you're manually constructing transactions, or using a watch-only wallet, always verify your change address before broadcasting. An attacker who can modify your transaction can replace your change address with their own — and quietly steal everything that was supposed to come back to you. Always verify on your hardware device screen.

Transaction Fees and Mempool Dynamics

Before a transaction is confirmed, it lives in the mempool — the memory pool. This is a holding area, maintained by

Bitcoin nodes worldwide, where unconfirmed transactions wait to be picked up by a miner and included in a block. The mempool is not one single thing — every node has its own view of pending transactions. But they largely agree on what's waiting. And crucially, miners choose which transactions to include in each block based on the fee offered.

THE MEMPOOL: BITCOIN'S WAITING ROOM

High Priority
40–100+ sat/vB
Next block (~10 min)

Medium
15–40 sat/vB
~30 minutes

Low Priority
1–15 sat/vB
1–2 hours or more

Always check mempool.space before sending to see current fee conditions. Fees are dynamic — they spike during high-activity periods and drop when the network is quiet.

Fees are measured in satoshis per virtual byte — sats per vbyte. The higher your fee rate, the more attractive your transaction is to miners, and the faster it gets confirmed. When network activity is low, even a 1 to 2 sat/vbyte fee may confirm in the next block. When activity spikes — during a bull run, a major on-chain event, or an ordinals inscription wave — fees can rise dramatically and underpaid transactions can wait hours or even days. The fee market is dynamic. Always check current conditions before you send, especially for time-sensitive transactions.

The good news: most modern wallets and hardware wallet companion apps will suggest fee rates based on current mempool conditions. For the most accurate real-time view, mempool.space is the go-to public tool. It’s free, open source, and shows you exactly how congested the network is and what fee rate you need to get confirmed in your target timeframe. Bookmark it. You’ll use it regularly as a Bitcoin holder.

Reading a Block Explorer: mempool.space Walkthrough

A block explorer is a public interface for reading the Bitcoin blockchain. Every confirmed transaction, every block, every address — all publicly visible, permanently. Let’s walk through what you see on mempool.space. At the top is the Transaction ID — the TXID — a unique 64-character hash that identifies this specific transaction. Below that are two columns: inputs on the left and outputs on the right. Each input shows the address that was spent and the amount. Each output shows the destination address and the amount received.

Below the inputs and outputs you'll see the fee paid and the fee rate in sats per vbyte. You'll also see how many confirmations the transaction has — each confirmation means one additional block has been mined on top of the block that included your transaction. One confirmation means your transaction is in the blockchain. Six confirmations is the traditional standard for considering a large transaction fully settled — enough accumulated Proof of Work sits on top that reversing it would be economically catastrophic for any attacker.

Block explorers are powerful tools for your everyday Bitcoin life. Use one to verify that a transaction you've sent has been confirmed. Use one to show proof of payment. Use one to investigate an address you're curious about. Use one to look up your own receiving addresses and confirm that a deposit arrived. Get comfortable reading them — mempool.space in particular. It's one of the most important tools in your Bitcoin security toolkit.

KEY TAKEAWAYS

Let's bring this together. A Bitcoin transaction consumes specific UTXOs as inputs and creates new outputs for the recipient and for any change. Your wallet balance is the sum of your UTXOs — separate, distinct pieces of Bitcoin tied to specific addresses. The mempool is where unconfirmed transactions wait, and miners prioritise by fee rate. And a block explorer like mempool.space lets you read everything on the public blockchain directly. Understanding this layer isn't just academic — it's the foundation for the privacy and security thinking we build on in later modules.

In our final lesson of Module 1, we tackle one of Bitcoin's most powerful properties — the 21 million cap, the halving

schedule, and why digital scarcity is not just a feature but the very foundation of Bitcoin’s value proposition. See you there.

LESSON 1.5

Bitcoin's Fixed Supply

Why 21 million is not arbitrary: the economic design of Bitcoin's issuance schedule, the halving, and why scarcity is a feature, not a bug.

The 21 Million Cap **Block Subsidy & the Halving** **Bitcoin vs. Gold**

In the previous four lessons we’ve covered what Bitcoin is, how the blockchain works, how wallets and keys protect your ownership, and how transactions and UTXOs move value on the network. Now we arrive at one of Bitcoin’s most important and misunderstood properties: why there will only ever be 21 million Bitcoin. Not as a marketing claim. Not as a hope. As a mathematical certainty baked into the protocol from the very first block.

The 21 Million Cap and Why It Matters

Twenty-one million. That is the total number of Bitcoin that will ever exist. Not 21 million today with more to come. Not 21 million unless the protocol is changed. Twenty-one million, full stop. This cap is written directly into Bitcoin’s code and enforced by every node on the network. No government, no

company, no foundation, no group of miners can change it without the consensus of the entire network — which means in practice it cannot change at all.

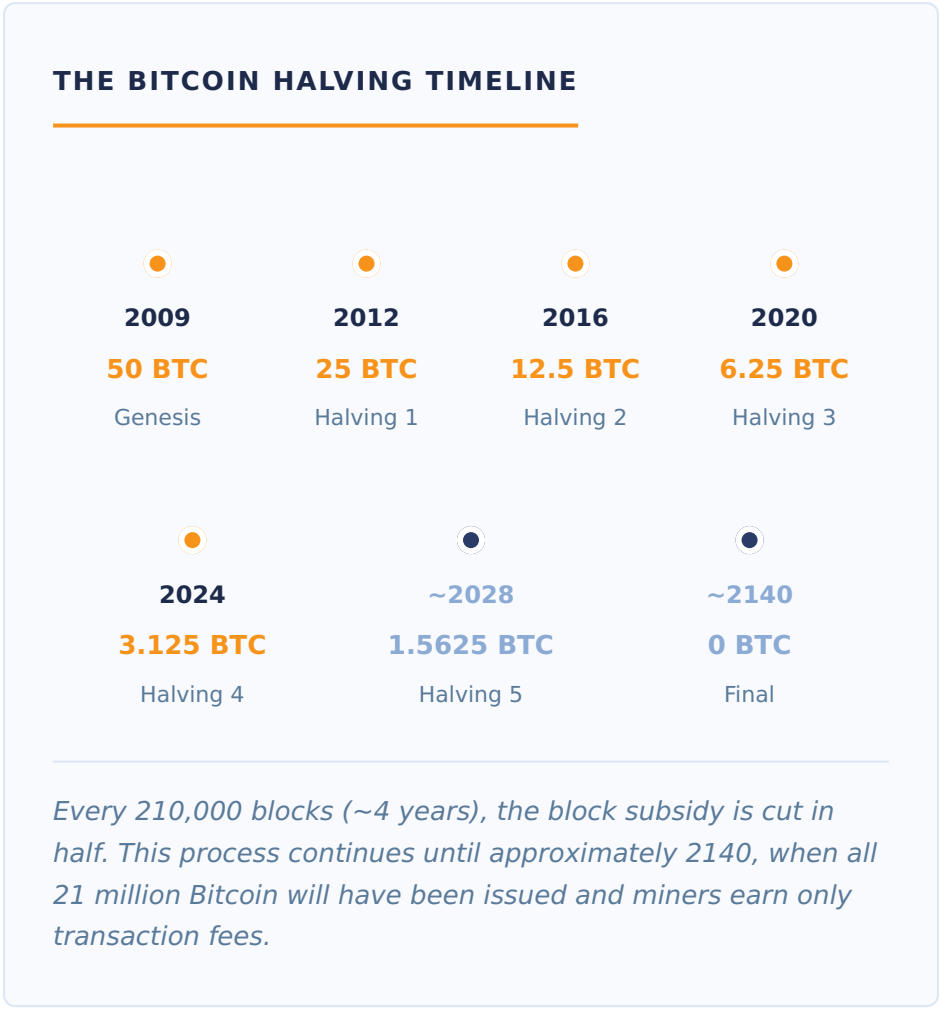
Compare this to every fiat currency in existence. The US dollar has no hard cap. The Federal Reserve can create new dollars at any time — and does. Since 2020, the US money supply has expanded massively. Every new dollar created dilutes the purchasing power of the dollars you already hold. This is not a conspiracy theory — it is a mechanical consequence of unlimited money creation. Bitcoin was designed to be the opposite: a money where no one can inflate your holdings away.

Of the 21 million Bitcoin, approximately 19.8 million have already been mined. The remaining 1.2 million or so will be released slowly over the next century — with the last Bitcoin mined sometime around the year 2140. The issuance schedule is not random. It is governed by a mechanism called the block subsidy and an event called the halving. Understanding these two things explains everything about Bitcoin’s monetary policy.

The Block Subsidy and the Halving Schedule

When a miner successfully adds a new block to the blockchain — by solving the Proof of Work puzzle we covered in Lesson 1.2 — they receive two things. First, all the transaction fees from the transactions included in that block. Second, a freshly created amount of Bitcoin called the block subsidy. This subsidy is the only mechanism by which new Bitcoin enters existence. There is no central bank issuing Bitcoin. There is no company minting it. New Bitcoin comes

into being only through this process, one block at a time, roughly every ten minutes.



Every 210,000 blocks — roughly every four years — this block subsidy is cut in half. This event is called the halving. When Bitcoin launched in 2009, the block subsidy was 50 Bitcoin per block. In 2012 it halved to 25. In 2016 to 12.5. In 2020 to 6.25. In April 2024, the most recent halving brought it to 3.125 Bitcoin per block. The next halving will bring it to 1.5625. This process of successive halvings continues until the subsidy reaches zero — at which point all 21 million Bitcoin will have been issued, and miners will operate solely on transaction fees.

What makes this issuance schedule remarkable is not just the cap — it’s the predictability. You can calculate exactly how many Bitcoin will exist on any future date. You can verify the

total supply right now by running a full node. There is no opacity, no committee, no discretion. The monetary policy of Bitcoin is the most transparent and auditable in the history of money.

Bitcoin vs. Gold: Digital Scarcity

Bitcoin is often compared to gold, and the comparison is useful up to a point. Both are scarce. Both require work to produce. Both have historically been used as stores of value. But there is a critical difference: nobody knows exactly how much gold exists in the earth's crust, and new gold is mined every year, slowly inflating the supply. Bitcoin's supply is mathematically certain and completely transparent. Every Bitcoin that will ever exist is accounted for in the protocol.

BITCOIN VS. GOLD: COMPARING SCARCITY

PROPERTY	GOLD	BITCOIN
Supply cap	Unknown — new gold mined every year	Exactly 21,000,000 — hard cap
Verifiable supply	Requires specialist testing	Anyone can verify with a node
Portability	Heavy, costly to move	Send anywhere instantly
Storage	Requires physical security	12 words in your head

Inflation rate	~1–2% per year from mining	Declining to zero, schedule fixed
Confiscation	Can be seized physically	Cannot be seized without seed phrase

Gold is also physically heavy, difficult to transport, impossible to verify without specialist equipment, and easily seized at borders. Bitcoin, by contrast, can be stored in your head as a 12-word seed phrase. It can be transmitted across the internet to anywhere in the world in minutes, for minimal cost, with no intermediary. This is what people mean when they say Bitcoin is digital gold — and in several important ways, it is an improvement on the original.

Economists use a concept called the stock-to-flow ratio to measure scarcity — the ratio of existing supply to annual new production. Gold has historically had one of the highest stock-to-flow ratios of any commodity, which is part of why it has been a reliable store of value. After the 2024 halving, Bitcoin’s stock-to-flow ratio surpassed gold’s. And it will double again with every future halving. This is a property no commodity in the physical world can replicate.

KEY TAKEAWAYS

Let’s close Module 1 with the big picture. Bitcoin has a hard cap of 21 million. New Bitcoin enters existence only through the block subsidy. That subsidy halves every four years, slowing issuance over time. The entire schedule is public, predictable, and verifiable by anyone running a node. No authority can inflate the supply. No one can create Bitcoin out of thin air. In a world where every other

major currency is printed at will, Bitcoin's fixed supply is not just a feature — it is the foundation of its value as a long-term store of wealth.

That completes Module 1 — Bitcoin Basics. You now have a solid mental model of what Bitcoin is, how the blockchain works, how wallets and keys protect your ownership, how transactions and UTXOs move value, and why the 21 million cap makes Bitcoin categorically different from every other currency. In Module 2, we build on this foundation to answer the question you're probably already thinking: if Bitcoin is so good, why do thousands of other cryptocurrencies exist — and why do they fail the test that Bitcoin passes?

Module 1 — Practical Exercises

Complete all three before moving to Module 2. These exercises make the concepts concrete and testable.

1 **Generate a seed phrase on an air-gapped device and write it down by hand**

Use a Coldcard Q, Coldcard Mk4, Foundation Passport, or Blockstream Jade. Generate a new wallet and write every word of the seed phrase, in order, on paper. Verify each word carefully. Store it somewhere physically secure.

⚠ Always purchase your hardware wallet directly from the manufacturer's website. Never from Amazon, eBay, or third-party sellers — devices from unauthorized channels can be pre-tampered to capture your seed phrase the moment you set up.

2 **Look up a real Bitcoin transaction on mempool.space**

Navigate to mempool.space and paste any TXID into the search bar. Identify: the input addresses and amounts, the output addresses and amounts, the fee paid in satoshis, the fee rate in sat/vB, and the confirmation count. This exercise makes Lesson 1.4 completely concrete.

3 **Calculate how many satoshis are in 0.01 BTC**

1 Bitcoin = 100,000,000 satoshis. How many satoshis is 0.01 BTC? How many is 0.001 BTC? Understanding the denomination system from Bitcoin down to satoshis is foundational for reading fees, small amounts, and on-chain data.

Recommended Resources for Module 1

Bitcoin Whitepaper — Satoshi Nakamoto (bitcoin.org)

The original 9-page document that started everything. Short, readable, and foundational. Read it after Lesson 1.1.

The Bitcoin Standard — Saifedean Ammous

Deep dive into Bitcoin’s monetary properties. Chapters 1–3 pair well with Lesson 1.1 and Lesson 1.5.

mempool.space

Live block explorer. Use it for Practical Exercise 2 and to monitor the mempool and fee rates going forward.

learnmeabitcoin.com

Interactive visual explainer of Bitcoin’s technical layers. Excellent companion to Lessons 1.2 through 1.4.