



The Living Ledger

Understand blockchain, practice its core ideas, and make clearer choices about digital assets

Curiosity without the hype.

SHAD EDDIE MONGRUE

Free preview · Introduction and Chapter 1
shadeddiemongruebooksgallery.com

SHELF 15 OF 32 · BLOCKCHAIN · CORE BOOK

The Living Ledger

Understand blockchain, practice its core ideas, and make clearer choices about digital assets

SHAD EDDIE MONGRUE

ShadEddieMongrueBooks Gallery · shadeddiemongruebooksgallery.com

The Living Ledger. Free preview edition: Introduction and Chapter 1. © 2026 Shad Eddie Mongrue. All rights reserved. Published by the Shad Eddie Mongrue Books Gallery, shadeddiemongruebooksgallery.com.

This book is for education and general information. It is not personal financial, legal, tax, medical, mental-health, nursing, investment or other professional advice. Talk with a qualified professional about your situation.

Every statistic, study finding and documented example is numbered and listed in the Sources, with a link to the page it came from. Each was checked word for word against its source in October 2026. Stories marked "composite example" are illustrations drawn from common situations; their names and details are not real people. Stories marked "documented example" come from the cited sources.

Research credits: see "Research Credits" at the back of the book. Cover and design: Shad Eddie Mongrue Books Gallery.

Contents

INTRO	An Invitation
CH. 1	A New Way to Ask Who Keeps the Record
CH. 2	How Blocks Become a Shared History
CH. 3	Many Computers, One Agreement
CH. 4	Keys, Wallets, and the Meaning of Control
CH. 5	Digital Assets Without the Sales Pitch
CH. 6	Smart Contracts and the Rules They Cannot Read
CH. 7	Where the Idea Meets Everyday Life
CH. 8	Practice Reading Claims Like a Researcher
CH. 9	Avoid the Traps, Keep the Curiosity
CH. 10	A Long Practice in Clear-Eyed Wonder
RESEARCH	What the Evidence Says
PRACTICE	Your 30-Day Practice Plan
REFERENCE	Glossary
LETTER	Keep Going
BACK	Sources and Research Credits
BACK	About the Author

An Invitation

A ledger is a record of who owns what, what happened, or what someone agreed to do. We rely on records every day, usually without stopping to wonder who keeps them, who can change them, or how everyone else knows which version to trust. Blockchain begins with a wonderfully human question: can people maintain a shared record when they do not want one person or institution to be the only keeper? That question is worth your curiosity even if you never own a digital asset.

A blockchain is one way to keep a shared digital ledger. Its records are grouped into blocks, and cryptographic links connect each block to the one before it. If earlier data is changed, the links can reveal the alteration in later blocks¹. The design is not magic, and it does not make every recorded claim true. But following the pieces from a practical problem to a technical choice can be satisfying in the way a well-made puzzle is satisfying: you begin to see how the parts fit, and where they do not.

The subject also deserves a clear-eyed look because real people encounter real risks around digital assets. In 2024, the FBI's Internet Crime Complaint Center recorded \$9,322,335,911 in reported losses associated with its cryptocurrency descriptor². That figure is not a measure of every kind of cryptocurrency activity, nor does it tell you what any particular person should do. It is a reason to understand the terms, claims, and risks before you make choices involving money.

There is a more hopeful and useful reason to learn. Blockchain ideas are not limited to cryptocurrency. NIST describes possible applications in areas such as supply chains, digital identification, and records management¹. Considering those possibilities does not require you to believe that blockchain is the right tool for any of them. It gives you a better question to ask: what problem is this system meant to solve, and does its design actually help?

The answer will sometimes be no. A blockchain can make changes to recorded information detectable, but it cannot guarantee that the information was accurate when it was entered. It can also make correction difficult, and its limits depend on how a particular system is built and used. That tension is part of what makes the field interesting. You can admire the ingenuity of a

shared record while remaining unconvinced by a particular product, project, or promise.

This book invites you to bring both curiosity and judgment. You do not need a technical background, a digital wallet, or a willingness to invest. You will learn the basic ideas, try them with low-risk paper exercises, and practice asking better questions about evidence and trade-offs. The aim is not to turn you into a cheerleader or a skeptic by habit. It is to help you become a reader of blockchain claims who can enjoy the idea and still keep both feet on the ground.

Reasons to fall in love with this subject

- **It starts with a human question** Blockchain is easier to understand when you begin with the problem it is trying to address: how can a group keep a shared record without relying entirely on one keeper? That question connects the technology to familiar concerns about trust, cooperation, and accountability. You can explore those concerns without assuming that every group needs a blockchain. The pleasure is in seeing how a technical design responds to a human need—and in noticing when a simpler arrangement might serve people better.
- **The mechanics reward curiosity** Blocks, hashes, keys, and consensus can sound like a wall of jargon. They become more approachable when you follow a record step by step and test the pieces with paper. A small change to information can produce a different hash, making the change detectable³. That is a neat idea to hold in your hands, not just a phrase to memorize. As the mechanics become clearer, you can separate what the technology actually does from what a sales pitch says it does.
- **It connects technology to everyday systems** A shared ledger can be considered for more than payments. NIST lists supply chains, digital identification, and records management among areas where blockchain may be implemented¹. That breadth gives you a reason to look beyond coins and market prices. It also gives you a useful discipline: start with the people, the information, and the problem, then ask whether a blockchain is a sensible fit. The technology is more interesting when its purpose matters more than its label.
- **It teaches useful skepticism** Learning blockchain gives you practice noticing the difference between a record that is hard to alter and a record that is true. It helps you ask who entered the information, who can see it, what happens when an error appears, and what evidence supports a claim

of speed or security. Those questions are valuable even when the answer is that another tool would work better. You do not have to be cynical to be careful; you can stay open-minded and ask for proof.

- **It leaves room for wonder without hype** There is something compelling about a network of participants maintaining copies of a ledger and following shared rules for adding new records⁴. The design raises lively questions about coordination and governance: who sets the rules, who follows them, and how can they change? It does not settle those questions for us. That is precisely why the subject can stay interesting. You can appreciate the ingenuity while recognizing that people, institutions, and trade-offs remain part of the story.

BY THE END OF THIS BOOK, YOU WILL BE ABLE TO

- Explain what a blockchain is and why a group might choose a shared ledger.
- Trace how a proposed transaction can be checked, grouped into a block, and linked to earlier records.
- Describe nodes and consensus in plain language, including why no one consensus approach is best for every situation.
- Distinguish a wallet, private key, public address, and the digital asset recorded on a network.
- Sort out cryptocurrencies, tokens, stablecoins, and NFTs without treating them as interchangeable.
- Identify what smart contracts can do and where they depend on sound code, outside information, or human judgment.
- Check a blockchain claim by tracing its source, date, definitions, and evidence.
- Use a safe learning checklist to recognize common risks and avoid putting money at risk just to understand the ideas.

How to use this book

You can read the chapters in order, because the later ideas build on the earlier ones. If you have a particular interest, you can also use the chapter titles as a map: start with keys if you want to understand control, smart contracts if you want to understand automated rules, or everyday deployments if you want to evaluate real-world uses. When a term feels unfamiliar, pause and return to

the chapter where it is introduced. There is no prize for pretending the jargon was obvious.

The exercises are designed for learning, not for handling real funds. Use paper, a pencil, and a little patience to explore how hashes, links, and instructions work. When the book asks you to assess a claim, write down what it promises, what evidence supports it, and what important question remains unanswered. A short note is enough. The habit of slowing down to check is more useful than memorizing a long list of technical terms.

As you read, keep asking who benefits, who bears the risk, and what happens when something goes wrong. You may find a use case intriguing and still decide it is not useful for your own needs. You may also change your mind as you learn more. That is not a failure to reach a conclusion; it is what thoughtful learning looks like. You can finish the book with stronger questions rather than a new financial commitment.

HOW THIS BOOK HANDLES EVIDENCE

This book treats blockchain as a subject to investigate, not a solution to assume. Numbered citations point to the sources behind factual claims, so you can check their wording and context. Documented examples use only the information provided by those sources; composite examples are fictional illustrations, not reports about real people. Evidence can change, and demonstrations do not by themselves establish lasting public benefit. This is educational material, not personal financial, investment, or legal advice. You can learn the ideas without buying, transferring, or risking digital assets.

A New Way to Ask Who Keeps the Record

A COMPOSITE EXAMPLE · NAMES AND DETAILS ARE ILLUSTRATIVE

Mara helps coordinate a neighborhood tool library. A drill goes out on Tuesday, a hedge trimmer comes back on Thursday, and someone needs to know whether the charger was included. The record is a shared spreadsheet. It works—until two volunteers update different copies, a typo makes the return date look wrong, and nobody is quite sure which version to trust.

The problem is not that anyone is dishonest. People are busy, files get copied, and memories disagree. Mara could ask one volunteer to keep the official record and give everyone else read-only access. That might settle things. Or the group could agree on a process for checking changes together.

This small puzzle points toward a much larger question: when people need a common history but do not want to rely entirely on one record keeper, what arrangement might help? Blockchain offers one answer. It is not automatically the best answer, and it does not make people trustworthy by magic. But tracing how a real coordination problem can lead to a technical design is a satisfying kind of thinking. You start with a human need, follow the choices, and see where the design helps—and where it asks more of everyone.

The record is a social agreement

A record is more than a pile of facts. It is also an agreement about what counts as an entry, who may add one, how mistakes are handled, and which version people will treat as current. A tool-library list, a shared calendar, and a bank ledger all depend on some arrangement for answering those questions. The software matters, but so do the people and rules around it.

When everyone trusts one organization to keep the record, a central database can be a sensible arrangement. One operator controls the system, sets

permissions, keeps backups, and corrects errors. Users know where to go when something breaks. In many ordinary situations, that is not a flaw; it is the point. A central record can be simpler to run and easier to manage than asking many participants to coordinate a shared system.

The question changes when several parties need to write to or check the same record, while none wants another party to have unquestioned control. Think of organizations tracking a product as it moves between them, or groups that need to check whether a record has changed. The issue is not necessarily distrust in the dramatic sense. It may be a practical desire for a common history that no single participant can quietly rewrite.

That is the human problem blockchain is designed to address: how a community can maintain a shared ledger without relying on a central repository or, usually, a central authority. NIST describes blockchains as distributed ledgers of this kind.⁵ This design shifts some responsibility from a single record keeper to shared rules and network participants. It can make a particular kind of coordination possible, but it does not remove the need to decide who participates, what may be recorded, or how disagreements are handled.

Start with the ordinary database

Before asking whether blockchain belongs in a project, describe the record in plain language. Who needs to see it? Who needs to change it? Who is allowed to approve a change? What happens when an entry is wrong? Then ask a deceptively powerful question: could one responsible organization run a database that meets those needs?

Picture the tool library again. If one volunteer group manages the tools, members are happy to accept its record, and a coordinator can correct mistakes, a shared spreadsheet or conventional database may be enough. It can give people one current version without requiring them to maintain a network together. Adding a more elaborate system would not make the hammers more honest; it could simply add work.

A central system also gives people a clear place to ask for help or request a correction. That is valuable when accountability is concentrated in an organization that users can identify. Of course, the organization still needs sensible security and procedures. A database is not automatically safe or accurate just because it is familiar. The point is to compare arrangements

against the actual problem, rather than treating any technology as a universal upgrade.

Blockchain becomes more worth examining when multiple participants need to share updates and would rather not give one participant sole control of the record. Even then, the design may involve trade-offs in complexity, control, and the process for correcting mistakes. NIST cautions that blockchain is not a complete solution: malicious users, controls, and implementation limitations still require attention.⁶ A good first step is not to ask, “How can we put this on a blockchain?” Ask, “What problem with our current record are we trying to solve, and what would count as success?”

A ledger that carries its history

A blockchain is a ledger: a record of transactions or other entries, grouped into blocks. The blocks are connected cryptographically, so each one refers back to the previous one. NIST describes blockchain as a shared digital ledger designed to be tamper-evident and tamper-resistant.¹ In everyday terms, tamper-evident means that a change can leave signs; tamper-resistant means the design makes changing the record harder. Neither phrase means that every entry is true.

Here is a simple way to picture the link. Imagine that each page in a shared notebook carries a special summary of the page before it. If someone secretly edits an earlier page, its summary changes. The next page no longer matches the summary it recorded, and the mismatch can be noticed. In a blockchain, cryptographic links make changes to earlier data detectable in later blocks.¹ The analogy is not the mechanism itself, but it helps reveal the idea: the history is connected, rather than being a stack of unrelated pages.

A blockchain also uses agreed rules for adding entries. In a distributed network, participants maintain copies of the ledger; new blocks are added according to validation and consensus rules.⁴ You can think of consensus as the network's way of deciding which proposed history to accept, though the exact rules vary. This is not the same as every participant personally checking every real-world fact. A network can apply its rules correctly to information that was entered inaccurately.

This design makes the record's history important. Under normal operation, a blockchain transaction cannot be changed once published.⁵ That quality can be useful when participants want later changes to be detectable. But it can also make correction awkward: a group must have a sound way to record that an

earlier entry was mistaken, rather than pretending mistakes are impossible. Shared history is a technical feature; deciding what the history means remains a human task.

The pleasure of matching design to need

There is a quiet pleasure in following the chain of reasoning. A group has a coordination problem. It identifies what it needs from a record. It chooses rules for who can propose and validate entries. A technical design makes those rules easier to carry out, perhaps by distributing copies and linking blocks. Then you inspect the result and ask what the design still cannot do. This is less like finding a magic tool and more like fitting a key to a particular lock.

That way of thinking helps separate the useful idea from the fashionable label. If the essential need is to keep one organization's records consistent, a standard database may be a better fit. If several parties need a shared history and do not want one party to be the sole keeper, a distributed ledger may deserve a closer look. The choice depends on relationships, governance, correction procedures, privacy needs, and practical operation—not just on whether the word blockchain appears in a proposal.

You can also be curious without being credulous. Blockchain technology has potential uses beyond cryptocurrency, including supply chains, digital identification, and records management.¹ That range is interesting, but a possible application is not proof that a particular project is useful. You still need to know what is being recorded, who checks it, who can see it, and what happens when a person needs a correction.

So the opening question is not simply who keeps the record. It is who gets to participate in keeping it, what rules govern the shared history, and whether that arrangement improves on a simpler alternative. Those questions make blockchain worth studying even if you never use a blockchain product. They turn a technical subject into a practical inquiry about trust, coordination, and the records people rely on.

RESEARCH SPOTLIGHT

Research spotlight

NIST's description of blockchain emphasizes a shared, tamper-evident and tamper-resistant digital ledger.¹ It explains that blocks are cryptographically linked, so changing data in an earlier block changes the link and can be detected later.¹ These ideas help explain why a blockchain can make quiet alterations to recorded history harder to hide. They do not show that the original information was correct, that every participant has equal power, or that a blockchain is the best record system for a given job. Tamper-evident is not the same as error-proof, and resistant is not the same as impossible. A record can preserve a mistaken entry very reliably. The practical lesson is to ask both how a system protects its history and how people will check information before it enters that history. The technology can support an agreement; it cannot decide whether the agreement is fair or useful.

A life example

A DOCUMENTED EXAMPLE

Estonia's KSI: a narrow, useful claim

A documented example helps show how to keep a technology claim in proportion. The Estonian Government and Guardtime began developing Keyless Signature Infrastructure, or KSI, in 2008 to improve public-administration data security and information authenticity through time-proof stamping.³ The described mechanism relies on hashes: because hash functions are deterministic, even a minor change to a document produces a different hash from the original, so the modification can be detected.³

Notice what this example gives you. It connects a public-sector need—checking whether information has changed—to a technical design that can reveal a change. That is more informative than saying only that a government “uses blockchain.” It also gives you a careful question to carry forward: what exactly does the system protect, and what evidence supports the claim?

The facts here do not establish that every government record is on a blockchain, that all information entered is accurate, or that the system solves every public-administration problem. They describe a technology and its stated purpose, not a universal verdict on its effects. That distinction is not a reason

to dismiss the example. It is how you learn from it without asking it to prove more than it can.

TRY THIS

Try this: choose the record before the technology

Use a low-stakes example, such as a shared list of items borrowed by a club, and compare a central database with a shared ledger on paper.

1. Write down what the record needs to contain and who needs to read it.
2. Name who should be allowed to propose, approve, and correct an entry.
3. Describe how a central database could meet those needs, including who would operate it.
4. Describe what problem would remain if one organization controlled the record.
5. Sketch how a shared ledger might address that problem, then list the new responsibilities or complications it could introduce.
6. Decide which design seems simpler for this particular example, and write down what evidence might change your mind.

Myths and honest truths

- **Myth:** Blockchain is always better than an ordinary database. **Truth:** A conventional database may be simpler when one trusted organization can manage the record and correct errors. Compare the design with the actual need rather than assuming newer means better.
- **Myth:** A blockchain makes every recorded fact true. **Truth:** The design can help make changes to recorded history detectable, but it cannot guarantee that the information was accurate when entered.
- **Myth:** Tamper-resistant means absolutely impossible to change. **Truth:** The terms describe resistance and evidence of alteration, not a promise that change can never happen. A system also needs a thoughtful way to handle mistakes and disagreements.

KEY TAKEAWAYS

- Blockchain addresses a coordination problem: sharing a record when participants may not want one party to control it alone.
- A central database can be the better answer when it meets the need with less complexity.
- Cryptographic links can help make changes to earlier records detectable, but they do not certify that an entry is true.
- Every system depends on people, rules, and decisions about corrections, access, and responsibility.
- Start with the record problem, then judge whether blockchain is a useful fit.

REFLECT

1. *What shared record in your life works well because one person or organization manages it?*
2. *When would you want several participants to share responsibility for a record instead?*
3. *What would you need to know before trusting a technology claim about a public or community record?*

Nine more chapters are waiting

You've read the Introduction and Chapter 1. The full 92-page book continues with:

- CH. 2 How Blocks Become a Shared History
- CH. 3 Many Computers, One Agreement
- CH. 4 Keys, Wallets, and the Meaning of Control
- CH. 5 Digital Assets Without the Sales Pitch
- CH. 6 Smart Contracts and the Rules They Cannot Read
- CH. 7 Where the Idea Meets Everyday Life
- CH. 8 Practice Reading Claims Like a Researcher
- CH. 9 Avoid the Traps, Keep the Curiosity
- CH. 10 A Long Practice in Clear-Eyed Wonder

Plus the research analysis "What the Evidence Says", a 30-day practice plan, a glossary, and every source with full research credits.

JOIN FREE OR GO INSIDER

Join the free Reader's Circle at shadeddiemongruebooksgallery.com to read the full book online, listen with AI reading mode in a man's or a woman's voice, and download the PDF. Want every shelf? Reserve an Insider membership.

Sources for these chapters

Numbers in the text (like ³) point to these sources. Every statistic, finding and documented example was copied from its source page, checked word for word against that page in October 2026, and is restated here in plain English. Figures can change as sources update. This book is for education and is not personal financial, legal, medical, mental-health, nursing, investment or other professional advice.

- 1 **NIST**. *Blockchain | NIST*. <https://www.nist.gov/blockchain>
- 2 **Federal Bureau of Investigation**. *2024 IC3 Annual Report*. 2024. https://www.ic3.gov/AnnualReport/Reports/2024_ic3report.pdf
- 3 **Interoperable Europe Portal**. *The use of the National Blockchain Infrastructure to support the E-Residency Initiative in Estonia*. <https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/use-national-blockchain-infrastructure-support-e-residency-initiative-estonia>
- 4 **NIST**. *Blockchain | NIST*. August 27, 2026. <https://www.nist.gov/information-technology/blockchain>
- 5 **National Institute of Standards and Technology**. *Blockchain Technology Overview*. October 3, 2018. <https://www.nist.gov/publications/blockchain-technology-overview>
- 6 **National Institute of Standards and Technology (NIST)**. *Beyond Bitcoin: Emerging Applications for Blockchain Technology*. February 14, 2018. <https://www.nist.gov/speech-testimony/beyond-bitcoin-emerging-applications-blockchain-technology>