

NINE PAGES

P R A I S E F O R
NINE PAGES

There is none yet.

This book went to print before anyone outside a small circle had read it. That is the correct order of events, and the exact reverse of how these pages are normally produced.

The convention is that a manuscript circulates for eight weeks among people who owe the author a favour, and the resulting sentences appear here in a typeface slightly smaller than the rest of the book. Some of those sentences are written by people who read the whole thing. The proportion is not published.

We are doing it the other way round. The book is in your hands. The praise, if any arrives, will come from people who paid for it and finished it — which is a considerably higher bar than a galley proof and a deadline.

If quotes turn up, they will appear here in the next printing.

If they do not, this page stays exactly as it is, and you will have learned something useful about the book you are holding.

Praise is a claim about a book, made by somebody you have not met. Here are claims you can verify yourself, before deciding to trust a word of it.

Every entry in the Dated Record carries a handle — a block height, a transaction, a docket number, a filing. Ninety-eight of them, from the thirty-first of October 2008 to the cut-off date. Appendix B tells you how to pull each kind. The chain handles take about ninety seconds each.

The supply is checkable. Compare the coinbase at block 210,000 with block 209,999, subtract the fees, and the subsidy halves. Repeat at 420,000, 630,000 and 840,000. Chapter 12 walks you through it in an afternoon, on a laptop, without an account.

The position the author took on the twelfth of May 2020 is public, timestamped and described in Chapter 20. What it became is not in this book, and the Preface says why.

If a handle does not check out, the process for saying so is in Chapter 32, and the original error is not deleted when it is corrected.

That is a better guarantee than a sentence from somebody who owed the author a favour.

NINE PAGES

*How Bitcoin was built, and why you
never have to take it on trust*

D R . C L E M E N C H I A N G

T H E D I S C L O S E D R E C O R D · B O O K T H R E E

NINE PAGES

How Bitcoin Was Built, and Why You Never Have to Take It on Trust

Copyright © 2026 Clemen Chiang

First published 2026 by SPIKING PRESS

An imprint of Aly Pte. Ltd. (UEN 201213696E), Singapore

All rights reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means without the prior written permission of the publisher, except in the case of brief quotations embodied in reviews and certain other non-commercial uses permitted by copyright law.

ISBN 978-981-94-7861-3 (hardcover)

ISBN 978-981-94-7860-6 (paperback)

ISBN 978-981-94-7859-0 (ebook)

Disclosure. The author owns bitcoin.institute, where the Dated Record in this book is maintained, and Spiking, a commercial platform selling market education. Neither sells, custodies or takes a fee from any digital asset, and nothing either sells appears in these pages. Their relationship to the book is stated on the page headed This Book and the Platform.

No endorsement or sponsorship has been sought or received for this book from any exchange, custodian, broker, hardware manufacturer, issuer, platform, fund or regulator. No party has been paid for inclusion, no party has been given approval over the text, and no provider is named for the reader to use.

Disclaimer. This book is for general information and education only. It is not financial, investment, legal or tax advice, and it is not a recommendation to buy, sell or hold bitcoin or any other asset. It contains no price target, no forecast, no allocation guidance and no statement of return. Bitcoin is volatile, has fallen by more than three-quarters from its high on four occasions, and its transactions cannot be reversed. The legal and tax treatment of digital assets differs by jurisdiction and changes, sometimes at short notice. **Where this book names a rule, threshold, fee, date or procedure, it does so as the position at the date of writing only, and it must be verified against the record it cites before being relied upon.** The author and publisher accept no liability for any loss arising from reliance on this book. Readers should obtain independent professional advice.

Currency. All figures are in United States dollars unless otherwise stated. Quantities of bitcoin are given in whole coins unless otherwise stated.

Sources. This book states the record as it stood on 27 September 2026. The maintained Dated Record, with its corrections dated and its errors preserved, is kept at bitcoin.institute, which carries no advertising and no product. The record will change after publication; the handles will not.

This book was written with the assistance of artificial intelligence tools, with extensive editing by the author. No images in this book are AI-generated.

Published in Singapore. Distributed worldwide.

Also by the author: *The Wall Came Down* (Spiking Press, 2026); *Long Island* (Spiking Press, 2026); *Spiking To The Moon*.

Cover: Spiking Press. Set in Georgia, Courier New and Trebuchet MS.

To God.

*Every ledger in this book asks who keeps it.
You gave me Your Son, Jesus,
and kept my name where I could never have written it.*

For Nicole,
my best friend and my wife.

*This book asks the reader to take nothing on trust.
Everything I have, I hold with you.*

For Yee, Le and Loong,
who grew up while the blocks kept coming.

*The record is what anyone can check.
You are what I could never replace.*

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

COINBASE OF BLOCK 0

18:15:05 UTC, 3 JANUARY 2009 · DATED RECORD
2

C O N T E N T S

This Book and the Platform..... xi

Preface xiii

How to Read This Book..... xvii

Acknowledgements.....xix

PART ONE · How It Came to Exist1

1 Money Is a Ledger 3

2 The Ancestors..... 11

3 Nine Pages19

4 The Genesis Block..... 27

5 Two Pizzas 35

6 The Author Leaves 43

PART TWO · The Mechanics51

7 There Is No Coin 53

8 Proof of Work in Plain Arithmetic.....61

9 Twenty-One Million.....71

10 Difficulty, Hashrate and the Ten Minutes 79

11 Keys..... 87

12 Read the Chain 95

PART THREE · What It Survived 103

13 Mt. Gox.....105

14 The Block Size War 113

15 What a Fork Proves123

16 Silk Road133

17 Twelve March 2020139

18 The Hashrate Migration147

19 The Year the Middlemen Failed153

PART FOUR · The Institutional Turn 161

20 The Twelfth of May163

21 The Corporate Treasury173

22 Legal Tender 181

23	Custody, Futures, and a Decade of Refusals	187
24	Ten January 2024	193
25	What the Chain Is For	199
26	The Energy Accounting	207
27	What Is Settled, What Is Not	213
28	The Bridge.....	221
PART FIVE · What Transfers		227
29	Regulation by Activity	229
30	Alongside, Not After.....	237
31	What Transfers	243
32	bitcoin.institute	251
33	The Quantum Question	257
34	The Clock Nobody Stops.....	265
Reference.....		271
The Dated Record		273
Appendix A · The Whitepaper, Section by Section		307
Appendix B · How to Verify Every Claim in This Book		311
Appendix C · Custody, Ranked by What Actually Happens.....		315
Appendix D · The First Purchase, Mechanically.....		319
Glossary.....		325
Further Reading		329
Sources and Attributions.....		331
What Comes Next		333
About the Author.....		335
Index		337
Reader Invitation.....		341
Colophon		343

I run a company that teaches people about markets, and I am telling you that on the second page rather than the last.

Its name is Spiking. It sells education — courses, a masterclass, a platform that tracks institutional flows. It has customers, revenue and an interest in you thinking well of me. **You should read everything that follows with that in mind**, which is easier to do when somebody says it plainly than when you find it on a website afterwards.

Here is what the company is not.

It does not sell this asset, custody it, or take a fee from anybody who does. No exchange, custodian, broker, hardware manufacturer, issuer or platform has sponsored this book, endorsed it, or been asked to. The copyright page says so in formal language and Chapter 32 explains what that costs.

And bitcoin.institute, where the maintained version of the record lives, carries no advertising and no product. Not now and not later. The prohibitions are printed in Chapter 32 so that they outlive any decision I might regret.

The reason for the separation is narrow and worth stating. **This book asks you to check its claims rather than to trust its author.** A reader who discovers, three hundred pages in, that the author is paid by somebody with a position in the subject has been given a reason to stop reading — and would be right to take it.

So: the company exists, it sells things, and none of what it sells is in these pages.

Five things before you begin, so that you can put this down now if it is not what you wanted.

There are no returns in this book.

No portfolio value, no entry-and-exit table, no chart with an arrow on it, no screenshot of an account. I took a position in Bitcoin on the twelfth of May 2020 and this book tells you the date, the instrument and the size, because all three were public at the time and can be checked. It does not tell you what any of it became. A return is a fact about a period, and whoever chooses the period chooses the fact; I set out that argument at length in Chapter 2 of *The Wall Came Down* and I have not found a reason to soften it since. The subject of this book is a record. My results are not part of it.

Every claim here can be checked against a public record.

This is the one genuine advantage Bitcoin has over every other subject I have written about. An options chain has to be printed in an appendix before you can verify anything computed from it. A reclamation project keeps its cost assumptions inside a ministry. Bitcoin's entire history — every coin issued since January 2009, every transaction, every rule change and every failed rule change — sits on a public record that anyone can read, for free, without asking permission and without an account.

So the book closes with the Dated Record: ninety-eight entries, from the thirty-first of October 2008 to the cut-off date, each carrying the handle that proves it. A block height. A transaction. A filing. A docket number. Not a citation of somebody's article about the event — the thing itself. Appendix B shows you how to pull any of them in about ninety seconds.

Which means you can check me. Not in principle — actually, on a laptop, tonight. It is the only guarantee I have to offer that is worth anything, and it happens to be a stronger one than I was able to offer in either of the previous books.

It will not tell you what to buy.

There is no price target in these pages, no forecast, no allocation percentage, no argument that you should own any of this. I have views. They are not the product. What is here instead is how the thing was built, what it has survived, what it has cost the people who held it, and enough mechanical detail that you can evaluate the next confident claim you hear without needing to trust the person making it — including when the person making it is me.

There is one appendix on the mechanics of acquiring any — the order of operations, the costs, and the errors that cannot be undone. It names no provider and contains no allocation. It is there because a reader who has decided to act should not have to learn the sequence from a mistake, and because the most expensive errors in this subject are procedural rather than analytical.

You should also know that no exchange, custodian, broker, issuer or platform has sponsored, endorsed, or been asked to endorse this book, and none will be. The copyright page says so in more formal language. It closes off a good deal of money and it is the price of the sentence above.

It names people and companies where the record is documentary.

Filings, judgments, court dockets, announcements a company made under its own name. Where something has been alleged and never proved, the conduct is described and no name is attached to it. That distinction is applied consistently and there is exactly one place in the book where it bites, which says so at the time.

This book supersedes *Spiking To The Moon*.

I wrote an earlier book about whales in the cryptocurrency market. It was a beginner's guide, written when the subject was younger and so was my understanding of it, and where the two books disagree, this one is the later view and the better sourced. I am not withdrawing it. I am telling you which one to read.

On how to read it. Part Two runs to six chapters of mechanics and contains no history, no personalities and no price. It is the part you will want to skip and the part that decides whether the rest is worth anything, because almost every bad argument about Bitcoin is a mechanical error wearing a philosophical costume.

If you are impatient, read Chapter 12 first. It is short and it asks you to verify one thing yourself, which takes an afternoon and changes how every chapter after it reads. Then come back to the beginning.

On timing. **This book states the record as it stood on the twenty-seventh of September 2026.** The most consequential piece of crypto legislation in American history passed one chamber, sat for a year, and then failed a procedural vote in the other by a single ballot — and I have written that chapter accordingly: what is settled, what is not, and the date of the last event I can verify. Nothing here is written as though a question still open had been closed. The maintained version of the Dated Record is kept at bitcoin.institute, a domain I own, which carries no advertising and no promotion of any asset.

The position I took on the twelfth of May 2020 is a matter of public record, and this book describes it. It says nothing about what I hold today, where it is held, or what any of it is now worth. The first two are questions of security, and I would give you exactly the same advice about your own. The last is a question of arithmetic, and I explained above why I will not choose that date for you.

It began with nine pages that anyone could read. Everything since has been recorded the same way, and almost nobody reads that either.

Dr. Clemen Chiang

Singapore, 2026

The book is in five parts and they do different jobs.

Part One is how the thing came to exist — the problem, the people who failed at it, the paper, and the first fortnight. Read it in order.

Part Two is the mechanics: six chapters on what a transaction is, how a block is made, where the twenty-one million comes from, and what a key actually is. **It contains no history, no personalities and no price.** It is the part you will want to skip and the part that decides whether the rest is worth anything.

Part Three is what the system survived — and, more often, what the businesses around it did not.

Part Four is the institutional turn, and it is the most American section of the book, because that is where the argument happened.

Part Five is what transfers, what does not, and what is still unsettled.

If you are impatient, read Chapter 12 first. It is short, it asks you to verify one thing yourself, and it takes an afternoon. Then start at the beginning; every chapter after it reads differently.

If you already know the subject, start at Chapter 9 and read to 12. If those four chapters tell you nothing you did not know, the rest of Part Two will not either, and you can move to Part Three.

On the Dated Record. Ninety-eight entries at the back, each with a handle. The chapters cite it by entry number. A finding list on its opening page tells you which numbers cover which years. **You are meant to open it while reading, not afterwards.**

On the appendices. A is the whitepaper in summary. B is how to pull any handle in this book — the chain ones in about ninety seconds, the court and agency ones in rather longer, and B says which is which. C is the ranked list of how people actually lose coins. D is how to make a first purchase without being sold anything.

On what is not here. No price target, no forecast, no allocation, no returns. If that is what you came for, this is the wrong book and you have lost only the time it took to read this page.

ACKNOWLEDGEMENTS

This book was written from other people's work, almost none of which was done for a book.

To the developers. The reference implementation is public, and so is every argument about it. I have read code I did not write, in a language I do not work in, and found it commented by people explaining themselves to strangers they would never meet. Chapter 4's genesis constants, Chapter 8's header, Chapter 9's supply schedule and Chapter 10's retarget were all checked against that source rather than against anybody's description of it, and that was possible only because the people who maintain it decided, from the beginning, that it should be.

To the ones who argued in public and lost. A great deal of what this book can state as settled is settled because somebody proposed the alternative, made their case at length, and was not persuasive enough. The record of those arguments is as valuable as the record of the decisions, and several chapters here are built on threads whose authors were on the losing side. **They wrote it down anyway.**

To the people who kept the archives. Mailing lists from 2008, forum threads from 2010, release tags, court filings, insolvency dockets. Somebody chose to preserve each of those, usually without being asked and usually without credit. A book that claims every one of its facts carries a handle is a book standing entirely on that choice.

To the ones who did the arithmetic first. The supply audits, the chain analyses, the address studies, the independent replications of numbers everybody else was quoting. Where this book corrects a figure that three technical references had wrong, it is almost always because somebody else had already done the work and published it where I could find it.

And to the HODLers.

The word is a typographical error. In December 2013, in a falling market, somebody posted to a forum under the title *I AM HODLING* — misspelled, at length, and by his own account not sober. The thread is still there. The word outlived the error, as words do, and came to name something the language did not otherwise have a word for.

What it names is the subject of Chapter 30 and the hardest thing this asset asks of anybody.

Not conviction, which is cheap and mostly retrospective. **Duration.** Holding something through a stretch when holding it is unfashionable and unpleasant and nothing in the design forces you to decide. Four completed cycles, four falls of at least three quarters, and two to three years back to a high each time — and through all of it, the people who simply did not sell.

They did not maintain the code or write the proposals. **But a network of nodes nobody pays, securing coins nobody has to hold, only works because enough people keep holding them.** That is not a technical contribution and it does not appear in any repository. It is, however, the reason there was anything here to write about seventeen years later.

I should say what this page is not.

Nobody named or described above was contacted about this book. No interviews were conducted, no quotations were solicited, and nobody has reviewed a word of it. The debt is entirely to published work, which is the only kind of debt a book written this way can incur — and the only kind that leaves the reader free to check it.

Where I have got something wrong, none of them are responsible. **Chapter 32 explains what happens then.**

And to the students

There were several hundred people in a room that was not a room on the twelfth of May 2020, watching me say something I had spent eleven years saying the opposite of.

Some of them are still here.

That is the part I did not expect. Not the decision itself, which is described in Chapter 20 and cost me nothing but pride. What I did not expect was that a group of people would decide to find out with me, in public, on a timetable nobody controlled, and then stay when finding out turned out to mean what Chapter 31 says it means.

They have now been through the whole of it once. The rise that made everybody feel clever. The fall of more than three quarters that took two years to come back, and the long middle of that fall when there was no information, no deadline and nothing to do — which is the hardest part and the part nobody warns you about. **And they are in another one now**, as I write this, roughly half down from a high, with the same absence of anything forcing a decision.

I taught them the arithmetic. They taught me what it costs to hold it.

Those are not the same lesson, and only one of them can be taught from a slide.

This book exists because of a crossing I did not make alone, and a fire I did not walk through alone either. **Every one of you who stayed in the water when it would have been easier to turn back — this is yours.**

And to the thousands I never met

Over those years I gave Bitcoin away. Not to students, not to customers, not to anybody who had bought anything from me — to **thousands of wallets belonging to people I did not know and will never meet.**

Small amounts each. They are still there, most of them. **Anybody can look**, which is the whole argument of this book arriving in the one place I did not plan to make it: I cannot tell you who those people are, I cannot reverse what I sent, and I do not need to be believed about any of it, because the transactions are on the chain and the chain does not care whether you trust me.

I am not going to tell you what those coins are worth now.

I know the number. It is not small. But the rule set out in the Preface applies to me most strictly where it would flatter me most — a value is a fact about a date, and whoever chooses the date chooses the fact. I did not print what my own position became and I am not going to print what somebody else's gift became either.

Almost nobody has ever come back to say thank you.

I record that without complaint, because I have thought about it for a long time and I think the absence is the point. A gift that requires acknowledgement is a transaction with a delayed invoice. These were not that. Most of the recipients have no idea who sent them anything, and a few of them will find it years from now in a wallet they had forgotten, long after they have stopped being able to ask.

The sower does not follow each seed. That was never the arrangement, in this or in anything else worth doing.

Whatever those coins become, and whoever they become it for: **it is theirs, and I would rather they never knew my name than that they felt owed.**

And at home

To Nicole, and to Yee, Le and Loong. Book One took the evenings and the weekends. This one took the mornings as well, because the record does not close at any hour and I kept opening it. **A book about a ledger nobody keeps was written in a house where the accounts are kept by somebody, and she has never once presented the bill.**

Whatever this book gets right, the duration was theirs before it was mine.

On how it was made

The text was drafted with AI assistance under my direction, and the copyright page says so in the form Amazon requires. Every handle was opened by me, every figure was checked against the record rather than against the draft, and every error that survives is mine. The book was typeset in the same three faces as Book One, set out in the Colophon, and printed and bound on demand by Amazon KDP under the Spiking Press imprint of Aly Pte. Ltd., which bears the cost of it.

P A R T O N E

How It Came to Exist

*The problem, the people who failed at it, the paper, and
the first fortnight*

Six chapters, and every one of them is about something that happened before anybody was arguing.

The first asks what money is, and arrives at an answer most of us have never been taught: a record before an object. The second is about the people who spent a quarter of a century trying to build a record nobody keeps, and the wall each of them hit. The third is about nine pages. The fourth is about a block, the fifth is about two pizzas, and the sixth is about the day the author stopped writing.

Read them in order. Everything after Part One is an argument about what these six chapters established, and it is easier to weigh the argument once you have seen the evidence.

Money Is a Ledger

Ask most people what money is and they will describe what money looks like. The two have almost nothing to do with each other.

There is a version of monetary history that most of us absorbed without ever being taught it. Barter comes first — a man with a cow and a need for grain, hunting for a man with grain and a need for a cow. The difficulty of that search produces coins, which are easier to carry than cows. Coins produce banks, because coins are heavy and thieves exist. Banks produce notes, notes produce cheques, cheques produce cards, cards produce whatever is on your phone. Each step a convenience laid over the step before it, each one solving the friction the last one left behind.

It is a tidy story, and its first step has been contested for a century.

Anthropologists have long argued that the barter economy the story requires has never been observed as a general system anywhere, and that what the record shows instead is credit arriving early — arrangements recording who owed what to whom, denominated in something standard, settled periodically or not at all. Economists have pushed back, defending the logic of the original account and questioning how much the anthropological evidence can bear.

I do not need to settle that argument, because the strongest evidence for what I want to say is not disputed by either side.

The oldest writing anybody has found is accounting.

The proto-cuneiform tablets excavated at Uruk — some six thousand of them and their fragments, from the end of the fourth

millennium BC — are overwhelmingly administrative. Not literature, not law, not scripture. Lists. So much grain received, so many animals disbursed, by whom, to whom. The standard scholarly reading is that writing appears to have emerged in response to bureaucratic pressure: somebody needed to keep track of obligations at a scale too large to remember.

That is worth a moment, because the order is the wrong way round from the one most of us assume. Writing did not produce accounting. **Accounting produced writing.** The ledger came first, and the alphabet is a by-product of it.

So:

Money is a record of obligation before it is an object, and the object is a portable summary of the record.

The stones of Yap

The example everybody uses here is the limestone discs of Yap, and I hesitated to use it because it has been worn smooth by repetition. I am using it anyway, and using a different part of it than the part you have probably heard.

The discs — *rai* — were quarried on another island and carried across open water by raft, at genuine risk. Some were enormous, too large for any individual to shift.

Ownership changed hands regularly, in settlements and exchanges and compensation, and the stones did not move. A disc sat where it had always sat and the community simply knew whose it now was.

Then Germany acquired the island from Spain in 1899, and its administrators ran into a problem familiar to every government: they wanted the footpaths repaired and the residents saw no reason to repair them. Orders failed. Fines failed.

So the officials went round the island and **painted a black cross on the stones** — marking them as belonging to the government, to be unmarked when the work was done.

The paths were repaired.

Nothing had moved. Nothing had been seized in any sense a bailiff would recognise. A government had made an annotation, the annotation was recognised by everyone who mattered, and the annotation had the force of confiscation. Milton Friedman, whose 1991 essay is why most people now know this story, drew the comparison himself: it is precisely what happens when gold sitting in a vault at a central bank is earmarked from one country's account to another's. The metal stays where it is. Somebody writes something down.

And he was not the first economist to reach for Yap. Keynes had reviewed Furness's book in the *Economic Journal* in 1915, seventy-six years earlier.

A mark on a stone is a ledger entry.

Somebody will object that gold is different, and they are right, which is why it is worth dealing with here rather than leaving it to sit.

A gold coin genuinely is not a record. It is a quantity of metal, and whoever holds it owns it, and no ledger anywhere needs to agree. That is the one form of money where the object is the whole of the title.

Which is exactly why almost nobody has settled anything in gold for a century and a half. They settled in **claims** on gold — certificates, deposits, allocated accounts, entries in a vault's book — because moving the metal is expensive, slow and risky, and moving the entry is not. The gold stayed in the vault. The ownership moved as an annotation, which is the black cross on the stone at national scale.

The two genuine exceptions in this chapter — a gold coin and a banknote in your hand — are the two instruments where possession settles the question without anybody's record. And both have been steadily engineered out of the settlement of anything large, for the same reason: **the record is cheaper to move than the thing.**

There is a second and more famous Yap story — a disc lost overboard in a storm during the crossing, which continued to be owned and traded by the family who had commissioned it, on the general understanding that it existed and was theirs at the bottom of the sea. Divers have since located stones underwater, and the anecdote is almost certainly true in outline. But I should tell you exactly what it is: an account given in 1903 to an American anthropologist by an informant, about an event two or three generations before that. It is not an observation. And it has grown in the retelling — one later economist's version has the sea flooding the site where all the stones were kept, which appears in none of the primary sources.

I mention that not to undermine the story but because this is a book about checking things, and the most-repeated illustration in monetary economics turns out to be a second-hand recollection that has been embroidered on its way to us. It would be poor form to point that out about other people's evidence and not about my own.

Your own money, described the same way

Consider a payment you have made recently. You transferred a thousand dollars from your account to somebody else's.

Nothing travelled. No object left your possession. If you and the recipient bank at the same institution, one number in that institution's records decreased and another increased, and the institution's total obligations were unchanged — it simply owed a different set of people.

If you bank elsewhere, more ledgers become involved. Your bank must settle with theirs, which happens through a further institution — a clearing system, an account at a central bank, and in a cross-border case a chain of correspondent banks each holding balances with the next. Each link keeps its own record. Each record is reconciled against the others. The "money" is the agreed state of that chain of records at a point in time.

This is not a criticism, and it is no longer slow in the way people assume. Measured across the main international network by the central banks' own committee, the median payment now completes in **under two hours**, and about half reach the beneficiary within thirty minutes.

But the average is far worse than the median, because the distribution has a long tail — and the tail is not random. That same analysis found the delay concentrates at the **receiving** bank, and that the slowest routes run into low and lower-middle income countries, where capital controls, compliance processes, limited banking hours and batch processing add hours or days.

Hold on to that for Chapter 29. A chain of ledgers is fast between the places that already have everything and slow into the places that do not. Nothing about that is a conspiracy. It is what a network of intermediaries produces when every link has its own hours, its own regulator, and its own reasons to be careful.

What it should dislodge is the intuition that a dollar is a thing. Your dollars are entries. They have always been entries. The paper in your wallet is the exception, and it is the exception precisely because it settles without anybody's ledger being consulted.

The only question that has ever mattered

Once money is understood as a ledger, the history of monetary technology collapses into one question asked over and over in different costumes:

Who keeps the book, and what stops them writing in it?

Every answer humanity produced before 2009 names somebody. A temple, whose scribes recorded the grain. A chartered bank. A central bank. A clearing house. A card network. A state.

In every case the integrity of the record depends on the honesty, competence and continued existence of an identifiable party. And the monetary failures we have records of are, overwhelmingly,

failures of that party rather than of the concept of money. Coins debased by the authority that minted them. Notes issued beyond the reserves behind them. Deposits lost when the institution holding them failed. Balances frozen, seized, reversed, or simply mistaken. Currencies destroyed by the governments that issued them — sometimes through malice, more often through desperation.

I want to be careful not to turn this into an indictment. Most keepers of most ledgers, most of the time, have done the job properly. The observation is narrower and more useful: **if you hold money, you hold a claim on a record somebody else maintains, and your ability to enforce that claim depends on institutions that were not designed with you specifically in mind.**

For most people in most decades that is a perfectly good arrangement. It is also, unavoidably, a relationship of trust — with a party you did not choose and cannot inspect.

Why the digital era sharpened this

Physical cash is the one everyday instrument where possession settles the question. Hand over a note and the transaction is complete. No third party is consulted, no record is updated, no permission is sought, and neither party need know who the other is.

Cash is being used less. In Sweden, about one in ten in-store purchases is now made with cash, after a steep fall between roughly 2010 and 2020 that has since levelled off. In Australia, cash fell from seventy per cent of consumer payments to sixty-four in three years, and from ninety-five per cent to seventy-eight for payments under ten dollars in six. The direction is the same nearly everywhere it is measured.

But here is the part that is usually left out. **Over the same period, the quantity of cash in circulation rose.** People are transacting in it less and holding more of it.

An instrument that people stop spending and start keeping is not disappearing. It is changing jobs — from a medium of exchange into something closer to a store of value held outside the system. Chapter 30 is about what that distinction costs the person doing the holding, and it is worth noticing that the oldest and least sophisticated money in your wallet got there first.

What has genuinely disappeared is cash's *role in ordinary payment*. Everything that replaced it is a claim on somebody's ledger. A card payment is a message asking a network to move an entry. A transfer is a message asking a bank. A wallet application is a message asking a company that is asking a bank.

Each of those intermediaries can decline. Not usually maliciously — a fraud rule fires, an account is under review, a jurisdiction is sanctioned, a business category is deemed too risky to serve. But the capacity to decline is structural, not incidental. It is what being the keeper of a ledger means.

So the question that the people in the next chapter spent thirty years attacking was this:

Can you have a ledger that **nobody** keeps?

Not a ledger kept by a trustworthy party. Not one kept by a regulated, audited, well-capitalised party with a good record. A ledger with no keeper at all — one that mutual strangers, some of them actively dishonest, can nonetheless agree about; where an entry once written cannot be altered by whoever wrote it, or by anyone else, or by everyone acting together.

For a quarter of a century the answer was no. The reason was a single obstinate problem with a name, and the next chapter is about the people who ran into it.

Read the Chain

If you do only one thing this book asks of you, do this. It takes an afternoon and it permanently changes how you read every claim anyone makes about this subject.

Everything in Part Two can be checked by you, today, without an account, without permission, and without spending anything. This chapter is the instruction rather than the description.

One thing before we start, because it would be absurd to leave it out of this chapter of all chapters.

Exercises one to four send you to a public block explorer, and an explorer is somebody else's website. It is a company, running software you cannot inspect, showing you what it says the chain contains. Nothing about that is sinister — an explorer that misreported the subsidy in block 210,000 would be caught within hours and has no reason to try — but you should know that in those four exercises you are trusting a website, and that the fifth exercise is the one that removes the need to.

Exercises one to four teach you what to look at. Exercise five means you never have to take anyone's word for what you saw.

One · Look at where it began

Go to an explorer and search for block 0.

You will get the genesis block. Look for the coinbase transaction — the first and, here, only transaction — and find its input script,

usually shown as a long hexadecimal string with a decoded ASCII version beside it.

Read the decoded text. The newspaper line from January 2009 is there. If your explorer shows only the hex, paste it into any hex-to-text converter; the words appear.

Then look at the output: 50 coins, to an address beginning 1A1zP1. Note that its balance is not zero — people have been sending coins there for years — and that the original 50 has never moved and never can, for the reason Chapter 4 gives.

You have now verified, personally, something usually presented to you as a story.

Two · Confirm the supply

This is five minutes and it establishes the entire scarcity argument from primary evidence.

Go to block 210,000. Find the coinbase output value. It is 25 coins.

Go to block 209,999. The same field reads 50.

Repeat at 420,000 (12.5 after, 25 before), **at 630,000** (6.25 after), **and at 840,000** (3.125 after).

That is it. You have just confirmed, from the record rather than from a chart on a website that wants something from you — and rather than from Chapter 9 of this book — that the issuance rate halves on schedule and always has.

And you now know exactly what somebody would have to change if they told you the supply could be altered. Ask them who would do it, and what would happen to everybody who declined to run their software. Chapter 15 has the answer.

Three · Take a transaction apart

Go to block 57,043 and find the transaction with a 10,000-coin output. That is the pizza, and Dated Record 7 gives you the height rather than an identifier, for the reason the Record explains.

Count the **inputs**. There are a hundred and thirty-one of them — every one a small output left over from mining, gathered up to make a single payment.

Now count the **outputs**. There is one. No change came back, because the inputs happened to cover the payment almost exactly.

Add up the inputs. Subtract the output. The difference is the fee — a shade under one whole coin. That subtraction is the whole of Chapter 7 on one screen, and the hundred and thirty-one inputs are the reason it cost what it did.

Now find the block containing it, note its height, and subtract that from the current height. **That number is how many blocks would have to be redone to reverse this payment** — the confirmation count, which Chapter 8 explained and which you can now see rather than accept.

Four · Watch it happen

Open a page showing the mempool — transactions broadcast but not yet in a block. You will see a queue, sorted by what people are paying per virtual byte.

Watch until a block arrives.

Several thousand transactions move from waiting to settled in a single event. Then the queue starts filling again.

It is the least dramatic thing you will ever see, and it is the entire system operating in front of you: the auction from Chapter 7, the ten minutes from Chapter 10, and the proof-of-work from Chapter 8, all in one screen refresh.

Five · Verify it yourself

The previous four exercises show you the chain. This one is the chain.

Download Bitcoin Core from the project's own site, and verify the download's signature before you run it. The instructions for that are on the same page, they take ten minutes, and skipping them means trusting whoever served you the file — which would be a strange way to begin this particular exercise.

You do not need seven hundred and forty gigabytes. That is the size of the full archive, and it is not what most people should run.

Set `prune=550` in the configuration file. The software then downloads every block, **checks every signature, executes every script, and builds the complete set of unspent outputs** — and afterwards discards the raw block data it no longer needs. **Pruning controls storage. It does not skip a single check.**

Total footprint in practice: **about nine to eleven gigabytes.** Any ordinary laptop.

The trade-offs are real and small. A pruned node cannot serve historical blocks to other people, cannot look up arbitrary old transactions, and going back to a full archive means downloading everything again.

And now the part I have to tell you

By default, Bitcoin Core does not check every signature.

The software ships with a setting called `assumevalid`, containing the hash of a specific historical block. Signatures in blocks before that point are **not verified**. Everything after it is checked normally.

The reasoning is practical: signature checking is most of the cost of the initial sync, and the block chosen is one whose validity nobody

anywhere disputes. It is not concealed — the block is named in the source code and updated with every release.

But it means that a default installation has not, in fact, checked everything from the beginning.

If you want that, set `assumevalid=0`. The sync will take several hours longer, and at the end of it your machine will have verified every signature in every block since 2009, on its own, having trusted nothing.

I would do it once. Not because the default is unsafe — it isn't — but because doing it once means you know the difference between a machine that verified the chain and a machine that was told most of it was fine.

What you get at the end is not a wallet. It is the position of not needing anybody's website. Your own machine has checked the rules for itself and will reject an invalid block regardless of who produced it or how much work stands behind it.

Anyone who has done this holds a different relationship to the subject than someone who has read about it, and the difference is not knowledge. It is standing.

Three things this system asks you to take on trust

Which brings me to the honest ending for this part of the book.

Part Two has been about verification, and it would be easy to close by telling you that everything here is checked by everybody, always. That is not true, and you have now met all three of the exceptions.

The genesis block was never verified by anyone. It could not be — there was nothing before it and nobody to broadcast it to. It is a constant compiled into the software, and every node that has ever started up began from it on the software's say-so. Chapter 4.

The retarget contains an error that will never be fixed. It measures 2,015 intervals where it should measure 2,016, so blocks

target 10.005 minutes rather than ten. Correcting it would require every node on earth to agree to a new rule, and agreement costs more than the error does. Chapter 10.

The default installation skips historical signature checks. Not hidden, not disputed, and switchable — but a default, and defaults are what most people run.

Three compromises. Every one of them documented, every one disclosed by the people who made it, none of them concealed, and each carrying a reason you can evaluate for yourself.

That is what trust actually looks like in a system that claims not to require it. Not an absence of assumptions — an absence of *hidden* assumptions, and a dial you are permitted to turn.

Every claim in the chapters that follow and in the Dated Record carries a handle that lets you do what you have just done here, to that claim, without asking me.

That is what the phrase *the disclosed record* is meant to mean. Not that I have been candid.

That you do not need me to be.

The chapter in one page

- Everything in Part Two is checkable today, without an account or permission.
- **Exercises one to four rely on a public explorer, which is somebody else's website.** They teach you what to look at. Exercise five removes the need to trust anyone.
- **Block zero:** decode the coinbase, read the January 2009 newspaper line, see that the original 50 coins have never moved and cannot.
- **The supply:** compare the coinbase value at 210,000 against 209,999, then at 420,000, 630,000 and 840,000. Five minutes, primary evidence, the whole scarcity argument.

- **A transaction:** inputs, outputs, change; inputs minus outputs is the fee; current height minus block height is the cost of reversal.
- **The mempool:** watch a block arrive and thousands of transactions settle at once — Chapters 7, 8 and 10 in a single screen refresh.
- **A node:** download from the project's site and verify the signature. Set `prune=550` and full validation runs in **nine to eleven gigabytes** on an ordinary laptop. Pruning controls storage, not checking.
- **The default skips historical signature checks** via `assumevalid`. Set `assumevalid=0` to verify everything from 2009 forward. Do it once, to know the difference.
- **Three things this system asks you to take on trust:** the hardcoded genesis block, the preserved off-by-one in the retarget, and the assume-valid default. All documented, all disclosed, none concealed.
- Trust here is not the absence of assumptions. It is the absence of *hidden* assumptions, and a dial you may turn.

P A R T T H R E E

What It Survived

And, more often, what the businesses around it did not

Seven chapters, and in almost every one the thing that failed was not the system.

An exchange in Tokyo. A two-year war over one number. A fork that proved what a fork proves. A marketplace, a Thursday in March, a government that could ban half the world's mining and did, and a year in which the middlemen failed one after another.

The chain produced a block roughly every ten minutes through all of it. That sentence will be true for the rest of the book, and it is the reason this part is about the businesses rather than the ledger.