

The Handover and the Ledger

Blockchain, Computation,
and the Limits of Distributed Trust

Forrest Landry

UVSM PUBLICATIONS
Wytheville, Virginia

© 2026 Forrest Landry. Some rights reserved.

Published by UVSM Publications LLC
965 Reed Creek Mill Rd
Wytheville, VA 24382-8287
USA

uvsmpublications.com
contact@uvsmpublications.com

ISBN 979-8-90710-223-1

DOI: https://doi.org/10.67291/VJRC4176

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0).

You may share this work for non-commercial purposes with proper attribution, but you may not adapt, transform, or build upon it.

Full license text: https://creativecommons.org/licenses/by-nc-nd/4.0/

Author's Open Researcher and Contributor ID (ORCID): 0009-0005-6275-0362

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), except as permitted under the license above, without prior written permission of the publisher.

Contents

Preface iv

Chapter 1. The Promise and Peril of Decentralization 1

Chapter 2. How Distributed Ledgers Work 8

Chapter 3. Anonymity, Identity, and the Problem of Trust 17

Chapter 4. Bearer Certificates and the Failure of Ledger Systems 29

Chapter 5. The Decentralization Dilemma 41

Chapter 6. The Structural Critique of Cryptocurrency 48

Chapter 7. Decentralization, Ethics, and the Foundations of Governance 57

Chapter 8. Beyond Computational Infrastructure 68

Glossary 78

Bibliography 90

Index 97

Preface

This book asks one question of a technology that drew a generation of capable people: does it serve the goals that drew them? Decentralized governance, economic sovereignty, identity that serves persons rather than institutions: these were the goals, and distributed ledgers were offered as the way to reach them. The book's answer is that distributed ledgers do not reach them, and it gives its reasons in a form a reader can check and carry.

The title names the question that carries most of the weight. Every way of paying, trading or transferring something of value finishes in one of two ways. Either something is handed over, and the handover completes the transfer, as when one person hands another a coin; or a shared record changes, and the transfer exists only as that change, as with a bank balance or a blockchain. The handover needs only the two people who make it. The ledger needs a record of everyone's dealings, and a record of everyone's dealings draws those who would misuse it, however widely the record is copied.

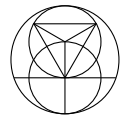
The book asks its question twice. It asks it first of ledgers: Chapter 4 shows that every cryptocurrency is a ledger, and what follows for every ledger. It asks it then of all high-technology computation, for three further reasons, each enough alone: security that rests on mathematics can be broken by later mathematics; no community can build or repair the machines; and the pursuit of efficiency carries control back to the center. Chapter 8 gathers both answers.

The book is built in two movements. Chapters 2 through 6 ask what the machines can do: how distributed ledgers work (Chapter 2), what becomes of anonymity and identity on them (Chapter 3), why the handover and the ledger differ in kind (Chapter 4), why decentralized systems drift back to a center (Chapter 5), and why cryptocurrency, built with the tools and on the infrastructure of the system it meant to escape, reproduces that

system (Chapter 6). Chapters 7 and 8 ask what people must be able to do, because every design in the first movement stays decentralized only while the people using it value decentralization more than convenience. Chapter 7 finds the depth at which the problems have to be met: the rules a community lives by have to be made by its people, and enforcing rules does not make them; the value of money rests on trust that exchange will continue, and that trust rests on a civilization and on the living world beneath it. Chapter 8 sets out what can stand where computation cannot: exchange completed in a handover, machines simple enough for a community to build and repair, identity anchored in a body present, and a culture whose choices rest on care rather than on survival.

Chapter 1 begins with what the blockchain era got right: it gathered people who cared about governance and gave them a vocabulary for finding one another. The book ends by giving those people, and anyone else, six questions to ask of the next new system, beginning with the question the title names. A warning protects a person once; the questions are a skill, and a skill protects them always.

Each technical term is explained where it first appears, and the Glossary gathers them all. Each chapter closes with a summary and a list of its key concepts.



Chapter 1. The Promise and Peril of Decentralization

On why distributed systems attracted enormous energy and enthusiasm, what genuine value emerged from that era of exploration, and why the technology has eclipsed the problems it was supposed to solve.

I. The Vocabulary of Finding

Something important happened in the years between the Arab Spring and the boom in initial coin offerings (ICOs: the sale of a newly created token to the public to raise money, often on the strength of a white paper alone, a white paper being a paper announcing a project and its plans). A community formed, not around a product, not around a company, but around a vocabulary. The language of decentralization, of distributed ledgers (shared records of transactions, copied across many computers) and autonomous organizations, gave people a way to find one another who shared a concern that the prevailing structures of governance and exchange were inadequate to the problems they could see approaching.

The technology was the occasion, not the cause. People who were genuinely interested in decentralization found a vocabulary that at least made them able to find each other. To have found, after five years of work, the people you want to work with on the problems you want to solve is no trivial thing. That is a genuine accomplishment. Even if all the technology is crap (and much of it is), the social connections it enabled have real value.

This book begins from that acknowledgment. The blockchain era produced something worthwhile: a network of people oriented toward the question of how governance, identity, and economic exchange might be

reorganized on fundamentally different terms. The question this book addresses is whether the technical approaches that brought them together are adequate to the problems they set out to solve, and what follows from the conclusion that, in most respects, they are not. Whether you were drawn to that question as someone who wrote code, joined a project, or only watched, you can follow what comes next; no technical training is assumed, and the technical terms the book needs are explained where they first appear.

II. The Attractive Basin

A flag that recurrently arises in the consideration of blockchain is the kind of risk that goes along with excitement and momentum. When something is within its window of possibility and much is moving and much immediate advantage seems available, it becomes an attractive basin for activity, whether or not it should be the attractive basin for the kinds of activity that we need. An attractive basin is a place where activity collects because activity is already there, as water collects in a low place.

This is the concern: not that blockchain is useless, but that its momentum diverts energy from the harder, less glamorous work that the situation demands. The most significant problems (identity, the representation of economic value without creating real conflicts, the question of governance at scale) are being eclipsed by the sheer velocity of coding activity.

The coders, for the most part, are taking a hard-line approach. They are moving forward rapidly, building systems at speed, without having considered many things that are important to get right. The conversation about the deeper issues is not even happening within the communities that have the technical capability to address them.

And so the energy that might have gone into solving identity, into developing governance structures, into thinking carefully about what it means to represent value in a system: that energy has been captured by the more immediately rewarding work of writing code and launching tokens.

III. The Technology Is Fundamentally Wrong

The claim is structural. (Structural here means that the outcome follows from how the system is built, whoever builds it and whatever they intend.) The technology is fundamentally wrong as a path to the goals it was supposed to serve.

If the goal is decentralized governance, if the goal is economic sovereignty, if the goal is identity that serves persons rather than institutions, then the architectural assumptions of distributed ledger technology run contrary to what those goals actually require.

This is a strong claim and requires careful statement. It does not mean that distributed ledgers are technically broken in the narrow sense of failing to do what they promise. Bitcoin does, in fact, maintain a distributed ledger. Ethereum does, in fact, execute smart contracts (programs stored and run on its shared ledger). The technology works on its own terms. It fails on the terms of the goals it was built to serve.

One question carries most of the weight: does a transaction finish when something is handed over, or only when a shared record changes? Chapter 4 shows what follows from the answer for every ledger. Three further reasons, each decisive alone, hold for any system built on high-technology computation: security that rests on mathematics can be broken by later mathematics (Chapters 4 and 6), no community can build or repair the machines (Chapter 6), and the pursuit of efficiency carries control back to the center (Chapter 5). So the book asks its question twice, first of ledgers and then of all high-technology computation, and Chapter 8 gathers both answers.

Here is the route again, the order in which the chapters develop the argument, with the terms the chapters will use. The data volumes, energy requirements, and consensus mechanisms of blockchain (Chapter 2). The structural impossibility of achieving meaningful anonymity (anonymity that survives the first link between a key and a person) within a system where every transaction is permanently visible (Chapter 3). The information-topology argument (information topology is where the information about a transaction has to be: only with the two parties, or in a record that everyone shares) that distinguishes bearer certificates from ledger systems and shows why only bearer certificates are structurally trustworthy (Chapter 4). The paradox by which efficiency-seeking inevitably produces re-centralization (Chapter 5). The specific critique of cryptocurrency as using Game A methodologies to escape Game A (Chapter 6). (Game A is the name that people of the Game B community, among them Jim Rutt and Jordan Hall, give to the present game of rivalry for money and power, played with the tools and incentives of the existing system. Game B names a hoped-for successor to it, built on cooperation.) The difference between enforcing rules and choosing them, what trust in money rests on, and the deeper question of what governance and culture would actually serve decentralization (Chapter 7). And finally, the considered conclusion that the real work lies beyond computational infrastructure entirely (Chapter 8).

IV. What Was Diverted

Cryptocurrency diverted so much energy from how we deal with the real hard problems. How do we address the big issues that the current systems never were able to address? This huge amount of energy was diverted and is still being diverted; I call this energy diversion.

The diversion took specific forms. People split from collaborative groups to go start coins. Collaborations that had been oriented toward governance, toward ecological sustainability, toward the development of ethical frameworks: these collaborations lost their most energetic participants to the ICO wave.

Someone would say: you should do an ICO, you can get thirty million dollars, it is just a white paper. And the gravitational pull of that possibility was strong enough to redirect years of accumulated effort away from the problems that had brought people together in the first place.

The loss was financial and temporal, and it was also a loss of attention. The kind of careful, patient thought required to develop new governance structures (thought that operates on a timescale of years and decades) cannot survive in an environment where thirty-million-dollar possibilities appear every quarter. The time horizon contracts. The thinking becomes shallow. The hard problems remain unaddressed.

V. The Internet Precedent

The pattern is not new. In the early 1990s, the internet was touted as a gift that would unite humanity and change the way in which humanity could collaborate and create choice-making that would be responsive to genuine issues. It had a normalizing and decentralizing effect inherently, as a protocol rather than as a platform (a protocol is a published set of rules that anyone can follow; a platform is a service one company runs).

The turn from protocol to platform began around 2001, after the dotcom crash: it was then, as Shoshana Zuboff has documented, that Google began to sell advertising aimed by what it learned about its users, and the social platforms (Facebook in 2004, YouTube in 2005, Twitter in 2006) were founded in the years just after. That transition (the move from protocol to platform) represented a fundamental shift of power. A shift that was hidden, that operated like a cult dynamic: gradually enough that people did not notice what had been taken from them until it was already gone.

Blockchain repeated this pattern at an accelerated pace. The decentralizing promise was genuine at the protocol level. But the implementations (the exchanges, the wallets, the DAOs, which are decentralized autonomous organizations whose rules are written as programs on a blockchain) rapidly centralized around the same dynamics of convenience and net-

work effects (the way a service becomes more useful as more people use it, so that people go where the people already are) that had centralized the internet a generation earlier.

The lesson is structural, not contingent. It is not that the wrong people were in charge. It is that the same dynamics reproduce the same outcomes regardless of intention. This is the argument that the remaining chapters will develop.

VI. Summary

What was gained. A vocabulary, a community, a shared orientation toward the problems of governance and exchange. These have real value and persist beyond any particular technology.

What was lost. Time, energy, and attention diverted from the harder questions. A generation of technically capable people whose problem-solving capacity was absorbed by systems that reproduce the asymmetries they set out to eliminate.

What follows. The task now is neither to abandon the community nor to persist with the technology. It is to redirect the energy (the relationships, the vocabulary, the shared concern) toward approaches that are structurally adequate to the problems that originally motivated the work. This book sets out what those structural requirements are.

KEY CONCEPTS IN THIS CHAPTER

- **Attractive basin**: a phenomenon whereby momentum and immediate advantage draw activity toward a domain, regardless of whether that domain serves the deeper goals that motivated the activity.
- **Protocol vs. platform**: the distinction between decentralized communication standards (protocols) and centralized service providers (platforms); the transition from the former to the latter represents a fundamental shift of power.
- **Vocabulary of finding**: the social function of technical language in enabling people with shared concerns to locate one another.
- **Energy diversion**: the structural tendency of exciting technologies to absorb attention and effort that might otherwise address the harder, less glamorous problems they were supposed to solve.



Chapter 2. How Distributed Ledgers Work

On how distributed ledgers work: the mechanics of blockchain, the alternative approach of Hashgraph, and the range of distributed systems including Holochain, Secure Scuttlebutt, and Ethereum.

I. The Problem of Distributed Consensus

Every distributed ledger system begins from the same structural problem: how can multiple parties, who do not necessarily trust one another, agree on a shared record without relying on a central authority?

This is not a trivial problem. In a centralized system (a bank, a government registry, a corporate database) the answer is simple: one entity holds the authoritative record, and everyone else trusts that entity. The distributed approach rejects this architecture on the grounds that no single entity can be trusted with that power.

The challenge, then, is to devise a mechanism by which consensus emerges from the interactions of many parties, none of whom individually controls the outcome. The various distributed ledger technologies differ in how they solve this problem, and in the costs they incur in doing so.

II. Blockchain Mechanics

The blockchain approach is the most familiar. A miner (a computer that competes, by doing costly computation, for the right to add the next entry) earns the right to add something to the end of the chain: a new

block containing a set of verified transactions. As soon as a miner has earned this right, he broadcasts that new block to all the rest. They, in turn, add it to their copy of the chain.

The consequence of this architecture is immediately apparent: a full copy of the Bitcoin chain was about 150 gigabytes of data in 2017 and had passed 750 gigabytes by October 2026. Every full node (a computer that keeps and checks the whole record, as every miner must have at hand) keeps one in order to check the next block-add operation. A lot of data floating around. A lot of energy required. This represents an enormous amount of waste: of bandwidth, of data storage, and of computational capability.

The waste is not incidental. It is structural. The consensus mechanism (proof of work) functions precisely by requiring that computational resources be expended. The expense is the security model. To attack the chain, an adversary would need to expend more computational work than all the other miners combined.

The expense has a second use: it is a signal that cannot be faked. A miner who adds a block shows that real energy was spent, and no one can show that without spending it. Most signals in a market are cheap to copy: a label, a review, a polished presentation can be produced without the thing it advertises. Proof of work ties the signal to the cost, so the only way to show the work is to have done the work. My book *The Displacement of Choice* develops this kind of signal as a general test of whether something is good or only looks good.

This architecture limits the transaction volume that can be recorded in any one block, because the blocks cannot be bigger than a certain amount without further increasing the already-extreme bandwidth and storage requirements. If you wanted to increase the transaction rate, you would need to distribute the blocks across multiple parties and devise a different consensus algorithm for how blocks get added. You might not want a vast number of copies of the same blockchain. You might want different partitions.

But in every case, you still need some form of transactional record-keeping that can be verified in a distributed way. The question is whether there exists a more efficient method of achieving this verification.

III. Hashgraph: Gossip-About-Gossip

Hashgraph proposes exactly such a method. The details of the method matter less than one point: consensus can be achieved through the structure of communication patterns rather than through brute-force computation. It is one of at least three proposed systems that attempt to do blockchain-type transactions with less waste; the other two, Holochain and Secure Scuttlebutt, are described in Section IV. The Hashgraph algorithm accomplishes distributed consensus through a different mechanism entirely.

Consider four separate streams of events: four computers, each belonging to a different person. Call them A, B, C, and D. Messages go back and forth between these computers at random intervals. Each node can say: I have received a message from A at such a time, and then a message from C, and then a message from D.

Over time, each node accumulates visibility to what prior nodes have reported as their internal state. This is the gossip-about-gossip mechanism: each communication carries not only the sender's own state but information about what other states the sender has already seen.

The Hashgraph algorithm then constructs a kind of voting algorithm from these visibility rules. From the future, looking into the past: each node has a transaction history of what it has seen the other nodes declare. The algorithm identifies an event in the past (a witness) that has full visibility to events prior to itself: an event that can be retroactively elected as having global visibility to the state of the system at that moment.

There is a distributed algorithm that allows each node to identify the same event as being in a position of visibility to all prior events. Because of the random nature of the communication pattern, you do not necessar-

ily know in advance which event that will be. But you can have consensus as to which one it is, after the fact. This is virtual voting: consensus without explicit ballot-casting.

The advantages are significant. The saving is in what each computer must send: no votes cross the network and no work is burned, because each computer can work out how every other would vote from the gossip it already holds. Every member still learns every event, so the record each one keeps is as large as before. Instead of a round of ballots sent from everybody to everybody, the gossip itself carries enough information to get consensus on every transaction.

This is a rough version of how Hashgraph is constructed. The details are considerably more involved; Leemon Baird published them in 2016, and the Hedera network is built on them.

IV. Other Approaches

Hashgraph is not alone in proposing alternatives. Holochain takes a different approach entirely, focusing on agent-centric rather than data-centric architecture. Each participant maintains their own chain of activity, and validation occurs through the interactions of local neighborhoods rather than through global consensus. Taken apart, Holochain is three known parts put together: a log of signed messages that each person keeps and passes directly to others (the method of Secure Scuttlebutt, below); a distributed hash table, which spreads data over many computers so that any piece can be found by its key without a central index; and a mutual credit system, in which members extend credit to one another directly and each balance records what one has given and received, with no central bank issuing money. Judged as a design for coordinating a group, it is sound, it is not built to extract rent or attention from its users, and it keeps no central keeper, and my book *The Valley Crossing* rates it, for those reasons, above systems built on one shared chain, such as many of the projects built on

Ethereum. Judged by the question of Chapter 4, whether a transfer finishes in a handover or in a record, it is still a ledger: a mutual credit balance is a record.

Secure Scuttlebutt is a protocol that was created with the capacity to do some similar things. It emphasizes social relationships as the basis of network topology: you see what your friends share, and their friends, but there is no global view.

Ethereum occupies a different niche. It uses blockchain as a foundation but treats transactions as a kind of basis for computation. Since September 2022 Ethereum has used proof of stake, in which the right to add blocks goes to those who lock up coins as a deposit, in proportion to the deposit. The change cut its energy use by about 99.95 percent and, as Chapter 3 shows, turns voting power into a direct function of wealth. You could think of it as a CPU (a central processor: the part of a computer that carries out its instructions) whose operations are distributed across a whole pile of nodes. As a single node, you cannot change how the computation is being performed. If an algorithm written on the blockchain requires a certain operation to occur, nobody can fiddle with the numbers or change the output by messing with the computer.

On conventional hardware, one could freeze the clock, use wiring to attach to memory directly, change any of the bits and values, and then turn the clock back on. The computer picks up and does not know that anything has changed, but the calculation no longer represents what it used to. The Ethereum computer is a method by which computations can be performed that nobody can, in practice, tamper with.

This is interesting in a number of respects, but it is also fairly hazardous, because it is effectively a computer you cannot unplug. If somebody wanted to stop a particular computation (if Ethereum became the basis for an artificial intelligence and all of a sudden we say: we do not want it to launch the missiles), there is nowhere to pull the plug and shut the thing down.

There is a film called *WarGames* that explored precisely this scenario. If you tried to unplug the thing, it would launch all the missiles. A program on a chain reaches the world through the people and machines that act on what its record says, such as an exchange that pays out when the record shows a sale; so whatever is wired to obey that record obeys a computer that no one can stop.

A case in which the Ethereum community did reach in shows the same point from the other side. On 17 June 2016 an attacker drained funds from The DAO, an early decentralized autonomous organization, taking about 3.6 million ether, then worth some fifty million dollars. The network did not malfunction: it did exactly what it was built to do. The contract code held an oversight of the kind any competent programmer might make, and the network ran that code exactly as written, on every node, so the mistake was carried out as faithfully as the intent. Code on an unchangeable record keeps the intention of whoever wrote it first, mistakes included, for everyone who later depends on it. On 20 July 2016, at block 1,920,000, the community changed its software so as to move the funds of The DAO, about twelve million ether in all, out of the attacker's reach and into a recovery contract, and the chain split in two over it: the unchanged chain continues as Ethereum Classic. No single node could pull the plug, but a small group of developers and miners, acting together, could rewrite the record; that is the drift back to the center that Chapter 5 describes.

The unstoppable computer is a structural hazard (more than a convenience) that the design community has not adequately reckoned with. A computer that no one can stop is a small and concrete case of a larger question: whether a machine that acts on the world can be kept under control. My book *Why AGI Cannot Be Made Safe; The Argument, Its Physics, and the One Choice That Remains* treats that question in full; it argues that artificial general intelligence cannot be made safe, and that the reasons lie in logic and in physics, not in goals. Two points from that book bear on ledgers directly. First, decentralized autonomous organizations are a ready vehicle for corporations that run with no people in them at any level: once the work, the management and the investing are automated,

the organization's rules on a blockchain are all that is left of it. Second, proposals to hold an artificial intelligence in check with a distributed ledger ask a fixed set of rules to contain a system that learns and changes; the companion volume *Why No Control Suffices* shows that a rule set of that kind cannot contain such a system for long.

V. Attacks That Bypass the Cryptography

A full catalog of the ways these systems can be attacked belongs to a technical book, because so many things matter in protecting a system from being compromised. Two kinds matter here, because they show that the cryptography is rarely the weak point.

There are rubber-hose attacks (getting a key by threatening or hurting the person who holds it), side-channel attacks (reading a secret from what a device gives off as it works, such as its timing or its power use), and all sorts of vulnerabilities that do not even have to do with the cryptographic algorithms themselves. And then one can look at how the usage of the system can be distorted in various ways. A system is broken wherever it is easiest to break, and that is seldom the mathematics. Chapter 3 comes to the same place from the other side: the cryptography can be intact while the person behind it is found.

VI. The Energy Cost

One Bitcoin transaction accounts for over a thousand kilowatt-hours of electricity (1,135 in CoinLedger's estimate for late 2025), all of it burned in computing; that is more than an American household uses in a month (about 900 kilowatt-hours, by the United States Energy Information Administration's figure for 2022). The network as a whole used about 138 terawatt-hours a year in the Cambridge estimate of April 2025, about half of one percent of the world's electricity. This fact alone (the sheer thermodynamic cost of maintaining consensus through computation) should give pause to anyone who imagines blockchain as the foundation for a global economic system. The energy budget of civilization cannot sustain that

cost multiplied across all the transactions that a functioning economy requires. The figure for one transaction is an average of what the whole network burns, and what that energy pays for is security: the expense is the security model (Section II). The security a chain needs rises with the value it holds, so a chain that carried the transactions of a world economy would hold the value of that economy, and would have to burn energy in proportion to that value. Proof of stake, which Ethereum adopted in 2022 (Section IV), cuts that cost; it keeps the shared record, and it gives the say over that record to wealth (Chapter 3).

VII. Summary

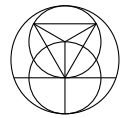
What works. Distributed consensus is achievable. Multiple mechanisms exist (proof of work, gossip-about-gossip, agent-centric validation), each with different tradeoffs in efficiency, scalability, and security.

What the costs are. Every system examined still requires some form of shared record. The data volumes, energy costs, and architectural complexities are not incidental but structural. They are the price of consensus without a trusted central party.

What comes next. This chapter describes how these systems function. It does not yet address whether they should function: whether the goals they serve are achievable by these means, or whether the costs they impose are justified by what they deliver. Those questions require examining what happens when we ask these systems to do the things that motivated their creation: identity, anonymity, governance, exchange.

KEY CONCEPTS IN THIS CHAPTER

- **Consensus algorithm**: the mechanism by which distributed nodes agree on a shared state without central authority.
- **Proof of work**: a consensus method in which the right to add blocks is earned through computational expenditure; secure but thermodynamically wasteful.
- **Hard-to-fake signal**: a signal that can be shown only by having the thing it signals, as proof of work can be shown only by spending the energy.
- **Gossip-about-gossip**: Hashgraph's mechanism whereby each communication carries information about prior communications, enabling virtual voting without explicit ballots.
- **Virtual voting**: consensus achieved through analysis of communication patterns rather than through explicit ballot-casting.
- **Unstoppable computer**: Ethereum's architectural property of being a distributed computation that no single party can halt; both a feature and a structural hazard.



Chapter 3. Anonymity, Identity, and the Problem of Trust

On the structural tension between privacy and accountability in distributed systems: how anonymity works and fails in blockchain, the transparency-opacity framework, proof of personhood, the decentralized identity trilemma, and the dimensions of trust.

I. Anonymity in a Transparent System

Can a person stay anonymous on a blockchain? Yes, it is possible within blockchain systems, and only with difficulty: blockchain is only vaguely able to achieve it. It is not good at anonymity, because of a structural feature that cannot be designed away: everybody knows every transaction that has ever been performed in the system.

All of the anonymity, therefore, belongs to whether or not you can identify any particular transaction as belonging to any particular person. Every transaction is tagged with a public key identity (a public key is the address others see; the private key is the secret that lets its holder spend from that address). That identity is associated with a private key that a person has or presumably has. If someone loses their private key, they lose the ability to spend what is held at that address, and no one else can spend it either, because at that point it is lost to the system.

The consequence is stark: if you can associate a public key with a person, then you now have visibility to every transaction that person has ever done, for all of time. Using a new key for each payment helps less than it seems to. A payment drawn from several keys shows that one person holds them all, and the change from a payment returns to a key of the payer's, so keys fall together into clusters; in one study, by Sarah Meiklejohn and her colleagues, about twelve million public keys collapsed into

about 3.3 million clusters. Tie any one key in a cluster to a person, and the whole cluster is tied to that person. The ledger forgets nothing. The anonymity of the person is binary: either the association between key and person is unknown, or it is known, and everything is exposed at once. Anonymity that survives that first link is what Chapter 1 called meaningful anonymity, and the ledger makes it impossible.

II. The Fragility of Pseudonymity

Pseudonymity is acting under a name, here a public key, that is not tied to the person. There are technologies (Bitcoin tumblers, or mixers, and applications like them) that mix up transactions, splice and dice them to try to make it harder to associate a particular public key with a particular person. But these are services built on top of the Bitcoin protocol and do not necessarily give you very strong anonymity. They are good enough for most applications, which is to say, they are good enough until they are not.

A person who is pretty careful about how they use their public key, who makes sure there is no real way to track the transactions to specific places, people or times, or to patterns that could be linked into a map of whom the person deals with, may maintain anonymity. But consider: every time a certain transaction occurs, if a certain cell phone is within one hundred feet of it, then we are pretty sure that cell phone is associated with that identity, and therefore we can figure out that person is that Bitcoin operator.

Association attacks of this kind do not require breaking the cryptography. They exploit the fact that human beings exist in physical space, carry devices that emit signals, and move in patterns that can be correlated with transaction patterns. The cryptography is intact; the person behind it is not.

Stronger systems exist. The onion-type protocol (which passes each message through several relays, each knowing only the one before and the one after; the Tor project is an example) bounces a signal around, disen-

tangling the transaction from the computer, and so the place, that sent it. This achieves much stronger levels of anonymity. But then we are in the space of asking: is strong anonymity a good thing?

There are definite cases where strong anonymity is good, and there are very definite cases where it is bad. You do not get to pick which purpose a person will use any given tool for. This is the fundamental tension.

The tension has a line through it, and the line falls where a system needs to know what happened, or who chose. Some systems need only to check what happened: that a payment cleared, that a message arrived unaltered, that a computation was done correctly, that a coin was not spent twice. There anonymity does no harm and often protects; a pseudonym bound to its consequences serves every purpose the system has. Other systems need to know who chose: who is party to an agreement, who consented, who is answerable, whose values are shaping a rule. I call the first need, to check what happened, causal verification, and the second, to know who chose, choice attribution. There anonymity corrodes, because an agreement is a relation between persons, and a person who cannot be identified cannot stand in the relation. My book *Wisdom and the Limits of System* draws this line, and *Choosing Together* applies it in layers: a person can take part anonymously at first, when little rests on what they do, and give up anonymity step by step as they gain influence over what the group decides, so that whoever holds real influence answers for it as a known person. Most designs built on ledgers, decentralized autonomous organizations among them, set one level of anonymity for everyone, whatever each person is doing, and so suit one of the two kinds of purpose and fail the other.

III. Transparency and Opacity

The language of transparency and opacity provides a more precise framework for thinking about these problems. Transparency is: information is available. Opacity is: information is not available. Think of it as another language for access controls.

The ideal architecture would allow for global anonymity while maintaining local transparency. People in your immediate peer group (those you work with) would know who you are and could verify your identity. But that identity would not be visible at a distance, not available to state actors or distant adversaries who might exploit it.

Developing a system that does this (that balances local transparency and global opacity) is not a simple thing to do. The fundamental difficulty is aggregation: anybody who can aggregate data over vast tracts of system infrastructure could take localized visibility and convert it into global visibility.

We would all benefit from getting this technical problem right. It would allow people to know who they are dealing with and understand the balance in any negotiation, without feeling that they are going to be entrapped by state actors or by distant adversaries. When someone far away has just as much access to you as your next-door neighbor, the proximal relationship is violated, and that violation is part of the reason why things have become problematic with the internet.

IV. The Failure of Resource-Based Membership

For blockchain networks to move from financial services into social and political applications, decentralized protocols for verifying unique human identities must be devised. The reason is structural: when membership, and with it voting power, comes from owning resources such as coins or computers, the people with the most of them rule. That is plutocracy, not democracy, and it is what most crypto governance has become; Siddarth and colleagues (2020) make this point.

One-CPU-one-vote, the original vision of proof of work (the phrase is Satoshi Nakamoto's own, in the Bitcoin white paper), quickly becomes one-dollar-one-vote when the cost of computation is denominated in currency. Proof of stake makes this explicit: your voting power is proportional to your wealth. Neither mechanism produces democracy. Both produce

plutocracy with a thin veneer of decentralization. Picture a vote among a thousand holders in which one holder owns more than half the coins: under proof of stake, that one holder outvotes all the others together.

The alternative is proof of personhood: verifying that a participant is a unique human being, rather than verifying that they have expended resources. This shifts the basis of membership from wealth to existence, from property to presence.

V. The Decentralized Identity Trilemma

The challenge of proof of personhood reveals a structural trilemma, which Siddarth and colleagues call the decentralized identity trilemma, taking the name from a 2019 essay that they cite as "Maciek, 2019". Three properties are desired simultaneously: sybil resistance (a Sybil attack is one person posing as many; sybil resistance prevents it), self-sovereignty, and privacy preservation. But achieving all three at once, by the design of a protocol alone, is impossible.

Sybil resistance requires that every identity within a domain be unique: no two people have the same identifier, and one person cannot obtain more than one identifier. Self-sovereignty requires that the person controls their own identity without reliance on any central issuer. Privacy preservation requires that the verification process does not expose personal information to parties who do not need it.

Any two of these can be achieved together. All three at once cannot be had from a protocol alone, for a reason the three everyday cases below show: a protocol with no body present can tie one token to one person only through an issuer who vouches, through other people who vouch by name, or through nothing at all, and each of these gives up one of the three.

Three everyday cases show the pairs. A government identity card is sybil-resistant, since each person gets one, and it can be shown without telling strangers anything more, but it is not self-sovereign: the state issues it and can withdraw it. A key you make for yourself is self-sovereign and

private, but it is not sybil-resistant: anyone can make a thousand. A public web of people vouching for one another by name is sybil-resistant and needs no central issuer, but it is not private: every name in it is exposed.

These three are the only ways open to a protocol alone. With no body present, the protocol meets a person only as information: a key, a document, a list of who knows whom. Information can be copied, so it counts a person once only if someone who knows the person vouches that there is no other copy; that someone is either an issuer or the person's peers, named. Resources such as coins or computers are no better, since one person can hold many of them (Section IV). Where nobody vouches, nothing ties the token to one person. Schemes that look like a fourth way rest on a body after all: a scan of a face or an iris needs the body at the scanner, and a test that everyone must sit at the same hour counts on one person being able to sit only one test at a time. Both are forms of the physical presence that the next section takes up. Zero-knowledge proofs (methods by which one party proves a statement true without revealing anything beyond its truth) do not make a fourth way either. They can show that a credential was not issued twice without showing whose it is, which reduces how much anyone must be trusted; the first issue of the credential still needs an issuer, named peers, or a body present.

VI. Physical Copresence as Authentication

A simple security foundation holds: real humans can only be in one place at a time. Authentication comes from being physically present at a specific place and time. When the gatherings are held at the same hour in every place, no one can attend two of them, and so no one can receive two tokens: each person is counted once.

This approach works with the physics of the world rather than against it. Pseudonym parties (gatherings at which each person present receives one anonymous token, a mechanism proposed by Bryan Ford and Jacob Strauss in 2008) provide significant accountability, since membership

rights are limited and can be revoked, while preserving a high degree of anonymity (the point is Siddarth and colleagues'). The identity is anchored in the body, not in a database.

Take the three properties of the trilemma in turn. One body in one place gives each person one token: that is sybil resistance. The token is issued by the gathering of peers, not by a central issuer: that is self-sovereignty. The token carries no name: that is privacy. Physical presence is the way through the trilemma that mathematics alone does not provide. What the token is made of is a further choice. It can be a physical object handed over at the gathering, which is the bearer form of the same idea, or a key registered there. A key's later use rests on mathematics, and the first reason of Chapter 8 reaches it; the count of one person to one token still rests on the body present.

The way through has a price, and the price is paid locally. In the design for proof of personhood that Maria Borge, Bryan Ford and their colleagues built on pseudonym parties in 2017, the people at each gathering trust that at least one of its organizers witnesses the count faithfully, the gatherings in different places trust one another to have been held at the same hour, and each body is seen by the people in the room at the moment its token is issued, though a face may be covered. Trust in at least one organizer is the one-of-many model of Section VII below (a system that works as long as any one of many actors does what is expected), held gathering by gathering: close to zero trust, and trust in people one can see. Measured against the three properties as this chapter defines them, the gathering meets all three. Measured against a stronger sense of anonymity, anonymity even toward the people in the same room, the gathering gives up anonymity toward the room; my book *Wisdom and the Limits of System* uses that stronger sense, and so finds that the trilemma holds in a room as well, at a price paid locally and briefly. The two accounts describe the same gathering and the same price.

The price buys something that grows more valuable as machines grow more capable. Online, a program can pass as a person, and the largest Sybil attack possible is to replace the human members of a system with

machines acting in their names, so that people stop counting as economic actors at all. A body in a room cannot be replaced that way. The binding of one person to one identity is best made where agreements are first made, in person, before any ledger records anything: decentralization requires distributed authority, and it does not require that people be turned into records.

VII. The Dimensions of Trust

Trust is the use of any assumptions about the behavior of other people. (The definition and the labels of the models below are Vitalik Buterin's, from his essay "Trust Models", 2020.) It admits of analysis by what this book calls trust dimensions: how many actors must behave as expected.

The *one-of-one* model is centralized: a single entity is trusted entirely. Banks, governments, and corporate platforms operate in this mode. The risk is total: if that one entity fails, everything fails.

The *all-of-many* model (*n-of-n*, in Buterin's labels) is dystopian, in Buterin's word: every actor must behave as expected, with no backups. A single defection breaks the system. This is impractical for any real application.

The *majority-of-many* model (*n/2-of-n*) is how blockchains work: a majority of participants must behave honestly for consensus to hold. The system becomes more valuable the larger the number of participants gets, because corrupting a majority becomes progressively more difficult.

The *few-of-many* model (*few-of-n*) requires that at least some small fixed number of actors, fewer than half, behave as expected. It sits between the blockchain model and the one-of-many model.

The *one-of-many* model (*one-of-n*) requires only one actor among many to behave as expected. This is much closer to zero trust than the blockchain model: it requires only that one participant who follows the rules exists somewhere in the system.

The *none-of-many* model (*zero-of-n*) works as expected without any dependence on external actors. This is the trustless ideal, and it is approximated only by bearer certificates (anything, like cash, whose possession is ownership and whose handover completes the transfer; Chapter 4 examines them) and physics-based authentication, not by any distributed ledger system.

A payment in cash and a payment through a bank show the two ends. When I hand you a banknote, the payment depends on no one else behaving as expected: that is the none-of-many model. When my bank moves the money, the payment depends wholly on that one bank: that is the one-of-one model.

The six models, side by side:

Model	**Whom you must trust**	**Example in this book**
One-of-one	A single entity, entirely	A payment through a bank; governments and corporate platforms
All-of-many (*n-of-n*)	Every actor, with no backups	No real application: a single defection breaks the system
Majority-of-many (*n/2-of-n*)	A majority of the participants	A blockchain
Few-of-many (*few-of-n*)	At least a small fixed number of actors, fewer than half	None here; it sits between the blockchain model and the one-of-many model
One-of-many (*one-of-n*)	At least one actor among many	The organizers of a pseudonym party, at least one of whom witnesses the count faithfully (Section VI)
None-of-many (*zero-of-n*)	No one	A banknote handed over; physics-based authentication

These models count whom a system must trust to keep its record correct. That is trust in infrastructure, and a protocol can secure it for as long as the mathematics under the protocol holds (Chapter 4, Section II). A second kind of trust is the confidence that someone will accept the coin tomorrow, next year, in a decade: trust in the continuing possibility of ex-

change. That is cultural trust, and no protocol reaches it. A blockchain secures trust in infrastructure by building a system in which no participant needs to trust any particular other, only a majority of all of them (the majority-of-many model above). Where strangers under adversarial conditions must keep one shared record, that does the job of keeping the record; Chapter 4 shows why exchange itself should not rest on such a record at all. The blockchain works around the absence of trust and does nothing to build trust where it is absent; my book *The Reach of Trust* shows what that costs when the same stance is taken toward the people closest to us. Chapter 7, Section III, takes up the second kind of trust and what it rests on.

VIII. The Monopoly on Identity

While the state holds the monopoly on the legitimate use of physical force (as Max Weber defined it, in his lecture "Politics as a Vocation", 1919), the surveillance state or surveillance capital is the monopoly on identity. Today, to prove you are a person, you hand over private details, and the companies and states that collect them become monopolies on identity (Siddarth and colleagues call them credential monopolies); that threatens democracy. A website that will not let you in until you give it your telephone number is a small case of the same thing: the number ties the account to a person the telephone company can name.

Proof of personhood systems that rest on a body being present, such as pseudonym parties, counter this logic by creating building blocks of a human-centered economy where individuals directly control and have governance rights over their networks. The best of these technologies do not try to abstract away subjectivity (human judgment); they embrace it "as a necessity, and strength", in the words of Siddarth and colleagues.

IX. Summary

What the analysis reveals. Anonymity in blockchain is not a design feature but an accident of incomplete association. It is fragile by construction. The structural requirement for global state means that any breach of pseudonymity is total and retroactive.

Where anonymity belongs. Anonymity serves a system that needs only to check what happened, and harms a system that needs to know who chose. Influence over a group's decisions calls for a known person who answers for it.

Where hope lies. In the direction of physics-based authentication, proof of personhood that rests on a body being present, and architectures that balance local transparency with global opacity. These approaches work with the constraints of the physical world rather than trying to overcome them through mathematics alone.

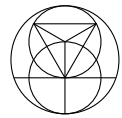
The deeper problem. The dimensions of trust reveal that blockchain's majority-of-many model is far from the zero-trust ideal. Bearer certificates and physical presence achieve closer approximations to structural trustlessness than any distributed ledger mechanism.

The question to carry. Does this system know a person by a body present, or by resources held?

What comes next. Chapter 4 asks why a ledger must hold what it holds, and finds that the answer lies in how a transaction is completed.

KEY CONCEPTS IN THIS CHAPTER

- **Association attack**: identifying a pseudonymous user by correlating transaction patterns with physical-world signals (location, timing, device proximity).
- **Transparency and opacity**: the framework of information availability vs. information concealment, used as an alternative vocabulary for access controls.
- **Proof of personhood**: verifying that a participant is a unique human being, as an alternative to proof of work or proof of stake.
- **Decentralized identity trilemma**: the structural tension between sybil resistance, self-sovereignty, and privacy preservation, which no protocol alone can meet all at once; physical presence, as in pseudonym parties, meets all three as this chapter defines them, at a price paid locally: trust in at least one organizer at each gathering, gatherings held at the same hour, and each body seen in the room.
- **Causal verification and choice attribution**: the two things a system may need to know about an action: that it happened correctly (where anonymity does no harm), or who chose it (where anonymity corrodes).
- **Trust dimensions**: the spectrum from one-of-one (centralized) through majority-of-many (blockchain) to none-of-many (trustless), characterizing how many actors must behave honestly for a system to function (the definition and labels are Vitalik Buterin's).
- **Infrastructure trust and cultural trust**: confidence that a system keeps its record correctly, which a protocol can secure for as long as the mathematics under it holds, and confidence that exchange will remain possible and meaningful, which no protocol reaches (Chapter 7).
- **Monopoly on identity**: the surveillance state or surveillance capital as the monopolistic controller of credential mechanisms.



Chapter 4. Bearer Certificates and the Failure of Ledger Systems

On the two fundamental methodologies for transactions, the information topology that distinguishes them, and why ledger systems (including all cryptocurrencies) are structurally untrustworthy.

I. The Two Kinds of Money

Are there really only two kinds of transaction methodology? Setting aside the question of what unit of account is used, and focusing instead on the structural methodology by which a transaction is effected, there are exactly two kinds.

The first is the bearer certificate. You have it, it cannot be duplicated, and you hand it over. This category includes not only paper currency but gold, copper, coins, and in principle any physical item used as a medium of exchange, even a car driven to someone's house and handed over. The defining characteristic is that possession constitutes ownership, and the transfer is local and complete.

Consider what this means. When I hand you a coin, no third party needs to know. No record needs to be updated. No network needs to be consulted. The transaction is between us, entirely contained in physical space, and the moment the coin changes hands it is done. The information about this transaction is local to the parties involved and need never propagate beyond the immediate context.

The second is the ledger system: some methodology changes how records are updated, and the records represent the overall market action within a particular group or community. The transaction is not effected by physical transfer but by a change in the record. Without the record changing, the transaction has not occurred.

Every cryptocurrency ever devised is a ledger system. Bitcoin is a ledger. Ethereum is a ledger. Every token, every coin, every chain: all of them are record-based systems in which the transaction exists only as a change in shared state.

A reader may ask whether this is too stark, since there are surely hybrid systems. Hybrids exist in implementation but not in fundamental structure. A system either requires that some shared record be updated for a transaction to be considered valid, or it does not. If it requires the record, it is a ledger system, regardless of how cleverly the record is distributed. If it does not (if the transfer is complete in the physical handover itself), then it is a bearer certificate.

Two cases test this, and the test sorts both. The first is a ledger that hides who paid whom: David Chaum's electronic cash, conceived in 1982 on blind signatures (a way for an issuer to sign a token without seeing it), the shielded transactions of Zcash, used since 2016, and other coins built for privacy, such as Monero. By the test these are ledgers: the issuer, or the chain, must record each token as spent. Their records hide the parties and the amounts, but the record is still global and permanent, and its privacy rests on mathematics; when that mathematics is broken, the entire system fails at once, retroactively and completely, as Section II below shows. A hidden ledger is a honeypot whose lock has a date on it (a honeypot is a store of valuable information that draws those who would misuse it; Section IV below). The honeypot is there from the first day, because anyone can copy the record now and read it on the day the lock fails. And the fees that keep such a record running are collected whether or not anyone can read it, which is the rent-seeking of Section IV. The second case is a bearer object that sits on a ledger: a sealed device holding the private key to a

coin, handed over in person. By the test, the handover is a bearer transfer, since no record changes, and the coin behind it remains a ledger entry. The test sorts transactions, not products, and that is what makes it exact.

The same test sorts the systems that seem to have no chain. Holochain keeps no single global chain, but a transfer in it is valid only once it is recorded in the parties' own chains and published to the table of records that the participants share; by the test, it is a ledger. Payment channels, such as the Lightning Network, settle most payments off the main chain, but each payment changes a record that the two parties share, and settlement changes the chain itself; by the test, they are ledgers too.

A further case is the tab. Two neighbors keep a notebook of who owes whom, or a shop carries a customer until payday. By the test, nothing has been paid while the notebook changes. The notebook records a promise, and the transaction is still open; it finishes when something is handed over, and the handover needs no notebook. Where a community stops settling and lets balances stand as its money, as a mutual credit system does (Chapter 2, Section IV), the record has become the transfer, each member's balance has to be kept where the members can all rely on it, and by the test it is a ledger. A promise becomes a balance at the point where the parties stop settling.

The cases of this section, sorted by the test:

Case	**Does a shared record have to change?**	**Result**
A banknote handed over	No	Bearer transfer
Gold or copper handed over	No	Bearer transfer
Bitcoin	Yes: the chain	Ledger
Zcash, shielded	Yes: the chain records each token as spent, with the parties and amounts hidden	Ledger (a hidden ledger)
Chaum's electronic cash	Yes: the issuer records each token as spent	Ledger (a hidden ledger)
A sealed device holding a key, handed over in person	No, for the handover; the coin behind it is a ledger entry	Bearer transfer riding on a ledger entry
Holochain	Yes: the parties' own chains and the table the participants share	Ledger
A payment channel, such as the Lightning Network	Yes: the record the two parties share, and the chain at settlement	Ledger
A tab between neighbors	The notebook records a promise; the transfer finishes in a handover	An open promise, settled by a bearer transfer; a ledger once balances stand as money

The classification is not about technology. It is about information topology (where the information about a transaction has to be). And information topology determines everything that follows.

II. The Immutability Requirement

Each system has to guarantee something in order to function. Both systems share a requirement of immutability, but they achieve it by different means.

Bearer certificates must be impossible or prohibitively difficult to duplicate. It is precisely the difficulty of printing gold or forging a dollar bill that gives these instruments their value as currency. If anyone could print them, they would be worthless. The immutability is physical: it resides in the material properties of the object itself. Gold is hard to synthesize. Currency paper is hard to reproduce. The security model is grounded in physics.

Ledger systems have an analogous requirement: not just anything can make an update. The record must be protected against unauthorized modification. This is the basis of the double-spending problem (making sure that the same unit of value cannot be spent twice) that all distributed ledger technologies attempt to solve. The immutability is informational: it resides in the cryptographic and consensus mechanisms that prevent unauthorized changes to the record. The security model is grounded in mathematics.

Note the difference carefully. Physics-based security degrades slowly: it requires physical access, physical capability, physical effort at a scale that is observable and interruptible. Mathematics-based security can fail catastrophically: if the algorithm is broken, or if enough computational power is brought to bear, the entire system fails at once, retroactively and completely.

A reader may say that the mathematical security of modern cryptography is extremely strong. It is strong today. Whether it will be strong tomorrow is a function of mathematical progress that cannot be predicted. Gold that was hard to make in 1800 is still hard to make today. A cryptographic algorithm that was secure in 2000 may not survive the next advance in quantum computing or number theory. The time horizons are

fundamentally different. The one cipher proved unbreakable shows the same difference from the other side: the one-time pad, a key as long as the message and used only once, which Claude Shannon proved perfectly secret in 1949, protects a message and yet rests on no mathematical difficulty at all; its security lies in a key carried by hand, which is a physical handover.

A reader may point out that paper money is issued by a central bank, so that cash too depends on trusting one institution. The issuer's power sits in the instrument, not in the transfer. A central bank can print more notes, and so lower the value of each one, and it can withdraw a series of notes; that is trust placed in the issuer of the instrument. On the night of 8 November 2016 the government of India withdrew the legal tender status of its 500 and 1,000 rupee notes, about 86 percent of the value of the cash in circulation. The power is real, and it belongs to the issuer: what failed in India was the issuer's promise, and no note was copied or broken. But the bank cannot see a handover of cash, cannot stop it, and cannot reverse it; the transfer itself depends on no one. Gold and copper have no issuer at all.

A reader may also ask about serial numbers, by which cash can be traced too. The difference between the instrument and the transfer answers this. A serial number lets a note be traced only where someone records it, as a bank does when the note passes through its hands; that record is a ledger built beside the cash, not part of the handover. Two people who hand a note from one to the other write nothing down, and the handover is complete without any record.

A reader may also ask about theft: if possession is ownership, does a thief who takes a coin own it? Stealing a coin takes a person at a place, one coin purse at a time, and that effort can be seen and stopped. The theft reaches only what that person could reach and carry. An attack on a shared record reaches every entry at once, from anywhere. And a ledger's power to reverse a theft is the power a small group used over The DAO (Chapter 2, Section IV): whoever can undo a theft can undo anything else.

III. Local Against Global Information

The critical structural difference between the two systems is where the information has to be. The decisive difference is in the information topology. Bearer certificates require only local information. The parties to a transaction need know nothing about any other transaction anywhere in the world. There is no global state to maintain, no reconciliation to perform, no record to synchronize.

This is a structural property (more than a convenience), with profound consequences for privacy, sovereignty, and resilience. A system that requires only local information cannot be surveilled at a distance. It cannot be shut down by disabling a server. It cannot be corrupted by compromising a central point. It is robust in the deepest sense: its operation does not depend on anything beyond the immediate participants.

Ledger systems, by contrast, always require global information and may not even maintain local information. The change is not represented solely in the parties' own systems; it is represented in a shared record, and reconciliation is needed to prevent one party's system from doing something the other party's system cannot verify.

This means that for a ledger system to function, there must exist somewhere (whether centralized or distributed) a record that contains information about all transactions in the system. That record is, by definition, a concentration of global information. And a concentration of global information is a target.

IV. The Honeypot Problem

Can any organization be trusted with global transaction information? The experience of surveillance capitalism has demonstrated conclusively that no centralized repository of information can exist without being misused. A ledger copied to every node does not escape this. Distribution changes who holds the record, not what the record holds: every full copy holds every transaction, so whoever holds a copy holds the whole honeypot. A

public chain is a honeypot left open to anyone who downloads it, and the analytics firms described below read it in exactly that way. A honeypot of global transaction data will invariably attract one of three pathologies: extortion, rent-seeking, or extraction through misuse of information.

Extortion: whoever controls or can access the record gains leverage over everyone whose transactions are in it. The threat need not be explicit: the mere possibility of exposure creates a power asymmetry that can be exploited.

Rent-seeking: whoever mediates access to the record can charge for that mediation. Transaction fees, gas fees (the fees paid to run a transaction or program on Ethereum), validation costs: these are the rents extracted by those who maintain the ledger. The distributed character of the ledger does not eliminate this dynamic; it merely distributes the rent-seeking among miners or validators rather than concentrating it in a bank.

Extraction: the information in the record is itself valuable. Transaction patterns reveal purchasing habits, social connections, economic status, geographic movement. This information can be sold, correlated, and used for purposes the transacting parties never consented to and cannot prevent. Whole companies now do this for a living: blockchain-analytics firms, the best known of them, Chainalysis, founded in 2014, sell the tracing of public ledgers to governments and exchanges.

This is not a contingent failure of particular institutions. It is a structural consequence of concentrating global information in any organization. The incentives are too strong and the opportunities too numerous for any governance arrangement to reliably prevent abuse.

The conclusion follows directly: ledger systems are structurally untrustworthy. Bearer-certificate systems (which require no global information) remain the only sound basis for exchange. This is the fundamental argument in favor of cash, generalized beyond paper currency to any transaction methodology in which the transfer is local and the information is local.

V. Quantum Methods and the Three Directions of Attack

This section is for the reader who wants to see what quantum computing does to the cryptography that guards a ledger. A reader who is content with Section II's point, that mathematics can be broken by later mathematics, can go on to the Summary without losing the thread. Section II said that a cryptographic algorithm may not survive the next advance in quantum computing. What does quantum computing do to the cryptography that guards a ledger? Speaking as a security analyst and as a mathematician: cryptography has three branches. The first is the hash function (a method that turns any data into a short fingerprint of it). The second is symmetric cryptography (in which the two parties share one secret key). The third is public key cryptography (in which each party has a pair of keys, one published and one kept secret, so that strangers can exchange secrets and check signatures without first sharing a secret). Shor's algorithm (a method, found by the mathematician Peter Shor in 1994, by which a quantum computer quickly solves the problems of number theory, factoring large numbers and its relative, the discrete logarithm, on which most of the public key cryptography in use today rests) disables a substantial number of the public key functions, and that has enormous implications for our current economic infrastructure.

The cryptographic community has been scrambling to develop public key algorithms that are not susceptible to Shor's algorithm or its relatives, and some in that community doubt that such algorithms are even possible. The first standards for such algorithms were published in 2024 by the National Institute of Standards and Technology (Chapter 8, Section II), and those standards also rest on the difficulty of mathematical problems. Whether classical public key cryptography (public key cryptography that runs on ordinary computers) can be made resistant to quantum methods is still an open question.

There are cryptographic methods that depend directly on quantum substrates (hardware whose working rests directly on quantum physics), such as the methods that use the no-cloning theorem (the result of quantum physics that an unknown quantum state cannot be copied exactly), and these methods would enable a new kind of public key infrastructure. But their cost, their energy needs and their fragility put them out of reach of better than ninety-five percent of the public, so they are more the idea of a replacement than a replacement. Protocols that use a quantum computer to generate fresh random bits are an example of such methods. Anywhere hard randomness (randomness that no one can predict) is part of the infrastructure, you are assuming that the randomness is perfect, and assuming that the bits come, as claimed, from the physical substrate that produces them. So even the quantum methods carry an assumption that someone has to trust, and the person relying on them usually cannot check it.

One more danger comes into view when the attacker is no longer a person. Such systems can resist quantum computing because they depend on quantum substrates, but I do not see that this changes the dynamics of concern here, which are these. If an artificial intelligence uses quantum computing as part of its mechanism, then distributed ledger technology is risky from three directions at once: classical hacking; nanotech intrusion (entry into a machine by devices built at the scale of molecules; no substrate can block all nanotech intrusion out); and now Shor's algorithm and quantum methods. Anything that depends on algorithms or causal mechanisms that are breakable from any classical point of view is too risky to contemplate from a security point of view.

VI. Summary

What the chapter establishes. Every method of transaction is either a bearer certificate, where the handover completes the transfer, or a ledger, where the transfer exists only as a change in a shared record. Every cryptocurrency is a ledger.

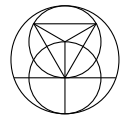
What follows. A bearer certificate needs only local information; a ledger needs global information. A record of global information, held in one place or copied across many machines, is a target that draws extortion, rent-seeking and extraction. The record of a ledger is guarded by mathematics, and Shor's algorithm, run on a quantum computer, disables a substantial number of the public key functions that guard it. If an artificial intelligence uses quantum computing as part of its mechanism, a ledger is risky from three directions at once: classical hacking, nanotech intrusion, and quantum methods.

The questions to carry. Does a transaction finish in a handover, or only in a change to a shared record? Does its security rest on physics, or on mathematics that a later advance can break?

What comes next. If ledgers fail because they gather information, a natural hope is to keep the ledger and spread its control widely. Chapter 5 shows why spread control does not stay spread.

KEY CONCEPTS IN THIS CHAPTER

- **Bearer certificate**: any transaction methodology in which possession constitutes ownership and transfer is effected by physical handover of an item that is impossible or prohibitively difficult to duplicate; requires only local information.
- **Ledger system**: any transaction methodology in which the transaction is effected by a change in a shared record; requires global information and reconciliation.
- **Immutability requirement**: the shared structural requirement of both systems: bearer certificates must resist duplication, and ledger entries must resist unauthorized modification.
- **Information topology**: the critical distinction between local-only information (bearer certificates) and global information (ledger systems), which determines the trustworthiness of the transaction methodology.
- **Honeypot**: a record of global transaction data, held in one place or copied across many machines, that structurally attracts extortion, rent-seeking, and information extraction.
- **Double-spending problem**: the fundamental challenge of ledger systems: ensuring that the same unit of value cannot be transferred twice through unauthorized modification of the record.
- **Shor's algorithm**: a method by which a quantum computer quickly solves the problems of number theory on which most public key cryptography in use today rests; it disables a substantial number of the public key functions that guard ledgers.



Chapter 5. The Decentralization Dilemma

On why decentralized systems tend to re-centralize through user convenience, the inverse relationship between learning curves and adoption rates, and why the pursuit of efficiency and scale produces exactly the asymmetries that decentralization was supposed to prevent.

I. Saturday Afternoon

Imagine that you have decided to stop using a company's email and to run your own. You give it a Saturday afternoon. By evening the server runs, and your messages are landing in other people's spam. You give it Sunday. On Monday you have work to do, and the company's service is still there, free, and it has never once asked you for an afternoon. Why does decentralization end this way so often, and why does it not take a villain to end it?

The decentralization dilemma arises from the interaction of three relevant concepts: the user learning curve, the user adoption rate, and user convenience. These three forces operate in tension, and their interaction produces a predictable outcome that contradicts the intentions of decentralized system designers.

Two central factors decide how these three play out: the relative difficulty of running your own server as an absolute beginner, and the difficulty of learning how to do so. These factors determine whether a decentralized system will remain decentralized in practice or will centralize under the pressure of ordinary human behavior.

II. The Learning Curve Inversion

The learning curve of any decentralization technology is inversely related to its adoption rate. The harder something is to learn, the fewer people will learn it. This seems obvious, but its consequences are severe and underappreciated.

Every decentralized system asks more of its users than the corresponding centralized alternative. Running your own email server is harder than using Gmail. Running your own Mastodon instance (Mastodon is a social network made of independently run servers) is harder than using Twitter (now X). Running your own cryptocurrency node is harder than using an exchange.

The centralized alternative exists precisely because someone has taken on the complexity on behalf of the user. They offer convenience in exchange for control. And convenience always wins, not because people are lazy, but because time and attention are finite, and most people have problems to solve that are not the problem of maintaining infrastructure.

III. The Convenience Trap

When faced with the dilemma of running their own server versus using existing infrastructure, the user will always choose the latter for convenience. This is not a moral failing. It is a rational response to the constraints of a finite life. That is the default: it holds wherever nothing in the person's culture weighs sovereignty above the hours it costs. Section VI below asks what can change the default.

Without specific steps taken, there will eventually be a re-centralization as a side effect of convenience. Some people will assemble to take advantage of others by charging rent. The most well-run versions of any decentralized service will attract the most users, and the system will centralize around those well-run instances just as surely as the internet centralized around Google, Amazon, and Facebook.

The crypto world has already run this experiment. Many people who bought coins never ran a node or held their own keys; for convenience, they left both with an exchange. When the exchange FTX failed in November 2022, its customers found that what they held was an entry in FTX's own records, and the entries could not be paid. (The case also shows Chapter 4's point in miniature: the customer's "coin" was a ledger entry inside a ledger entry.) The same drift reaches the rules themselves. When the Ethereum community reversed the theft from The DAO in 2016 (Chapter 2, Section IV), a small group of developers and miners decided what the shared record would say.

Convenience chosen in the present will result in eventual costs in the future. But the costs are deferred and the convenience is immediate, and human decision-making consistently discounts the future in favor of the present.

IV. Efficiency as the Engine of Asymmetry

Decentralization takes effort. It takes a certain amount of energy. It creates robustness. But in one sense, it is not efficient. And this is precisely the point at which the dilemma becomes acute.

Whenever someone says “let us make it more efficient”, somewhere that added efficiency is going to produce a surplus of resource, and that surplus is going to go as profit to someone.

To think about scale, to think about efficiency, to think about the ways in which we can effectively gain some leverage: these are all techniques by which asymmetries emerge. They raise the Gini coefficient (the Gini coefficient is a measure of inequality, zero when everyone has the same and one when one person has everything). The very tools of optimization that seem neutral or beneficial are the mechanisms by which wealth concentrates and power centralizes.

This is not a critique of efficiency per se. It is a structural observation: in any system that permits the accumulation of advantage, efficiency is the mechanism by which that accumulation occurs. Efficiency is, in this

sense, an engine of asymmetry. The efficient actor outcompetes the inefficient one. The efficient provider displaces the distributed ones. The efficient platform absorbs the protocol.

Bitcoin's mining shows the engine running. One-CPU-one-vote was the original vision (Chapter 3, Section IV). The race to do the work more cheaply moved mining first to specialized machines, whose largest maker held 82 percent of their market in the Cambridge study of April 2025, and the three largest makers more than 99 percent; and then into pools, six of which were mining more than 95 percent of the blocks in April 2025, by one analyst's count from the chain's own data. No one chose this. Each step was the efficient thing to do.

A reader may ask whether the surplus could be shared instead, as a cooperative shares what its members save together. Among the people who run a system, it can, where their culture holds the default off (Section VI below); the surplus of making the machines the system runs on still goes to whoever owns the plants that make them (Chapter 8, Section II). That is what the question of who collects the surplus is for.

V. The Paradox of Game A Escape

The deeper form of the dilemma is this: the tools and incentives of the existing system (what some have called Game A) cannot be used to escape that system, because they reproduce its asymmetries at every scale.

Cryptocurrency sought to escape centralized finance. But it did so using the tools of finance: markets, speculation, token economics, returns on investment. These tools do not produce different outcomes merely because they are applied in a different context. They produce the same outcomes (concentration, exclusion, hierarchy) because those outcomes are structurally inherent in the mechanisms themselves.

The blockchain world has reproduced within itself every pathology of the financial system it sought to escape: insider advantages, speculative bubbles, regulatory capture by the wealthy (a regulator coming to serve those it is meant to regulate), and the conversion of technical knowledge

into economic power. This is not an accident. It is the predictable consequence of using Game A methodologies to try to produce Game B outcomes.

VI. Robustness Rather Than Efficiency

What a decentralized system needs are robust solutions that are actually inefficient, and that do not necessarily, at least initially, look like they are about scale at all.

This is a counterintuitive conclusion. Every instinct of modern design pushes toward efficiency, toward scale, toward optimization. But those instincts were formed within a system that rewards exactly the dynamics we are trying to escape.

A robust system is one that continues to function under adverse conditions. A robust decentralized system is one that resists re-centralization even when centralization would be more convenient. Such a system must be designed to be difficult to optimize, because optimization is the vector through which centralization enters.

This means accepting that decentralized systems will always be slower, more effortful, and less convenient than their centralized alternatives. The coin of Chapter 4 is the instructive case, because a handover is not a system that anyone runs. Two people together can finish a payment in a moment, with nothing to run and nothing to learn. What a coin costs is carrying it and getting it across a distance; Chapter 8 takes up that cost. The question is not how to make them competitive on efficiency grounds; that competition is one they cannot win without sacrificing the property that makes them worth building. The question is how to make people willing to bear the additional cost of genuine decentralization. The answer is cultural, and the rest of the book gives it: a community that values sovereignty over convenience, the discernment of Chapter 6, and the attunement of Chapter 7. The complement to technical design is cultural commitment: a community that values sovereignty over convenience, robustness over efficiency, and long-term autonomy over short-term ease.

VII. Summary

The structural finding. Decentralization is not self-sustaining. It requires continuous expenditure of effort to maintain against the gravitational pull of convenience and efficiency. Any system that does not explicitly design against re-centralization will centralize.

The implication for design. Systems designed for genuine decentralization must be designed for robustness, not efficiency. They must accept their own inefficiency as a structural feature, not a bug to be fixed. They must resist the pressure to scale because scaling is the mechanism through which the dilemma resolves in favor of centralization.

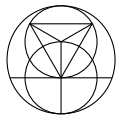
The implication for culture. Technical design alone cannot solve this problem. A technology that is merely available will be used conveniently, and convenient use leads to centralization. The complement to technical design is cultural commitment: a community that values sovereignty over convenience, robustness over efficiency, and long-term autonomy over short-term ease.

The question to carry. Does efficiency here produce a surplus, and who collects it?

What comes next. If spread-out systems drift back to the center, it matters who can build and repair the machines they run on; Chapter 6 asks that of cryptocurrency.

KEY CONCEPTS IN THIS CHAPTER

- **Decentralization dilemma**: the structural tendency of decentralized systems to re-centralize through the dynamics of user convenience, efficiency-seeking, and the inverse relationship between learning curves and adoption rates.
- **Learning curve inversion**: the principle that the difficulty of a decentralization technology is inversely related to its adoption rate, ensuring that easier centralized alternatives always attract more users.
- **Convenience trap**: the dynamic whereby users rationally choose centralized services over self-hosted alternatives, producing re-centralization as an emergent outcome of individual rational choices.
- **Efficiency as asymmetry engine**: the structural observation that optimization and efficiency-seeking produce surplus, and surplus concentrates into asymmetry and power differential.
- **Robustness over efficiency**: the design principle that genuine decentralization requires accepting inefficiency as a structural feature, since efficiency is the vector through which centralization enters.



Chapter 6. The Structural Critique of Cryptocurrency

On why cryptocurrency uses Game A methodologies to attempt to escape Game A, the need for low-tech infrastructure that communities can maintain sovereignly, the distinction between physics-based and math-based security, and the critique of tokenomics as an expression of domination culture.

I. The Wrong Runway

Cryptocurrency is like an aircraft on approach. It is going for the wrong runway, and the runway has problems. There is a big crack in the middle of it, and it will tear your landing gear off. It is not a good place to land.

This is the summary assessment, blunt because the situation warrants bluntness. Cryptocurrency, with all its energy and momentum, is aimed at a destination that cannot support what arrives there. The navigational system needs adjustment: not toward a slightly different runway in the same airport, but toward a fundamentally different landing field.

Most of the people in crypto are there for the money. The minority who are not think they can out-circumvent Game A (the present game of rivalry for money and power) while using Game A methodologies, and in that exact sense they are naive. The technology is built on Game A substrates. You cannot escape a system by using the tools of that system, because those tools carry the logic of the system within them.

II. The High-Tech Dependency

Crypto is built on a very high-technology computational infrastructure. This means that there is no community in the world that can maintain it: not intrinsically, not in any sovereign way.

Consider what is required to run a blockchain node. You need modern processors manufactured in billion-dollar fabrication plants. You need an operating system maintained by a corporation or a large community with decades of accumulated expertise. You need network infrastructure that depends on submarine cables, satellite systems, and internet service providers that are themselves centralized entities subject to state control.

No community (no village, no region, no small nation) can manufacture these components. No community can maintain the full stack of dependencies that cryptocurrency requires. The sovereign capacity to operate the system does not exist at any scale below the multinational corporation.

This is not a contingent limitation that will be overcome by better engineering. It is a structural consequence of the complexity of modern computation. Any system that depends on that complexity is dependent on the entities that control it, which are, without exception, centralized institutions operating within Game A.

The dependency is also a fragility. A chain runs on processors made on other continents, on power grids, and on supply chains whose parts are specialized and slow to replace. A single severe disruption to the electrical grid, of the kind a strong solar storm could cause, could take that infrastructure away for years, and no amount of decentralization in the rules protects against a failure in the machines the rules run on. A way of governing is only as resilient as the layer where its rules are run, as well as the layer where they are written; my book *Choosing Together* makes this point of the decentralized autonomous organization. Money that runs on machines is only as resilient as those machines. In a breakdown, cryptocur-

rency fails before paper money does, because it needs more of the civilization around it: the chips, the power, and the networks, as well as the willingness of others to accept it.

III. The Low-Tech Alternative

I prefer, therefore, to achieve the same kinds of things (decentralized autonomous organizations, distributed coordination, sovereign economic exchange) but by using low-tech: eight-bit compute, or maybe sixteen-bit compute, or basic thirty-two-bit compute using simple infrastructure. Things that can be inspected directly.

Not relying on massive layers of some corporation-mediated language or platform-defined systems, either in hardware or operating system or firmware. We have to get clear of those dependencies if we have any chance of getting out from under the gun.

A system built on eight-bit compute can be understood by a single person. Its behavior can be verified by inspection of the hardware. Its manufacture can be accomplished without billion-dollar fabrication plants. The 6502, the eight-bit processor of the Apple II, the Commodore PET and other early home computers, has been rebuilt, transistor by transistor, from 3,218 individual transistors, and a college student has made integrated circuits of a hundred transistors each in his home garage. The rebuild shows that the design of such a processor is small enough to lay out by hand and to watch working, one transistor at a time, though its parts are still bought. The garage shows that the making of the parts can begin at home, with homemade equipment and no clean room. Put together, the two give a measure of the distance: thirty-three of those hundred-transistor chips would hold all the transistors of the rebuilt 6502. The operation of such a system does not depend on any external party's continued cooperation. It achieves sovereignty not through cryptographic complexity but through structural simplicity. This is low-tech sovereignty.

Picture a cooperative that keeps its accounts on such a machine. The machine sits in a locked room in the cooperative's own building and has no network connection. To change a record, a person has to be in that room, where the members can see who comes and goes; a change made from a distance is impossible, because there is no distance from which to make it. The security comes from physical isolation, the subject of the next section, and not from a cipher that a new algorithm could break. These accounts remember transfers; they do not make them. A member has already been paid, in a handover, before anyone writes it down, and if the machine burned, the payment would stand. By the test of Chapter 4, a record of this kind is a memory and not a ledger. It holds only the cooperative's own dealings, and it is kept where the people it describes can see who touches it. Where members carry balances with one another, each balance is a promise, open until it is settled in a handover (Chapter 4, Section I). The locked room protects against people, who must come into the room to make a change. It is no defense against the artificial intelligence of Chapter 4, Section V, whose devices built at the scale of molecules no substrate can wholly keep out; that danger reaches every machine, simple or not.

IV. Physics-Based Rather Than Math-Based Stabilization

Can man, machine, and nature be rightly oriented (the question my book *The Geometry of Man, Machine, and Nature* takes up in full) with crypto as a tool of decentralization? The answer is not so much crypto in the sense that it depends on math for stabilization as technology that depends on physics for stabilization: embodied physics. Stabilization here means what keeps a system's records and rules from being changed by anyone not entitled to change them. Physics-based stabilization is that protection when it rests on physical properties of the world; Chapter 3 applied it to identity as physics-based authentication, and Chapter 8 calls the systems built on it physics-embodied systems. Two kinds of physical security are at work here. A law of physics, such as a body being in one place at a time, does

not degrade at all. A physical instrument, such as a coin that is hard to copy, degrades slowly, and only through effort that is physical, observable and interruptible (Chapter 4).

Math-based stabilization means that the security of the system rests on the difficulty of certain mathematical operations. If those operations become easier (through advances in algorithms, quantum computing, or sheer computational power), the security fails. The failure is catastrophic and retroactive: everything that was once secure is now insecure, all at once.

Physics-based stabilization means that the security of the system rests on physical properties of the world. Physical isolation. The difficulty of being in two places at once. The impossibility of duplicating a physical object without detectable evidence. Being in one place at a time is a law of physics and does not degrade with time, and none of these properties becomes vulnerable to mathematical advances. Against mathematical advances, they are as secure today as they were a thousand years ago and will be a thousand years hence.

This is crypto in a different way. It is based more upon physical isolation than upon digital cryptographic isolation. The shift is fundamental: from trusting mathematics to trusting physics: from abstractions that can fail all at once to embodiments that cannot fail all at once.

V. The Tokens and the Culture That Launched Them

Chapter 1 described how the ICO wave pulled people out of collaborative groups oriented toward governance problems and into the coin-launching business. The tokens they launched had a second problem.

The tokenomics models (the rules a token's designers set for how many tokens exist, who gets them and when), generally speaking, do not work. The economic policies embedded in token designs are created by people who are not central bankers and do not have the training to under-

stand monetary policy. The math does not work. This was clear to anyone with mathematical training who examined the underlying economics: the theory does not make mathematical sense.

The Terra token UST shows the failure in one case. UST was meant to stay worth one dollar because its rule let anyone exchange one UST for one dollar's worth of a sister token, LUNA, made new for the purpose; and UST was advertised as paying as much as 20 percent interest through the Anchor Protocol, a lending program built on Terra. The promise of one dollar rests on a circle. A dollar's worth of LUNA is worth a dollar only while people want LUNA, and people wanted LUNA because they wanted UST: each token was worth something only because the other was. That circle is what I mean by mathematics that does not work: the value of each term is defined by the other, and nothing outside the pair sets either. When holders sold UST in May 2022, the rule made more and more LUNA to buy it back, and the more LUNA was made, the less each was worth, until the price of both fell close to zero.

I now say something about the people, and I mean it as a statement about what a certain kind of offer selects for: an offer of easy wealth draws those who cannot refuse it. But beyond the technical failure of the models, there is a deeper cultural failure. The ICO wave, and the wave of NFTs after it (non-fungible tokens: ledger entries recording ownership of a unique item, often a digital image), are expressions of domination culture: my coin is going to be bigger than everybody else's, the best, the first: the domination culture's testosterone-fueled dream of reaching the top in a single step.

People who do not have the emotional development and spiritual development to resist the temptation of easy wealth are not getting sorted into the real decentralized movement. They are getting sorted out of it: into the coin-launching, hype-driven world where the next pump is always just around the corner and the underlying problems remain permanently unaddressed.

VI. The Displacement of Discernment

The deeper damage is not financial. It is epistemic (concerning how people come to know things). When a veteran who has seen the pain of people who made mistakes (releasing their "shitcoins", getting nowhere, and going through all the legal trouble) passes that pain on to newcomers as a harsh warning, there is a risk: you are displacing their capacity to be discerning and sensitive in the future.

That means they are vulnerable to the next cryptocurrency hype thing that comes along. They have not learned the skill of discernment. They have merely been warned about one specific danger. The warning protects them once; the skill would protect them always.

The distinction matters because the crypto space produces a new hype cycle every few years. Bitcoin, then Ethereum, then ICOs, then DeFi (decentralized finance: lending and trading run by programs on a blockchain), then NFTs, then the next thing. Each cycle captures energy from people who were warned about the previous cycle but lack the underlying discernment to recognize the pattern in its new form.

Discernment can be practiced on people as well as on projects. A young field draws three kinds of people at once: those doing original work at real depth, those who have convinced themselves of things that will not survive contact with reality, and those who have learned the surface signals of expertise without its substance. In the blockchain space all three spoke the same vocabulary of decentralization and self-sovereign identity, and an outsider could not tell them apart by what they claimed. They can be told apart by how they talk. The poser makes easy, obvious mistakes, the kind a competent listener catches at once. The disoriented thinker shows no contact with the known hard difficulties of the problem being claimed. The person doing real work inquires: asks real questions, follows them, and can say which questions are the right ones to ask. These

tests need no expertise in the field; they need attention to the shape of a conversation. My book *Narrative, Memory, and Neurodivergence* sets out the method in full.

VII. Summary

The structural critique. Cryptocurrency fails not because of technical bugs but because of architectural assumptions. It depends on high-tech infrastructure that no community can maintain sovereignly, and it fails first when that infrastructure fails. It uses Game A methodologies to attempt Game B outcomes. It produces the asymmetries it was designed to prevent.

The alternative direction. Low-tech infrastructure. Physics-based rather than math-based security. Systems simple enough to be inspected directly. Approaches that achieve sovereignty through structural simplicity rather than cryptographic complexity.

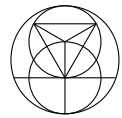
The cultural requirement. It is good to hope. But it is also a good thing to have the conversations to get people rightly oriented. The work is not to perfect the technology but to develop the discernment (both individual and collective) that prevents the next attractive basin from capturing the energy that should go to the real work.

The question to carry. Who can build and repair the machine it runs on?

What comes next. Simple machines and physical security are necessary and not sufficient; Chapter 7 asks what the people who use them must be able to do.

KEY CONCEPTS IN THIS CHAPTER

- **Game A substrates**: the high-tech, corporation-dependent infrastructure on which cryptocurrency is built, which embeds the logic and power structures of the system it claims to escape.
- **Wrong runway**: the analogy for cryptocurrency's trajectory: approaching a destination that cannot support what arrives there.
- **Physics-based stabilization**: security grounded in physical properties of the world (isolation, non-duplicability, presence) rather than mathematical difficulty; not subject to catastrophic algorithmic failure.
- **Low-tech sovereignty**: the principle that genuine community autonomy requires infrastructure simple enough to be manufactured, maintained, and inspected without external corporate dependencies.
- **Displacement of discernment**: the process by which hype cycles and external warnings substitute for the development of genuine epistemic skill, leaving people perpetually vulnerable to the next cycle.
- **Tests of discernment**: telling original work from self-deception and from posing in a young field by how people talk: the mistakes they make, their contact with the known difficulties, and whether they inquire.



Chapter 7. Decentralization, Ethics, and the Foundations of Governance

On why platforms cannot do what needs to be done, the hierarchy from finance through infrastructure to culture and ecology, why enforcing rules is not governing, what trust in money rests on, the concept of triplication as the resolution of polarization, and attunement as an epistemological method for collective wisdom beyond individual experience.

The chapters so far asked what the technology does. This chapter asks what people must be able to do, because Chapters 5 and 6 found that no design keeps decentralization in place unless the people using it value it more than convenience.

I. The Platform Problem

What went wrong with the internet's promise of decentralization? As Chapter 1 described, the internet started to become taken over around 2001: the transition from protocol to platform. There was a lot of hype about the internet at that point, about how it would unite humanity and create the capacity for democracies to be far more potent in terms of how they could operate as a decentralized autonomous organization (of course, that language was not used then).

Platforms are fundamentally not able to do the things that need to be done, because the move from protocol to platform was a hidden shift of power (Chapter 1, Section V). The things that need to be done are the making of rules by the people who live under them and the keeping of

choice in their hands. A platform answers to whoever owns it, and the shift of power put the rules in the owner's hands; so the people a platform serves cannot use it to make their own rules.

If the problem goes deeper than the technology, at what level does it lie? Working at the level of finance is not addressing the fundamental problems. We have to get down to the level of infrastructure. And then below that to culture. And then think about the relationship between culture and ecology.

If we want to understand how we got to where we are today, and what would be needed in order to get to a place where we had actual clarity about what it means to be decentralized in a way that is robust, we have to think at a depth that the technology conversation does not reach.

Finance is the shallowest layer. Infrastructure is beneath it. Culture is beneath infrastructure. And ecology (the relationship between human communities and the living systems they depend upon) is beneath culture. Governance problems cannot be solved at the finance level. They cannot be solved at the infrastructure level alone. They require attention to culture, and culture requires attention to ecology. Call this the hierarchy of finance, infrastructure, culture and ecology. Chapter 1 told this story to show the pattern; here it shows the depth at which the pattern has to be met.

Cryptocurrency shows the hierarchy at work. It is a change at the layer of finance, built on the existing internet and the existing legal system, and it has reproduced the concentration of the financial system it meant to replace. A new form of money on old infrastructure is absorbed into the old infrastructure's logic, and new infrastructure cannot be conceived until a culture has the ideas to conceive it. My book *The Aerodynamics of Civilization* traces this dependency from finance down through infrastructure to the ideas a civilization holds about itself.

II. Governance Is Not Enforcement

What can a blockchain do for a group that wants to govern itself? It can enforce rules. A blockchain, a smart contract, a decentralized autonomous organization: each is very good at keeping an agreement once it is written, and at carrying out exactly what the code says. Being good at enforcing agreements is a different thing from being good at finding which agreements should be made. A fast and efficient car is no help if it is headed for a wall; an efficient way of enforcing contracts is no help if the contracts are the wrong ones.

Enforcement is a complicated problem: given the rules, carrying them out can be specified in advance and computed. Governance is a complex problem: deciding which rules should hold means weighing competing values among people whose situation changes as they decide, and no specification written in advance settles it. (A complicated system has many parts arranged predictably, as an engine has; a complex system behaves in ways that emerge from its parts and cannot be fully predicted from them, as an ecosystem or a culture does.) A ledger is a sophisticated answer to a complicated problem. Governance needs an answer to a complex one. Verification replaces trust in the other parties with proof: it can confirm that a transaction happened and that the rules were followed, and it cannot say whether the rules themselves serve the whole community.

From this follows the governance paradox of blockchain. A blockchain can enforce rules, and it cannot determine who makes them. Before a community has solved the problem of governance, a blockchain only automates whatever distribution of power already exists, since someone still writes the rules it enforces. Once a community has solved it, and can make and keep just rules, the blockchain adds nothing that a conventional record, kept by the same trusted process, would not do as well; and either kind of record is still a ledger, with the costs Chapter 4 describes.

MakerDAO, a decentralized autonomous organization running a currency on Ethereum, met the paradox in practice. Its smart contracts could carry out decisions, and the decisions it most needed (about the effects on its community, about the ripple effects in the economy, about growing from a small team into an institution) could not be written into the contracts in advance. The DAO of Chapter 2 showed the same thing from the other side: when its code was exploited, the only remedy was a decision made by people, outside the code. Code can carry out a decision; people still have to make it.

Where people make their agreements matters as well. People mostly form relationships and agreements in person, in small groups, and then keep them up at a distance, rather than the reverse. The forming of agreements comes first: the questions and conversations through which a group finds what it values and becomes coherent around it. That work cannot be turned into code, because what matters to a group is discovered by the group as it goes, not given in advance. Governance and enforcement both have to be solved; treating them as one problem, or solving only the second, guarantees failure. I set this out in the documents gathered in *The Ephemeral Group Process Papers*; *Civilization Design and Conscious Sustainable Evolution* states the paradox, and *The Architecture of Choice* records the MakerDAO case.

III. What Trust Rests On

Chapter 3, Section VII, distinguished trust in a system's record from trust that exchange will remain possible. The claim that cryptocurrency is trustless rests on trust in the record: its proponents hold that the protocol guarantees that no one has falsified the record, and the guarantee holds for as long as the mathematics under it holds and no group able to command the network chooses to rewrite the record, as one did over The DAO (Chapter 2, Section IV). Trust that exchange will remain possible is the confidence that someone will take the coin tomorrow. A perfectly kept record of tokens that no one will exchange for anything is a perfectly useless

record. The value of a token is not in the mathematics; it is in the shared belief of everyone involved that the token can be exchanged, and that belief is cultural.

What money is shows why. As a unit of account, money names what can be chosen. As a medium of exchange, it carries the trust that choosing will still be possible. As a store of value, it moves a present choice into the future. In each role, what money stands for is choice: a claim on a future action. The claim is worth something only if the future holds a working marketplace, people willing to trade, and a civil order that makes exchange possible.

So every currency, paper or crypto, rests on the civilization that makes exchange possible. Where a civilization fails, all of its currencies fail, paper and crypto alike. Weimar Germany, Zimbabwe and the Confederacy each show a currency failing with the civil order behind it, at the scale of one state, and in each the holders of the failing money fled to a currency backed by a civil order that still held; Zimbabwe gave up its own dollar in 2009 for the United States dollar and the rand. At the scale of the one global marketplace there is no other civil order to flee to. Even if the Bitcoin network kept running through such a collapse, it would record, perfectly, the ownership of tokens no one wants.

The mistake is the one Section II found in governance: a complicated instrument asked to secure a complex foundation. The token, the ledger and the protocol are the complicated part of money; the belief that makes them money lives in the complex system of a civilization. Engineers are trained to solve problems of infrastructure, so an unreliable currency looks to them like a problem of infrastructure. It is a symptom of a civilization under strain: of governments that have lost their citizens' trust, of institutions that serve narrow interests, of a culture fraying under inequality, extraction and ecological damage. No protocol reaches those causes.

That puts the remedy at the depth Section I found. If the value of money rests on civilization, and civilization rests on the living world, then the soundest store of value is what makes exchange possible at all: the

soil, the water and the forest themselves, whose capacity to feed and shelter people lasts whether or not any registry records who owns them, and from which a civilization rebuilds. What lasts is that capacity; a deed to a woodlot is a claim on it that a civil order honors, and a buyer still uses one. Restoring a woodlot, tending farmland, or supporting a trust that cares for a watershed invests in that capacity directly. This recommendation concerns money as a store of value. Within a working civilization, cryptocurrency still serves some uses as a medium of exchange, such as transfers across borders and resistance to seizure of the coins by an authoritarian state; those uses rest on the same civilization, and the tracing of Chapter 4 still reaches the people who make them. My book *What Trust Rests On* develops this account of money and trust in its first chapter.

IV. Polarization and Triplication

Polarization can be a gateway to triplication. When two positions oppose each other, you look for a synthesis. It is the idea of thesis, antithesis, and synthesis: the triad of terms named by Fichte and usually attached to Hegel's dialectic (reasoning by opposed positions). Once you learn the synthesis, you have transformed the polarization, and therefore it becomes a gateway to yet another process.

With luck you learn the technique, because that synthesis can itself be treated as a new polarization, and then you do it again. At that point a meta-order process begins (a process that works on the process before it), and it asks a new question: can we actually hold triples fundamentally? Here things get interesting. To hold triples fundamentally is to take the three terms (thesis, antithesis and synthesis) together as the basic unit of thought from the start, instead of reaching the third only after the first two have opposed each other. Triplication names the whole of this: the repeated resolution of polarizations, and the holding of the triple that the repetition teaches.

How does this apply to the polarizations in the decentralization space? The polarization between centralization and decentralization is itself an instance of thesis and antithesis. The centralized approach: one authority, efficiency, control. The decentralized approach: distributed authority, robustness, freedom. Each defined in opposition to the other.

The synthesis is not a compromise between them. It is not half-centralized and half-decentralized. It is a third thing that resolves the opposition by operating at a different level. This is the opposition every earlier chapter has met: the shared chain against the bank, the self-run server against the platform, the token vote against the institution. Each time, the answer this book has given is a third thing on a different level: the handover in place of either kind of record (Chapter 4), the body present in place of either the issuer or the key (Chapter 3), a culture that values sovereignty in place of either design of machine (Chapters 5 and 6), and the making of agreements in place of their enforcement (Section II). The synthesis for decentralization as a whole is distributed coordination that does not require a ledger, that does not require consensus, that operates through culture and relationship rather than through computation and protocol.

Once you hold the triple (thesis, antithesis, synthesis) you can treat the synthesis as a new thesis. And find its antithesis. And seek the next synthesis. This recursive process is how understanding deepens. It is how design evolves beyond the false choice between the two obvious options.

V. Decentralization and Group Wisdom

Why does decentralization matter beyond the technical question of system architecture? Life is too short for us to learn all the lessons that we need to learn. The kinds of problems we are trying to solve are multi-generational kinds of issues. And to that extent, we have to become wiser than ourselves in a specific sense.

This is why decentralization is so interesting: a group can hold wisdom in a different way than an individual can. A group can integrate experience across multiple lifetimes, across multiple perspectives, across multiple failure modes. No individual can hold all of that. But a group (if rightly structured) can hold what no individual member knows.

The interest in decentralization, therefore, is epistemological as well as technical (epistemological: concerning how people come to know things, as with the epistemic damage of Chapter 6). It is about the conditions under which collective intelligence can exceed individual intelligence: not through voting, not through averaging, but through the structural capacity of a well-organized group to integrate more information than any of its members possess individually.

A reader may observe that most decentralized systems do not seem to produce collective wisdom, and seem instead to produce collective confusion. A group whose members can learn from one another's experience (Section VI below) is wiser than its members; spreading a group across many machines does nothing, by itself, to what the group knows. The capacity for people to take on ideas in a trustable collective sense (rather than through some reputation score or prestige status) is what gives me hope. If hope is to be placed anywhere, it is in that capacity, the human capacity for collective insight that does not require any individual to be omniscient, and not in the technology, the coins or the protocols.

VI. Attunement as Epistemological Method

Chapter 6 said that a warning passed on from a veteran's pain protects a newcomer once, and that the skill of discernment would protect them always. How can one person learn from another's experience without going through the same suffering? If a group is to hold more than any member knows, its members must be able to learn from each other's experience, and that is a matter of how people learn, not of software. I say this part in the first person, because this method can only be described from inside it. What do I need to do in my nervous system to be able to learn from an-

other person's experience? There is an acceptance involved. And it is not thinking; we are talking about the difference between thinking and feeling.

If I am trying to think through it, it is not going to happen. But if I attune, I can, to some extent, feel in me the sensations that you are feeling. Like you are touching the stove. Your finger is burning. You are hurting. In that moment, if I am attuned to you, I am feeling your pain.

This is not mysticism. It is the ordinary operation of empathic resonance: the capacity of one nervous system to model the state of another. What makes it epistemologically significant is that it allows learning without direct experience. I do not need to burn my own finger. I can learn from your burning.

You are using the matrix of the experience as a lens into the principle. And once you are able to get clarity at that level of principle, it is like the whole world opens up. And it is ethical. It is fundamentally that.

What does this have to do with decentralization and governance? Discernment is essentially an exercise (a meditation) whose long-term effect is attunement. If you have attunement, you can learn from the collective experience of your community without having to repeat every error yourself.

The deeper foundation for any governance that would work is the capacity of participants to feel into the consequences of choices before those consequences arrive, and to learn from one another's experience through attunement rather than through the slow accumulation of personal suffering; voting, consensus algorithms and token-weighted decision-making all come after that.

A group with this capacity is wiser than its members. A group without it is merely a collection of individuals who happen to be using the same software. The difference is not technological. It is developmental. It is cultural. And it is the thing that no protocol can provide.

VII. Summary

The hierarchy. Finance sits atop infrastructure, which sits atop culture, which sits atop ecology. Governance problems cannot be solved at any layer above the one where they originate. The crypto conversation operates at the finance layer and occasionally reaches infrastructure. It rarely touches culture. It almost never reaches ecology.

Enforcement and governance. A blockchain enforces rules and cannot determine who makes them. Before a community governs itself well, a blockchain automates the power that already exists; afterwards, it adds nothing a conventional record, kept by the same trusted process, would not do. Making agreements is the complex part, and it happens among people, mostly in person.

Trust. A protocol can secure a record, for as long as the mathematics under it holds. The value of every currency rests on trust that exchange will continue, which rests on a civilization, which rests on the living world; the soundest store of value is that living world itself.

The method. Polarization resolved through triplication: thesis, antithesis, synthesis, recursively applied. This is not a theoretical abstraction but a practical method for moving beyond false dichotomies in design and governance.

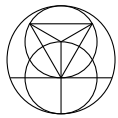
The foundation. Attunement as the basis of collective wisdom. Not algorithms but empathic resonance. Not protocols but developmental capacity. The technology is secondary. The human capability is primary.

The question to carry. Does it help people decide which rules to keep, or only enforce rules that someone else wrote?

What comes next. Chapter 8 gathers the reasons of the whole book into one conclusion and turns them into questions a reader can carry.

KEY CONCEPTS IN THIS CHAPTER

- **Protocol vs. platform**: the distinction between decentralized communication standards and centralized service providers; the transition from protocol to platform (circa 2001) as a fundamental power shift.
- **Hierarchy of finance, infrastructure, culture and ecology**: the ordering of layers at which governance problems must be addressed: finance (shallowest), infrastructure, culture, ecology (deepest).
- **Complicated and complex**: a complicated system has many parts arranged predictably and can be specified in advance (enforcing given rules); a complex system behaves in ways that emerge from its parts and cannot be fully predicted (deciding which rules should hold).
- **Governance paradox of blockchain**: a blockchain can enforce rules and cannot determine who makes them; before a community has solved governance it automates the existing distribution of power, and after, it adds nothing a conventional record kept by the same process would not do.
- **Cultural trust**: the shared confidence that exchange will remain possible and meaningful; the value of every currency rests on it, and no protocol secures it.
- **Money as choice**: the account of money as a claim on future choice (naming what can be chosen, carrying trust that choosing stays possible, moving a choice into the future), worth something only while a civilization makes exchange possible.
- **Triplication**: the resolution of polarization through thesis-antithesis-synthesis; a recursive method applicable to false dichotomies in design and governance; at its meta-order, the holding of the three terms together as the basic unit of thought.
- **Group wisdom**: the capacity of a well-structured group to hold knowledge that exceeds what any individual member possesses.
- **Attunement**: the empathic capacity to feel into another's experience as a basis for learning without direct personal suffering; the epistemological foundation of genuine collective intelligence.



Chapter 8. Beyond Computational Infrastructure

On why I have leaned away from dependence upon computational infrastructure for civilization design, what physics-embodied alternatives might look like, and where the real work of decentralization lies: not in code, but in culture, ethics, and choice.

I. The Considered Judgment

Computation is insufficient as the foundation for civilization-critical systems, for four reasons that Section II sets out: the first, second and fourth are each decisive alone against any civilization-critical system built on high-technology computation, and the third is decisive alone against every ledger. Computation is not useless. For building systems with distributed characteristics, there is much in this space that is good. In a period of transition, some blockchain elements, rightly built, can remove the extractive middlemen who stand between people who exchange goods, services or information, so that more goods reach more people at lower prices, and facts put on a shared record are harder for any one intermediary to falsify; my book *Design Before Strategy* counts such uses as worth doing while a better foundation is built. They are transitional uses: worth making during the transition, and not the foundation, during the transition or after it. The question of this chapter is what that foundation should be.

Two further judgments belong here. To prevent a system from being captured (taken over and turned to the use of a few), its designers have to weigh the trade-offs between anonymity and non-anonymity, which is to say between privacy and accountability (Chapter 3). And a system can be judged by which way it leans. A past-leaning system is built to fix and

keep what has happened; a future-leaning system is built to keep open what people may yet choose. A ledger's whole purpose is to make the past unchangeable, and so, judged by which way they lean, these systems are at a disadvantage in any work that has to keep the future open.

Given the overall balance of factors, I have leaned away from dependence upon computational infrastructure for civilization-type design. If I evaluate all the factors, that is where it lands. Each of the four reasons of Section II settles the matter for the systems it reaches, so the four are not weights against one another. What I have weighed is how much of computation remains worth using while something better is built, and the answer is the transitional uses named at the start of this section: worth making during the transition, and not the foundation.

This is not despair. It is a considered judgment, made after weighing everything examined in this book: the blockchain mechanics and their thermodynamic costs, the fragility of pseudonymity, the honeypot problem inherent in all ledger systems, the re-centralization dynamics that defeat decentralization through convenience, the Game A substrates on which cryptocurrency is necessarily built, the difference between enforcing rules and making them, the trust in exchange that no protocol reaches, and the inability of computational systems to address the cultural and ecological depths where governance problems actually originate.

Building civilization-critical systems on a foundation that is insufficient is worse than building nothing, because it absorbs the energy and attention that might otherwise go to approaches that are structurally adequate.

II. Why Computational Infrastructure Is Insufficient

The insufficiency has four dimensions. The first, second and fourth are each decisive alone against any civilization-critical system built on high-technology computation; the third is decisive alone against every ledger. The third is the question the title names, the one the Preface put first; the first, second and fourth are the three further reasons of the Preface.

First: computational infrastructure depends on math for stabilization. Math can be broken by better math. A system that a civilization depends on reaches beyond any one locked room, so its messages cross wires and air that no one in the system controls; what protects a message there is either the difficulty of a mathematical problem or a key carried by hand, and a key carried by hand is a handover. A security model that rests entirely on the computational difficulty of certain mathematical operations is a security model with an unknown and unknowable expiration date. Every cryptographic system whose security rests on the difficulty of a mathematical operation will eventually be broken or will require migration to a new system. The one cipher proved unbreakable, the one-time pad of Chapter 4, Section II, confirms the rule from the other side: its security rests on a key carried by hand, not on any mathematical difficulty. SHA-1, a standard hash function (a method that turns any data into a short fingerprint of it) for two decades, was shown broken by a practical collision in 2017. In 2024 the National Institute of Standards and Technology, the United States standards body, published its first replacement standards for the public-key methods that a quantum computer would break, and the migration of the world's systems to them has begun. That expiration date makes such security unsuitable as the foundation for institutions that need to persist across generations.

Second: it requires high-tech substrates that no community can maintain sovereignly. As argued in Chapter 6, the full dependency chain of modern computational systems runs through fabrication plants, operating system corporations, network infrastructure providers, and hardware supply chains that are all centralized, all vulnerable, and all subject to state control. Sovereignty built on these dependencies is not sovereignty at all.

Third: it creates global information requirements. As argued in Chapter 4, every ledger system requires a repository of global transaction data. That repository is a honeypot that structurally attracts extortion, rent-seeking, and surveillance. No governance arrangement can reliably prevent its misuse.

Fourth: it reproduces Game A asymmetries. As argued in Chapter 5, the pursuit of efficiency and scale (which computational systems both enable and incentivize) is the mechanism by which centralization reemerges. A community can hold that default off in how it runs its own machines (Chapter 5, Section VI). It cannot hold it off in how high-technology machines come to exist: they are made in a few plants, at a cost that only the pursuit of scale repays, and the surplus of that scale goes to whoever owns the plants. That the plants exist is a fact this reason shares with the second; the two reasons stay distinct, since the second concerns who can build the machine and this one who collects its surplus. The tools of optimization produce the concentration they were meant to prevent.

Together, they constitute a decisive case against building civilization-critical systems on computational infrastructure.

III. The Alternative: Physics-Embodied Systems

Technology that depends on physics for stabilization, embodied physics: this can work. But it is not crypto in the ordinary way. It is crypto in a different way. More based upon physical isolation than on digital cryptographic isolation.

What would this look like in practice?

Local rather than global information. Systems in which transactions are completed in the handover itself, without reference to any shared state. Bearer-certificate methodologies in which the value is embodied in the object and the transfer requires no third party's knowledge.

Which object? A community need not be able to make it; it has to be able to test it. Copper and gold can be weighed and assayed, with a balance and a touchstone, by anyone taught to do it, and they were tested that way for thousands of years before there was a bank. A banknote is the harder case: it comes from a plant no community owns, and its issuer keeps the powers that Chapter 4, Section II, describes.

Things that can be inspected directly. Infrastructure simple enough that a single person can understand its operation. Eight-bit or sixteen-bit compute, not because more powerful systems do not exist, but because simpler systems can be verified, manufactured, and maintained without corporate dependencies. Sovereignty through simplicity.

Physical presence as authentication. The fact that a human being can only be in one place at one time as the basis of identity verification. The body as credential. Proximity as trust. These are not vulnerable to quantum computing advances or algorithmic breakthroughs. They are as secure as the laws of physics and will remain so.

What of exchange between people far apart, such as two cooperatives in different towns, each keeping its accounts on its own machine in a locked room? The payment still finishes in a handover. What crosses the distance crosses it as a bearer object (goods, coins or notes), carried by the payer or by a courier whom both parties trust with that one delivery. That trust is the one-of-one model of Chapter 3, but it is named, it is limited to one object on one journey, and it gathers no record of anyone else's dealings, so it makes no honeypot. Each cooperative records only what it has itself handed over and received, which is local information. None of this needs a network that the cooperatives cannot build or repair.

What can one person do now, when cards are easier and cash is disappearing? Keep some savings in a form that needs no record, such as the land of Chapter 7, Section III, or metal that can be weighed and tested; pay in person, in a handover, where one can; and ask the six questions of Section V before joining anything new. A pension or a mortgage is a long promise: like the tab of Chapter 4, Section I, it is open until it is settled in a handover, and what it is worth rests on the civil order that will honor it when it falls due (Chapter 7, Section III).

A community needs one shared record of a different kind: a memory of its own thinking. Without one, a community does not mature; it repeats its discoveries instead of building on them. The memory has to keep the questions that led to each decision as well as the decision, it has to be kept

in many places, and no faction of the community may be able to alter it against the interests of the whole over time. Many people point to blockchains for this. A blockchain rests on transactions, so a memory kept on one would rest on exchange, the way of relating that I have found weaker than care for what another person cares about. My book *Software, Wildness, and the Normal Form* sets out the memory such a community needs as the third layer of its governance: kept in many places, unalterable by any faction, and resting on no transactional basis. That memory records the questions and decisions the community has chosen to record, not the private dealings of its members, so it gathers nothing that others could profit by extracting, and it serves the making of agreements, which Chapter 7 found to be the part of governance that no ledger can do.

IV. The Deeper Foundation: Beyond Survival

Whenever people try to manipulate the world from survival orientation, as almost all market activity does, their risk mitigation is fundamentally going to become a problem down the road. It will lead to slavery of one sort or another. To act from survival is to secure oneself against what others might do. In a market everyone does this at once, and whoever secures the most gains the most leverage; as Chapter 5 showed, the surplus that efficiency produces goes to someone, and advantage accumulates. Accumulated leverage over others becomes control over their choices. Control over another person's choices, held without that person's consent, is what slavery is, whatever form it takes.

Slavery is bad because it is especially bad for choice. And we need to get choice right because that is the future. The capacity for genuine choice (not the market's simulated choice between competing products, but the real choice about what kind of world to create) is the thing that matters most.

To think about the basis of choice on a completely different basis than survival (which means returning to love and life as the basis): this is the re-orientation that the technology conversation has been avoiding. This is

the move beyond survival orientation. Love, as I defined it, "is that which enables choice" (*An Immanent Metaphysics*, aphorism 2.44-2). That is why love, and not survival, can be the basis of choice: to act from survival is to secure oneself against what others might choose, and in a market that ends in control over their choices; to act from love is to act so that choice, one's own and other people's, is enabled. It is easier to talk about algorithms than about love. It is more comfortable to discuss protocols than to examine whether our fundamental orientation is toward domination or toward care.

But the technology cannot save us from getting the orientation wrong. No algorithm compensates for a community organized around extraction. No protocol prevents the reproduction of domination by people who have not examined their own survival orientation. The real work is prior to the technology.

V. Synthesis: Where Decentralization Actually Lives

The arc of this book has moved from the promise of decentralization (Chapter 1) through the technical mechanics (Chapter 2), the structural critiques (Chapters 3 through 6) and the depth at which they have to be met, where rules are made and trust is held (Chapter 7), to this conclusion: the real work of decentralization lies not in computational infrastructure but in culture, ethics, and the capacity for choice.

The vocabulary mattered. The people found through that vocabulary matter. The years of exploration (however misdirected in their technical ambitions) produced relationships and shared understanding that have value independent of any technology.

The task now is redirection. The energy that went into blockchain, into smart contracts, into token economics: that energy needs to go somewhere: into the patient, unglamorous work of building culture that supports genuine choice, governance that serves life rather than extraction,

and infrastructure simple enough to be maintained by the communities that depend on it, and not back into the same patterns with slightly better algorithms, or into the next hype cycle.

The book has taught six questions to ask of the next new system. Does a transaction finish in a handover, or only in a change to a shared record (Chapter 4)? Does its security rest on physics, or on mathematics that a later advance can break (Chapters 4 and 6)? Does it know a person by a body present, or by resources held (Chapter 3)? Who can build and repair the machine it runs on (Chapter 6)? Does efficiency here produce a surplus, and who collects it (Chapter 5)? Does it help people decide which rules to keep, or only enforce rules that someone else wrote (Chapter 7)? A warning protects a person once; these questions are the skill that protects them always.

Here are the six, asked of three things the book has examined: a coin of copper, Bitcoin, and a pseudonym party.

Question	**A coin of copper**	**Bitcoin**	**A pseudonym party**
Handover, or a change to a shared record?	A handover	Only a change to a shared record	It makes no payment; it issues one token to each person present
Physics, or mathematics that a later advance can break?	Physics	Mathematics	Physics, for the count
A body present, or resources held?	The question does not arise: a coin knows no one	Resources held	A body present
Who can build and repair the machine?	There is no machine; anyone taught can weigh and test the coin	No community	A room, which any community has
A surplus, and who collects it?	There is no surplus to collect	Yes; miners and exchanges collect it	No surplus
Help to decide the rules, or only enforcement?	The question does not arise	Only enforcement	It helps a group know who may decide, and leaves the deciding to them

Run the six on the next system you are offered.

This is not the end of the conversation. It is a reorientation. The navigational system is being adjusted. The aircraft is banking away from the wrong runway, beginning its approach toward something that can actually bear the weight of what needs to land.

VI. Summary

What is concluded. Computational infrastructure is insufficient as the foundation for civilization design. It is dependent, fragile, centralizing, and addressed to the wrong layer of the problem.

What is proposed. Physics-embodied systems, local information, simple inspectable infrastructure, bearer-certificate methodologies, and presence-based authentication. These approaches align with the structural requirements that the preceding chapters have identified.

Where the work is. The development of culture adequate to the task. Not code, but ethics. Not protocols, but relationships. Not efficiency, but robustness. Not survival, but love and life as the basis of choice. This is where the real work of decentralization lives, and it is work that no technology can do for us.

KEY CONCEPTS IN THIS CHAPTER

- **Insufficiency of computational infrastructure**: the conclusion that computation is insufficient as a foundation for civilization-critical systems, for four reasons: the first, second and fourth each decisive alone against any such system built on high-technology computation, and the third decisive alone against every ledger (Section II); for that reason I have leaned away from depending on it.
- **Transitional uses**: uses of blockchain elements worth making during a transition, such as removing extractive middlemen, as distinct from a foundation for what comes after it.
- **Collective memory**: a community's record of its questions as well as its conclusions, kept in many places and unalterable by any faction, without a transactional basis.
- **Physics-embodied systems**: technology whose security and operation rest on physical properties of the world rather than mathematical abstractions; not subject to algorithmic obsolescence.
- **Sovereignty through simplicity**: the principle that genuine community autonomy requires infrastructure simple enough to be understood, manufactured, and maintained without external dependencies.
- **Beyond survival orientation**: the reorientation from market-driven, risk-mitigating approaches (which produce slavery) toward love-and-life-based approaches to choice.
- **Redirection**: the task of channeling the energy, relationships, and understanding produced by the blockchain era toward approaches that are structurally adequate to the underlying problems.

Glossary

The defined terms of the Key Concepts boxes, gathered in one place, with the plain explanations of the technical terms given where each first appears.

Association attack: identifying a pseudonymous user by correlating transaction patterns with physical-world signals (location, timing, device proximity) (Chapter 3).

Attractive basin: a phenomenon whereby momentum and immediate advantage draw activity toward a domain, regardless of whether that domain serves the deeper goals that motivated the activity (Chapter 1).

Attunement: the empathic capacity to feel into another's experience as a basis for learning without direct personal suffering; the epistemological foundation of genuine collective intelligence (Chapter 7).

Bearer certificate: any transaction methodology in which possession constitutes ownership and transfer is effected by physical handover of an item that is impossible or prohibitively difficult to duplicate; requires only local information (Chapter 4).

Beyond survival orientation: the reorientation from market-driven, risk-mitigating approaches (which produce slavery) toward love-and-life-based approaches to choice (Chapter 8).

Bitcoin: the first cryptocurrency, described by Satoshi Nakamoto in a white paper of 2008; its blockchain is kept by proof of work (Chapters 2 and 3).

Blind signature: a way for an issuer to sign a token without seeing it; the basis of David Chaum's electronic cash (Chapter 4).

Blockchain: a distributed ledger kept as a chain of blocks, each block a set of verified transactions added to the end of the chain (Chapter 2).

Causal verification and choice attribution: the two things a system may need to know about an action: that it happened correctly, where anonymity does no harm, or who chose it, where anonymity corrodes (Chapter 3).

Classical cryptography: cryptography that runs on ordinary computers, as distinct from methods that depend directly on quantum substrates (Chapter 4).

Collective memory: a community's record of its questions as well as its conclusions, kept in many places and unalterable by any faction, without a transactional basis (Chapter 8).

Complicated and complex: a complicated system has many parts arranged predictably and can be specified in advance, as enforcing given rules can; a complex system behaves in ways that emerge from its parts and cannot be fully predicted, as deciding which rules should hold cannot (Chapter 7).

Consensus algorithm: the mechanism by which distributed nodes agree on a shared state without central authority (Chapter 2).

Convenience trap: the dynamic whereby users rationally choose centralized services over self-hosted alternatives, producing re-centralization as an emergent outcome of individual rational choices (Chapter 5).

Cryptocurrency: a currency kept as entries on a blockchain or another distributed ledger; by the test of Chapter 4, every cryptocurrency is a ledger (Chapters 1 and 4).

Cultural trust and infrastructure trust: confidence that exchange will remain possible and meaningful, on which the value of every currency rests and which no protocol reaches; and confidence that a system keeps its record correctly, which a protocol can secure for as long as the mathematics under it holds (Chapters 3 and 7).

Decentralization dilemma: the structural tendency of decentralized systems to re-centralize through the dynamics of user convenience, efficiency-seeking, and the inverse relationship between learning curves and adoption rates (Chapter 5).

Decentralized autonomous organization (DAO): an organization whose rules are written as programs on a blockchain (Chapter 1).

Decentralized finance (DeFi): lending and trading run by programs on a blockchain (Chapter 6).

Decentralized identity trilemma: the structural tension between sybil resistance, self-sovereignty, and privacy preservation, which no protocol alone can meet all at once; physical presence, as in pseudonym parties, meets all three as Chapter 3 defines them, at a price paid locally: trust in at least one organizer at each gathering, gatherings held at the same hour, and each body seen in the room (Chapter 3).

Dialectic: reasoning by opposed positions; the triad of thesis, antithesis and synthesis is usually attached to Hegel's dialectic (Chapter 7).

Displacement of discernment: the process by which hype cycles and external warnings substitute for the development of genuine epistemic skill, leaving people perpetually vulnerable to the next cycle (Chapter 6).

Distributed hash table: a way of storing data spread over many computers so that any piece can be found by its key without a central index (Chapter 2).

Distributed ledger: a shared record of transactions, copied across many computers (Chapter 1).

Double-spending problem: the fundamental challenge of ledger systems: ensuring that the same unit of value cannot be transferred twice through unauthorized modification of the record (Chapter 4).

Efficiency as asymmetry engine: the structural observation that optimization and efficiency-seeking produce surplus, and surplus concentrates into asymmetry and power differential (Chapter 5).

Energy diversion: the structural tendency of exciting technologies to absorb attention and effort that might otherwise address the harder, less glamorous problems they were supposed to solve (Chapter 1).

Epistemic: concerning how people come to know things; epistemological has the same sense (Chapters 6 and 7).

Ethereum: a blockchain that treats transactions as a basis for computation, running programs (smart contracts) that no single party can halt; it has used proof of stake since September 2022 (Chapter 2).

Full node: a computer that keeps and checks the whole record of a blockchain (Chapter 2).

Game A and Game B: Game A is the name that people of the Game B community, among them Jim Rutt and Jordan Hall, give to the present game of rivalry for money and power, played with the tools and incentives of the existing system; Game B names a hoped-for successor to it, built on cooperation (Chapters 1 and 5).

Game A substrates: the high-tech, corporation-dependent infrastructure on which cryptocurrency is built, which embeds the logic and power structures of the system it claims to escape (Chapter 6).

Gas fees: the fees paid to run a transaction or program on Ethereum (Chapter 4).

Gini coefficient: a measure of inequality, zero when everyone has the same and one when one person has everything (Chapter 5).

Gossip-about-gossip: Hashgraph's mechanism whereby each communication carries information about prior communications, enabling virtual voting without explicit ballots (Chapter 2).

Governance paradox of blockchain: a blockchain can enforce rules and cannot determine who makes them; before a community has solved governance it automates the existing distribution of power, and after, it adds nothing a conventional record kept by the same trusted process would not do (Chapter 7).

Group wisdom: the capacity of a well-structured group to hold knowledge that exceeds what any individual member possesses (Chapter 7).

Hard-to-fake signal: a signal that can be shown only by having the thing it signals, as proof of work can be shown only by spending the energy (Chapter 2).

Hash function: a method that turns any data into a short fingerprint of it (Chapter 8).

Hashgraph: a system that reaches agreement through gossip about gossip and virtual voting instead of mining (Chapter 2).

Hierarchy of finance, infrastructure, culture and ecology: the ordering of layers at which governance problems must be addressed: finance (shallowest), infrastructure, culture, ecology (deepest) (Chapter 7).

Holochain: a system in which each participant keeps their own chain of activity and validation occurs through the interactions of local neighborhoods rather than through global consensus; by the test of Chapter 4 it is a ledger (Chapters 2 and 4).

Honeypot: a record of global transaction data, held in one place or copied across many machines, that structurally attracts extortion, rent-seeking, and information extraction (Chapter 4).

Immutability requirement: the shared structural requirement of both systems: bearer certificates must resist duplication, and ledger entries must resist unauthorized modification (Chapter 4).

Information topology: where the information about a transaction has to be, only with the two parties or in a record everyone shares; the distinction between local-only information (bearer certificates) and global information (ledger systems), which determines the trustworthiness of the transaction methodology (Chapter 4).

Initial coin offering (ICO): the sale of a newly created token to the public to raise money, often on the strength of a white paper alone (Chapter 1).

Insufficiency of computational infrastructure: the conclusion that computation is insufficient as a foundation for civilization-critical systems, for four reasons: the first, second and fourth each decisive alone against any such system built on high-technology computation, and the third decisive alone against every ledger; for that reason I have leaned away from depending on it (Chapter 8).

Learning curve inversion: the principle that the difficulty of a decentralization technology is inversely related to its adoption rate, ensuring that easier centralized alternatives always attract more users (Chapter 5).

Ledger system: any transaction methodology in which the transaction is effected by a change in a shared record; requires global information and reconciliation (Chapter 4).

Low-tech sovereignty, or sovereignty through simplicity: the principle that genuine community autonomy requires infrastructure simple enough to be understood, manufactured, maintained, and inspected without external dependencies, corporate or other (Chapters 6 and 8).

MakerDAO: a decentralized autonomous organization running a currency on Ethereum, whose smart contracts could carry out decisions and could not make the decisions its community needed (Chapter 7).

Mastodon: a social network made of independently run servers (Chapter 5).

Meta-order: a process that works on the process before it; in triplication, the stage at which the three terms are held together as the basic unit of thought (Chapter 7).

Miner: a computer that competes, by doing costly computation, for the right to add the next entry to a blockchain (Chapter 2).

Money as choice: the account of money as a claim on future choice (naming what can be chosen, carrying trust that choosing stays possible, moving a choice into the future), worth something only while a civilization makes exchange possible (Chapter 7).

Monopoly on identity: the surveillance state or surveillance capital as the monopolistic controller of credential mechanisms (Chapter 3).

Mutual credit system: a system of exchange in which members extend credit to one another directly, each balance recording what one has given and received, with no central bank issuing money; by the test of Chapter 4 it is a ledger (Chapter 2).

Nanotech intrusion: entry into a machine by devices built at the scale of molecules; no substrate can block all of it out (Chapter 4).

Network effects: the way a service becomes more useful as more people use it, so that people go where the people already are (Chapter 1).

No-cloning theorem: the result of quantum physics that an unknown quantum state cannot be copied exactly; some cryptographic methods that depend on quantum substrates use it (Chapter 4).

Node: a computer that takes part in a network, here one that keeps a copy of a shared record; a full node keeps and checks the whole record (Chapter 2).

Non-fungible token (NFT): a ledger entry recording ownership of a unique item, often a digital image (Chapter 6).

One-time pad: a cipher whose key is as long as the message and used only once, which Claude Shannon proved perfectly secret in 1949; its security rests on a key carried by hand, not on mathematical difficulty (Chapters 4 and 8).

Onion-type protocol: a protocol that passes each message through several relays, each knowing only the one before and the one after; the Tor project is an example (Chapter 3).

Payment channel: an arrangement, such as the Lightning Network, in which two parties settle most payments off the main chain by changing a record they share, and settle the balance on the chain; by the test of Chapter 4 it is a ledger (Chapter 4).

Physics-based stabilization: security grounded in physical properties of the world (isolation, non-duplicability, presence) rather than mathematical difficulty; not subject to catastrophic algorithmic failure (Chapter 6).

Physics-embodied systems: technology whose security and operation rest on physical properties of the world rather than mathematical abstractions; not subject to algorithmic obsolescence (Chapter 8).

Plutocracy: rule by the people with the most wealth, which is what membership and voting power drawn from resources held produce (Chapter 3).

Private key: the secret that lets its holder spend from a blockchain address (Chapter 3).

Proof of personhood: verifying that a participant is a unique human being, as an alternative to proof of work or proof of stake (Chapter 3).

Proof of stake: a consensus method in which the right to add blocks goes to those who lock up coins as a deposit, in proportion to the deposit (Chapters 2 and 3).

Proof of work: a consensus method in which the right to add blocks is earned through computational expenditure; secure but thermodynamically wasteful (Chapter 2).

Protocol vs. platform: the distinction between decentralized communication standards (protocols) and centralized service providers (platforms); the transition from the former to the latter represents a fundamental shift of power (Chapter 1).

Pseudonym party: a gathering at which each person present receives one anonymous token, a mechanism proposed by Bryan Ford and Jacob Strauss in 2008 (Chapter 3).

Pseudonymity: acting under a name, here a public key, that is not tied to the person (Chapter 3).

Public key: the address others see on a blockchain (Chapter 3).

Public key cryptography: cryptography in which each party has a pair of keys, one published and one kept secret, so that strangers can exchange secrets and check signatures without first sharing a secret; one of the three branches of cryptography, beside hash functions and symmetric cryptography (Chapter 4).

Quantum substrate: hardware whose working rests directly on quantum physics (Chapter 4).

Redirection: the task of channeling the energy, relationships, and understanding produced by the blockchain era toward approaches that are structurally adequate to the underlying problems (Chapter 8).

Regulatory capture: a regulator coming to serve those it is meant to regulate (Chapter 5).

Robustness over efficiency: the design principle that genuine decentralization requires accepting inefficiency as a structural feature, since efficiency is the vector through which centralization enters (Chapter 5).

Rubber-hose attack: getting a key by threatening or hurting the person who holds it (Chapter 2).

Secure Scuttlebutt: a protocol that takes social relationships as the basis of the network: you see what your friends share, and their friends, but there is no global view (Chapter 2).

Self-sovereignty: a person's control of their own identity without reliance on any central issuer; one of the three properties of the decentralized identity trilemma (Chapter 3).

Shor's algorithm: a method, found by the mathematician Peter Shor in 1994, by which a quantum computer quickly solves the problems of number theory (factoring large numbers, and its relative, the discrete logarithm) on which most of the public key cryptography in use today rests; it disables a substantial number of the public key functions (Chapter 4).

Side-channel attack: reading a secret from what a device gives off as it works, such as its timing or its power use (Chapter 2).

Smart contract: a program stored and run on a shared ledger such as Ethereum's (Chapter 1).

Sovereignty through simplicity: see Low-tech sovereignty, or sovereignty through simplicity (Chapter 8).

Stabilization: what keeps a system's records and rules from being changed by anyone not entitled to change them; physics-based when it rests on physical properties of the world, math-based when it rests on the difficulty of mathematical operations (Chapter 6).

Structural: said of an outcome that follows from how a system is built, whoever builds it and whatever they intend (Chapter 1).

Sybil resistance: a Sybil attack is one person posing as many; sybil resistance prevents it (Chapter 3).

Symmetric cryptography: cryptography in which the two parties share one secret key; one of the three branches of cryptography (Chapter 4).

Tab: a running record of what one person owes another, as between neighbors or at a shop; it records a promise, the transaction finishes in a handover, and where balances stand as money the record is a ledger (Chapter 4).

Tests of discernment: telling original work from self-deception and from posing in a young field by how people talk: the mistakes they make, their contact with the known difficulties, and whether they inquire (Chapter 6).

Token: a unit recorded on a blockchain, or, at a pseudonym party, the one anonymous credential that each person present receives (Chapters 1, 3 and 6).

Tokenomics: the rules a token's designers set for how many tokens exist, who gets them and when (Chapter 6).

Transitional uses: uses of blockchain elements worth making during a transition, such as removing extractive middlemen, as distinct from a foundation for what comes after it (Chapter 8).

Transparency and opacity: the framework of information availability vs. information concealment, used as an alternative vocabulary for access controls (Chapter 3).

Triplication: the resolution of polarization through thesis-antithesis-synthesis; a recursive method applicable to false dichotomies in design and governance; at its meta-order, the holding of the three terms together as the basic unit of thought (Chapter 7).

Trust dimensions: the spectrum from one-of-one (centralized) through majority-of-many (blockchain) to none-of-many (trustless), characterizing how many actors must behave honestly for a system to function (the definition and labels are Vitalik Buterin's) (Chapter 3).

Unstoppable computer: Ethereum's architectural property of being a distributed computation that no single party can halt; both a feature and a structural hazard (Chapter 2).

Virtual voting: consensus achieved through analysis of communication patterns rather than through explicit ballot-casting (Chapter 2).

Vocabulary of finding: the social function of technical language in enabling people with shared concerns to locate one another (Chapter 1).

White paper: a paper announcing a project and its plans (Chapter 1).

Witness (in Hashgraph): an event in the gossip history that the algorithm elects, after the fact, as having visibility to all prior events (Chapter 2).

Wrong runway: the analogy for cryptocurrency's trajectory: approaching a destination that cannot support what arrives there (Chapter 6).

Zero-knowledge proof: a method by which one party proves a statement true without revealing anything beyond its truth (Chapter 3).

Bibliography

0xB10C. “Bitcoin Mining Centralization in 2025”. b10c.me, 15 April 2025. https://b10c.me/blog/015-bitcoin-mining-centralization/.

Badham, John, dir. *WarGames*. MGM/UA Entertainment, 1983. Film.

Baird, Leemon. “The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance”. Swirlds Technical Report SWIRLDS-TR-2016-01, 2016.

Bery, Suman. “Demonetisation: India's Stress Test”. Bruegel, 30 January 2017. https://bruegel.org/2017/01/demonetisation-indias-stress-test/.

Bloomberg. “FTX Files for Bankruptcy; Bankman-Fried Resigns as CEO”. Published in *InvestmentNews*, 11 November 2022. https://www.investmentnews.com/alternatives/ftx-files-for-bankruptcy-bankman-fried-resigns-as-ceo/229108.

Borge, Maria, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. “Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies”. In *IEEE European Symposium on Security and Privacy Workshops* (IEEE Security and Privacy on the Blockchain), 2017.

Buterin, Vitalik. “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform”. White paper, 2013 to 2014.

Buterin, Vitalik. “Hard Fork Completed”. Ethereum Foundation Blog, 20 July 2016. https://blog.ethereum.org/2016/07/20/hard-fork-completed.

Buterin, Vitalik. “Trust Models”. vitalik.ca, 20 August 2020.

Cambridge Centre for Alternative Finance (Alexander Neumueller, Gina Pieters, Kamiar Mohaddes, Valentin Rousseau and Bryan Zhang). *Cambridge Digital Mining Industry Report: Global Operations, Sentiment,*

and Energy Use. Cambridge Judge Business School, April 2025. Reported by Cambridge Judge Business School, 28 April 2025 ("the study estimates Bitcoin's annual electricity consumption at 138 TWh"). https://jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/.

"Chainalysis". *Wikipedia*. Accessed 5 November 2026. https://en.wikipedia.org/wiki/Chainalysis. The company's own site: https://www.chainalysis.com/.

Chaum, David. "Blind Signatures for Untraceable Payments". In *Advances in Cryptology: Proceedings of Crypto 82*, 199 to 203. New York: Plenum, 1983.

CoinLedger. "How Much Energy Does Bitcoin Use? (November 2025 Data)". 10 December 2025. https://coinledger.io/research/how-much-energy-does-bitcoin-use-november-2025-data.

Dingledine, Roger, Nick Mathewson, and Paul Syverson. "Tor: The Second-Generation Onion Router". In *Proceedings of the 13th USENIX Security Symposium*, 2004. https://www.torproject.org.

Ethereum Foundation. "The Merge". ethereum.org. Accessed 5 November 2026. https://ethereum.org/roadmap/merge/.

Fichte, Johann Gottlieb. *Foundations of the Entire Science of Knowledge* (*Grundlage der gesamten Wissenschaftslehre*). 1794 to 1795.

Ford, Bryan, and Jacob Strauss. "An Offline Foundation for Online Accountable Pseudonyms". In *Proceedings of the 1st Workshop on Social Network Systems* (*SocialNets 2008*), 31 to 36. ACM, 2008.

Harris-Braun, Eric, Nicolas Luck, and Arthur Brock. "Holochain: Scalable Agent-Centric Distributed Computing". White paper, 2018.

Hegel, Georg Wilhelm Friedrich. *Phenomenology of Spirit*. Trans. A.V. Miller. Oxford University Press, 1977 [1807].

Landry, Forrest. *An Immanent Metaphysics*. First published 2001. Wytheville, Virginia: UVSM Publications. ISBN 979-8-9896628-4-5. Cited by aphorism number.

Landry, Forrest. *Choosing Together; Law, Consensus, Meritocracy, and Democracy*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-355-9. DOI: https://doi.org/10.67291/MIPQ1939.

Landry, Forrest. *Civilization Design and Conscious Sustainable Evolution; Existential Risk, Governance, and the Architecture of a Living World*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-360-3. DOI: https://doi.org/10.67291/PIHE5046.

Landry, Forrest. *Design Before Strategy; Voice Messages on Leadership, Networks, and Civilizational Design*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-397-9. DOI: https://doi.org/10.67291/XEMT5490.

Landry, Forrest. *Narrative, Memory, and Neurodivergence; Being, Becoming, and Doing in a Shared Life*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-266-8. DOI: https://doi.org/10.67291/GPNJ6350.

Landry, Forrest. *Software, Wildness, and the Normal Form; From the Architecture of Code to Life, Justice, and Wisdom*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-237-8. DOI: https://doi.org/10.67291/AWME8110.

Landry, Forrest. *The Aerodynamics of Civilization; Why Seven Independent Problems Trace to One Diagnosis and One Instrument*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-951203-48-9. DOI: https://doi.org/10.67291/FZBB3545.

Landry, Forrest. *The Architecture of Choice; Dialogues on Governance, Community, and Organizational Design*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-386-3. DOI: https://doi.org/10.67291/IPMC7207.

Landry, Forrest. *The Displacement of Choice; The Catastrophe of the AI We Might Build*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-243-9. DOI: https://doi.org/10.67291/DXJL7493.

Landry, Forrest. *The Ephemeral Group Process Papers; Early Documents and Proposals, 2017 to 2021*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-951203-70-0. DOI: https://doi.org/10.67291/YQOO8105.

Landry, Forrest. *The Geometry of Man, Machine, and Nature; Care, Community, and the Design of Technology*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-244-6. DOI: https://doi.org/10.67291/ZIHO9910.

Landry, Forrest. *The Reach of Trust; Trust in Groups, Institutions, and Civilization*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-334-4. DOI: https://doi.org/10.67291/FQQP1342.

Landry, Forrest. *The Valley Crossing; Technology, Wisdom, and the Design of Governance*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-364-1. DOI: https://doi.org/10.67291/WOTP8305.

Landry, Forrest. *What Trust Rests On; Money, Manipulation, and the Information Commons*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-305-4. DOI: https://doi.org/10.67291/IBAC8609. Chapter 1, "Crypto Cynicism; On Bitcoin, Trust, and the True Basis of Value".

Landry, Forrest. *Why AGI Cannot Be Made Safe; The Argument, Its Physics, and the One Choice That Remains*. Volume 1 of The Impossibility of AGI Safety; The Substrate Needs Convergence Argument. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-951203-02-1. DOI: https://doi.org/10.67291/UIBT8862.

Landry, Forrest. *Why No Control Suffices; The Technical Case for the Impossibility of AGI Safety*. Volume 2 of The Impossibility of AGI Safety; The Substrate Needs Convergence Argument. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-951203-03-8. DOI: https://doi.org/10.67291/MZQS9079.

Landry, Forrest. *Wisdom and the Limits of System; Intelligence, Judicial Process, and the Design of Governance*. Wytheville, Virginia: UVSM Publications, 2026. ISBN 979-8-90710-354-2. DOI: https://doi.org/10.67291/SZIC5393.

Maciek. "Decentralized Identity Trilemma". Essay, 2019. Cited as "Maciek, 2019" in footnote 8 of Siddarth and colleagues (2020), below.

Meiklejohn, Sarah, and colleagues. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names". In *Proceedings of the 2013 Internet Measurement Conference* (*IMC 2013*). ACM, 2013. Also in *;login:* 38, no. 6 (December 2013). Summarized by Adrian Colyer in *the morning paper*, 20 February 2017. https://blog.acolyer.org/2017/02/20/a-fistful-of-bitcoins-characterizing-payments-among-men-with-no-names/.

MOnSter 6502. "A complete, working transistor-scale replica of the classic MOS 6502 microprocessor". Designed by Eric Schlaepfer, in collaboration with Evil Mad Scientist Laboratories, 2015; 3,218 transistors and 1,019 resistors. https://monster6502.com/.

Mueller, Gustav E. "The Hegel Legend of 'Thesis-Antithesis-Synthesis'". *Journal of the History of Ideas* 19, no. 3 (1958): 411 to 414.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System". White paper, 2008.

National Institute of Standards and Technology. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards". 13 August 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

Poon, Joseph, and Thaddeus Dryja. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments". White paper, 2016.

Rutt, Jim. "A Journey To GameB". Medium, 13 January 2020. The essay uses "GameA" for the status quo and "GameB" for the social operating system meant to replace it. https://medium.com/@memetic007/a-journey-to-gameb-4fb13772bcf3.

Shannon, Claude E. “Communication Theory of Secrecy Systems”. *Bell System Technical Journal* 28, no. 4 (1949): 656 to 715.

Siddarth, Divya, Sergey Ivliev, Santiago Siri, and Paula Berman. “Who Watches the Watchmen? A Review of Subjective Approaches for Sybil-Resistance in Proof of Personhood Protocols”. *Frontiers in Blockchain* 3 (2020): 590171. doi:10.3389/fbloc.2020.590171.

Siegel, David. “Understanding The DAO Attack”. *CoinDesk*, 25 June 2016.

Stevens, Marc, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov. “SHAttered”: the first practical collision for SHA-1. CWI Amsterdam and Google, 23 February 2017. https://shattered.io/.

Tarr, Dominic, Erick Lavoie, Aljoscha Meyer, and Christian Tschudin. “Secure Scuttlebutt: An Identity-Centric Protocol for Subjective and Decentralized Applications”. In *Proceedings of the 6th ACM Conference on Information-Centric Networking (ICN 2019)*. ACM, 2019.

United States Energy Information Administration. “How much electricity does an American home use?” Frequently Asked Questions (figures for 2022). https://www.eia.gov/tools/faqs/faq.php?id=97&t=3.

United States Securities and Exchange Commission. “SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX”. Press release 2022-219, 13 December 2022. https://www.sec.gov/news/press-release/2022-219.

United States Securities and Exchange Commission. “SEC Charges Terraform and CEO Do Kwon with Defrauding Investors in Crypto Schemes”. Press release 2023-32, 16 February 2023. https://www.sec.gov/news/press-release/2023-32.

Weber, Max. “Politics as a Vocation”. Lecture, Munich, 1919. Published as *Politik als Beruf*. Munich and Leipzig: Duncker & Humblot, 1919. English translation in *From Max Weber: Essays in Sociology*, translated and edited by H. H. Gerth and C. Wright Mills. New York: Oxford University Press, 1946.

YCharts. “Bitcoin Blockchain Size” (779.01 gigabytes on 28 October 2026). https://ycharts.com/indicators/bitcoin_blockchain_size.

Zeloof, Sam. Home-built integrated circuits, reported by Shawn Knight in “This college student made his own processor in a home garage”. TechSpot, August 2021. https://www.techspot.com/news/90826-college-student-made-own-processor-home-garage.html.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

Index

A

Access controls, Ch. 3, p. 19

Anonymity, Ch. 1, p. 4, Ch. 3, p. 17, Ch. 8, p. 68

Arab Spring, Ch. 1, p. 1

Association attack, Ch. 3, p. 18

Asymmetry (economic), Ch. 5, p. 43, Ch. 6, p. 55

Attractive basin, Ch. 1, p. 2, Ch. 6, p. 55

Attunement, Ch. 7, p. 65

B

Bearer certificate, Ch. 3, p. 25, Ch. 4, p. 29, Ch. 8, p. 71

Bitcoin, Ch. 2, p. 9, Ch. 3, p. 18, Ch. 4, p. 30, Ch. 6, p. 54, Ch. 7, p. 61

Bitcoin tumbler (mixer), Ch. 3, p. 18

Blind signature, Ch. 4, p. 30

Blockchain, Ch. 1, p. 2, Ch. 2, p. 8, Ch. 3, p. 17, Ch. 4, p. 36, Ch. 5, p. 44, Ch. 6, p. 49, Ch. 7, p. 59, Ch. 8, p. 69

Blockchain analytics, Ch. 4, p. 36

Borge, Maria, and colleagues, Ch. 3, p. 23

Buterin, Vitalik, Ch. 3, p. 24

C

Cash, Ch. 3, p. 25, Ch. 4, p. 36, Ch. 8, p. 72

Causal verification and choice attribution, Ch. 3, p. 19

Chainalysis, Ch. 4, p. 36

Chaum, David, and electronic cash, Ch. 4, p. 30

Choice (basis of), Ch. 8, p. 73

Choice attribution, Ch. 3, p. 19

Collective memory, Ch. 8, p. 72

Complicated and complex, Ch. 7, p. 59
Consensus algorithm, Ch. 2, p. 9
Convenience (and re-centralization), Ch. 5, p. 42
Cooperative (in a locked room), Ch. 6, p. 51, Ch. 8, p. 72
Cryptocurrency, Ch. 1, p. 4, Ch. 4, p. 30, Ch. 5, p. 44, Ch. 6, p. 48, Ch. 7, p. 60, Ch. 8, p. 69
Cultural trust, Ch. 3, p. 25, Ch. 7, p. 60
Culture and ecology, Ch. 7, p. 58, Ch. 8, p. 76

D

DAO, The (theft and reversal, 2016), Ch. 2, p. 13, Ch. 5, p. 43, Ch. 7, p. 60
Decentralization, Ch. 1, p. 1, Ch. 5, p. 43, Ch. 7, p. 64, Ch. 8, p. 74
Decentralization dilemma, Ch. 5, p. 41
Decentralized autonomous organization (DAO), Ch. 1, p. 5, Ch. 6, p. 50, Ch. 7, p. 57
Decentralized finance (DeFi), Ch. 6, p. 54
Discernment (displacement of), Ch. 6, p. 54, Ch. 7, p. 65
Discernment (tests of), Ch. 6, p. 54
Distributed hash table, Ch. 2, p. 11
Domination culture, Ch. 6, p. 53
Double-spending problem, Ch. 4, p. 33

E

Efficiency (critique of), Ch. 5, p. 43, Ch. 8, p. 71
Eight-bit compute, *see* Low-tech infrastructure
Empathic resonance, Ch. 7, p. 65
Energy costs (blockchain), Ch. 2, p. 14
Enforcement and governance, Ch. 7, p. 59
Ethereum, Ch. 1, p. 3, Ch. 2, p. 12, Ch. 4, p. 30, Ch. 5, p. 43, Ch. 6, p. 54, Ch. 7, p. 60
Exchange at a distance, Ch. 8, p. 72
Extortion, Ch. 4, p. 36

F

Fichte, Johann Gottlieb, Ch. 7, p. 62
Ford, Bryan, and Jacob Strauss, Ch. 3, p. 22
FTX, Ch. 5, p. 43

G

Game A / Game B, Ch. 1, p. 4, Ch. 5, p. 44, Ch. 6, p. 48, Ch. 8, p. 69
Geometry of Man, Machine, and Nature, The, Ch. 6, p. 51
Gini coefficient, Ch. 5, p. 43
Global vs. local information, Ch. 4, p. 35, Ch. 8, p. 71
Gold and copper, Ch. 4, p. 34, Ch. 8, p. 71
Gossip-about-gossip, Ch. 2, p. 10
Governance, Ch. 1, p. 1, Ch. 3, p. 20, Ch. 4, p. 36, Ch. 6, p. 52, Ch. 7, p. 58, Ch. 8, p. 74
Governance paradox of blockchain, Ch. 7, p. 59
Group wisdom, Ch. 7, p. 64

H

Handover, Ch. 1, p. 3, Ch. 4, p. 30, Ch. 8, p. 71
Hard-to-fake signal, Ch. 2, p. 9
Hash function, Ch. 4, p. 37, Ch. 8, p. 70
Hashgraph, Ch. 2, p. 10
Hegel (thesis/antithesis/synthesis), Ch. 7, p. 62
Holochain, Ch. 2, p. 11, Ch. 4, p. 31
Honeypot problem, Ch. 4, p. 36, Ch. 8, p. 70

I

ICO (initial coin offering), Ch. 1, p. 1, Ch. 6, p. 52
Identity (decentralized), Ch. 1, p. 3, Ch. 3, p. 20
Identity trilemma, Ch. 3, p. 21
Immanent Metaphysics, An, Ch. 8, p. 74

Immutability, Ch. 4, p. 33
India (withdrawal of notes, 2016), Ch. 4, p. 34
Information topology, Ch. 4, p. 32
Infrastructure trust, Ch. 3, p. 25
Insufficiency of computational infrastructure, Ch. 8, p. 68

K

Key clusters, Ch. 3, p. 17

L

Learning curve inversion, Ch. 5, p. 42
Ledger system, Ch. 4, p. 30, Ch. 8, p. 70
Lightning Network, Ch. 4, p. 31
Love, Ch. 8, p. 73
Low-tech infrastructure, Ch. 6, p. 50, Ch. 8, p. 72

M

MakerDAO, Ch. 7, p. 60
Mastodon, Ch. 5, p. 42
Meiklejohn, Sarah, and colleagues, Ch. 3, p. 17
Miner / mining, Ch. 2, p. 8, Ch. 5, p. 44
Monero, Ch. 4, p. 30
Money as choice, Ch. 7, p. 61
Monopoly on identity, Ch. 3, p. 26
MOnSter 6502, Ch. 6, p. 50
Mutual credit system, Ch. 2, p. 11

N

Naivete (of crypto community), Ch. 6, p. 48
Nakamoto, Satoshi, Ch. 3, p. 20
Nanotech intrusion, Ch. 4, p. 38
NFT (non-fungible token), Ch. 6, p. 53

No-cloning theorem, Ch. 4, p. 38

O

One-CPU-one-vote, Ch. 3, p. 20
One-time pad, Ch. 4, p. 34, Ch. 8, p. 70
Onion routing, Ch. 3, p. 18
Opacity, *see* Transparency and opacity

P

Physical presence (copresence) as authentication, Ch. 3, p. 22, Ch. 6, p. 52, Ch. 8, p. 72
Physics-based stabilization, Ch. 6, p. 51, Ch. 8, p. 71
Platform (vs. protocol), Ch. 1, p. 5, Ch. 7, p. 57
Polarization and triplication, Ch. 7, p. 63
Post-quantum standards, Ch. 4, p. 37, Ch. 8, p. 70
Private key, Ch. 3, p. 17
Proof of personhood, Ch. 3, p. 21
Proof of stake, Ch. 2, p. 12, Ch. 3, p. 20
Proof of work, Ch. 2, p. 9, Ch. 3, p. 20
Protocol vs. platform, *see* Platform (vs. protocol)
Pseudonym parties, Ch. 3, p. 22
Pseudonymity, Ch. 3, p. 18, Ch. 8, p. 69
Public key, Ch. 3, p. 17
Public key cryptography, Ch. 4, p. 37

Q

Quantum computing, Ch. 4, p. 33, Ch. 6, p. 52, Ch. 8, p. 70

R

Re-centralization, Ch. 1, p. 5, Ch. 5, p. 42, Ch. 8, p. 69
Rent-seeking, Ch. 4, p. 36
Robustness (vs. efficiency), Ch. 5, p. 45, Ch. 8, p. 76

Rubber-hose attack, Ch. 2, p. 14

S

Secure Scuttlebutt, Ch. 2, p. 12
SHA-1, Ch. 8, p. 70
Shannon, Claude, Ch. 4, p. 34
Shor's algorithm, Ch. 4, p. 37
Siddarth, Divya, and colleagues, Ch. 3, p. 20
Side-channel attack, Ch. 2, p. 14
Six questions, Ch. 8, p. 75
Slavery, Ch. 8, p. 73
Smart contract, Ch. 1, p. 3, Ch. 2, p. 13, Ch. 7, p. 59, Ch. 8, p. 74
Sovereignty (community), Ch. 6, p. 49, Ch. 8, p. 72
Store of value, Ch. 7, p. 61
Substrate (resilience of), Ch. 6, p. 49
Surveillance capitalism, Ch. 4, p. 35
Surveillance state, Ch. 3, p. 26
Survival orientation, Ch. 8, p. 73
Sybil resistance, Ch. 3, p. 21
Symmetric cryptography, Ch. 4, p. 37

T

Tab, Ch. 4, p. 31, Ch. 8, p. 72
Terra (UST and LUNA), Ch. 6, p. 53
Theft (of a bearer object), Ch. 4, p. 34
Three directions of attack (on a ledger), Ch. 4, p. 38
Tokenomics, Ch. 6, p. 52
Tor Project, Ch. 3, p. 18
Transitional uses, Ch. 8, p. 68
Transparency and opacity, Ch. 3, p. 19
Triplication, *see* Polarization and triplication
Trust dimensions (one-of-one through none-of-many), Ch. 3, p. 24

U

Unstoppable computer, Ch. 2, p. 12

V

Virtual voting, Ch. 2, p. 11
Vocabulary of finding, Ch. 1, p. 1

W

WarGames (film), Ch. 2, p. 13
Weber, Max, Ch. 3, p. 26
Weimar Germany, Ch. 7, p. 61
Witness (in Hashgraph), Ch. 2, p. 10
Wrong runway (analogy), Ch. 6, p. 48, Ch. 8, p. 76

Z

Zcash, Ch. 4, p. 30
Zeloof, Sam, Ch. 6, p. 50
Zero-knowledge proof, Ch. 3, p. 22
Zimbabwe, Ch. 7, p. 61
Zuboff, Shoshana, Ch. 1, p. 5