Bitcoin Clarity

Kiara Bickers

The Complete Beginners Guide to Understanding

Bickers & Son was an old and well-known book publishing house of 1 Leicester Sq. London. The publishing house was the principal business of the Bickers family, but it was destroyed during the World War II "Blitz" bombing in 1940. In 2019, Bickers & Son was brought back to continue disseminating information in the name of the family tradition.

Published by Bickers & Son softcover second edition May 2020

BICKERS & SON and colophon are registered trademarks of BICKERS & SON Inc.

For information about special discounts for bulk purchases please contact Bickers & Son sales at business@bickersandson.com.

All diagrams are designed by Kiara Bickers unless otherwise credited
All artwork is illustrated by Jordan Wesolek ©
Edited & Produced by Josh Raab, www.raabandco.com

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

ISBN 978-1-7338712-0-4 (Paperback)

Visit: getbitcoinclarity.com

PGP Key: https://keybase.io/kiarabickers/pgp_keys.asc

To my Dad, Mike Bickers, my Granddad Mike Bickers,
to my great grandparents, and all my ancestors, recursively.

Part I
CONCEPTUAL REFRAMING

Chapter 1 – Challenges in Understanding Bitcoin **1**
Problem 1 - Finding a Signal in the Noise 6
Problem 2 - The Breakdown of Metaphors and Analogies 11
Public and Private Keys 13
Addresses 16
Wallets 17
Bitcoin as Your Own Bank 19
The Blockchain as DNA 20
Bitcoin as Digital Gold 21
Problem 3 - Asking How Instead of Why 22
The Language of Abstraction 25
How This Book is Organized 28

Chapter 2 – A Trust "less" Timechain **31**
Bitcoin as a Blockchain 34
The Speed of Data 36
The Blockchain as a Timechain 38
Control-Loops and Feedback 43

Part II
ANALYSIS & KNOWLEDGE

Chapter 3 – Information Integrity: Balance and Validation **49**
The Evolution of Accounting 49
The Magic of Double-Entry and Double-Think 54
Balancing the Ledger 61
Making Change with UTXOs 63
UTXOs, Transactions, and Blocks 65
Chaining Blocks on the Blockchain with Hashes 67
Full Nodes, Full Validation 69
Light Nodes, Partial Validation 72

Chapter 4 – Information Propagation **75**
The Evolution of Nodes 76
Full Node Implementations 78
Mining Hardware Development 78
Scaling Light Clients into Mobile 80
The Propagation Cycle 81
The Mesh Model 82
The Cake Model 82
Fundamental Limits 84

Chapter 5 – Confirmation, Not Consensus **87**
A Manager-Worker Relationship: Full nodes and Miners 88
Proof-of-Work as a Puzzle 90
Hashes as a Measure of Work 91
Proof-of-Work as a Dice Game 92
The Alchemy of Mining 95
Confirmation and Its Undoing 96
The Dreaded 51 Percent Attack 96
The Test of Fees 100

Chapter 6 – Smart Contracts: Locking and Unlocking **109**
The Usefulness of Bitcoin Script 111
Opcodes and Transaction Types 114
The Most Common Transaction: Pay to Pubkey Hash 114
Fancy Transaction Types 116
The Civil War of Segwit 117
Questionably Smarter Contracts 119
Problem 1 – Not Security Focused 120
Problem 2 – Secure Code is Beyond Hard 120
Problem 3 – Token Incentives are Terrible 122
Problem 4 – The Gap Between Tokens and the Real World 125
Problem 5 – Off-Chain Data and Trusted Oracles 126
Off-Chain Payment Channels 128
Why the Lightning Network? 130

Part III
PROPERTIES OF THE SYSTEM

Chapter 7 – Governance **135**
The Potential Dangers of Blockchains 137
Improvements with BIPs 141
Soft and Hard Forks 144

Chapter 8 – Approximating Decentralization **147**
Types, Trade Offs, and Costs 151
Gaming Decentralization 154
Problem 1 - Number of Developers 155
Problem 2 - Developers' Contributions 155
Problem 3 - Number of Full Nodes Implementations 153
Problem 4 - Mining Pool Percentage 157
Problem 5 - Counting the Number of Full Nodes 158

Chapter 9 – The Properties of Money **161**
The Economics of Money and Trust 164
The Properties of Fiat and Cryptocurrency 167
Implementing Money In "Crypto" 169
Privacy and Fungibility: Two Sides of the Same Coin 170

Part IV
SYNTHESIS & UNDERSTANDING

Chapter 10 – Getting Started **177**
Understanding Exchange Incentives and Custodial Risk 178
The Right Wallet for You 180
Holding Strategies 182

Chapter 11 – Markets **187**
The Hype Panic Cycle 189
Types of Change 192
The Value of Information 194
Is Crypto a Scam? 198
Market Manipulation 199
Pump-and-Dumps 200
Wash Trading 201
Is Bitcoin a Bubble? 202

Chapter 11 – Mindset **205**
The Value Equation 207

Glossary **215**

PART I

CONCEPTUAL REFRAMING

CHAPTER 1

Challenges in Understanding Bitcoin

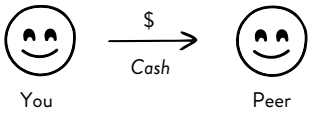
"If you don't believe me or don't get it, I don't have time to try to convince you, sorry."
– Satoshi Nakamoto, pseudonymous Bitcoin creator

You might as well admit it: Part of why Bitcoin is so hard to understand is because so many of us are clueless about money. Bitcoin is everything people don't know about computers, combined with everything they don't understand about money. It's already difficult for many of us to understand what gives money its value. Our culture treats money as an end in itself, yet most people are incapable of holding on to it beyond what they need to get by. Although it's certainly possible that money can play a higher role in our lives, it may not be the best place to start when grappling with Bitcoin. To understand Bitcoin, we first have to understand what motivated the technology.

A lot of what makes building the digital world interesting is trying to replicate existing models of human connection, online. When the internet was in its infancy, many **cypherpunk**[1] activists—advocates for privacy online, felt that users should have the same control of their own money online as they did offline. Ideally, even more control, if there was a technical way it could be done. The same way you pay a friend with the cash in your wallet, cypherpunks felt you should be able to hand someone digital cash from your digital wallet.

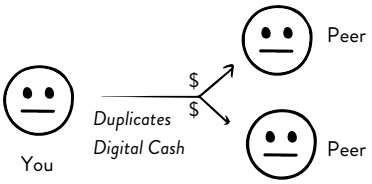
[1] For definitions of words in **bold** refer to the glossary.

A one-to-one, peer-to-peer cash transaction:



Passing physical cash to a friend or peer is simple enough, but duplicating this reality in the digital world was far from simple. Instead it was one of the biggest cryptographic breakthroughs of the decade. Because of the nature of digital data being so easy to copy-paste, there was no known way to move the digital cash file from one wallet to the next with any real guarantee the first person hadn't already spent that exact same money with someone else. This is known as a double-spend, or the **double-spend problem**.

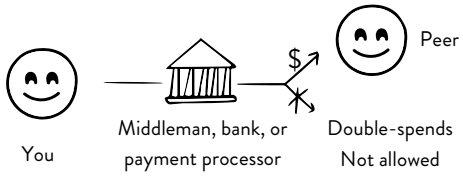
The same unit of digital currency being double spent:



While being able to double your money may sound like a compelling get-rich-quick scheme, to me it sounds like the beginning of some bad financial advice; and if everyone could double their money instantly, the concept of money wouldn't be worth much. So, for a long time people thought the vision of a digital currency was a dead end.

Even when PayPal started, its founders initially wanted to create a digital currency that would be independent from banks. But with all of the regulations and this technical double-spend problem they quickly turned from the idea of creating a new currency and settled for the possibility of processing payments between existing currencies. **Payment processors** like credit cards, PayPal, or Square are third parties that sit between merchants and customers to solve the double-spend problem, verify each transaction, mediate disputes, and to ensure that funds can only be spent once.

The payment processor solution:



While payment gateways stop users from double-spending, they are a far cry from the dream of the Internet being fully decentralized or having anything resembling a fully decentralized digital cash. The early "network of networks" that was funded by the U.S. Department of Defense to connect college campuses, eventually became the Internet. The vision of the Internet we wanted was always intended to be decentralized. So that global communications would survive end of the world scenarios like world wars or authoritarian shutdowns. If one part of the system was shut down or failed, the rest would still function.

The internet we got was much more fragile and vulnerable to even nationwide censorship. You see, data needs a physical way to travel from you to me, and in the early days of the Internet we would use home phone lines. But this process was painfully slow and not great for any more than the 90's version of the Internet which was mostly text-based. Internet service providers (ISP) stepped in and first offered copper-based coaxial cables that transferred data through electricity. Now they offer fiber-optic cables that are much faster and transfer a substantial amount more data over strands of glass or plastic with light.

Some interconnections of our internet, into and out of smaller countries are based on a single-wired connection. Which makes it technically possible to shut down the internet in Armenia with an axe[2]. In countries like China, Venezuela, Russia, or Iran where the government owns and controls wires at the base of their local Internet, governments can control the flow of information or pull the plug on connectivity entirely.

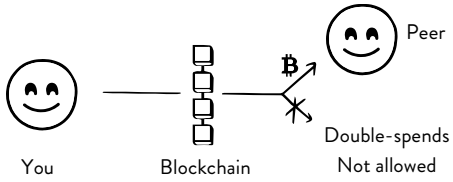
Even in countries like the U.S. that have a more robust connection of wires that move data around, still need computers to store large scale

[2] This is something that actually happened back in 2011, when a woman was out scavenging for scrap copper to sell and cut the cable.

memory. So, the big tech giants: Amazon, Google, and Facebook, step in to organize, store and give us access to our data. This adds another layer where censorship, suppression, and control is possible.

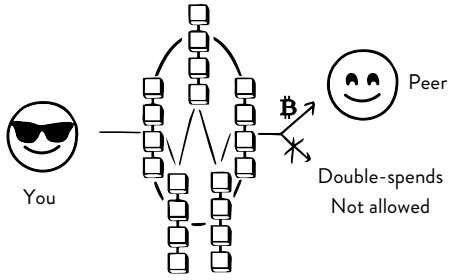
Ideally, we want a system for communication and payments where it isn't technically possible to implement censorship at all. The idea of Bitcoin was to create a form of digital resilience, which could also solve the double-spend problem in a novel way. By putting all of its transactions on a public ledger (now more popularly called the blockchain). Bitcoin allowed people to independently verify the history of all transactions without relying on any single third-party service, company, or government.

Bitcoin's double-spend solution:



Funds sent in bitcoin on its blockchain are only allowed to be spent once. But Bitcoin didn't just cut out the middleman to become the new middleman. What was unique about Bitcoin's shared ledger was that it wasn't limited by one centralized choke point. Bitcoin isn't a single ledger, but thousands of independent instances of the ledger, that are all synchronized to the same state.

The peer-to-peer network of Bitcoin users:



The peer-to-peer network of
independent blockchains in Bitcoin

Anyone with minimal resources and ambition can run their own copy of the blockchain. It's this property of the blockchain that people are celebrating as trustless. But the term "trustless" is somewhat ambiguous. What cryptographers mean when referring to trustless systems is that the trust required from any single entity in the system is minimized, because verification and mediation are distributed among the users of the network. Now that the hype of the cryptocurrency industry and decentralization is in full effect, it is more important than ever to be as clear about the blockchain's purpose and capabilities as possible. What exactly is the purpose of the digitally shared ledger concept?

The purpose of the ledger in the "blockchain" is to give users a shared history of transactions to agree on.

This shared history makes it possible for people to trade **peer-to-peer** without the use of a trusted middleman, third-party, or clearinghouse. For the first time in history, every person in the world can accept funds and be certain that ownership of those funds is irrevocable. But the blockchain is not without its costs. Ironically, one of the costs requires that users understand cryptography enough to trust it.

The simple questions like, what exactly is Bitcoin? Is it finance, economics, or is it just some new technology? How you answer this question is likely to influence the way you look at Bitcoin from here on out. Bitcoin is full of pain points, and at the top of the list are questions loaded with "shoulds." "Should I buy?", "Should I invest?", "How much should I invest?", "Should I use this wallet or that wallet?", "Should I do it now or later?"

Although this book is not in any way intended to be investment advice or a practical guide to getting Lambo style rich with Bitcoin, it will give you the tools needed to make those important investment decisions on your own. This first chapter covers the three primary problems I see people struggling with the most: finding a signal in the noise, the breakdown of metaphors and analogies, and asking why instead of how.

Problem 1 Finding a Signal in the Noise

While I was spending time away from my home in Silicon Valley, crashing at a then girlfriend's house over in UT Dallas, her engineering friends convinced me that if I wanted to understand Bitcoin I should learn how to code. So that's what I did. I spent about a year learning how to code in C++, the primary language Bitcoin is written in. But as any experienced programmer knows, a year of studying doesn't take you far past the most basic "Hello, World!" program, and it definitely wasn't enough for me to do anything useful with Bitcoin.

Learning how to code gave me more questions than answers, it took up all of my time, and it didn't get me any closer to my objective of understanding Bitcoin. What I hadn't realized at the time was that (1) learning how to code does not reliably produce understanding of complex coded systems, and (2) when attempting to learn something new, the first thing you have to do is to clearly define the ends, then work backwards to achieve them. So, what are you trying to achieve? When I decided to learn how to code, I wasn't very clear on what my objective for understanding Bitcoin was.

Do you want to be a Bitcoin user, an investor, a trader, or a programmer? I had no idea. When I started out I was wandering aimlessly, pursuing an interest on a whim. Sure, Bitcoin sounded technically and economically interesting to me, but when I look back on my first few years of learning about Bitcoin now, I realize I wasn't trying to build a skill, I was looking for a lifeline. Intellectually I was interested in economics but underneath, emotionally, I was more interested in any massive adrenaline shot that had the potential to change my life; so I did the online equivalent of playing the lottery, I bought Bitcoin. What did I have to lose? I had no college degree and no plan, and I was stuck working a catering job at Stanford, which I leveraged to get into every Bitcoin event on campus.

On campus—and even more so on social media—I learned that there were quite a number of people who considered themselves "crypto influencers." Cryptocurrency is complicated, and because of that, it's easier to trust what someone is confidently telling you than it is to do your own research. It quickly became apparent to me that knowing whom to listen to and whom to trust was one of the hardest problems in Bitcoin. "Trust but verify" is a popular phrase in this new

world. But unless you're a cryptographer, everybody has to believe somebody, and most people choose the wrong people to believe.

Bitcoin has a lot of cheerleaders, and the loudest among them often enjoy fighting online in an entertaining display of social dominance or over some perceived notion of control in Bitcoin. Can people in the short-term change the perception of Bitcoin by amplifying an opinion from authority? Sure. But in the long term, the truth is that no one controls Bitcoin, which on the surface may be difficult to understand and even harder to internalize. There is no ultimate or leading Bitcoin company, there is no Bitcoin CEO, there is only software. Bitcoin is **open source**, meaning that the code behind the software is fully available to the public for people to copy, or modify, on their own terms. To ask who's the leader of Bitcoin is akin to asking who's the king of the internet. On the internet, everyone is the king of their own following and audience.

What I quickly learned is that the thought leaders and influencers are generally not invested in improving your understanding; they are focused on building a brand. Worse still, many of the loudest on social media have no recognized credibility by any actual developers. But because both ignorance and fraud are widespread in the extended cryptocurrency community, it's difficult to distinguish between the well-intentioned people who are unintentionally ignorant and the scammers who are being intentionally deceptive. Intentionally or unintentionally, the information promoted by influencers is often for personal and tribal gain. This is not something to take lightly, given that once you're exposed to the wrong information, it can become very difficult to unlearn. At a certain point, once a person has invested so much time in any particular belief system, they're indoctrinated, and it's nearly irreversible.

Luckily, in the first few years I spent learning about Bitcoin, I did manage to learn a few correct things along the way. For three years—during my one-hour commute to and from Stanford—I would listen to lectures from the Mises Institute, forming my view on Austrian economics. For anyone that hasn't studied economics, the Austrian brand of economics is rarely taught in any school, because its principles contradict so much with the way society, governments, and banks are currently structured. The Austrian School of economics teaches that the value of money originates from the market itself—not from the State

that issues it. This exact realization is part of what led to the creation of Bitcoin. Bitcoin was created to have the properties of money that would be the most valuable in the market. It was this "non-certified economics degree" that I got from listening to free podcasts in my car that put Bitcoin on my radar in the first place.

Although taking an interest in economics and learning the basics of how to code didn't immediately help me in understanding Bitcoin, it did help me understand the mental models of programming enough to hack together a few open-source projects that worked with Bitcoin. I ranted about Bitcoin to anyone who would listen. I wrote the first Bitcoin paper wallet[3] generator for iOS, and a proof-of-concept project that stored data on the blockchain. First slowly, then seemingly all at once, I went from merely being interested in Bitcoin to working at the Bitcoin company Blockstream, close to many of Bitcoin's protocol developers.

What I've learned from walking the path of a Bitcoin enthusiast to more of an educated skeptic is that even the wizard-level crypto-magic developers aren't clear about the best way to go about explaining Bitcoin. It's the difference between hard and soft skills. The hard skill of knowing how to best progress to the Bitcoin protocol is different from the soft skill of know-how required to explain it.

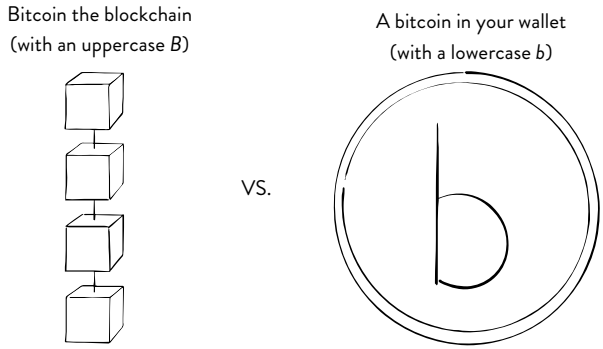
This is where the idea for Bitcoin Clarity came in, because I recognized that Bitcoin was being explained fairly poorly by everyone else. If you've ever tried to explain Bitcoin, you know from experience exactly how hard that is.

One of the more commonly overlooked problems in Bitcoin, is the temptation for Bitcoiners to write about every tangential topic that's interesting, instead of focusing on what's directly *useful* to the reader. The problem with interesting is that almost everything is interesting to someone. For Bitcoin developers, what's *interesting* tends to be some new advanced feature that the average user isn't exposed to. To journalists, interesting seems to be entirely focused on the volatility of the price, the perceived wastefulness of mining, or my favorite topic, grammar!

We should get this out of the way now, and I have the guts to say it. The term "block chain" looks better as one word. The industry uses

[3] A paper wallet is a way to print out the keys that store your bitcoin digitally, and instead keep them offline on paper.

the word Bitcoin with a capital *B* to refer to the Bitcoin blockchain, and a lowercase *b* to refer to specific bitcoin or the value that is traded within that system. See? There I go focusing on things that aren't useful to you. . . .



This is generally what everyone in the industry does, they rant about what's interesting to them. There are tens of thousands of blog posts that address every issue possible in Bitcoin. But not one complete explanation of Bitcoin as a system. That is what I'll attempt to do here. The simplest definition of **Bitcoin** is that it is a protocol for transferring value securely over the insecure internet. That's it. To me personally, interesting is that which makes all this complexity simple. So, for the sake of simplicity, I treat Bitcoin as a signal and everything else in the cryptocurrency world as noise.

In this industry, what are called **whitepapers** are often issued as a way of publishing the technical outline to a new system, blockchain, or token issuance. In the early days of cryptocurrency, there were so few whitepapers that it was relatively easy for the community follow the development of the alternative cryptocurrencies (or **altcoins**). But over the years, the industry has evolved into using whitepapers not much more than mere marketing pamphlets. Now, there are more blockchains than there are competent developers to program them, and more whitepapers than there are individuals capable of understanding them. It's a mess.

It took me several years to understand Bitcoin, but without that deeper level of understanding, I would have never been able to seriously evaluate any other cryptocurrencies.

A firm understanding of Bitcoin is the best possible place to assess the technical viability of any other blockchain.

Not everyone can immediately see the value of Bitcoin, most people only see the price. Without fail, a pattern that plays out when people first hear about Bitcoin is that many of them will want to know, "Which altcoin will be the *next* Bitcoin?" To me this mentality in people amounts to looking for a tip on a fast pony, and the mindset means that they've missed the point of Bitcoin entirely. Their perception is that bitcoin is overpriced, and that they'll personally be the lucky ones to get their bet in early on next blockchain before it becomes overpriced too. It's a confident bet on their abilities, but it's a bet that saner minds wouldn't take.

I recognize that we live in a world where the Bitcoin price dominance can at times be in flux, I believe this is because people don't understand the technology behind Bitcoin in the first place. Bitcoin was real innovation, but the same can't be said about every blockchain.

I don't divide cryptocurrencies into either profitable or unprofitable. Cryptocurrencies are either interesting or boring.

And from my perspective there is no altcoin, initial coin offering (ICOs), tokenized asset, or stablecoin as interesting or innovate as Bitcoin. The story arc of every altcoin and token is always the same, some are pumping, some are dumping, and eventually most are forgotten. But arguably worse than being boring, many of them are outright scams. And the best antidote to scammers is accurate information about their products, which is what I'll attempt to provide you within this book.

While I'll discuss some of the market noise later on, this book is focused on Bitcoin (abbreviated as BTC). I believe that without a solid foundation in the properties of Bitcoin, learning about other blockchains is nearly impossible. Learning the technical details of how Bitcoin works may at times seem like noise, and in other contexts it often is. Although the average user does not need to have read every

line of Bitcoin's code to use it, there is some minimum level of technical knowledge necessary to understand it. If you don't learn enough to critically think about these systems for yourself, someone else will do the thinking for you, and it will likely be to their advantage. Because of this, the first half of this book pertains to standard Bitcoin terminology, and the second half more controversial truths about Bitcoin—as I see it.

I've chosen to write all of this in a book instead of a series of blog posts because books are the best way to organize long thoughts. But the sad reality is that most people don't read more than one book a year. So, for the people who prefer a more interactive environment for learning, I've also released this content as an online training platform at **getbitcoinclarity.com**. Both the online training and the book are designed to provide new abstractions and mental models to help you bring disconnected bits of knowledge together and to form a comprehensive understanding of Bitcoin as a whole.

Problem 2 The Breakdown of Metaphors and Analogies

In the early days of the Internet, there was a lot of confusion about how basic tools like: emails, websites, ads, and the internet itself worked. All of these services that we take for granted today were once hard to explain concepts just like the blockchain. On one 1994 episode of The Today Show, two hosts fumbled around explaining this new technology.

Bryant Gumbel: *"What is Internet anyway?"*
Katie Couric: *"Internet is, um, that massive computer network? The one that's becoming really big now."*
Bryant Gumbel: *"What do we write to it, like mail?"*
Katie Couric: *"No, a lot of people use it to communicate with writers and producers. Allison, can you explain what internet is?"*
Bryant Gumbel: *"No. She can't say anything in 10 seconds or less."*

This mess goes on until another colleague chimes in, describing the internet as "a computer billboard." Replace the word "internet" with

"blockchain" and suddenly their confusion seems all too relatable. For over a decade, techies were trying to explain *how* email worked, but what most technical people didn't realize is that for the general public, technical explanations are not particularly useful. The purpose, when dealing with the general public, isn't to help them understand the intricacies of mail servers, but for them to feel comfortable enough to use email successfully.

Emails *appear* to go directly from sender to recipient:

> The sender's inbox → The recipient's inbox

We all know the details are more complicated, but this basic explanation is a good enough mental model for most people to work with. Once people started using the Internet regularly, explaining the details of how it worked became less and less important. The same will likely be true for Bitcoin. When you send bitcoin to a friend, you don't need to know much about how Bitcoin works. In that sense, even the intricacies of Bitcoin itself are, to a degree, noise. In the future, the average user will be less motivated to know the details about how a transaction works because society as a whole will be comfortable sending it without that deeper knowledge. But until that day comes, knowing the details about how a transaction works can give early adopters more confidence in using Bitcoin and explaining it to others.

Most of the terminology in cryptocurrency has a historical basis in cryptography and was originally designed by engineers to analyze and explain how a part of the system works in one instance, and not to explain why those parts work in the system as a whole. The result of this is that Bitcoin's technical language of keys, addresses, and signatures are all metaphors for preexisting cryptographic tools. But as with any metaphor, people can interpret them differently, and they can break down into meaninglessness.

It's not that metaphors are entirely useless; they do simplify Bitcoin for non-technical users, but only as long as the conversation doesn't go too deep. Analogies are similarly great linguistic tools for introducing a world that we've never heard of before. Any kid that's never heard of a unicorn would easily understand it if they were told it's like a horse

with a horn on its head. The use of comparisons to express ideas and solve problems has the power to open up new mental spaces.

But there is an obvious inadequacy to metaphors when people take things too literally. The consequences of sending your bitcoin to the wrong bitcoin address are a lot more serious than if you send an email to the wrong email address. It's important to recognize the limits of analogy and to understand how to map each term to the underlying technical details. I'll go into some of the most common metaphors applied to Bitcoin here.

Public and Private Keys

Like email, Bitcoin transactions appear to go from sender to recipient:

> The sender's private key → The recipient's public key

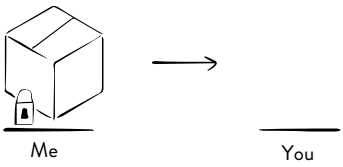
The truth is that there is no sender address at all in Bitcoin, only private keys and recipient addresses. A more accurate understanding of Bitcoin transactions is less about sending and receiving bitcoin, and more about locking and unlocking value on the blockchain:

> The private key *unlocks* the sender's bitcoin → The public key *locks* the recipient's bitcoin

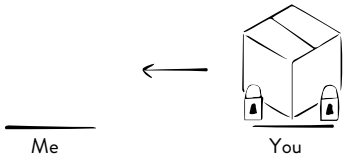
In the context of Bitcoin, a **private key** is the key that allows bitcoin to be spent (by unlocking bitcoin the sender owns). And a **public key** is the key that allows bitcoin to be received (by locking bitcoin for the recipient). To better understand the relationship between sending and unlocking we can run through some thought experiments.

If we take it all the way back to the basics, a lock is any device that's used to prevent opening, and a key is the device that's used to open it. The oldest known lock and key ever discovered by archaeologists is estimated to be somewhere between 6,000 to 4,000 years old. For thousands of years, and until fairly recently, people assumed that to lock something up with a key meant you had to open it up with the same key. But with a few different examples we can see that's not necessarily the case.

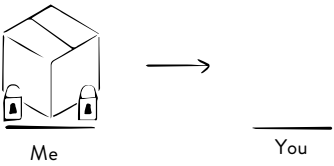
1. First, I put a secret in a box, lock it, then send the box to you.



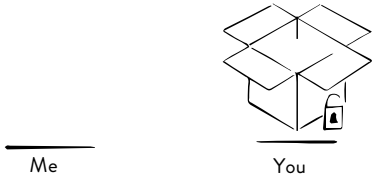
2. When you get the box, you put your own lock on it and then send the box, with both of our locks on it, back to me.



3. When I get the box, I take my lock off and send it back to you with only your lock on it.



4. At this point only your lock is left on, so you can unlock the box and claim the secret for yourself.

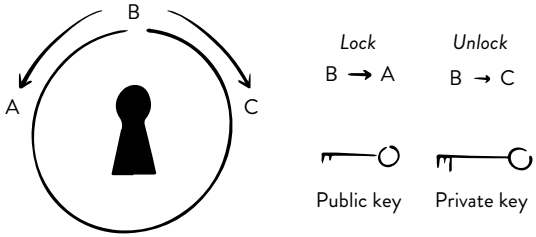


This way, the secret in the box can be sent securely. While traveling, the box is always locked, and neither party ever has to send the key in a separate (unprotected) channel. Neat, huh?

Although this is not at all how public-key cryptography works, it makes the point that a locked box can literally be opened with a different key than the key that first locked it. A more accurate example of public key cryptography requires that the sender and receiver each have their own set of two keys.

We all understand that a standard lock has only two possible positions or states: locked or unlocked. Imagine that each of those two states are separated into two separate keys: one key to lock the door and another to unlock the door. If you can imagine a lock that has two keys, one for locking and one for unlocking, this will get you pretty far in understanding Bitcoin without knowing any actual cryptography.

Public-key cryptography model[4]:

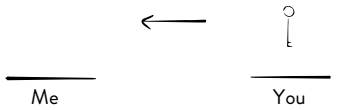


The public-key is, you guessed it, shared publicly! So, anyone with your public key can lock secrets for you. And the private key is kept private so that only you can unlock the secrets locked on your behalf. Anyone with your public key can lock up secrets (or bitcoin) for you, while only your private key can unlock your secrets (and move your bitcoin). In public key cryptography, the public key locks the secrets and a private key unlocks them. In Bitcoin, the secrets are the bitcoin you own on the blockchain.

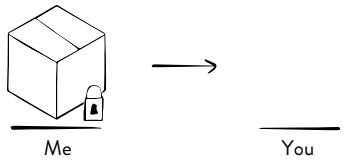
[4] The visual expression of public-key cryptography as a single lock split into two keys comes from Panayotis Vryonis "Explaining public-key cryptography to non-geeks." *Medium*, 2013.

To use the box example again, we can visualize how public-key cryptography works in Bitcoin.

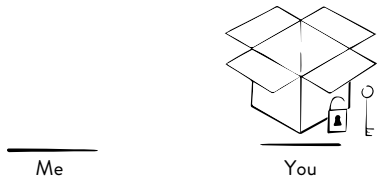
1. You send me a copy of your public key.



2. I put bitcoin in a box and lock it using your public key, then send the box back to you.



3. When you get the box, you open it with your private key and claim the bitcoin I sent you.



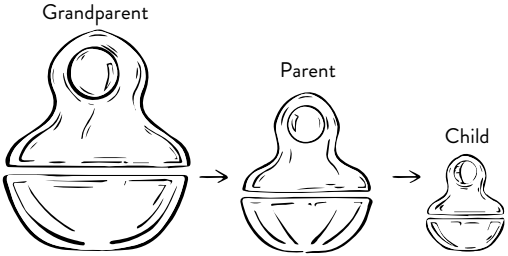
In this way bitcoin are *sent*, or more accurately, the bitcoin are *locked*, on your behalf. If you already have some experience using bitcoin, you may be asking yourself why you've never interacted with public keys like this? In Bitcoin, we refer to public keys as addresses, or **QR codes**. Which are basically just smaller versions of the underlying public key.

Addresses

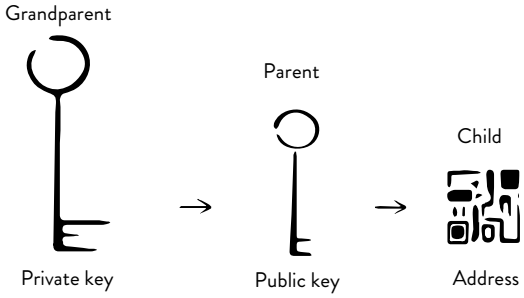
In public-key cryptography, public and private keys are generally used for locking and unlocking messages or emails. The two keys are mathematically related in that the public key is made from the private

key, but the private key can't be regenerated from the public key (which is exactly why the public key can be public). In Bitcoin, keys are used for locking and unlocking bitcoin on the blockchain. Addresses are related to public keys, in the same way public keys are related to private keys. The public keys are generated from the private key, and the bitcoin address is generated from its public key. With new terminology this can seem a bit complicated, but we can make it much simpler by visualizing the relationship between keys and addresses with Russian dolls.

The inheritance of nested Russian dolls:



Key derivation from private keys to public keys to addresses:



Because the "child" address is a smaller piece of data, it's impossible to use it to re-create the parent. The problem with the terminology "address" is that we assume a Bitcoin address works something like an email address or a physical address. But with a Bitcoin transaction, you can't return to sender. Each address is intended to be used only once. There are a few different kinds of Bitcoin addresses, but they all have this same property and similar function, as a one-time destination on the Bitcoin network for a single transaction. A more accurate way to

think of an address is as a one-time lock. If you lock some bitcoin up with a lock you don't have the key for, you're never going to be able to unlock that bitcoin again.

Wallets

The assumption with the term wallet is that a Bitcoin wallet functions something like a cash wallet, which is generally true. The functions of digital wallets and physical wallets are more or less the same—to store and spend money—but the properties of the two are very different.

With a physical wallet, you are directly holding cash that has value, but with a digital wallet you never hold the value directly, you only ever hold access to it on the blockchain. If you cross a national border from one country into another, did your bitcoin move with you? Well, no.

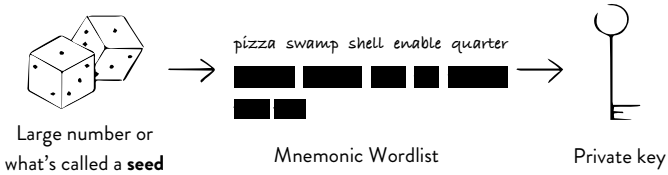
On the Internet we often say we are either online or offline, we either have a profile on a particular social media platform or we don't, but those facts have little to do with our physical selves. The digital world represents a secondary layer to the world we inhabit and is largely independent of where we are physically. If we think about the digital world this way, the movement and possession of bitcoin makes sense only in the context of transactions on the blockchain, because we never hold them physically.

The private keys stored in your bitcoin wallet represent only the ability to move funds, not the funds themselves. Although it's true for both digital and physical wallets that if you lose them, you lose access to your funds, only with digital wallets can you create a backup.

The same way the number "0" and the word *zero* represent the same information in two different ways, we can also store our private keys in different ways. A Bitcoin private key in its simplest form is just a big secret number. That number can be represented digitally as bits, visually as a machine-readable QR code, or conceptually as a human-readable word list called a **mnemonic phrase**[5].

[5] Refer to page 112 for more detailed information on mnemonics.

Bitcoin private keys represented in several different ways:



In Bitcoin, this means that you can store the information that gives you access to your funds entirely in your head without the need for much of a wallet at all. It would be more accurate to think of wallets as a keychain, but that term was already taken in cryptography.

Digital wallets also have the additional functionality of being protected with a password. A hardware wallet is a special type of bitcoin wallet that stores the information of a user's private keys in a secure hardware device to isolate and protect their private keys by keeping them **air-gapped** and offline.

The analogy that a bitcoin wallet is like a cash wallet breaks down further around the words "account" and "balance." People often associate the term *wallet* with something like their online bank account, but there is no concept of an account or balance in Bitcoin. These are convenient metaphors intended to make Bitcoin more user-friendly.

Bitcoin as Your Own Bank

I have to assume that when people say, "Bitcoin is like a bank," they say that because when you own bitcoin, you're taking full responsibility for your private keys and full control over your money. But this comparison has always bothered me because I would hate Bitcoin to be anything like banks.

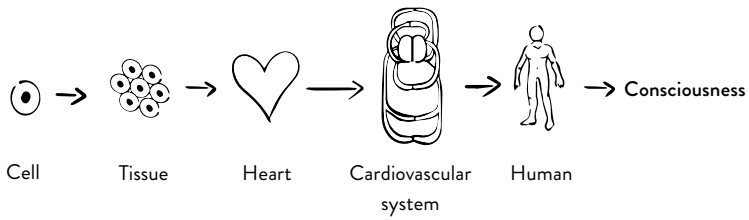
With Bitcoin you and only you can move your funds. Bitcoin is scarce and limited, whereas the money created by central banks is backed by nothing. Central banks are privately owned institutions, whereas Bitcoin has no chief executive officer, no chairman of the board, and no majority shareholder. Bitcoin gives you far more responsibility over your funds than any bank. Bitcoin wasn't created to be like banks, it was created to because of the global failure of banks.

The Blockchain as DNA

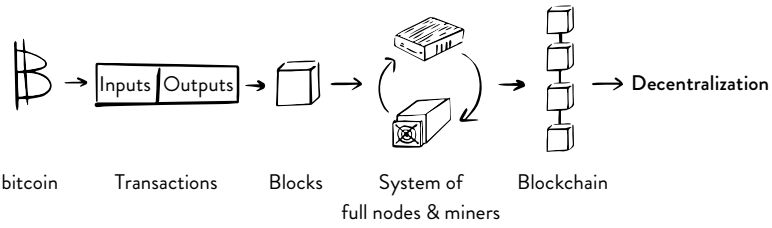
I have heard people describe the blockchain as something like DNA or early AI because they're both stored forms of code that self-execute. The difference being that genetic data encodes *off of* DNA for specific proteins, whereas financial data is written *on to* the blockchain for long term storage. But a decentralized hard drive for financial data is not exactly what most people think of when they're imagining the future of artificial intelligence.

Still, it's interesting to think of blockchain as something lifelike that grows. Because the blockchain is designed to be a form of digital resilience, there are a lot of similarities to the resilience we see inherent to life. Both blockchain and biological organisms have emergent properties of resilience, that is to say, properties that come from the system working as a whole. An **emergent property** of a system is a property that the individual parts of the system don't have on their own. For blockchains, that emergent property of resilience is its decentralization and censorship-resistance. For an organism, that property is life and consciousness, the ability to perceive and respond to its environment.

Consciousness is the basic emergent property of organisms:



Decentralization is the fundamental emergent property of Bitcoin:



Bitcoin as Digital Gold

The claim that Bitcoin is like gold is based on the fact that Satoshi designed the system for there never to be more than 21 million bitcoin in supply. The implication that follows from the gold comparison is that if gold is scarce, and Bitcoin is scarce, then Bitcoin should be valued similarly to gold. Critics of gold will note that the price of it has fluctuated quite a bit over the past decades. Still, it's fair to recognize that the perception of Bitcoin being like gold probably increases the value of both gold and Bitcoin overall.

In truth, Bitcoin's total controlled supply is provably much less than 21 million. In part because so many people lose their keys and therefore lose access to those funds forever. And in part because it's also possible to provably destroy bitcoin, and for the miners of currency to allow some fraction of that 21 million to never be created in the first place. Although this fact may shock some, many who hold bitcoin regarded the destruction or loss of some proportion of the total supply as a net benefit to everyone else holding, since losses only makes the total supply scarcer.

Although comparing Bitcoin to gold, or Bitcoin to banks may work for a sound bite, if you ask anyone (including Google) for a more in-depth explanation, what you'll get is likely to only be understood by your company IT guy. The average Bitcoin step-by-step, comprehensive, or under the hood guide is generally not written with empathy for the less technical audience. Engineers have a trained drive for objectivity. In debates on technical subjects there is generally a right and a wrong way to do things, and logic is a more reliable way to getting at objectivity than emotions. What some engineers may forget is that the opposite of a good idea can also be another good idea. Maybe some scientists could test if training the analytical parts of the brain comes at the expense of the empathetic portions of it. Because it certainly seems like that's the case. It's my belief that in life people start off curious, but along the way their ego gets hurt by the objectivity of being wrong and they start to self-identify as non-technical.

How do you know whether you're a technical or non-technical person? Being technical has nothing to do with your ability to do math, your background in a STEM field, or how many letters you have after your name. It really just comes down to curiosity. And it helps if you

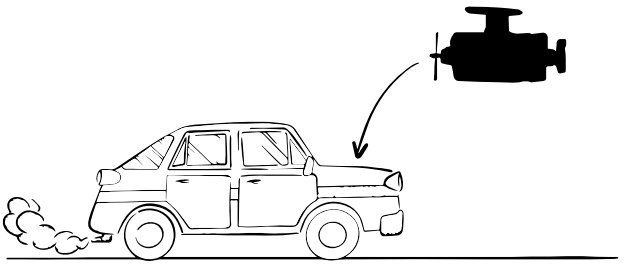
can maintain that curiosity even after you're proven wrong in a given case. Technical people may not enjoy being proven wrong, but they'll surrender to it if your superior logic can prove it. Technical people are curious about how things work, they enjoy getting closer to the truth, and being less wrong. Non-technical people find those same details confusing, overwhelming, or just plain boring. If you're reading this book, we already know you're curious. My job is to explain the details of a complicated system in a way that fuels that spark curiosity instead of extinguishing it.

Problem 3 Asking How Instead of Why

When people ask what Bitcoin is, Bitcoin's community of technically inclined people will often rush in with explanations about how it works. But explaining how Bitcoin works is not exactly simple. Explaining how Bitcoin works isn't a clickbait headline, it can't be reduced to a single sentence or a meme. A complete explanation about the system is naturally as complicated as the system itself. To illustrate the problem with asking "how" questions a bit more, I'll steal an example of *systems thinking* from the professor who originally showed me this mental model: Dr. Russell Ackoff.

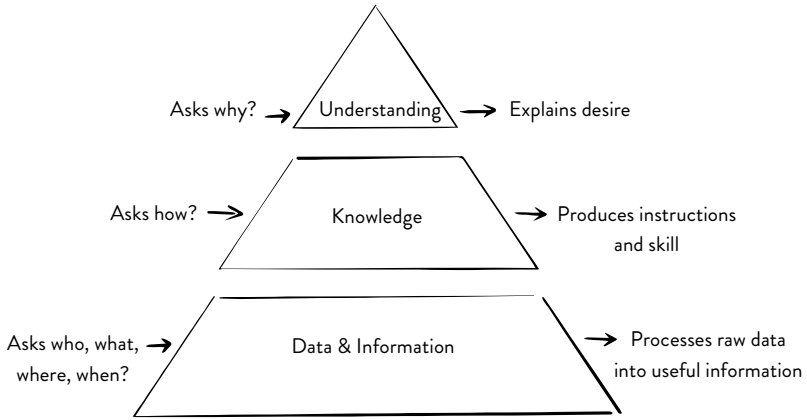
A car is a simple mechanical system that everyone in the world has experience with. If you ask a mechanic how the engine works to move the car forward, he can explain *how* the engine combines fuel and air to create a combustion reaction under pressure of its pistons, and then he can show you how the system works by taking the engine apart.

But if you ask the mechanic *why* the engine is upfront, taking the car apart won't help you.



Most of us already know why the engine is in the front; it's because the car used to be called the horseless carriage, so the motor was put up front where the horse used to be. But asking how the engine works can't answer this question. The word how is a tool, that takes us inside of the system, but in this case the answer to our question lives outside. "How" questions only give us answers specific to the internals of a system; "why" questions might give us insight into the bigger picture by stepping out of the system entirely. But sometimes we don't have access to that level of understanding, because we're incapable of stepping out of the system we're locked in.

The difference between knowledge and understanding:



Answers to "why" questions are called explanations. "Why" questions take us *outside* of the system in a process called **synthesis**. Synthesis builds on understanding and explains desire or intent.

Answers to "how" questions are called instructions. "How" questions take us *inside* the system in the process of **analysis**. Analysis builds on our knowledge, and our ability to leverage knowledge produces skill. The process of analysis gives us knowledge about how systems work, but it can never explain why they work the way they do. Both synthesis and analysis are needed for a complete interpretation of any system. This concept is called **systems thinking**.

When you recognize that most people and especially engineers think analytically, understanding Bitcoin becomes much easier.

This process of analytical thinking is the dominant mental model that organizes society, and few recognize any possibility of an alternative. You may not see the problem here, but as you get a higher perspective on how analysis dominates all of our thinking, you'll begin to see the cultural blind spot.

When a student goes to university to study any subject, each subject is taught nearly exclusively by breaking the subject up into parts. Take computer science for example. Most universities don't teach computer science as an evolving whole, its history, principles, and theory. Computer science is broken down into its component parts: discrete mathematics, data structures, database architecture, algorithms, and compiler design. The student studies each of the parts, and the assumption is that if they understand the parts taken separately, they'll be able to integrate that knowledge into an understanding of the whole of computer science.

Knowing one fact about a system is a single data point in a three-dimensional sculpture. Being an early Bitcoin millionaire and getting lucky on the markets up and downs doesn't mean you understand the technology. Being an engineer and understanding the language of keys, addresses, and wallets, doesn't mean you understand why people are driven to use something like Bitcoin. Even PhDs who study cryptography in academia, often don't understand the practical needs of cryptography in a cryptocurrency.

Understanding the basics of how any system works requires taking it apart to some degree. How far you choose to go down the Bitcoin rabbit hole is ultimately up to you—it's a long way down the hole before you hit any 1s and 0s. For the scope of this book, we won't be using any code, cryptography, or math to explain Bitcoin. But with a system as complex as the blockchain, you often do have to "go through" some amount of technical knowledge before you can come to any full understanding. In this Alice in Wonderland style elevator you have to go down before you can go up.

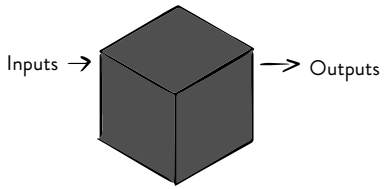
Understanding why Bitcoin was created, and why people value it doesn't require taking it apart, but it does require understanding people, behavioral psychology, and our existing financial system. People want to understand why Bitcoin is valuable so they can invest in it and start using it, but people don't understand it. Not because it's complicated (which it is) but because the industry is full of analytically minded

people collectively talking about how it works, not why it's needed. Most people don't need to know every detail of how Bitcoin works. You only need to know enough about how it works for you to trust it and feel comfortable using it.

The Language of Abstraction

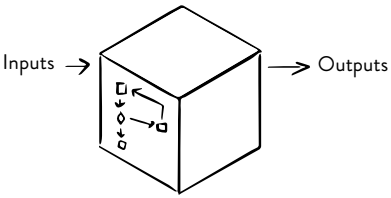
It's going to make the journey of learning about Bitcoin a lot easier if you can accept that there are things that you're going to have to ignore. For many of the concepts in this book, I'll start with high-level abstractions, and hide the unnecessary complexity away with a "**black box**." This is to keep both you (and me) focused on the topic in front of us, by not trying to explain everything all at once.

Black box thinking:



As you gain some knowledge about the system, I'll expose more of the details that were previously in the black box and continue with the relevant concepts while still hiding away some of the complexity.

Black box thinking exposed:



Although I'm not going to point out these black box moments directly, if you have some understanding of Bitcoin already, you may at times get the impression that I'm not explaining something fully, when in

fact I may be intentionally holding off a deeper explanation until we're further along in a new way of thinking.

Although you don't need to be a developer to understand Bitcoin, you do need to know how to think like a developer, and black box thinking is a big part of that. It's helpful to recognize that this type of thinking, even for non-developers, isn't new. Human pattern recognition is exceptionally good at using black boxes. We're all used to doing this because we're surrounded by black boxes all the time.

We can't see someone else's intent. If you don't understand why someone is doing something or acting in a certain way, you can look at the consequences of their actions (the outputs of the system) and then infer their intent from those consequences. We may not know why something like Stonehenge was built, but we can infer that it was some sort of temple based on its function as a lunar and solar eclipse clock. This type of thinking is so innate to us, that we've done it for all of recorded human history. At the root of consciousness is the ultimate black box. We have no objective answers on why we're alive. But we act as if life is valuable, and we infer that there is a higher value and purpose to our lives because of it.

Concrete words represent things that we can see, hear, and touch. Abstract and often loaded words like courage, honesty, love, and integrity are meant to describe things and concepts that we can't touch. The basic function of abstraction is not to be meaninglessly vague, but to encapsulate and ignore the irrelevant details and develop a precise language at a new level of thought.

The pre-classical Greek language used what we would identify as the words for eye and light interchangeably. Either word could also be used to describe or something beautiful or admired. The words were being used both in the concrete and in the abstract sense, because they hadn't fully separated the abstract from the concrete yet. Plato believed that light originated from the eye, whereas Aristotle believed that light was emitted from the sun and bounced off other objects making them visible to the human eye.

For the Greeks, light didn't travel through space and time, it was a bridge between this world and the next. And in the deepest sense, the idea of the sun being a bridge between this world, and another is still metaphorically true; the sun has existed for all life that lived in the past and will exist for all the life that lives on Earth in the future.

Though we don't think of it this way anymore. Today, we tend to look at people in antiquity as if they weren't scientifically minded at all, when in fact they were scrutinizing all the black boxes around them.

As modern people we have a bias toward thinking we're more intelligent or more objective about reality than ancestors living even just a few hundreds of years ago. We're too smart to consider that the language, belief systems, and mental models we are operating under affect us and the way we understand the world, just as it has for every generation. Take physics for example. Physics is the study of matter and its motion through space and time. But physics could also be correctly viewed as the study of symmetry, the function of harmonizing parts into a reflection of the whole.

Physics is primarily concerned with universal laws that act symmetrically. Culturally, we tend to think of symmetry as an artistic quality, but symmetry is a place where both the physicist and the artist have something of value to offer. The physicist asks where symmetry exists and how it behaves, while the artist asks how they can re-create it, mirror it. If we could conceive of it, a complete study of symmetry would have to include both the sciences and the arts. And it would represent the human attempt to cultivate order, perfection, and connection in the universe.

Abstractions can be expressed in a number of ways. Isaac Newton contributed to developments in the telescope, calculus, and discovered the three laws of motion. Leonardo da Vinci invented early concepts for the car and the helicopter, and his drawings of the muscular human structure were the basis of the first medieval anatomy textbook. Newton's inventions and theories were expressed in equations, while Da Vinci's inventions were expressed in drawings. You could say,

Artists see the world differently,
and scientists think about the world differently.

In this book I try to express my ideas about Bitcoin as visually as possible, because I believe thinking visually can make complex topics simpler, and more beautiful. Although I'll steer clear of using any math in here, we can recognize that any advancements in cryptocurrency and cryptography coincide with advancements in the underlying math that made those systems work.

Although we tend to think of Isaac Newton as the scientist and Leonardo da Vinci as the artist, both believed mathematics represented humanity's highest capacity and tool in the expression of truth. Today, despite the ease of access to and overflow of information, the notion of truth can feel as if it's in short supply. It takes effort to interpret facts and separate perception from reality. But data and facts are all just fragments of information, the truth is about meaning. We have a strong desire for truth, and a healthy skepticism toward anyone boldly making truth claims.

Because I'm also this kind of skeptic, I don't make a practice out of evangelizing future bitcoin prices that nobody can possibly know. The only thing we know for sure is the truth about what Bitcoin is today. Throughout this book, I will never tell you what bitcoin is worth, or speculate about how the bitcoin price is inevitably going to the moon. My primary goal here is to have more people in the world capable of evaluating these complicated systems on their own, and simply telling people to agree with me doesn't serve that goal at all.

There is a steep learning curve for any potential user or investor of Bitcoin, which may explain some of our hyper- obsessive fascinations with it. It's easy to watch the hyper volatility of the bitcoin price and miss the point of the technology entirely. Misunderstanding comes easy but understanding takes work. It means being willing to start from a place of ignorance and ask questions. If you have any questions, comments, or concerns that come up as you read, you can message me on Twitter or send me an email.

How This Book is Organized

This book is intentionally not like any other on the subject, and I make no apologies for that. This is not a normal book for people who want a traditional sell on Bitcoin from the perspective of finance, economics, raw programming, or hype. My goal is to get you as many 'WOW!' and 'AHA!' moments as possible. I see Bitcoin as a system, and as with any good technological system, its goal should be to strengthen our connections as a small part of a larger, connected whole.

This book is all about reframing the way you think about Bitcoin. To build up toward an appreciation for it by giving you the framework

in which to appreciate it. Its goal is to replicate my mental models in your head, so you can see what I see, and come to your own appreciation given this new way of seeing.

We've talked about the metaphors in Bitcoin and how they break down. That being said, there is one metaphor that is the least talked about, and the most strikingly beautiful in its functionality: before the concept of the blockchain was fully realized, the term "timechain" is mentioned exactly once, as a comment or afterthought, in the original Bitcoin source code by Satoshi. It's the metaphor of Bitcoin as a decentralized clock, and it is the subject of the next chapter, which will help you fully understand why Bitcoin's blockchain technology is celebrated as trustless.

Section two of this book is framed by the analysis half of systems thinking. Asking how before we start asking why. By going inside the blockchain we can see *how* the system works by breaking it down into its essential functions: ledger order, validation, confirmation, and authorizing transactions. Then we look at which part of the system that performs those functions: transactions, full nodes, miners, and blocks. We start with the reason for the function, then the object that performs that function. Most other resources do this the other way around. Unlike other explanations of Bitcoin, which can read like a dry textbook explanation of the protocol, I view Bitcoin as both an art and a science. There's a science to how it works, and an art to seeing the beauty in it. To show you both I have to explain why each part of the system is needed and how it evolved into what it is today. Although each chapter in this section is focused on an individual part of the system, we also want to understand how each of those parts work together. The main goal of this section is aimed at achieving a precise terminology around the blockchain so that we're speaking the same language when we discuss it.

The third section is on the emergent properties of Bitcoin that we don't find in any of the individual parts. Decentralization and censorship-resistance are the fundamental emergent properties of the blockchain. But Bitcoin is not just a decentralized payment platform, it's also a form of money. And money comes with its own set of properties. In this section, I show how the properties of money are implemented in a cryptocurrency, how those properties are governed in Bitcoin, and how technical upgrades to the system are implemented.

The goal of the section is to understand not if the price will go up and down, but *why* the system has any value in the first place. Here, we'll consider what properties are valuable in Bitcoin long-term, how those properties are preserved and evolve.

The last section of this book is framed by the second half of systems thinking and makes the final transition from knowledge to understanding. In the chapters of this section we go outside of the technicals of the blockchain into markets and your personal mindset. How do group dynamics, particularly the behavior(s) of producers and consumers, around Bitcoin affect its price? What are the signals that move the market? How does Bitcoin affect you as an individual? Why are you drawn to understanding Bitcoin in the first place? We'll also provide some frameworks for answering the more practical questions of how to buy, trade and store bitcoin if that's something you choose to do. The primary goal for this section is to understand why Bitcoin works and why you think it can work for you.

CHAPTER 2

A Trust "less" Timechain

"Care must always be taken when generalizing, and it's important to remember that no two different things are the same—even when we call them the same name; especially when what counts depends so tremendously on the details."

– Greg Maxwell aka gmax, Bitcoin developer

As cryptography spreads beyond academia and the cypherpunk mailing lists to us normies, you may have heard people celebrating the blockchain as something "trustless." But in a world where every business relationship is built on trust, celebrating the absence of it gives people the impression that we're not all speaking the same language. In business, trust is generally a positive thing. But in cryptography and security, trust is regarded as a very dangerous thing. Although the two worlds use the word trust differently, the underlying issue in both cases is the same. The issue is not trust itself, but risk and consequence. How much risk does an action carry? And what is the cost of the negative consequence(s) that could result from it?

To better distinguish between risk and consequence I'll use rock climbing as an example. An advanced climb that requires the climber to perfectly execute a series of difficult moves, but only six feet off the ground, represents a high risk with a relatively low consequence. Although the climb is difficult, the consequence of falling six feet isn't terribly devastating. You'll live.

Now imagine a much easier climb, but several hundred feet off the ground and without a rope to catch you if you fall. Free solo climbing is what crazy people who do this call it. In this situation, the climb may be easier, but the consequence for a mistake is as ultimate as anyone

can imagine. Risk is the probability of an event occurring, consequence is what happens if that event actually occurs.

In payments and banking, the reliance of any third-party service represents some probability and risk that your payment could be censored, or your funds could be seized. Operation Choke Point was the name of a 2013 United States Department of Justice initiative that choked off legal firearms businesses by pressuring banks into cutting off their access. In 2019, live during a presidential debate, Texas congressman "Beto" O'Rourke called out banks and credit cards companies to illegally block the payments on legally purchased firearms. Whistleblower organizations like Wikileaks and citizen journalists have had to use Bitcoin to avoid transaction censorship from their governments, and their governments' central banks. The story from journalism, guns, cannabis, or any other business that threatens the power of the government is the same. "Your business may be legal, but good luck getting access to our banks." Because banks are centrally controlled, they're just another lever for politicians to apply political pressure.

For normal people who are less concerned with what happens to the marginalized at the fringes of society, the risk of censorship might not seem too bad. Maybe even acceptable. But for those directly affected, the issue is life or death. Power is the true motive behind censorship, deplatforming, and authoritarianism. As long as there is only one centralized corporation or government that controls who is and who isn't allowed to make payments or have banking relationships, that entity has the ability to control who lives and who dies. In this situation, censorship represents a low risk with an unacceptably high consequence.

This is why Bitcoin doesn't just replace payment platforms to become yet another middleman. Payments in bitcoin are **censorship resistant**, meaning that the platform can't easily censor anyone's payments. But side stepping the trusted middleman doesn't just protect against censorship, it also protects against a **single point of failure**.

Because the U.S. dollar is the world's reserve currency, if the United States were to inflate and overprint the dollar, if its military were not to enforce its dominance, the dollar could collapse the global economy. Although the risk of complete government failure may be low, the consequence of failure would be extraordinarily high. Any centralized

currency that millions and billions of people rely on represents a single point of failure.

The blockchain was the first tool that made transacting online without a trusted middleman possible. As consumers, when we hear the word *middlemen* we tend to think of PayPal, whereas people in the banking world may think of Swift. But the role of middlemen isn't limited to payments and currency issuers.

Brokers, salespeople, brands, and social media platforms are all middlemen; any person or service who connects people in a network is a middleman. Can I really say that blockchains are here to replace all of them? No. But this wouldn't be an obvious answer if you look at the frenetic development of altcoins, ICOs, and custom blockchain solutions in nearly every industry. Cryptographers and educated crypto enthusiasts alike are highly sensitive to the word trustless, because it has a very specific technical meaning that the public has yet to fully grasp.

A trustless system is designed in such a way that the platform has no ability to censor you.

The blockchain doesn't provide full protection or a 100% guarantee against censorship, but it does dramatically minimize your chance of censorship by adding an economic disincentive for doing it. Calling the Bitcoin blockchain trustless is somewhat hyperbolic. The word trustless is reserved for systems that meet a very high technical standard, and Bitcoin isn't fully trustless. The terms trust-minimized or trust "less" are more accurate, and less likely to trigger the entire technical community.

The blockchain does not outright eliminate the use of a middleman in every instance, and it doesn't need to. In many cases middlemen add a substantial part of the delivered value to consumers. Middlemen mediate disputes, prevent fraud, and reduce the risk for each of the parties participating. What Bitcoin has proven is that its blockchain might be able to reduce *some* of our exposure to *some* risk, as introduced by *some* middlemen, *some* of the time. This a sensible conservative view on blockchains that is entirely meant to defuse the hype of the industry. There does not need to be a blockchain solution for everything. But the world is probably going to try anyway.

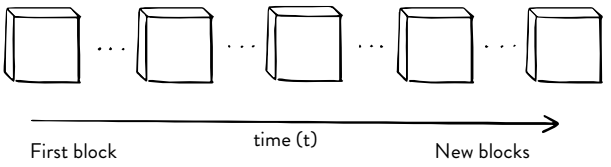
The relationship between trust and risk in the cryptographic world has not been well communicated to the growing cryptocurrency industry outside of it. Which explains a lot about why people mistakenly believe replacing every middleman with a blockchain would do anyone any good. In cryptographic systems, the more internal dependencies, the more layers of code software the system is built on, the more opportunities the system has for compromise, the less stable it is, and the more trust is required in using the system. Every layer of additional infrastructure should be well justified as an additional door vulnerable to compromise and worth protecting. In the context of system architecture, trusted middlemen represent a possible point of failure, and targets for malicious actors to exploit.

The minimization of trust is a design principle, and the basis of a secure system.

Now that you understand the property of trustlessness, I can show just how far this principle goes in Bitcoin. Bitcoin is a protocol that allows users to send value (in bitcoin) securely over the insecure internet. We're all used to referring to this as the blockchain, but the **timechain** is just a different way of thinking about the blockchain. A timechain is a decentralized time stamp server, that keeps time internal or relative to itself without relying a third-party source of time. By thinking of the blockchain as a timechain, or a decentralized clock, you can *see* how the blockchain was designed to be trust-minimized.

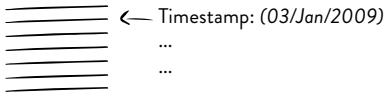
Bitcoin as a Blockchain

Let's do some compare and contrast, the blockchain versus the timechain. Visualizing the blockchain is straightforward: You put some transactions in a block, then connect the blocks to make a chain.



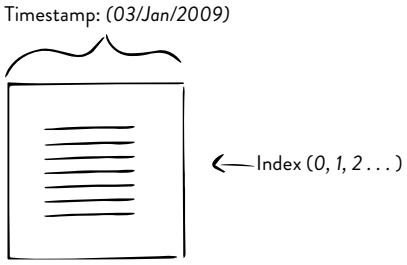
But why does the blockchain group transactions in blocks? Well, let's start with the ledger. The blockchain is a ledger and ledgers need to put each entry in order. So, the most basic requirements of any financial ledger—blockchain or otherwise—is the ability to record a **timestamp** to note the specific date and time a transaction occurred. The timestamp allows for each of the entries to be ordered, to know which transaction came first and which came after. You'd think that all of the transactions in Bitcoin then would be ordered individually, in the order they were received.

If transactions were individually timestamped:



But looking closer at the Bitcoin blockchain, you see that none of the transactions have an individual timestamp. Instead, transactions are numbered with an index 0 through ~10,000 and a timestamp is applied to the whole block.

A timestamp applied to the entire block:



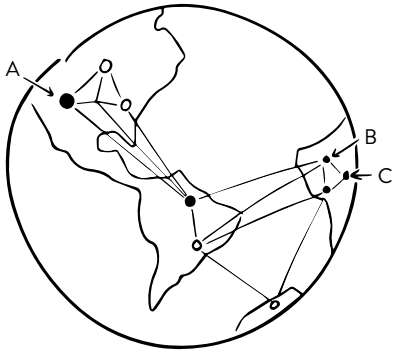
In Bitcoin, transactions that occur within about a 10-minute time window are grouped together in a block, and the timestamp is applied to the whole block instead of each of the transactions individually.

Okay, but why?

The Speed of Data

As far as we know, light speed is the ultimate speed limit for data travel in the universe. Still, it takes eight minutes for sunlight to travel through space to reach our eyes. By exploring a visual example I'll show exactly why the speed of data traveling maters in this network.

Consider the physical distance between computers:



These computers run the bitcoin program to process requests, deliver data to other computers, and are connected globally over the internet. But from computer to computer, data traveling on earth moves much more slowly than light traveling through space—since the data on earth has to go through copper wire or fiber-optic cable under the ocean. In the Bitcoin network, these computers are called nodes. A **node** is any computer that connects to the Bitcoin network.

A Bitcoin full node is a computer that:

1. Keeps a full record of the Bitcoin ledger via the blockchain.
2. Validates transactions and blocks on the network.
3. Propagates transactions in the network.

Full nodes are independently run by users all over the world. Unlike data traveling to centralized servers, your online banking website or a social media site, data in this decentralized network has to travel to every node in the network. Because it takes time for data to travel from a computer in one part of the world to a computer in another

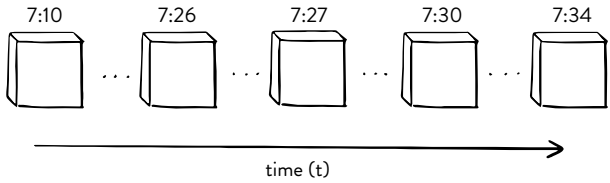
part of the world, nodes closer together will see transactions originating from their local area as having occurred *before* transactions on the opposite side of the world. Because there is no central server in this network that defines when a transaction occurred, if nodes attempted to timestamp transactions individually, each node would report and order the transactions in a different order.

To consider a specific example of this, if two people, Alice (A) and Bob (B), send bitcoin to each other in two independent transactions at exactly the same time, their friend Charlie (C), who operates his node closer to Bob than Alice, will see Bob's transaction sooner than Alice's. Because Bob's and Charlie's nodes are physically closer together, they will receive Bob's transaction data before Alice's, and they will perceive Bob's as having occurred before Alice's.

Transaction Order /	Alice's Node /	Bob's Node /	Charlie's Node
Transaction 1	A → B	B → A	B → A
Transaction 2	B → A	A → B	A → B

The takeaway from this is that blocks are not arbitrary groupings of transactions. Blocks are the way we order the transactions on this decentralized ledger. Because of decentralization and **network latency**, transactions can never be processed by every node in the network at exactly the same time. In Bitcoin, timestamps are applied to blocks instead of each transaction individually.

Timestamps are applied to each block in the blockchain:



In Bitcoin, a transaction isn't final until it's confirmed in a block and accepted by a majority of full nodes in the network. Because we can't know the exact order of transactions in real time, we say there is no exact order on the ledger until transactions are confirmed in a block. The purpose of blocks in the blockchain is to get an agreed upon order for transactions consistent for all the nodes in the network.

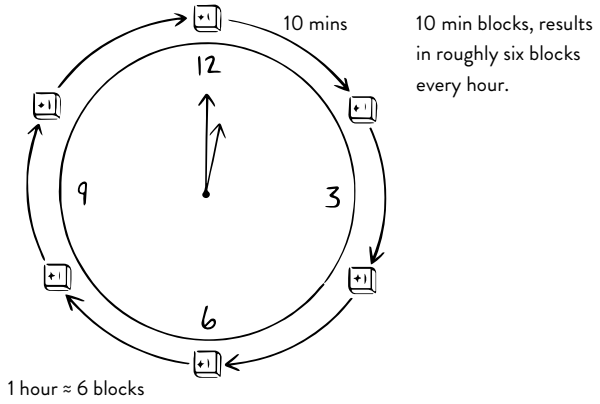
The Blockchain as a Timechain

The idea of the timechain might not conjure up an as clear or simple a visual as a blockchain, but it serves to highlight the more specific function of the Bitcoin system.

1. Merchants and anyone accepting bitcoin for payments need some guarantee that the transactions are final after some *window of time*.
2. New bitcoin need to be issued on a reasonably *consistent time schedule*.

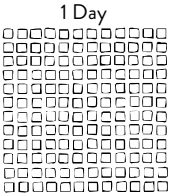
The Bitcoin blockchain does this by confirming payments and issuing new bitcoin in every block. You can imagine that each block serves as a "tick" in the blockchain's expansive decentralized clock, as new blocks confirm transactions roughly every 10 minutes.

The blockchain visualized as a timechain:

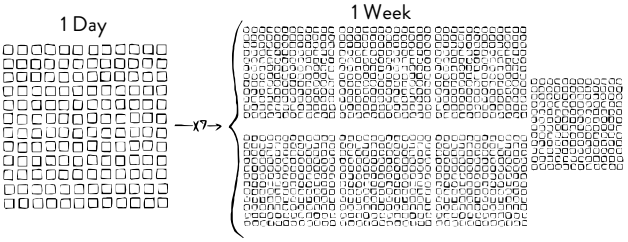


A clock is a system that's regulated by its internal structure to keep time. The blockchain is a clock that's regulated by its blocks to keep time.

On average, 144 blocks are added to the blockchain every day:



And 1008 blocks on are added to the blockchain every week:



The terms block number or block height are used to tell time on the blockchain. **Block number** refers to a specific block in the past, whereas **block height** refers to current length of the blockchain. Blocks function like receipts: to verify that a transaction is confirmed, we refer to the height or number of the block our transaction was included in. Each block represents one confirmation, and for large payments, it's standard to wait for six. **Block time** is the time between blocks, or the average time for a one block confirmation.

The first block, aptly named the **Genesis Block**, was timestamped by the creator of Bitcoin, **Satoshi Nakamoto**, on January 3, 2009. Since then, every subsequent block has been timestamped relative to the history of timestamps on the blockchain and its current network time. What is the significance of Bitcoin's system for regulating timestamps? The purpose of the block timestamp is to give the network a final time for those transactions included in it. And as we'll talk about here in a bit, the timestamp provides the network with a way to calculate what's called the **difficulty** to regulate the timing of new blocks.

When a new block is generated and timestamped, before it can be added to the chain, its timestamp must be validated by each of the full

nodes in the network. A valid timestamp has to be (1) greater than the past block timestamps, and (2) no more than two hours out into the future from the current network time. This functionality creates an upper and lower bound on acceptable timestamps for blocks. Why is this so important to the property of trustlessness on the blockchain?

It's because of this system of self-regulating timestamps, that Bitcoin possesses its own internal sense of time.

If the significance of this is too technical to amuse you, consider the more general significance of keeping correct time throughout history. Out of either ignorance or corruption and disputes between churches, more than a few Roman politicians added days to the calendar to extend their rule. Considering the average lifespan of a democracy is only 200 years, the Western world is overdue to overturn this cycle of democracy. Historically, inaccurate timekeeping has been a measure of incompetence and corruption. And with the invention of Bitcoin, we have a way of keeping time that relies on no one and trusts no one.

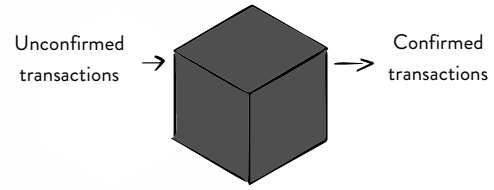
Bitcoin was designed to calculate time based on only the blocks recorded by its nodes in its network. But are the nodes in Bitcoin's network uniquely trustworthy? Well, no. Which is why each full node calculates the current **network time** by asking for the timestamp from all the peers it's connected to and calculating the median time from that. This means that the time that's represented in on the blocks timestamp is not exactly aligned with real-world time. But the timestamps on blocks don't need to be perfectly accurate for blocks to continue to be produced, payments to be processed, and for new coins to be issued. On average, timestamps are typically accurate to within an hour or two of real-world time.

There are two primary concepts that create the clock functionality in Bitcoin: mining and proof-of-work. **Miners** are the nodes in Bitcoin that devote computing power to the process of adding blocks to the blockchain and are paid out in bitcoin for doing so. The process of timing the blocks is called **Proof-of-Work** (PoW), it's called that because miners do the work of mining new blocks, then they share the proof of that work to the rest of the network. Get it? Proof of work!

Mining can be a bit tricky, since there are two different ways that people tend to explain it. The first is from the *altruistic* perspective of

the system that needs the miners to do a job for the sake of the rest of the network. The security and functioning of the blockchain needs miners to consume electricity, to produce blocks and confirm transactions. How does it do that? Well, the second explanation of miners is from the *selfish* perceptive of the miners themselves, they are rewarded and incentivized (in bitcoin) for doing the job of mining for the network. This is why they're called miners, because they "mine" bitcoin. Below is the black box visualization of the former explanation.

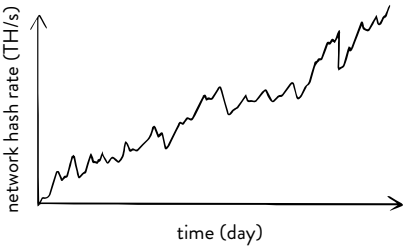
The role of miners in Proof-of-Work:



Miners: *do work and show proof*

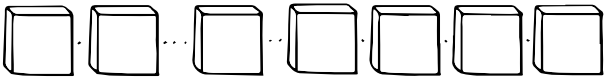
Hash rate is the unit for measuring the amount of work a computer contributes in the job of mining. Because Bitcoin is an open and **permissionless** network, meaning the computers that are doing the mining can join or drop off at any time. The **network hash rate** (also called the **network hash power**) is dynamic; that is, the total number of miners performing proof-of-work is always changing, typically growing over time.

A graph of network hash rate over time:

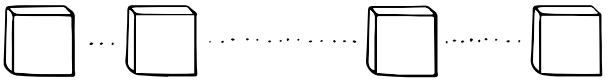


The number of miners performing proof-of-work in the network sets the pace for the time between blocks, and the confirmation of transactions on the blockchain.

If a bunch of miners join the network at once, the time between blocks is closer, and transactions are processed more quickly:



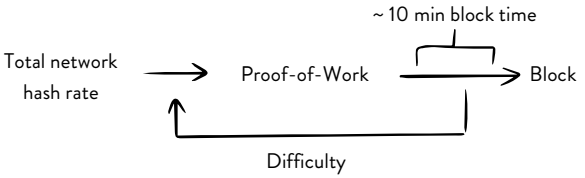
If a bunch of miners leave the network at once, the time between blocks is further apart, and transactions are processed more slowly:



But no matter how many miners there are in the network, ideally the blockchain should ensure that the time between blocks is consistent, so that transactions are processed, and new bitcoin are released with some consistency. The Bitcoin blockchain does this with a **closed-loop control system**. Recall that the timechain uses the blocks' timestamps to calculate a value called the difficulty? The difficulty is the control in the control system.

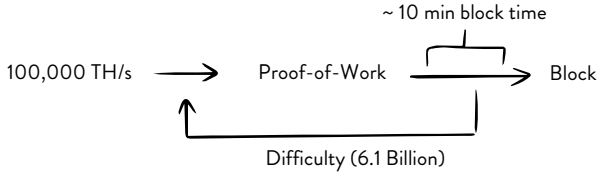
No functioning clock can fluctuate. So, in Bitcoin, although the time between blocks is occasionally further apart or closer together, by adjusting the miner's difficulty of performing proof-of-work, the timing of the clock is set back to target 10-minute blocks based on the current total hash power or the total number of miners in the network. Roughly every two weeks, or more specifically every 2,016 blocks the difficulty that sets the timing of the clock is reset.

The control loop in the timechain:

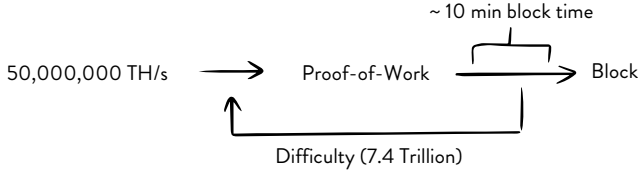


To take a historical example, we can compare the 50x increase in total network hash rate from 100,000 TH/s (terahash per second) in the year 2014 to 50,000,000 TH/s in late 2018 and see that block time stayed mostly the same.

Network hash rate from the year 2014:



Network hash rate from the year 2018:

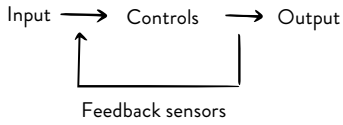


Both when the hash rate is 100,000 TH/s and 50,000,000 TH/s, the average block time is still 10 minutes on average. Instead of looking at the specifics of the control system in Bitcoin, let's take a step back and consider a control loop in the abstract.

Control Loops and Feedback

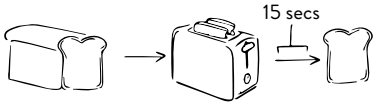
The general control loop has a variable input that is modified by some controls; some sensors check if the output target has been met, and the controls retarget the system toward that goal.

The generalized feedback control loop:



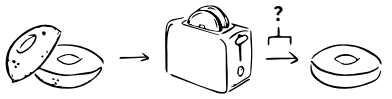
Control loops are structures commonly used by systems to self-regulate their behavior with sensors, feedback, and controls. Temperature control systems, house thermostats, and self-driving cars are all governed by control loops. Typically, why you would implement one is because you want to have a machine work on autopilot. You want to have the temperature regulate itself, the car to drive itself, or maybe you want a toaster to check its toasts' color by itself.

We can look at the humble toaster as one visual example of a feedback control loop system:



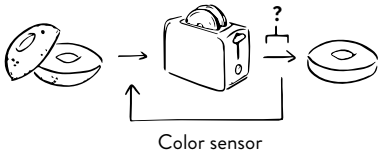
This toaster is controlled by a timer. Through trial and error, you've figured out that 15 seconds is the perfect amount of time to get bread the golden-brown color of toast you like.

But you can imagine a situation where you want to toast different types of bread, a frozen waffle, or a bagel:



The problem with this toaster is that you'll have to go through the trial and error process for every type of bread to figure out how long the timer needs to be set. But by using a color sensor instead of a timer, we can invent a more sophisticated toaster that can get you that golden-brown color for every type of bread with no trial and error process.

By closing the feedback loop with a color sensor, we can remove the need for a timer and repeated adjustments to the timer:



In Bitcoin, a 10-minute block time is the golden-brown color of toast. The variable input of bread is the fluctuating number of miners in the network. And the color sensor is the difficulty level that is periodically adjusted to keep block time steady as the network's hash power changes.

At this point in our understanding of the blockchain, you know more than 95 percent of crypto fanatics. You've learned that the Bitcoin blockchain was able to approximate trustlessness and create its own sense of interval time, independent from any third-party clock.

This decentralized clock is used to process payments and issue new bitcoin. Blocks serve as the blockchain's internal mechanism for keeping time, and the dynamic difficulty adjustment of hash power serves to keep the clock ticking at a steady pace.

Conceptually, this is a big shift from how most people are used to thinking about the blockchain, and I'd like to think it's a much more beautiful way to think about it too. Now that we understand why we need a ledger and blocks on the blockchain, we can shift from talking in terms of abstractions and get down to the concrete details. What are blocks, transactions, and bitcoin at the level of raw data? How does the data propagate across the network? How are transactions validated and confirmed, and why is it so important to recognize the difference between the two?