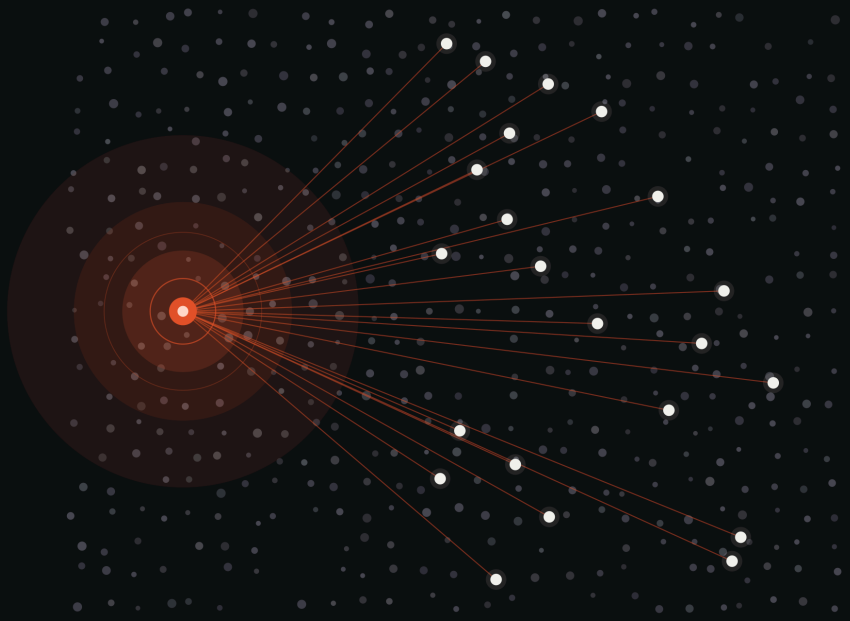
A FIELD GUIDE FOR BUILDERS

WILL NEVER DM YOU FIRST



INSIDE THE SCAM ECONOMY OF OPEN COMMUNITIES

BRUNO PIERRI GALVAO

BLOCKCHAIN ENGINEER · COMMUNITY BUILDER

Will Never DM You First

Inside the Scam Economy of Open Communities

By Bruno Pierri Galvao

Published via LeanPub. First public release: *to be set at v0.5 launch.*

Preface

This is a book about the scam economy of open communities — the sprawling, industrialized, surprisingly rational business of deceiving people in the rooms that were built to be open, and walking off with their money, their access, or their trust. It takes many forms — the impersonated admin, the deepfaked founder, the patient romance-and-investment con, the synthetic community with no real people in it — but underneath the variety it is a single business. It is about how that economy works, who runs it, what it costs the rest of us, and why two decades of clever people throwing clever defenses at it have not made it go away. It is also, by the end, a book about the direction the field is finally converging on to make it go away — not a single silver bullet, but a family of approaches that stack into something the economy has no cheap answer to.

Telegram runs through nearly every chapter, and it is worth saying plainly why — because the reason is the argument, not an apology for it. Telegram is one of the main places crypto and Web3 live — not the only one, but a central one. It is where the projects stand up their communities, where the founders and the traders and the targets all gather, where the tokens move and the deals get done. It is also the platform where the native notion of identity is thinnest: a display name, a throwaway number, and no real cost to being anyone — or to being a thousand anyones at once. Put the most instantly transferable value in history into the rooms with the weakest sense of who is actually in them, and you have not a coincidence but a laboratory: the clearest place on the internet to watch the scam economy operate at full strength. When you want to study a phenomenon at its most extreme, you go where the conditions are most extreme, and for this one that place is Telegram. So Telegram is my setting and my lens. It is the lab, not the specimen.

The specimen is something more general and more important: what happens to any open community that combines three ingredients — easy entry, weak identity, and something of value in the room. Get those three together and you get scams, and then an entire predatory economy, whether the room is a Telegram group, a Discord server, an X reply section, or a WhatsApp broadcast list. Wherever a pattern is genuinely Telegram-specific, I will say so. But most of what you are about to read is not specific to any one platform. It is structural. It would have found us on whatever app we happened to be standing in.

Underneath all of it sits a single question, and I want you to keep it in your pocket from here to the last page: *who is in the room?* Every spam message, every impersonation, every fake giveaway, every synthetic "support agent," every fabricated peer in a fabricated community is, at bottom, an exploitation of the fact that an open community usually cannot answer that question. It does not know who is talking. It cannot tell one person from a thousand puppets worn by one operator. For most of the internet's history we have treated this as an inconvenience to be patched. I am going to argue that it is the whole game.

You may already know this book's title, even if you have never seen this book. Pinned to the top of half the crypto channels on the internet, in the slightly frantic capitalization of people who learned the lesson the hard way, is a single line of advice: the admins *will never DM you first*. It is good advice. It is also a confession — a community admitting, on the way in, that it cannot tell its own founders from the impostors wearing their names and faces, so it has given up trying and asks you instead to trust no one. That pinned warning is this whole book compressed to a sentence: a thriving open community reduced to greeting newcomers with a plea to believe nothing. It is where the title comes from, and the chapters that follow are the long answer to how it came to that.

The promise

Here is what I am offering in exchange for your time. Read this book and you will understand the scam economy of open communities as a system — not as a scatter of annoyances to be swatted one at a time, but as an industry with a shape you can hold in your head and recognize anywhere you see it. You will know its history in three distinct eras, each with its own economics and its own characteristic attack. You will understand the supply chain behind a scam the way you understand the supply chain behind a product on a shelf — the tooling, the labor, the pricing, the margins. You will know, in technical detail, why every defense the industry has shipped keeps hitting the same wall. And you will know what the actual endgame looks like, why we have known about it for twenty years, and why it has not arrived yet.

That is a lot to claim. The book earns it by being concrete. Where I can show you the specific scam, the specific tool, the specific dollar figure, I will. Some statistics in this field are real and well-sourced; others are vendor marketing dressed as

research, and I will not pretend I can always tell which from the outside. When a figure comes from a company describing its own product or user base, I will label it as company-stated and unaudited, because that is what it is.

The three-era journey

The book moves through three eras, and the movement is the argument. Two inventions mark the borders between them — first cryptocurrency, then the adoption of large language models — and each one reset what a scam could be. So the eras sort cleanly by those two thresholds: the pre-crypto era, the crypto era, and the AI era we have just entered.

In the first era — the pre-crypto era — the noise in the room was mostly just noise. Annoying, voluminous, but rarely dangerous inside the community itself, because there was little to steal in a chat room about hobbies or code. This is not to say the early internet was safe — banking trojans and phishing were already draining real accounts in these same years — but that predation lived in the inbox and the browser, reaching for money held in a banking system built to claw it back, not in the open room. We got away with never answering "who is in the room?" because the stakes inside the room were low enough that the question did not seem to matter. It always mattered. We just could not see it yet.

In the second era — the crypto era — the value arrived. Crypto communities put enormous, instantly transferable value into open rooms full of strangers, and the noise turned predatory. What had been a nuisance became a way to take real crypto. And here the real shape of the problem finally became visible: behind nearly every attack is a single operator running not one account but hundreds — each a separate fake persona the room has no way to tell from a real person — and because spinning up a fresh account costs almost nothing, one human can be a thousand strangers at once. This is the Sybil problem, named after a famous case of one person who held many identities, and once you see it underneath everything, you cannot unsee it.

In the third era — the AI era — the machines became good enough to pass for human. The arrival of capable large language models, in public hands from late 2022 on, removed the last reliable tell — language itself — and let a single operator run thousands of fluent, autonomous, around-the-clock personas. Detection that depended on spotting bad content stopped working, because the content stopped looking bad. The arms race between filters and fakery became, in a precise and

demonstrable sense, unwinnable. This is the era you are living in as you read this — only a few years old, and already the one that breaks every defense the first two eras built. We are not looking back at it from safety. We are early inside it, watching it take shape, which is exactly why the question of what comes next is not yet settled.

Three eras, one escalating proof: you cannot win this by inspecting the message. The thing you actually need to inspect is the actor behind the message — whether it is a costly, persistent identity, whether that identity has earned any trust, whether a unique person stands behind it, and, increasingly, who is answerable for what it does. The back half of the book is about the family of approaches the field is converging on to ask that — why they are the structural cure rather than another patch, why the pieces finally exist, why they are nonetheless not yet assembled or adopted, and what happens to the scam economy we know today if they are. I will spoil only the direction, not the detail: if credible identity becomes expensive and reputation becomes real and actors become accountable, the economics that make industrial fraud profitable invert, and most of what fills your inbox and your group chats today goes extinct.

What this book is, and is not

This is a threat-understanding book. It is meant to make you fluent in a worldview — to change how you see every open community you walk into for the rest of your life. It is not a how-to-build-defense manual; you will not find configuration recipes or a buyer's guide. It is not a biography of Telegram or a profile of its founders; there are no chapters narrating a company's corporate history. And it is not an academic text, though it leans on serious academic work where that work is load-bearing. The voice is closer to a tired security engineer's blog than to a journal — opinionated, concrete, citation-rich, and honest about the limits of what anyone actually knows.

Why me

I am an engineer who has spent years building on Polkadot, which means I have spent years living inside exactly the kind of open, high-value, weakly-identified communities this book is about. I did not set out to write about crypto scams. I set out to help ship software. But every community I worked in — every group, every server, every channel — fought the same war, lost the same battles in the same

order, and reached for the same broken defenses. After watching it happen enough times, in enough places, the pattern stopped looking like a series of nuisances and started looking like a single unsolved problem with a knowable shape. This book is my attempt to write that shape down clearly enough that you will recognize it everywhere too.

A note on the half-life of what follows. The scam economy does not hold still — new attacks, new tools, and new numbers will land after these words do. Treat the specific figures and case studies here as snapshots of a fast-moving target, not as a current scoreboard. What endures is the structure they illustrate, and the structure is the point.

Before any of the history, though, I want to show you what this all became — the deepfaked video calls, the synthetic communities with synthetic citizens, the industry behind roughly $7.2 billion in reported crypto-investment-fraud losses in a single year — in a single room, on a single afternoon, happening to a single person who did everything right. The whole argument of this book is already present in that one incident, if you know where to look. So that is where we begin: not with the long quiet beginning, but with the reckoning.

Prologue

The message that took everything came from a friend.

That is the detail people skip past when they hear the story of J.P. Thor, a co-founder of the THORChain protocol, and it is the only detail that matters. The contact was real. The name was right. The conversation history was right. Everything that a careful person checks before they trust a stranger checked out, because the person on the other end was not a stranger at all — or rather, the account was not. It belonged to someone Thor knew, someone whose Telegram had been quietly taken over. From inside that borrowed identity, the attackers did not rush. They moved the conversation toward a video call, the kind of friction-free escalation that reads as ordinary diligence. The call, when it came, showed a face and a voice. Both were synthetic. That was September 9, 2025. By the time the math was done, roughly $1.35 million was gone.

Pull back from that single room and the pattern repeats at a scale that is hard to hold in your head. North Korean operators stole roughly $2.02 billion in cryptocurrency in 2025 by Chainalysis's count, up more than half from the year before — most of it in a single colossal exchange heist, the $1.46 billion Bybit hack. But the slice that should frighten anyone who runs a community is the work of the crew researchers track as BlueNoroff, which routed over $300 million through exactly the maneuver that took Thor's crypto: a trusted account, a pivot to a deepfaked Zoom or Teams meeting, a face you think you recognize asking you to do something you would never do for a face you didn't. Voice was enough on its own in thousands of smaller cases. As little as three seconds of audio — scraped from a podcast or a voicemail and run through a commodity cloning service — was enough to manufacture a daughter crying for bail money or a CFO authorizing a wire.

Trend Micro, working from the FBI's 2025 numbers, tied more than $5 million in losses that year to voice-clone distress scams alone, and that is only the slice that got counted.

Zoom out once more and the ground itself is moving. In 2025, Telegram banned 43.5 million groups and channels — not accounts, communities — by Check Point Research's tally of the platform's own enforcement numbers. After the platform's founder was arrested in France in August 2024 and the company's posture toward law enforcement shifted, the daily rate of takedowns climbed from a baseline of 10,000 to 30,000 into a sustained band of 80,000 to 140,000, with peak days clearing half a million. Malicious Telegram groups — the fake alpha channels, the airdrop traps, the counterfeit verification bots — surged roughly 2,000 percent between November 2024 and January 2025, by the count of the crypto anti-fraud firm Scam Sniffer. And the losses that all of this enables are no longer a rounding error in anyone's budget: the FBI's Internet Crime Complaint Center put reported crypto-investment-fraud losses — the category dominated by pig-butchering, the patient, relationship-built confidence scam that lives and breathes in these rooms — at roughly $7.2 billion in 2025.

These are not the numbers of a nuisance. What we still call a *scam* — as if it named one clumsy trick, a stranger's email, a link you should have known better than to click — has become something the word can barely hold: an industry whose product is fraud. It is staffed, capitalized, organized into specialized firms that rent each other tools and launder each other's proceeds, with research-and-development cycles faster than the defenders chasing them. It runs on stolen API keys and jailbroken language models priced like a streaming subscription. It runs on synthetic communities populated by experts who never existed and peers who are scripts. It runs, increasingly, with no human typing at all.

But here is the thing about the Thor story, and about almost every story in this book: strip away the deepfake and the billion-dollar headline, and what you are left with is embarrassingly old. A message arrives. It appears to come from someone you trust. It does not. Everything downstream — the loss, the laundering, the ruin — flows from that one unverified assumption at the top. The machinery has become spectacular. The wound is exactly the same wound it has always been.

I have spent years watching defenders pour ingenuity into the machinery and almost none into the wound. We built filters that read the words, and the machines learned to write better words than we do. We built reputation scores for accounts,

and the attackers spun up a thousand fresh ones for the price of a cup of coffee. We built shared blocklists, behavioral models, CAPTCHAs, aggressive-mode toggles, 99.7-percent-accurate moderation bots — and the flood kept rising, because every one of those tools was answering a question that was never the real question. They all asked: *is this message spam?* They almost never asked the only question that would have saved J.P. Thor his $1.35 million.

Who was actually in the room?

Not which account. Not which display name, which avatar, which verified-looking checkmark — all of those are costumes, and the costumes are cheap. Who. The human being, or the absence of one, behind the words. Whether they are who they claim to be. Whether they have ever been seen before, by anyone, doing anything trustworthy. In an open community — a place anyone can enter, where identity is a self-chosen handle and value is sitting in the room waiting to be taken — that question has no answer. It has never had an answer. We just got away with not answering it for a long time, because for most of the internet's history the rooms weren't worth robbing.

Then cryptocurrency arrived, and then the machines could pass for human, and the bill for two decades of not answering came due all at once.

This book is the story of that bill. It runs through three eras — the long quiet age before there was any crypto in the room, the violent decade when the crypto came and noise turned into predation, and the strange present in which the attackers no longer need to be human at all. It is a tour of an economy most people don't know exists, conducted in the place where it grew biggest and meanest, on the thinnest identity layer of any platform its size. And it is, in the end, an argument: that the question we keep refusing to ask is the one that actually has durable answers, that those answers have existed in scattered pieces for twenty years, and that if those pieces are finally assembled and adopted, the industry we are about to walk through goes extinct.

But none of that machinery is where the question came from, and you will not understand the answer until you understand how old the question is. It is far older than the internet. It belongs to any place where strangers gather in the open — the public square, the market, the coffee shop — where anyone may walk in and no one can say for certain who anyone else really is. So before any of the machinery, we go back there: not to a Telegram group or a crypto channel, but to that oldest open

room, the one that has been failing to answer *who is in the room?* since long before there was a wire to send a message down. We start there, where the stakes were still low enough that nobody had to get the answer right.