

A BEGINNER'S GUIDE

Broken money & the way out

From the mechanics of money to your first purchase of *Bitcoin*. No jargon, no promises, with data from primary sources.

17
CHAPTERS

≈ 90 min
READ

2.0
EDITION · 2026



EDITOR'S PREFACE

About this book

PUBLISHED

PRAGUE · 2026

EDITION

INVITY ACADEMY

VOLUME 01

FOR WHOM

BEGINNERS WHO KNOW BITCOIN
FROM HEADLINES, BUT NOT
FROM ITS MECHANICS.

LENGTH

≈ 90 MINUTES' READING

This book was created as the introductory material of the Invity Academy education platform. It is meant for people who know Bitcoin from headlines and debates, but never got an answer to the most important question: *why did it come about at all, and what problem does it solve?*

Unlike most guides, we don't start with the technology. We start with money itself — how it came about, how it works today, and why so many people feel that something about it „broke“. Only once we understand the problem does it make sense to talk about a solution.

You won't find investment advice here. You'll find a framework in which you can form your own opinion — and you should seek that opinion across as many sources as possible. The figures and citations here come from traceable public sources (Federal Reserve, ECB, World Bank, BIS, Eurostat, the Czech Statistical Office, Glassnode).

//
*Money is like a second language.
Until you understand it, it controls
you. Once you grasp it, you finally
start speaking with it.*

Adapted paraphrase · Lyn Alden



Enjoy the read. **The Invity.io team**

CONTENTS

Seventeen chapters, three parts, one question.

I.

PART ONE

Broken money

01	What is money, really?	05
02	A brief history of money	07
03	The gold standard and its end	10
04	How money is actually created today	12
05	Inflation is not an accident, it is the system's design	14
06	The Cantillon effect — who stands at the source of the tap	17
07	Debt, fiscal dominance and why there is no way back	19
08	The broken compass — why the old rules no longer hold	22

II.

PART TWO

Bitcoin as the answer

09	Satoshi and 30 years of cryptographic searching	25
10	What Bitcoin is — a network and an asset	27
11	Hard scarcity — 21 million and a stop-loss on power	30
12	Bitcoin is not “crypto”	32
13	Bitcoin vs. gold — two hard assets under the X-ray	34
14	Seven myths you hear at the Sunday lunch	37

III.

PART THREE + APPENDICES

The first step

15	How to start smart	40
16	Invity as a signpost	42
17	What to read and follow next	44
A	Glossary	46
B	FAQ — frequently asked questions	48
C	First-purchase checklist	49

PART ONE · CHAPTERS 01—08

Broken money ^{1.}

In the first part of the book we'll ignore Bitcoin. We first need to understand the world we live in — a world ruled by fiat. Only then will it be clear what Bitcoin actually brings.



What is money, really?

Before we start criticising today's money, we have to answer what we expect from money in the first place. The answer is surprisingly old — and surprisingly useful today.

Money is one of the oldest and at the same time least understood technologies of humankind. It is all around us, yet we think about it surprisingly little. The vast majority of people leave school knowing about genetics, quantum physics or the history of Rome — but with no idea at all of how the money they hold in their wallet comes into being.

Let's start with a very simple question: what is money for? The answer is surprisingly old. Already **Aristotle**, in the 4th century BCE, described that money serves three functions.

The three functions of money

- **A medium of exchange** — it lets you trade things without having to need exactly what your counterpart has.
- **A store of value** — it lets you defer the purchasing power of today's work into the future.
- **A unit of account** — it forms a shared language in which we compare the value of different things.

The properties of good money

For money to perform its functions well, it has to have certain physical and logical properties. Money historians usually name six.

Gold held its place in the competition of money media for five thousand years, because it combined all six properties above average. It was scarce enough, divisible by melting, verifiable by density, and durable forever.

CHAPTER 01 · WHAT IS MONEY, REALLY?

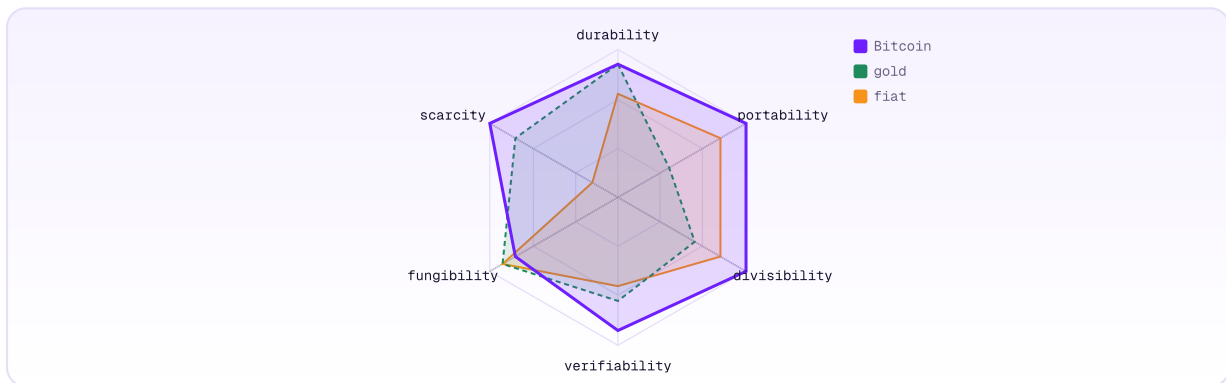
The six properties of money

- **Durability** — money must not decay.
- **Portability** — you must be able to move it easily from A to B.
- **Divisibility** — it must split into smaller and larger units.
- **Recognisability** — a counterparty must be able to verify authenticity and quantity.
- **Fungibility** — one unit must equal another.
- **Scarcity** — and this is the most important one. If anyone could make as much as they wanted, it would have no value.

 CHART 1

Own data

The six properties of money — a comparative diagram

**WHAT THE CHART SHOWS**

A radar chart with six axes and three layers: gold, fiat, Bitcoin.

DATA SOURCE

Own construction based on Menger, Mises, Ammous (2018), Alden (2023).

— KEY TAKEAWAY · CHAPTER 01

What is money, really?

- Money has three functions: exchange, store of value, accounting. The most problematic one today is the second.
- Good money has six properties. The decisive one is scarcity.
- Money is a technology that evolves. What we use today is not the last word.

A brief history of money

Humankind before money. The long road from shells to metal, from coins to paper, from paper to pixels.

If you have a childhood memory of trading stickers, you know what **barter** looks like — the direct exchange of goods for goods. It stops working the moment a carpenter needs shoes and the cobbler doesn't happen to need a table. Economists call this the “*double coincidence of wants*” and it is the first reason money came about.

Already in prehistoric cultures people noticed that some objects are accepted by everyone. Salt, grain, dried fish, furs, shells. They began to work as a universal medium of exchange. We call them **commodity money**.

Gold — a technology proven over 5,000 years

Why gold? Silver was more abundant. Copper oxidised quickly. Iron rusted. Gold was wonderfully excellent: chemically inert, scarce enough that only a fraction of the existing stock is added each year.

Gold has a property economists call a **high stock-to-flow**. Its worldwide stock is enormous, while the amount added each year is roughly 1.5–2%. Even if geologists found a huge gold vein tomorrow, they could not double the supply in a year, nor in ten years.

Coins and the first debasement

The early minting of coins from gold and silver brought an enormous innovation — standardisation. A merchant no longer had to weigh every transaction. He received a coin with the ruler's mark and trusted it weighed exactly what it promised. But with this act of trust, an institution entered the monetary system that gradually began to take care of it differently than the merchant expected: the **state**.

The first great debasement in history was the gradual dilution of the Roman denarius. Roman emperors began diluting silver with cheaper metals so that, for the same weight of coin, they could mint more coins and finance the army.

CHAPTER 02 · A BRIEF HISTORY OF MONEY

DATA

The Roman denarius — the first known monetary debasement

64 AD · silver content	~ 94 %
100 AD · silver content	~ 85 %
200 AD · silver content	~ 50 %
270 AD · silver content	~ 5 %
Decline over 200 years	- 90 %

The lesson: when a state needs more money than it collects in taxes, it starts adjusting the very definition of money.

Paper money and the great shortcut

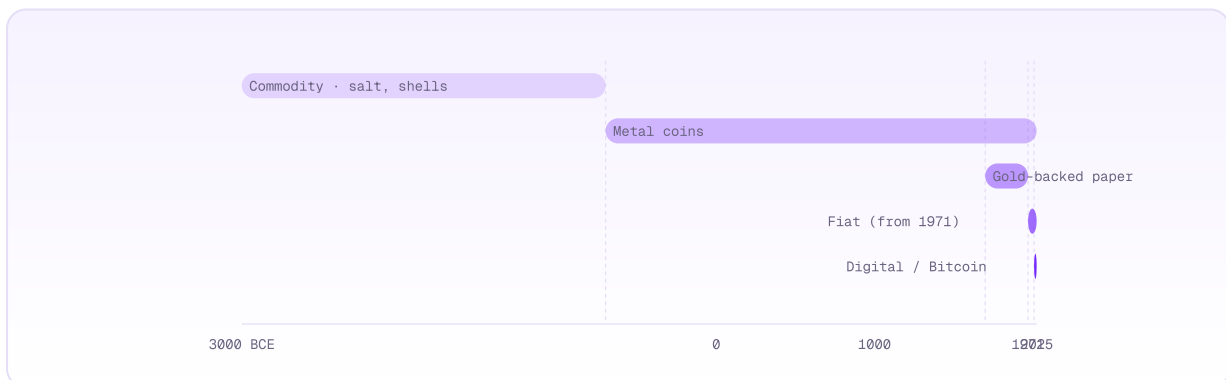
Paper money was invented in China under the Tang dynasty (7th century) and spread on a mass scale under the Song. The principle was simple: heavy coins stayed with a trustworthy custodian and the owner received a paper voucher he could redeem.

This system was robust for several centuries, as long as one condition held: **one note = one specific amount of gold in the vault**. The moment the issuer began printing more notes than it had gold to back — and history shows this happened almost every time — the paper began to lose value.

CHART 2

Own data

A timeline of monetary media



WHAT THE CHART SHOWS

A horizontal timeline from 3000 BCE to the present with five layers: commodity money, metal coins, gold-backed paper, unbacked paper, digital.

DATA SOURCE

Own construction after Alden (2023), Broken Money.

— KEY TAKEAWAY · CHAPTER 02

A brief history of money

- Money arose organically out of market exchange, not from a political decision.
- Metals won over other commodities because mining was difficult enough.
- Gold won over other metals thanks to the highest stock-to-flow in nature.
- The history of paper money is the history of the repeated temptation to print more than there is backing.

The gold standard and its end

How we parted, within a single century, with a millennia-old habit. And why you know so little about it.

If you were born after **1971**, you live in a historical anomaly. In an era when the world's money is backed by nothing tangible. In the entire preceding period of civilisation that was not the case — with the exception of brief periods of war and crisis, from which there was always a return to metal.

The classical gold standard (1870–1914)

The end of the 19th century was an incredibly stable period as far as money goes. Britain, the USA, Germany and France had their currencies backed by a fixed weight of gold. Fixed exchange rates between currencies were a simple consequence — each currency was just a differently named piece of gold.

Prices in this era fell. Between 1870 and 1914 the retail price index in the USA rather stagnated or fell mildly, while the economy grew about 4 % a year. Saving made sense.

1933: gold banned

In the Great Depression, President **Franklin D. Roosevelt** issued, in April 1933, executive order number 6102. Americans had to hand over their gold to the government in exchange for paper dollars at a rate of \$20.67 per troy ounce. Shortly after the mass confiscation the government rewrote the rate — 1 troy ounce = \$35. Overnight it devalued the dollar by 41 %.

//

No government survives long if it allows its citizens to hold a real alternative to its money.

A lesson from Executive Order 6102

CHAPTER 03 · THE GOLD STANDARD AND ITS END

15 August 1971 — the Nixon Shock

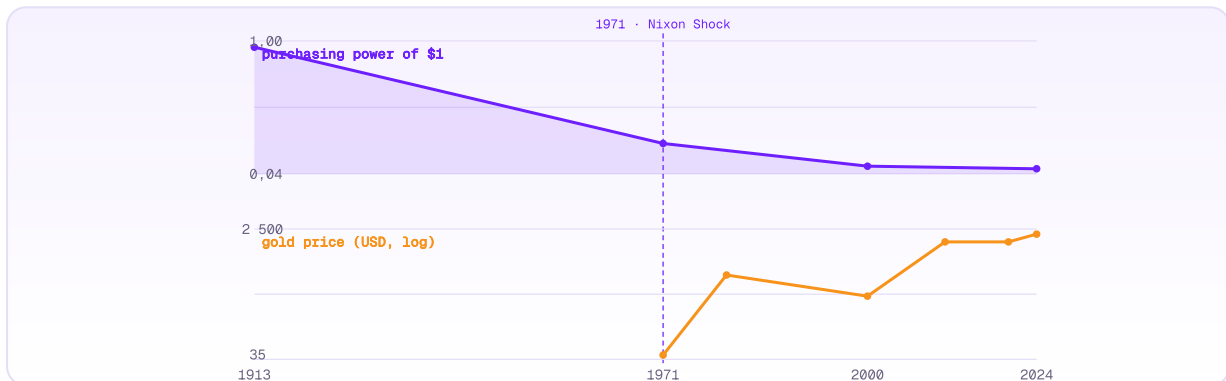
The Vietnam War, the Great Society social programmes, a growing American deficit. The USA was printing dollars faster than gold was accruing. Foreign central banks began to suspect that the promise of “\$35 an ounce” was ceasing to be backed.

On Sunday 15 August 1971, President **Richard Nixon** went on television and announced a “temporary” suspension of the dollar’s convertibility into gold. The suspension holds to this day — it has now lasted over 55 years. **From this moment on, all the world’s currencies are unbacked.**

CHART 3

Own data

The dollar’s purchasing power and the gold price after the Nixon Shock



WHAT THE CHART SHOWS

The purchasing power of \$1 falls from 1.00 to ~0.04. The gold price from 1971 (\$35) to today (~\$2,500).

DATA SOURCE

Federal Reserve Economic Data (FRED), BLS, World Gold Council.

— KEY TAKEAWAY · CHAPTER 03

The gold standard and its end

- 1913 the Fed, 1933 the ban on holding gold, 1944 Bretton Woods, 1971 the Nixon Shock — four steps from hard money to fiat.
- Since 1971 no currency in the world has been backed by anything tangible.
- Losing the golden anchor also meant losing the budgetary discipline of states.
- We live in a historical anomaly, not in a “normal” monetary system.

How money is actually created today

The answer surprises 95 % of people. It is not the printing press. It is not the central bank alone. It is a dance of two levels.

When you ask the average person where money comes from, the most common answer is: “the central bank prints it”, or “the state”. Both are — with a certain generosity — true only by a few percent. **The vast majority of the money you hold in your account never passed through any printing house.** It came into being as an accounting entry the moment someone took out a loan at a commercial bank.

Two levels of money

The modern monetary system is two-tiered. At the top stands the **central bank** — the Fed in the USA, the ECB in the euro area. It creates so-called base money (M0). Below it stand the **commercial banks**. They create the money you actually live with: the numbers in your account.

When a bank approves a mortgage or loan for you, it *does not lend you money from its vault*. It creates it in your account as an entry. The money is thereby new in the economy. When you repay the loan, the money disappears.

Monetary aggregates M0, M1, M2

Central banks track several “layers” of money. When people speak of “the amount of money in the economy”, they usually mean M2. And M2 is the chart everyone must see.

Three levels of monetary aggregates

- **M0** — the monetary base. Banknotes, coins and banks' reserves at the central bank. The only money a central bank prints directly.
- **M1** — M0 plus current accounts at commercial banks. Money available immediately for payment.
- **M2** — M1 plus savings and term accounts. Practically all household savings.

CHAPTER 04 · HOW MONEY IS ACTUALLY CREATED TODAY

DATA

Monetary growth 2000—2024

USA M2	4.6 → 21.0 tn USD (4.6×)
Euro area M3	5.0 → 16.0 tn EUR (3.2×)
Czech Republic M2	1.5 → 6.0 tn CZK (4.0×)
USA real GDP	+ 65 %
Czech real GDP	+ 90 %

The money supply grows much faster than output — the gap explains inflation in both prices and assets.

Quantitative easing (QE)

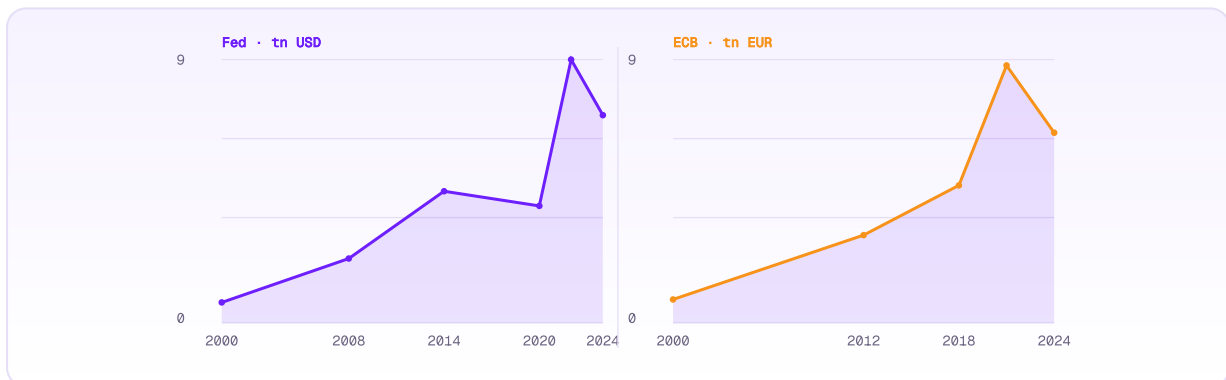
When the American financial system collapsed in 2008, the Fed turned to a tool that had until then existed mainly in textbooks. The central bank bought government bonds and paid for them with newly created reserves.

During the 2020—2022 pandemic the scale of QE was unprecedented: **the Fed expanded its balance sheet from 4 to 9 trillion USD in two years.** That is more than the entire QE after the 2008 crisis put together.

CHART 4

Own data

The monetary base of the Fed and ECB, 2000—2024



WHAT THE CHART SHOWS

The balance sheets of the Fed and ECB in trillions of USD/EUR. Visible jumps: 2008, 2010–2014, 2020.

DATA SOURCE

Federal Reserve H.4.1 Release, ECB Consolidated Financial Statement.

KEY TAKEAWAY · CHAPTER 04

How money is actually created today

- The vast majority of the money in your account was created by commercial banks, not the state.
- New money comes into being at the moment of a loan. When you repay the loan, the money disappears.
- QE lets a central bank create money in the order of trillions within weeks.
- The M2 money supply grows substantially faster than real output.

Inflation is not an accident, it is the system's design

Public conversation about inflation works like football over a beer. Everyone has an opinion, mostly emotional, and nobody cares much about the rules of the game.

When you hear on the radio that “inflation in October was 3.2 %”, what exactly is being said? The official definition of inflation — the one that appears in reports of central banks or the American BLS — is the year-on-year change in a basket of consumer goods and services. It is called the **CPI** (Consumer Price Index).

An alternative and historically older definition reads: inflation is the **increase in the amount of money in the economy**, independent of prices. The two are related but not identical. Money-supply inflation is the cause, price inflation is the symptom.

The problems of the consumer basket

Asset price inflation — the inflation nobody mentions

A new flat in Prague cost on average 25,000 CZK per m² in 2000. In 2024 its average price hovers around 160,000 CZK/m². That is more than six times as much. The average wage over the same period rose roughly fourfold.

The S&P 500 stood at around 1,500 points in 2000, and over 5,500 in 2024. Gold rose from 270 USD/oz to today's 2,500+. Bitcoin from practically nothing to ~100,000 USD. These assets are not rising because they produce that much more. **They are rising because the supply of money grows faster than the supply of assets.**

CHAPTER 05 · INFLATION IS NOT AN ACCIDENT, IT IS THE SYSTEM'S DESIGN

DATA

A Prague flat vs. the average wage over time

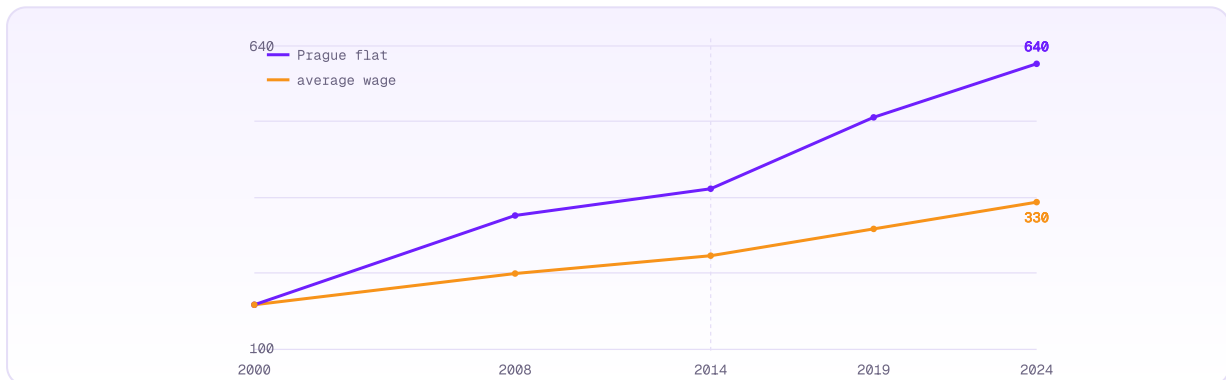
2000 · Prague flat 70 m ²	~ 1.75 m CZK
2000 · average wage	~ 18,000 CZK → 97 months
2024 · Prague flat 70 m ²	~ 11.2 m CZK
2024 · average wage	~ 60,000 CZK → 187 months
Change 2000–2024	+ 90 % in number of wages

If we also measured the interest cost of a mortgage, the difference would be even larger. Sources: CZSO, Deloitte Property Index.

CHART 5

Own data

House prices vs. average wages in the Czech Republic, 2000—2024



WHAT THE CHART SHOWS

Two curves normalised to 100 in 2000: a Prague flat vs. the wage. A clear divergence after 2014.

DATA SOURCE

CZSO, Deloitte Property Index, Sreality.cz index.

Inflation as a silent tax

If you sit on a current account with savings of 500,000 CZK at 5 % inflation, in a year you have lost real purchasing power equal to 25,000 CZK. Nobody touched your account. Nobody sent you a tax return. It is simply that what you can buy for that sum, you now buy less of.

The economist **Henry Hazlitt** called it an “invisible tax” — and from the state's point of view it is ingeniously inconspicuous. Nobody voted it through parliament, and you can't vote anyone in or out over it.



The only difference between inflation and taxation is that you don't have to approve inflation in parliament.

Ronald Reagan · attributed

CHAPTER 05 · INFLATION IS NOT AN ACCIDENT, IT IS THE SYSTEM'S DESIGN

— KEY TAKEAWAY · CHAPTER 05

Inflation is not an accident, it is the system's design

- The official CPI understates real inflation thanks to methodological adjustments.
- Inflation has two faces: consumer prices and asset prices. The second is more decisive for inequality.
- Inflation is worst for savings in current and savings accounts — a silent tax.
- In a system where money grows faster than goods, inflation is inevitable — it is a feature of the design, not an accident.

The Cantillon effect — who stands at the source of the tap

Inflation never falls on everyone equally. It depends how far you are from the tap through which it flows into the system.

In 1730 the Irish merchant and economist **Richard Cantillon** died in London. In his estate a manuscript of the book *Essai sur la nature du commerce en général* was found. It was published only 25 years after his death. It is one of the most remarkable economic texts ever — and it contains an observation that today looks like a prophecy.

Cantillon noticed that new money never enters the economy evenly. First it lands on particular places and particular people.

Who is first and who is last

Imagine a water tap. Whoever is at the tap always gets the water first — clean, cold, at full pressure. Whoever is at the end of the pipe gets the water last — warmer, with traces of rust.

At the tap stand

- **The state** — it spends new money first, at real prices, on contracts and social transfers.
- **Commercial banks** — they receive new reserves and can lend them at rates they don't set themselves.
- **Large corporations** — thanks to cheap credit they finance expansion and acquisitions.
- **Asset owners** — the value of their assets rises before inflation reaches consumer prices.

And who is at the end of the pipe

Modern central banking is often defended with the argument that it stimulates the economy and creates jobs. Even if we take that at face value, we must at the same time see the flip side: the money a central bank creates does not arrive for everyone at once. It travels a predictable path that structurally favours one group over another.

CHAPTER 06 · THE CANTILLON EFFECT — WHO STANDS AT THE SOURCE OF THE TAP

At the end of the pipe stand

- **The fixed-wage employee** — the wage is usually adjusted only with a delay, and not by the full extent of inflation.
- **The pensioner** — the pension is indexed once a year, slowly.
- **The young family without assets** — they own no assets to rise in value, yet pay higher prices for food, energy, rent.
- **The saver on a savings account** — the interest does not cover the loss of purchasing power.

DATA

The Cantillon effect in data (USA, 1989 vs. 2023)

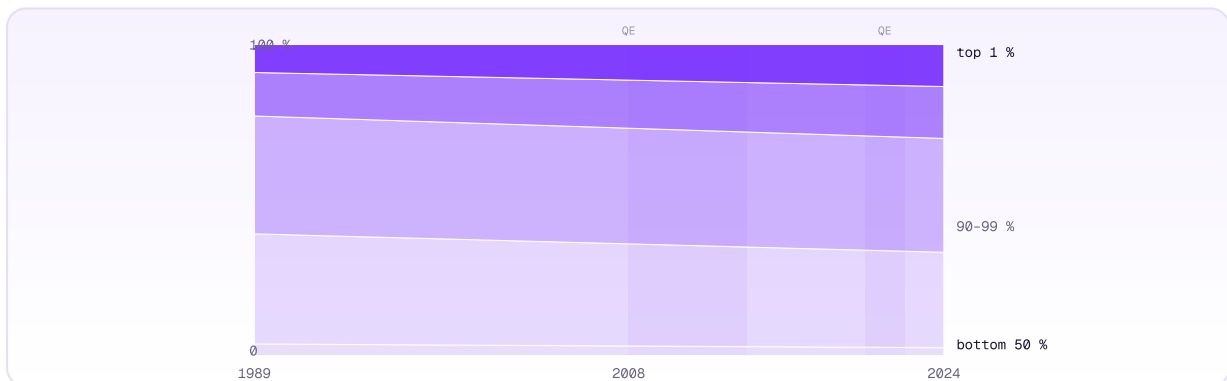
Wealth of the top 1 %	23.0 % → 30.2 %
Wealth of the top 10 %	60.9 % → 66.8 %
Wealth of the bottom 50 %	3.7 % → 2.5 %
Fed balance sheet 2008–2024	~ 5× (0.9 → 9 tn USD)

A coincidence? You'll find the answer in the rest of this book's data. Source: Federal Reserve Survey of Consumer Finances.

CHART 6

Own data

Share of wealth of the top 1 % vs. bottom 50 %, USA 1989—2024



WHAT THE CHART SHOWS

A stacked area chart from 1989 to 2024, five bands: top 0.1 %, top 1 %, next 9 %, next 40 %, bottom 50 %.

DATA SOURCE

Federal Reserve Distributional Financial Accounts (DFA).

— KEY TAKEAWAY · CHAPTER 06

The Cantillon effect — who stands at the source of the tap

- New money does not enter the economy evenly. Someone gets it first, someone last.
- The first recipients gain. The last (employees, pensioners, savers) lose.
- The rise in inequality over the past 35 years correlates precisely with the era of fiat and QE.
- It is not a conspiracy, it is a mathematical consequence of the way money is created.

Debt, fiscal dominance and why there is no way back

Why the monetary system, even if it wanted to, can no longer return to hard money.

Let's start with one number worth remembering. **Global debt (government, corporate, household) reached roughly 318 trillion USD in 2024.** World GDP was about 105 trillion USD. The debt-to-GDP ratio is therefore over 300 %. Historically we saw this level only just after the Second World War — and even then countries took decades to climb out of it.

How we got here

Under the gold standard before 1914, debt-to-GDP in advanced countries was usually between 20—60 %. A state borrowed only in emergencies (war, great crisis) and then gradually repaid the debt.

After 1971, in the fiat era, it turned out that if a currency is unbacked, the state has a cheaper way out than actual repayment — **inflation**. The debt is repaid in real terms with degraded money. The USA had a debt-to-GDP of 35 % in 1980, and 125 % today.

Fiscal dominance

An economic term returning to the debate in recent years is **fiscal dominance**. It means a state of affairs where the state's budgetary situation is so strained that the central bank cannot run an independent policy.

Lyn Alden describes that the United States entered this situation around 2022. The interest cost on US federal debt exceeded the defence budget in 2024 — and that is a defence budget which is itself larger than the budgets of the next ten largest countries combined.

CHAPTER 07 · DEBT, FISCAL DOMINANCE AND WHY THERE IS NO WAY BACK

DATA

Debt/GDP of selected countries over time

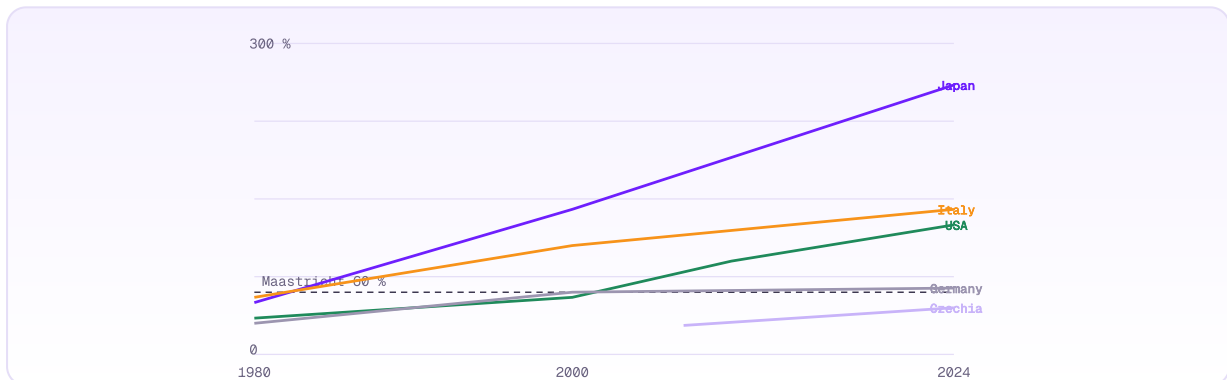
USA	35 % → 125 % (1980–2024)
Japan	50 % → 260 % (1980–2024)
Italy	55 % → 140 % (1980–2024)
Germany	30 % → 64 % (1980–2024)
Czech Republic	28 % → 45 % (2007–2024)

A historical reference value: 60 % was the Maastricht criterion in the 1990s. Today almost every large economy is above that ceiling.

CHART 7

Own data

Debt-to-GDP — USA, Japan, euro area, Czech Republic, 1980—2024



WHAT THE CHART SHOWS

Four line curves with a vertical axis of 0–300 %. All rise, Japan's highest.

DATA SOURCE

IMF Global Debt Monitor, 2024.

Why there is no way back

Imagine you wanted to “return” the system to hard money. It would mean deflation — a fall in the amount of money. It sounds tempting, but in a system with 300 % debt-to-GDP it is an economic atom bomb.

When the nominal value of money rises (inflation), the real value of debt falls. The debtor finds it easier to repay. When the nominal value of money falls (deflation), the real value of debt rises. **The debtor goes bankrupt.**

That is why no Western government today wants deflation. On the contrary — the official goal of central banks is 2 % inflation. Permanent, never-stopping inflation. It is a mathematical necessity at this volume of debt.



Inflation is the state's mother's milk. The state cannot do without it — but the citizen pays the bill.

Ludek Niedermayer · paraphrase

— KEY TAKEAWAY · CHAPTER 07

Debt, fiscal dominance and why there is no way back

- Global debt has reached a level at which deflation is economically unthinkable.
- Central banks are caught in the trap of fiscal dominance — they cannot fight inflation without destabilising the state budget.
- The system therefore structurally requires continuing inflation.
- Nominal prices rise. Real ones, measured in hard assets, stagnate or fall.

The broken compass — why the old rules no longer hold

“Save, invest in a mixed fund, pay off the mortgage.” The advice we have heard since the 1980s has ceased to be sufficient in the modern economy.

After the Second World War, a number of settled recommendations arose for the middle class in the USA and gradually in Europe. Save 10 % of your income. Keep money in the bank for harder times. Buy your own home. Invest in a diversified portfolio of 60 % equities, 40 % bonds. These recommendations worked for decades. **Today some of them actively harm those who follow them.**

The 60/40 portfolio — a former classic

The ratio of 60 % equities and 40 % bonds was the basis of modern asset management. Historically, between 1950—2020, 60/40 delivered a real annual return of around 5 %.

The year 2022 revealed a structural problem. Equities fell about 18 %. Bonds, which were meant to protect, fell about 13 %. The total drop of the 60/40 portfolio was about 16 %. In real terms, after including inflation over 8 %, the loss was over 24 %. The biggest drop of this portfolio in half a century.

A savings account — a guaranteed loss

The average interest rate on savings accounts in the Czech Republic in 2024 was roughly 4 %. Official inflation was around 2.5 %. A seemingly positive real return. In reality, don't forget you tax the nominal return with a 15 % withholding tax. Subtract real inflation (which households feel more strongly than the CPI) — and you have a real return close to zero or negative.

In 2020—2022 the situation was more drastic. Savings accounts offered 0—1 %, inflation reached 18 %. Each year you lost 16—17 % of real purchasing power. **Over three years, 500,000 CZK was left with ~330,000 CZK in real money.**

CHAPTER 08 · THE BROKEN COMPASS — WHY THE OLD RULES NO LONGER HOLD

So what advice holds today?

We will not give you a single piece of advice — we are not investment advisers and your situation is individual. But we can state an observation on which more and more analysts, institutional investors and economists agree.

Three observations for today's portfolio

- Holding large cash in the bank is, over the long run, a strategy by which the state really taxes your purchasing power.
- Diversification remains valuable, but it must include assets that respond to monetary degradation (hard assets).
- **Gold** passed the test of 5,000 years. Neutral, apolitical, independent of the banking system.
- **Bitcoin** is new — it has 15 years behind it. But if its properties are confirmed, it offers everything gold does, and more: portability, verifiability, divisibility and neutrality in a form gold can never have.

— KEY TAKEAWAY · CHAPTER 08

The broken compass — why the old rules no longer hold

- The classic 60/40 advice stopped protecting — in 2022 it lost the most in half a century.
- A savings account is, over the long run, a guaranteed loss of real purchasing power.
- For a generation without inherited assets, the traditional “way up” is markedly steeper than before.
- Diversification must include hard assets resistant to monetary degradation.

PART TWO · CHAPTERS 09—14

Bitcoin as the answer *//*.

The second part of the book is about the answer to broken money found by a group of programmers, cryptographers and economic dissidents. If you made it through the first half, the rest will be easy.

Satoshi and 30 years of cryptographic searching

Bitcoin did not fall from the sky in 2009. It was the result of a thirty-year intellectual journey that began with the birth of the internet.

In 1976 **Whitfield Diffie** and **Martin Hellman** published the paper *New Directions in Cryptography*. In it they described the principle of asymmetric cryptography. It looked like a mathematical curiosity. In reality it was one of the most important discoveries of the 20th century. Without it there would be no internet banking, e-shops, messengers, nor Bitcoin.

In the 1990s a loose movement of *cypherpunks* formed around cryptography — people who believed that strong cryptography is a basic human right.

Attempts at digital money

The first swallow was **DigiCash** by David Chaum (1989) — digital cash based on blind signatures. **E-gold** (1996) worked as an online gold-backed currency. **Hashcash** by Adam Back (1997) was the *proof-of-work* principle that Satoshi later adopted. **Nick Szabo** proposed *bit gold*. **Wei Dai** published *b-money*. All these projects shared one weakness: they could not solve the **double-spending** problem.

31 October 2008 — the whitepaper

On the cryptography mailing list metzdowd.com, on 31 October 2008, a post appeared from a user unknown to anyone, with the nickname **Satoshi Nakamoto**. It contained a link to a nine-page paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*.

It was a cruel irony. The paper came out in the middle of the worst financial crisis since the 1930s. The American government had just approved the 700-billion TARP package to rescue large banks.

// *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*

Text in the Genesis Block — Bitcoin block #0

Satoshi disappears

Satoshi communicated with the first few developers for two years. In 2010 he handed over the project to Gavin Andresen and disappeared. Nobody knows who Satoshi is. It is only known that he owns roughly **1 million BTC** (today worth ~100 billion USD) from early mining, and in over 15 years has never sold or used a single satoshi.

From the point of view of Bitcoin's future, Satoshi's *anonymity* and *disappearance* are a blessing. Bitcoin has no founder who could be sued, arrested, blackmailed or manipulated. **It is truly headless.**

— KEY TAKEAWAY · CHAPTER 09

Satoshi and 30 years of cryptographic searching

- Bitcoin is the result of 30 years of cryptographic research, not a chance discovery.
- Satoshi solved the double-spending problem with proof-of-work and distributed consensus.
- Bitcoin was born in the middle of the 2008 financial crisis as a direct answer to the bank bailouts.
- Satoshi's disappearance is a feature, not a bug — no founder to blackmail.

What Bitcoin is — a network and an asset

Bitcoin is two things. A network made up of thousands of computers all over the world. And an asset that moves across that network.

In English the distinction is made elegantly with a capital and a lower-case letter. **Bitcoin** (capital B) is the protocol — the network, the rules, the software. **bitcoin** (lower-case b) is the unit of the asset that circulates over that network.

The network — Bitcoin

Imagine a global ledger. Each page contains a list of transactions — who sent how much to whom. The pages are numbered from the start (from 2009) and link to each other so that every new page contains a cryptographic fingerprint of the previous one. The result is a **chain that cannot be changed retroactively**.

This chain — the *blockchain* — is kept not by a single institution, but by tens of thousands of computers all over the world. Each of them keeps a complete copy.

The asset — bitcoin

Bitcoin as an asset is the unit the network circulates. **The maximum number of bitcoins is fixed at 21 million**. By May 2024, ~19.7 million had been mined. The remaining ~1.3 million will be mined gradually until 2140.

Each bitcoin divides into 100 million smaller units — *satoshi*. One satoshi is the smallest unit of Bitcoin.

CHAPTER 10 · WHAT BITCOIN IS — A NETWORK AND AN ASSET

DATA

Bitcoin in numbers

Maximum supply	21,000,000 BTC
Mined by 2025	~ 19.8 m BTC (94 %)
1 BTC =	100,000,000 satoshi
Halvings	2012, 2016, 2020, 2024, 2028...
Last BTC mined	~ 2140
Active nodes worldwide	~ 17,000 public
Average time between blocks	10 minutes

In the code since 2009, unchangeable without the agreement of the vast majority of the network.

The halving — why supply slows down

The issuance of new bitcoins is set so that it halves precisely every four years. In 2009 a miner received 50 BTC per block. In 2024 only 3.125 BTC. By 2140 the reward will fall practically to zero.

Wallet, key, address. If you know the private key to a given address, you control the balance. If you lose the key, the balance is irrevocably frozen. This philosophy — “*Not your keys, not your coins*” — is one of the deepest differences between Bitcoin and a bank account.

 CHART 8

Own data

How a Bitcoin transaction works



WHAT THE CHART SHOWS

A scheme in five steps: Alice sends, the transaction propagates, miners include it in a block, the block is added, Bob sees the transaction.

DATA SOURCE

Own illustration derived from the Satoshi whitepaper (2008).

CHAPTER 10 · WHAT BITCOIN IS — A NETWORK AND AN ASSET

— KEY TAKEAWAY · CHAPTER 10

What Bitcoin is — a network and an asset

- Bitcoin = the protocol (network + rules) + bitcoin = the unit of the asset.
- The blockchain is a distributed ledger kept by thousands of computers independently of each other.
- Proof-of-work keeps the system secure — an attack would require enormous energy investment.
- The supply of 21 million is hard-coded. Ownership = control of the private key.

Hard scarcity — 21 million and a stop-loss on power

What does it mean to have truly limited money? And why is it so technologically difficult that for 30 years no one managed it?

Scarcity is the most fundamental property of money. If money grows faster than goods, its value falls. Historically we had this property in commodity money — salt, shells, gold. They all had one problem: under a strong enough technological change they could be mined more.

The difference between scarcity and unbendability

In monetary theory the term **unforgeable costliness** is used. It is the requirement that creating a new unit of money costs real work, energy or some other form of resources that cannot be bypassed.

Bitcoin takes this property to the extreme. Its supply grows according to a code-prescribed schedule that is perfectly predictable. Anyone can calculate exactly how many BTC will exist on 1 January 2030 — and that number will not change, whatever happens.

Why you can't just copy it

One of the most common arguments of opponents is: "Thousands of people have created copies of Bitcoin. Just fork it. So it isn't scarce."

Scarcity *does not come from the code itself*, but from trust that the rules will not change. Bitcoin is trustworthy not because it has the best code (many projects are technically more sophisticated), but because its rules have survived 15 years without fundamental change. That is the **Lindy effect**: the longer something exists unchanged, the more likely it is to last a long time more.

CHAPTER 11 · HARD SCARCITY — 21 MILLION AND A STOP-LOSS ON POWER

DATA

A comparison of the pace of monetary expansion

USA M2, 1971–2024	~ 6.5 % a year (+25 % in 2020)
Euro area M3, 2000–2024	~ 5–6 % a year
Czech M2, 2000–2024	~ 6–7 % a year
Gold – annual stock growth	~ 1.5–2 %
Bitcoin 2025	0.85 % a year
Bitcoin after 2028	0.43 % and falling
Bitcoin in 2140	0 %

The consequence for USD holders: at 6.5% compound a year over 50 years, the dollar loses roughly 95% of its purchasing power.

21 million as a stop-loss on power

If we reflect on what specifically makes Bitcoin exceptional from a political-economic standpoint, it is this: **it is the first monetary system in history where there is no one who could add money on top.** No central bank. No state. No group of developers. No one.

Every previous monetary technology had an issuer above it. The state cannot control gold, but it can confiscate it (1933). It can create the dollar. Bitcoin has no equivalent entity.

// *Bitcoin is the first money in history that has no boss above it.*

Parker Lewis · paraphrase

— KEY TAKEAWAY · CHAPTER 11

Hard scarcity — 21 million and a stop-loss on power

- Scarcity in money requires unforgeable costliness — a real cost to create a unit.
- Bitcoin has absolute scarcity: its supply is hard-coded at 21,000,000.
- It is not about technical un-copyability — it is about the credibility of the rules, which time builds (the Lindy effect).
- Bitcoin is the first monetary system without an issuer — no one can add money on top.

Bitcoin is not “crypto”

The vast majority of negative news about Bitcoin concerns something else. Understanding this difference is perhaps the most important skill for today’s investor.

When the crypto-exchange colossus FTX exploded in 2022, headlines around the world proclaimed a “crypto crisis”. Bitcoin itself fell about 70 % from its peak in that wave. Most people, including serious investors, placed Bitcoin in the same category as terra/luna, FTX tokens, NFT apes and thousands of altcoins. **This categorisation is — to put it bluntly — a mistake that costs people money.**

What clearly sets Bitcoin apart

Five fundamental differences

- **It has no founder.** No CEO, no foundation, no marketing team. Satoshi disappeared in 2010.
- **A fair launch.** No ICO, no pre-sale phase, no premine — the only way was to mine.
- **Proof-of-work vs. proof-of-stake.** Bitcoin uses PoW. Altcoins PoS — whoever has more tokens has more votes.
- **A monetary good vs. a platform.** Bitcoin solves a single problem — money. It doesn’t try to be a game or a metaverse.
- **The Lindy effect.** Bitcoin has run continuously since 3 January 2009 — over 15 years. It survived dozens of attempts at a ban.

What the regulators say

It is remarkable that regulatory classifications have long separated Bitcoin from the rest of the market. The US **CFTC** classifies Bitcoin as a commodity — the same category as gold, oil, wheat. The US **SEC** confirmed that Bitcoin is not a security.

In January 2024 the American authorities approved spot Bitcoin ETFs. BlackRock, Fidelity, Franklin Templeton and others together manage over **60 billion USD in Bitcoin ETFs within just 12 months**. For comparison: it took 19 years for the gold ETF (GLD) to reach the same amount.

CHAPTER 12 · BITCOIN IS NOT “CRYPTO”

DATA

Bitcoin in the light of regulation and institutions

USA classification	Commodity (CFTC), not a security
Spot BTC ETFs approved	10 January 2024 (11 funds)
AUM in BTC ETFs after 12 m	~ 60 bn USD
Gold GLD ETF (2004)	Same AUM in 19 years
MicroStrategy	250,000+ BTC on its balance sheet
Government reserves	USA, El Salvador

Sources: CFTC v. CoinFLEX, SEC Spot Bitcoin ETF Approval (2024), companies' quarterly filings.

CHART 9

Own data

What is left of past top-10 “cryptocurrencies”



WHAT THE CHART SHOWS

A comparison of the top 10 cryptocurrencies in 2014, 2018, 2021 vs. 2024. Bitcoin is always in the top 3.

DATA SOURCE

CoinMarketCap historical snapshots.

— KEY TAKEAWAY · CHAPTER 12

Bitcoin is not “crypto”

- Bitcoin is the only crypto project without a founder, without an ICO, without a premine.
- Proof-of-work enforces real economic costs; proof-of-stake re-creates a concentration of power.
- Regulatory classifications (commodity, spot ETFs) confirm Bitcoin's distinctiveness.
- Of the top-10 crypto projects 10 years ago, little is left today. Bitcoin was always in the top 3.

Bitcoin vs. gold — two hard assets under the X-ray

If Bitcoin makes sense, it has to hold up next to the asset that has held the monetary throne longer than all the states of the world combined — gold.

Gold is the only previous monetary asset worth comparing Bitcoin against. The other media — silver, copper, salt, shells — fell out of the monetary competition. Gold remains on central banks' balance sheets, households and states hold it as a reserve, and its market capitalisation exceeds 15 trillion USD.

A comparison framework — the six properties

We'll go through the six properties of money for both assets. **Durability:** both exceptionally robust. Gold physically, Bitcoin protocol-wise. **Portability:** Bitcoin anywhere in minutes. Gold requires physical transport. *A qualitative leap comparable to the move from the telegram to e-mail.*

Divisibility: Bitcoin divides into 100 million satoshi — it opens micro-payments gold could never serve. **Scarcity:** Bitcoin's is *absolute*, gold's relative (1.5—2 % a year).

Where gold is still better

Gold has several objective advantages Bitcoin cannot yet reach. **The historical record.** 5,000 years of monetary role vs. 15 years. **Market size.** ~15 trillion USD vs. ~2 trillion. **Volatility.** 10—20 % a year vs. 50—80 %. **Political neutrality and state reserves.** Central banks hold over 35,000 tonnes of gold.

CHAPTER 13 · BITCOIN VS. GOLD — TWO HARD ASSETS UNDER THE X-RAY

Where Bitcoin is qualitatively different

Confiscatability. Gold was seized in the USA in 1933. Bitcoin in self-custody follows a different logic. A private key can be memorised, split, stored outside the country without physical transport.

Borders. Moving 1 million USD in gold = 12 kg + insurance. The same value in Bitcoin crosses the border in 10 minutes.

Verifiability for a layperson. Bitcoin can be verified just by checking the balance in an open-source wallet — without trust in a third party.

DATA

Gold vs. Bitcoin — a 2024 comparison

Market capitalisation	15 tn USD / 1.5–2 tn USD
History of its role	5,000 years / 15 years
Annual supply growth 2024	~ 1.8 % / 0.85 %
Annual growth after 2028	~ 1.8 % / 0.43 % and falling
Historical volatility	10–20 % / 50–80 %
Confiscation in history	USA 1933, India 1963 / None

Sources: World Gold Council (Q4 2024), CoinMetrics, Federal Reserve Historical Documents.

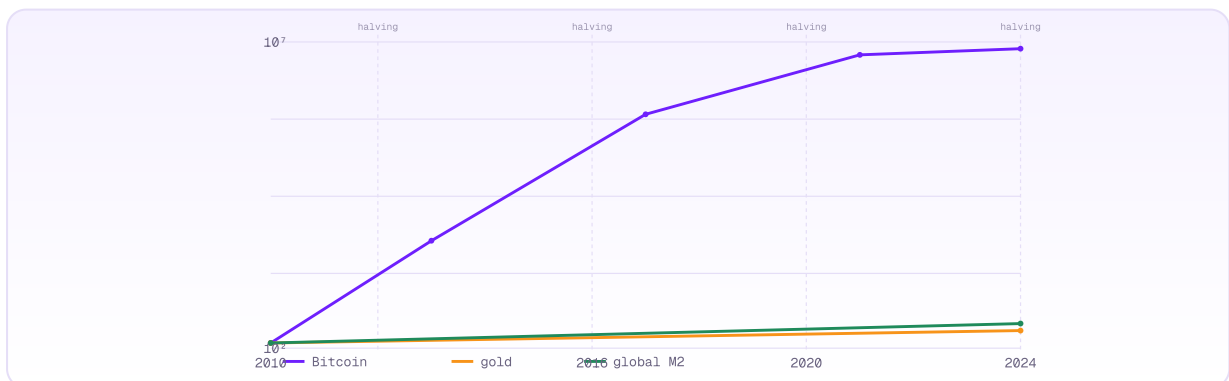
Not rivals, but heirs

The framework that makes the most sense for your own decision-making reads as follows: **Bitcoin and gold are not competitors — they are two generations of the same monetary family.** Gold is the proven, slow, physical variant. Bitcoin is the digital, fast, more volatile variant. For an investor with a long enough time horizon it makes sense to hold both — not as an “either/or” bet, but as genuine diversification within the “hard assets” category.

CHART 10

Own data

Bitcoin vs. gold vs. the global money supply, 2010—2024



WHAT THE CHART SHOWS

Three curves on a logarithmic axis, indexed 2010 = 100: global M2, the gold price, the Bitcoin price.

DATA SOURCE

FRED, ECB, BoJ, World Gold Council, CoinMetrics.

//
Bitcoin is gold 2.0 — not a competitor, but the technological successor of the same economic function.

A framework inspired by Lyn Alden · Broken Money (2023)

— KEY TAKEAWAY · CHAPTER 13

Bitcoin vs. gold — two hard assets under the X-ray

- Bitcoin and gold serve the same economic function — hard, neutral, apolitical money.
- Gold leads in history, market size, low volatility and state acceptance.
- Bitcoin leads in portability, divisibility, resistance to confiscation and programmability.
- A sensible strategy for a long-term investor: hold both, don't choose between them.

Seven myths you hear at the Sunday lunch

Bitcoin's real challenge is not the technology. It is the wariness built into our heads by half a century of a system in which money was a political question.

If you start talking about Bitcoin with family or in the office kitchen, you'll hear a set of seven objections that repeat almost word for word. They all have good roots — they are intuitions every reasonable person should have. At the same time, all seven have a sophisticated answer the objector has usually never heard.

Myth 1 — “It's backed by nothing, it's just code”

- This sentence has a true core — Bitcoin really is not backed by a physical commodity.
- **Nor is the dollar backed by anything since 1971.** The dollar is backed only by trust in the US government and the state's ability to enforce taxes.
- Bitcoin is backed by mathematics, by the energy spent on proof-of-work, and by the network effect of millions of users.

Myth 2 — “It uses too much energy”

- Bitcoin consumes ~130 TWh a year — similar to Argentina, ~0.4 % of global consumption.
- The global **banking system** consumes 260+ TWh a year. **Gold mining** ~240 TWh. **Christmas lights in the USA** ~7 TWh.
- More than 50 % of Bitcoin mining uses renewable or “stranded” energy — flare gas, geothermal, solar surpluses.

Myth 3 — “Only criminals use it”

- In 2023, illicit activity was ~0.34 % of all crypto transactions (Chainalysis).
- The UN estimates that 2—5 % of global GDP is laundered in cash. US cash is, per the DEA, 80 % linked to illicit activity.
- **Every Bitcoin transaction is publicly traceable.** For truly anonymous crime, cash is a far better tool.

CHAPTER 14 · SEVEN MYTHS YOU HEAR AT THE SUNDAY LUNCH

Myth 4 — “It’s too late to buy”

- This objection has repeated since 2013 (BTC \$100). Since then it has risen 1,000×.
- In 2017 “too late” at \$5,000. In 2021 at \$50,000. Every level was, in hindsight, early.
- Bitcoin’s market cap is still a few percent of the total market of hard and soft money.

Myth 5 — “It’s a bubble / a Ponzi scheme”

- Bitcoin has had at least four cycles with drops of 70—85% over 15 years. Each time it returned. *That is not the definition of a bubble — it is an adoption curve.*
- Bitcoin **promises no return**. It has no promoter. It has no structure that redistributes money from within. It is not a Ponzi.

Myths 6 and 7 — “The state will ban it” / “Something better will come”

- China banned mining in 2021 — the hashrate fully recovered within a year. India threatened, it never passed.
- Bitcoin holds 90%+ of the market share among real cryptocurrencies with neutral rules. **Money converges to a single standard.**

— KEY TAKEAWAY · CHAPTER 14

Seven myths you hear at the Sunday lunch

- It is not that Bitcoin has no weaknesses — it does. It is that most popular objections come from misunderstanding.
- Backing, energy, crime, “too late”, a bubble, a ban, a successor — seven objections, seven data-backed answers.
- If, after hearing the answers, someone still rejects Bitcoin, that is a legitimate choice — but an informed one, not a reflex.

PART THREE · CHAPTERS 15—17 + APPENDICES

The first step *///*.

Theory is nice. Now for practice. The third part of the book is about turning knowledge into reality — without needless mistakes, without expensive experiments, without the stress of technology.



How to start smart

Four principles that will save you more money than any technical skill.

Three practical rules that experienced investors repeat to the first-time Bitcoin newcomer.

1. Buy only as much as you can afford to lose

- Bitcoin is a volatile asset in an early phase of adoption. Over 15 years it has gone through four big drops over 70%.
- A typical recommendation: **1—5%** of the total portfolio for beginners.
- For strong exposure after verifying the framework: **5—10%**. More requires a high tolerance for volatility.

2. DCA instead of timing

- **Dollar Cost Averaging** — buying the same amount regularly regardless of the price.
- When the price is low you buy more. When high, less.
- Experience shows: *DCA beat the vast majority of attempts at active market timing.*

3. Self-custody, as soon as it is reasonable

After buying on an exchange, you have bitcoin in their account, not your own. An exchange can collapse (FTX 2022), be hacked (Mt.Gox 2014), or freeze your account. **Not your keys, not your coins.**

For small amounts up to about €2,000, holding on a reputable exchange is an acceptable risk. Above that threshold it is wise to move the coins to your own wallet.

CHAPTER 15 · HOW TO START SMART

DATA

Self-custody — 5 rules you must never break

Seed (12/24 words)	never in the cloud, a photo, e-mail
Writing the seed	BY HAND on paper / a metal plate
Hardware wallet	buy direct from the maker, not Amazon
First transaction	small test before a larger amount
A request for your seed	ALWAYS a scam, no exceptions

Recommended brands: Trezor, Ledger, Coldcard, BitBox, SeedSigner — all cost €80—200.

4. A loan against the asset — an advanced strategy

When holding any appreciating asset for a long time, you run into a practical question: I need liquidity, but I don't want to sell the asset. In the classical banking world a **lombard loan** is used for this.

For Bitcoin there are two models: *custodial platforms* (Ledn, Unchained, Bitfinex) — rates 10—17 % APR, LTV 30—50 %. *Decentralised protocols* (AAVE, Maker, Sovryn, Lava Vault) — rates 4—10 % APR, without counterparty risk.

For a beginner these tools are not the first step. They are an add-on for the phase when you already have a materially significant position and know you won't sell BTC long-term.

— KEY TAKEAWAY · CHAPTER 15

How to start smart

- Position size matches your tolerance for volatility — typically 1—10 % of the portfolio.
- DCA systematically beats attempts at market timing.
- Self-custody as soon as the position exceeds ~€2,000.
- A loan against BTC is a tool for advanced phases — not the first step.

Invity as a signpost

This chapter introduces the tools we build at Invity. It is not an advertisement — it is a summary of what steps you have available.

Invity was founded in 2018 as an independent comparison platform. **We are not an exchange or a bureau.** We don't offer our own "token", we don't provide investment advice, we don't manage your money. Our task is to keep you from entering the market with pocket-sized ignorance — to let you see comparable options, understand the differences, and decide on the basis of facts.

The exchange comparison

The most common opening task: where to buy your first bitcoin in euros or koruna. Invity integrates dozens of European and global exchanges. For each transaction it shows not only the spot price, but the **total cost including hidden spreads**, SEPA/card fees and minimum volumes.

The typical fee saved between the cheapest and most expensive exchange on a €400 purchase is 1—3 %. With monthly DCA of €200 over five years that comes to €120—360 — which is more than a hardware wallet costs.

The DCA calculator

A key tool for the decision whether to start. The DCA calculator lets you enter how much you would invest monthly and from what date — and shows how big a position you would have today and what the real return is.

A savings plan — automated DCA

For those who want to do DCA systematically, a savings plan is available: you set a one-time instruction, the payment is taken regularly, bitcoin is bought automatically and ideally sent to your wallet. **It removes decision fatigue** and the system handles the discipline for you.

CHAPTER 16 · INVITY AS A SIGNPOST

DATA

DCA scenarios — illustrative calculations

€80/m from 1/2020	€5,000 → ~ €17,000 (× 3.4)
€200/m from 1/2017	€19,000 → ~ €100,000
€400/m from 1/2023	€12,000 → ~ €27,000

The calculator computes current values from live prices. Past returns are no guarantee of the future.

What Invity does not offer

We are an independent comparison tool, not a broker. We don't actively sell you any financial product. **We have no commissions on whether you buy more or sell sooner.** Our business interest is that you use the platform long-term — which means you have to be satisfied with what you find here.

We provide no custody. We hold no customer deposits in our accounts. That is by *design*: we don't want to be another Celsius, FTX or BlockFi. The coins you buy via Invity are either at a partner exchange (briefly), or — ideally — in your wallet.

//

Transparency and neutrality are our core USP. If they ever stop holding, we stop making sense.

The Invity.io team

— KEY TAKEAWAY · CHAPTER 16

Invity as a signpost

- Invity = a comparison platform, not an exchange or custody.
- Exchange comparison + DCA calculator + savings plan = three tools with which you lower both costs and emotions.
- Transparency and neutrality are our core USP.

What to read and follow next

This book gave you a structured introduction. If you want to go deeper, here is a list of sources the Invity team uses personally.

A list of sources — books, essays, podcasts and data services — organised by entry threshold. Start with what suits you.

Books — to start

- **Lyn Alden:** *Broken Money* (2023) — the best book on the history and future of money. A neutral tone, rich data.
- **Saifedean Ammous:** *The Bitcoin Standard* (2018) — a classic. Austrian economics + Bitcoin.
- **Dominik Stroukal, Jan Skalicky:** *Bitcoin — The Money of the Future* (2015) — a Czech classic, readable, still relevant.
- **Parker Lewis:** *Gradually, Then Suddenly* (2023) — essays. The most convincing skeptic-turned-believer text.

Essays — a quick read

- **Lyn Alden:** “*The Fraying of the US Global Currency Reserve System*”
- **Lyn Alden:** “*Fiscal Dominance*”
- **Parker Lewis:** the “*Gradually, Then Suddenly*” series (20+ articles on the Unchained blog).
- **Hal Finney:** the first e-mails from 2009 — a historical document.

Podcasts

- **What Bitcoin Did** (Peter McCormack)
- **The Investor’s Podcast / BTC Fundamentals** (Preston Pysh)
- **Bitcoin Audible** (Guy Swann) — key essays narrated
- **The Bitcoin Standard Podcast** (Saifedean Ammous)

CHAPTER 17 · WHAT TO READ AND FOLLOW NEXT

Data and charts

- **mempool.space** — the state of the network in real time, fees, blocks.
- **Glassnode** — on-chain analysis (a basic version free).
- **CoinMetrics** — historical data for research.
- **FRED** — M2, the Fed balance sheet, interest rates.

In closing

Understanding money in 2026 is more than a skill — it is a **survival strategy**. The generation that understood it gained in every historical epoch. The generation that did not understand it grew passively poorer.

This book gives you no investment recommendation, will not replace a financial adviser and promises no miraculous gains. It gives you a framework in which you can form your own opinion. Your decision is yours — but now you make it with information the vast majority of people around you do not have.

Thank you for reading this far.

The Invity.io team

APPENDIX A

Glossary

Core terms to help you find your way through the book and the sources that follow.

Bitcoin (capital B)	the network, protocol, software.
bitcoin (lower-case b) / BTC	the unit of the asset on the Bitcoin network. 1 BTC = 100,000,000 satoshi.
Satoshi (sat)	the smallest unit of bitcoin, named after the creator.
Blockchain	a ledger formed by a sequence of blocks, each cryptographically linked to the previous one.
Hash	a mathematical fingerprint, a one-way function. Used to “sign” blocks.
Proof-of-work (PoW)	consensus in which a miner expends computational work. Bitcoin uses PoW.
Proof-of-stake (PoS)	consensus in which whoever holds more tokens has more say. Ethereum and most altcoins.
Mining	the process in which specialised computers compete to assemble the next block.
Halving	a halving of the block reward, every 4 years.
Wallet	software or hardware that manages your private keys.
Private key	a secret number that controls the bitcoins at a given address.
Seed / recovery phrase	12 or 24 words that let you restore a wallet.
Hot wallet	a wallet connected to the internet (a mobile app, Wallet of Satoshi).
Cold wallet	an offline wallet (a hardware wallet, paper wallet).
Self-custody	a state in which you hold your own private key, not a third party.
Custody	a third party (an exchange, a bank) holds the keys for you.

APPENDIX A · 2

Glossary — part 2

UTXO	Unspent Transaction Output, the way Bitcoin records balances.
Lightning Network	a second layer on top of Bitcoin for fast, cheap payments.
Node	a computer that keeps a complete copy of the blockchain and verifies transactions.
KYC	Know Your Customer — an exchange's duty to verify a customer's identity.
AML	Anti-Money Laundering — measures against money laundering.
DCA	Dollar Cost Averaging — the strategy of buying the same amount regularly.
ATH	All-Time High — a historical maximum price.
FOMO	Fear of Missing Out — fear of missing an opportunity, leading to impulsive buys at the top.
FUD	Fear, Uncertainty, Doubt — fear-inducing disinformation, typically before a drop.
Fiat	currency declared legal tender by a state (USD, EUR, CZK).
M2 / M3	monetary aggregates. The sum of money in the economy including deposits.
QE	Quantitative Easing — money printing by a central bank via asset purchases.
CBDC	Central Bank Digital Currency.
Stablecoin	a crypto token pegged to the value of a fiat currency (USDT, USDC).
Altcoin	a cryptocurrency other than Bitcoin.

APPENDIX B

FAQ — frequently asked questions

The nine questions we get asked most often.

Is Bitcoin legal in the EU?

Yes. Bitcoin is fully legal. Exchange and brokerage activity falls under regulatory supervision (since 2025 within the European MiCA regulation).

How is BTC taxed?

Tax rules differ by country. In many jurisdictions a holding period or an annual threshold applies. Consult the current law or a tax adviser. This is not tax advice.

What happens if I lose my seed?

If you lose the seed and also access to the hardware wallet, your bitcoins are irrevocably lost. No one can restore them for you. **That is why a safe backup of the seed is crucial.**

What if I'm forced to transfer BTC?

For larger amounts there are strategies: multi-sig (several signatures), time-lock (a transaction after a delay), decoy wallets. For beginners it is enough not to publicise that you hold BTC.

What is the Lightning Network?

A second layer on top of Bitcoin that enables instant and almost free micro-payments. Apps: Phoenix, Breez, Wallet of Satoshi.

Can a state ban Bitcoin?

Technically, very difficult. In practice some states are more willing (China, Nigeria). In the EU the trend is the opposite: Bitcoin recognised as a commodity, MiCA regulation.

What is the difference between Bitcoin and Ethereum?

Bitcoin is primarily money — the best store of value and a neutral payment medium. Ethereum is a platform for programmable contracts — tokenisation, DeFi, NFTs.

What is a Bitcoin ETF?

A fund whose shares trade on an exchange and are backed by real BTC. **Advantage:** simplicity. **Disadvantage:** an annual fee + a paper claim, not BTC.

What about stablecoins?

Crypto tokens pegged to the dollar. They solve volatility but inherit all the dollar's problems. A good tool for short-term liquidity, not for long-term store of value.

APPENDIX C

First-purchase checklist

Go through this checklist before you send the first money to buy bitcoin. Print it, tick the boxes — or use it inside the Invity app.

01 BEFORE BUYING

- 01 I have set my **position size**: ____ % of total financial assets.
- 02 The amount is one I can afford to lose without affecting the household.
- 03 I have chosen a strategy: lump sum / **monthly DCA** / a combination.
- 04 I compared at least 3 exchanges in the Invity comparison tool. I chose: _____.
- 05 I verified the tax implications in the current version of the law or with a tax advisor.

02 AT THE FIRST PURCHASE

- 06 I opened an account and passed **KYC verification**.
- 07 I sent a small test amount (e.g. €20), confirming the transfer works.
- 08 I made the first real purchase. Result ____ BTC for ____ €.

03 SELF-CUSTODY · IF I HOLD MORE THAN ~ €2,000

- 09 I ordered a **hardware wallet directly from the manufacturer** (Trezor, Ledger, Coldcard, BitBox). NOT from Amazon.
- 10 I wrote the seed down **BY HAND** on two pieces of paper / metal plates.
- 11 I did **NOT** upload the seed to the cloud, photograph it, or e-mail it.
- 12 I tested recovery: wallet reset, restore from seed, confirmed it works.

THANK YOU FOR READING THIS FAR

Now you *know* what the vast majority of people around *you* don't.

Understanding money in 2026 is more than a skill — it's a survival strategy. This book gives you no investment recommendation. It gives you a framework in which you can form your own opinion — and take the first step.

DOWNLOAD THE APP



Invity

App Store · Google Play
EU + Iceland, Norway,
Switzerland

CONTINUE ON THE WEB

invity.io/academy

DCA calculator · exchange comparison ·
savings plan · the Invity Beacon blog

