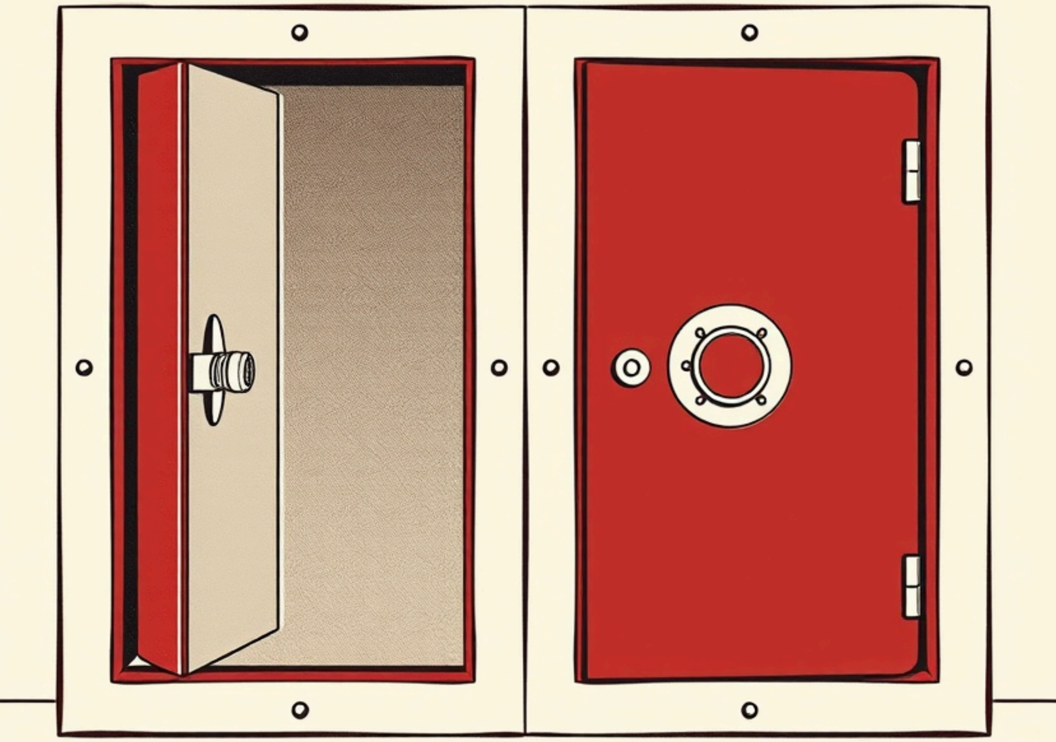
A field guide to the money you were told to fear

COMPARED TO WHAT?



The real dangers of crypto —
and the older ones already in your bank.

DMYTRO CHYSTIAKOV

COMPARED TO WHAT?

The real dangers of crypto —
and the older ones already in your bank.

DMYTRO CHYSTIAKOV

Introduction: The Deal

THERE ARE TWO KINDS of people who will tell you about crypto and neither of them is talking to you.

The first kind is selling. You know them already—the ones with the rented Lamborghini and the sunset and the word *freedom*, who have discovered that the easiest asset to sell is the feeling of having been early. They will tell you about the upside. They will not tell you what happens next, because what happens next is not in the deck.

The second kind knows what they're talking about, and writes for each other. Their work is real and it is excellent and it is unreadable, because it was never meant for you: it's addressed to investigators, to compliance teams, to people who already know what a nonce is. You could read every word of it and still not know whether to be afraid.

So there's a gap, and the gap is where everybody actually stands. Millions of people, arriving at a door, with the salesmen on one side and the specialists on the other, and no one in the middle who is neither selling nor showing off.

This is the book I wanted when I was standing there.

What this is

I spent years building a catalogue of every documented way people have lost money in this thing—hundreds of incidents, going back to 2010, each one sourced, cross-checked, and filed by mechanism rather than by drama. It is free and it is public and it is not this book. It is a reference work for professionals and it will bore you to death.

This is what the reference work *knows*, told as what it actually is: a set of stories about people, most of whom did nothing wrong.

Not a warning. Not a pitch. Not a course. **The thing I'd have wanted handed to me in one piece, at the door, before I made any of it up as I went along.**

The deal

Here is what I'm promising, and you should hold me to all of it, because a book like this is worth exactly what its worst sentence is worth.

Every number here is checkable, and the ones that aren't get thrown away in front of you. You will watch me discard my own best evidence more than once, because I have some spectacular figures available that would win arguments and that I cannot stand behind. If I use a number a vendor made up because it flatters me, you have no reason to believe any other number in the book, and you'd be right.

Every chapter has a verdict, and the verdicts don't all go one way. This is the device the whole book runs on, so here it is in advance: I take one danger in crypto, put it next to the version of that same danger already running in your ordinary financial life, and say plainly which is worse. Sometimes the answer is crypto. It's crypto in chapter two, and chapter seven, and badly in chapter eight. If every verdict came out on one side you should close the book, and so should I.

Nothing is reconstructed. Where I don't know something, I say so. There's a theft in here of $282M — bigger than anything else in these pages — that I decline to build a chapter around, because nobody can establish how it happened, and a story with the interesting parts invented is not a story, it's a lie with footnotes.

And I'm not going to tell you what to do with your money. Not once. I don't know your situation, I'm not your adviser, and the entire industry of people who *will* tell you is the reason you needed this book.

What you get

By the end you'll know what a wallet actually is and why the word is a lie. What a private key is, and why twelve words can be a quarter of a billion dollars. What a stablecoin is and what happens when the clever kind stops being clever. Why they want your passport, and what the system demanding it actually catches. How a memecoin is built, second by second, to take money from you legally. What "clean" means and why no coin has it.

And you'll know the shape of the thing, which is the part you can't get anywhere else: **that almost none of this is new.** The phone call that took $243M is the phone call your bank has been fighting for thirty years. The counterfeit hardware wallet is a skimmer in a petrol station. The memecoin is a boiler room, and boiler rooms are older than the telephone. The frauds did not arrive with crypto. They arrived with money, and they have been running, at scale, in the place you already keep yours, the entire time.

What crypto did was write them down.

That's the argument. Everything else is evidence, and there are two hundred pages of it, and you can check every line.

One thing, before chapter one

The fear that brought you here is correct.

I'm not going to talk you out of it and I'm not going to tell you it's safe. The first three chapters are the worst things in the book and they're deliberately at the front: a man losing $243M to a phone call, a system with no undo, and a decade of exchanges that turned out to be a number in somebody's database.

Read those first. If you close the book afterwards, that's a legitimate outcome and you'll have got your money's worth.

But if you stay, the question stops being *is this dangerous* — it is — and becomes the one nobody asks, which is the only useful question there has ever been about any of this:

Compared to what?

1
The Phone Call

THE FIRST CALL CAME from Google.

Not from someone claiming to be Google in the way that phrase usually goes — the bad line, the odd number, the link that lands somewhere wrong. The number on the screen was Google's. The voice knew what it was talking about. There was a problem with the account, and the man was calling to help sort it out.

By the end of that call they had his email and his cloud storage. Which is to say: they had everything he had ever written down about his money.

An hour later the second call came, and this one was from Gemini — a cryptocurrency exchange, one he actually used. The man on this call knew things. He knew which accounts existed. He knew roughly what was in them. He knew details no cold caller could know and no scammer had any business knowing, and every one of them was true, because an hour earlier the same people had taken them out of the victim's inbox.

That is the whole mechanism, and it is worth naming, because it is the difference between a scam anyone would catch and one nobody does: **each stage steals the credentials that authenticate the next.** The first call is thin and gets a little. The little makes the second call solid. The second call gets everything.

Somewhere in the second hour, on the nineteenth of August 2024, they walked him through resetting his two-factor authentication and moving his funds to a wallet they controlled. Four thousand and sixty-four bitcoin left in a single transaction. Two hundred and thirty-eight million dollars, one click. The total came to roughly $243M.

It is the largest amount of money ever taken from one person by talking to them.

A wallet is not a wallet

Two words in that paragraph — *wallet* and *left* — are doing a lot of quiet work, and if you're new here they are both lying to you slightly. Let's fix them now, because everything in this book runs on them.

A wallet holds nothing. Nothing goes into it and nothing comes out. It is not a container. What it holds is a *key* — a secret number — and what that key does is authorise the moving of coins that are recorded somewhere else. Think of it less as a purse and more as a signet ring: the ring isn't the estate, it's the thing that proves an instruction came from you. Lose the purse, lose what's in it. Lose the ring, and someone else can order the entire estate sold.

And the coins never "left" anywhere. They are in the ledger, and the ledger is where the second lie comes undone.

Picture the world's most boring book. Every page is a list of transfers — this much, from here, to there, at this second. When somebody sends money, a line gets added. That's it. That's the whole invention. There are no accounts in the sense you know, no names, no branches, no closing time. There is a list of who moved what to where, and your balance is not a number stored anywhere; it's what you get when you add up every line that ever mentioned you.

Three things about the book, and the third is why this story ends the way it does.

Nobody owns it. There is no company keeping it. Thousands of computers keep identical copies and agree, constantly, on what the next page says. That agreement — reached by machines that don't know each other and don't need to — is the thing people mean when they say "blockchain," and it is genuinely the clever part.

Nothing is ever erased. You cannot tear out a page. You cannot amend a line. A mistake is not corrected; a *new line* is added that moves the money back, if whoever holds it agrees to move it back. Nobody can reach into the past.

Anyone can read it. Not "anyone authorised." Not "anyone with a warrant." Anyone. Right now, on your phone, you can watch every transfer on earth as it happens, including the ones that just stole something. The book is written in public, permanently, and it always has been.

That last one is the strangest property in all of finance, and this chapter is about to show you both of its edges at once.

Because it's why the money left and could never come back—and it's why we know the names of the men who took it.

The man who lost it

He was a creditor in the Genesis Global Capital bankruptcy, and he lived in Washington, D.C.

The first fact is not incidental—it is why he was chosen, and it inverts the thing most people believe about how this happens. He was not careless. He was not a mark. He had not wandered in because a video told him to. He was a sophisticated institutional counterparty who had lent at scale to a lending company, and when that company collapsed, his claim became a matter of public record.

They did not find him. They looked him up.

This is the part that is hardest to hold, and the book returns to it: **finding a victim is a research problem, and the research is public.** The bankruptcy filings said who was owed. The chain said what was held and whether it had moved. In another case documented the same way, the attackers built their shortlist by scanning the ledger for large balances that had sat still for years—a dormant fortune is legible from outside, and its owner is a name attached to it somewhere.

The transparency that lets an investigator trace a theft is the transparency that lets an attacker build a target list. Nobody gets one without the other. That is not a flaw in the design; it is the design, and this chapter is where the bill comes due.

Every system worked

Here is what did not happen on the nineteenth of August.

No smart contract was exploited. No cryptography was broken. No wallet firmware was compromised, no exchange was breached, no protocol failed, no bug was found, no zero-day was burned. Nothing about the technology went wrong at any point in the two hours it took to move a quarter of a billion dollars.

Every component did exactly what it was specified to do. The wallet signed a validly formed transaction, because a validly formed transaction is what it was handed, and signing those is its entire purpose. The network confirmed it, because it was valid. The chain wrote it down permanently and showed it to anyone on earth within seconds, which is what the chain is *for*.

There is no component in that stack that failed. There is a man on a phone, and everything downstream of him working perfectly.

This is the concession the book owes before it argues anything: **there is a layer here no amount of engineering reaches, and it is the layer everything else is bolted to.** You can hold your own keys, refuse every custodian, buy the hardware, never touch a site you didn't type — and the whole edifice still terminates in a person who can be told something untrue by someone who sounds right and knows their balance.

The men who took it

They were kids.

Malone Lam was twenty. He was born in Singapore in July 2004 and grew up in Choa Chu Kang, a public-housing town in the island's west. He went to Unity Secondary School and dropped out as a teenager to spend his time trading crypto and living in the online communities that raised him — Minecraft servers and Discord.

With his roommates in Texas he co-founded, according to the federal indictment, a thing they called, without apparent irony, the **Social Engineering Enterprise**. It grew to fourteen people across several states. They worked from hacked databases, dark-web data, and phishing mail, and what they were doing was not hacking. It was calling people up.

Jeandiel Serrano was twenty-one, from Los Angeles, and went by "VersaceGod." **Veer Chetal**, who went by "Wiz," was younger still — a teenager.

A twenty-year-old who left secondary school for Discord took two hundred and forty-three million dollars from an institutional creditor in Washington by telephone, in about two hours, without breaking a single thing.

That is the sentence this chapter exists to deliver, and no part of it is exaggerated.

Then they filmed it

They live-streamed the heist to their friends.

Not as evidence. For the audience. There is a recording of the men who had just taken $243M from a stranger, watching the notifications land — the alerts, the confirmations, the money arriving — and celebrating, and talking about what came next. It was made for each other, for the reason people who have just done something enormous want the moment kept.

Then it leaked, and it became the thing that identified them.

What followed was thirty-three luxury cars. Watches. Nightclubs. Travel. It was not an attempt to get away with it; it was a spending spree conducted in public by people who did not appear to have thought past the week.

The FBI arrested Malone Lam in Miami on the eighteenth of September 2024, a month after the theft. An off-duty police officer had tipped him off that it was coming, and on his way to being arrested he threw his phone into Biscayne Bay.

Veer Chetal pleaded guilty. He forfeited nearly thirty designer watches, a wardrobe, and more than $36M in ether. Then, while out on bond awaiting sentencing for what was then the largest single-victim crypto theft on record, he lost the bond after prosecutors said he had taken part in stealing another two million dollars.

Hold all of it against the rest of the chapter, because it is the only light in here. This is a book that will spend most of its pages on people who lost money and were never told what happened to it. This one has names, ages, a video, three prosecutions, and a phone at the bottom of a bay.

The reason it has those things is the book from a few pages ago.

Here is what "following the money" actually means, because it is nothing like the phrase suggests and it is the single most useful thing a newcomer can understand.

When the $238M moved, a line appeared: *this much, from this address, to that address, at this second.* Public. Permanent. The thieves then did what thieves do — they split it three ways and started running. Fifteen or more exchanges. Bitcoin swapped for litecoin, litecoin for ether, ether for monero, faster and faster, each hop meant to break the trail.

Every hop wrote another line.

That's the trap, and it has no floor. In the world you know, following stolen money means asking. Asking a bank, which requires a reason; asking a bank in another country, which requires a treaty; waiting; being refused; asking again. Each hop is a door, and each door has a person behind it who can say no, and enough doors will exhaust anyone.

There are no doors. The ledger doesn't have permissions. A thief moving money across fifteen exchanges is not covering fifteen trails — he is writing fifteen more lines in a book that everyone can already read, and he cannot stop writing, because moving is what writing *is* here. He can make the path complicated. He cannot make it private, and he cannot make it stop being there tomorrow.

So somebody read it.

He does not go by his name, and that is deliberate, so we'll use the one he does: **ZachXBT**. His avatar is a cartoon platypus in a detective's trench coat. He is not a policeman. He is not a regulator, an agent, an analyst at a firm, or an employee of anyone. He has no training in investigation of any kind — none, not a course, not a badge, not a day. He has said so.

What he has is a grudge.

He arrived in 2017, during the boom when anyone could sell a token by writing a document about it, and he did what everyone did: he bought the hyped ones. He watched them disappear. Then in 2018 somebody hacked his wallet and took about fifteen thousand dollars, which was, at the time, a great deal of his money.

And somewhere in the aftermath of that — the specific aftermath this book has spent a chapter describing, the one with no fraud department and nobody to call — he did something almost nobody does.

He went and looked.

Not at his own theft. At the *ledger*. And what he found there was the thing everyone had been told and nobody had understood: it was all still there. Every hop the thief had made, still sitting in public, unerased, waiting. Nobody had taken it down because nobody could. Nobody had hidden it because nobody could. It was just *there,* and had been the whole time, and almost nobody was reading it.

That is the Michael Lewis moment, if you like—one person noticing something true about a system before the people paid to notice. Except it wasn't an insight about mortgage bonds. It was closer to walking into a library that everyone had been told was a vault.

He started publishing in 2021. By the time the men on that phone call took $243M off a stranger in Washington, he was the reason it took a month to name them instead of never.

By 2025 a co-founder of Paradigm put the figure he'd helped recover for victims at **over three hundred and fifty million dollars**.

A man who lost fifteen thousand and had no idea what he was doing has clawed back three hundred and fifty million for people he has never met.

No badge. No subpoena. No warrant. Nobody's permission. He read what was already public, and what will still be public in a hundred years.

He'll be back. The rest of this book keeps quietly turning on what he figured out.

(One note, since this book is about to spend two hundred pages naming people. His real name is a matter of public record—it came out in a court filing, because somebody who didn't like being investigated sued him. It is not going to appear here. He asks not to be identified, the book doesn't

need it, and there's a certain symmetry in it: the man who made everyone else's money visible is the only person in these pages whose name I'm not going to print.)

What this chapter is not

It would be easy, from here, to write the sentence that makes this bearable. That he should have hung up. That there was a rule, and he missed it.

He did not miss it. There was no moment where a careful person catches this, because by the time the second call came it *had evidence*—evidence taken from him an hour earlier, which is exactly why it was accurate. He was not fooled by a stranger who guessed well. He was fooled by a stranger who had read his mail.

And when it was over there was nothing to do. No recourse, no reversal, no authority above the transaction, because the transaction was valid and correctly formed and did precisely what it said. He watched $243M leave in a form that has no undo, and the system's correctness was the reason it could not be undone.

Some was recovered later—seizures, forfeitures, a wardrobe and a pile of watches and thirty-three cars. Most was not.

That is the fear, and the fear is correct. It is not superstition and it is not a media invention, and this book will not talk anyone out of it. **When money goes here it goes permanently, and permanence is a real property with a real cost, and the cost is exactly what it looks like.**

Sit with that for another chapter before anything gets argued. It has earned the room.

But carry two things through, because the rest is built on them.

The first is that **nothing broke.** Not a line of code, not a key, not a chain. What failed was a man believing a voice that knew his balance.

The second is that we know the names of the people who called him, how old they were, what they bought, and where the phone went in.