

A summary of the talks behind the book

The Internet of Money

Volume One

Why does Bitcoin matter? — The big ideas in eleven chapters

Andreas M. Antonopoulos

Summary by Turki Alsharari

Why is this book different?

Most Bitcoin books explain **how** it works: mining, signatures, blocks. The Internet of Money answers just one question: **why does it matter?** The book is not a text written from scratch; it is eleven talks that Andreas Antonopoulos gave to real audiences in different cities, later collected and edited into a book.

Antonopoulos is a Greek-British computer scientist who lived through the dawn of the internet in 1989 and discovered Bitcoin in 2011; he has said ever since that he had not felt that kind of awe since the early days of the internet. He is the author of *Mastering Bitcoin*, the best-known technical book in the field, yet he holds that his real message is not the technology but **the idea**: that Bitcoin is not a new digital currency but a transformation of the oldest technology humanity has known, the technology of money itself.

One central idea recurs throughout the chapters in different wording: **currency is only the first application**. What Bitcoin builds is a network of trust that is neutral, decentralized, open and requires no one's permission; currency is merely the first thing built on it, just as email was the internet's first application and not the internet itself.

Author	Book published	Chapters	Talks delivered
Andreas M. Antonopoulos	Merkle Bloom · 2016	11 talks	2013 – 2016

How to read this summary

Each chapter corresponds to one talk. It opens with the talk's context (place and date), then the main ideas, then a paraphrased quote that captures the spirit of the talk, then "The idea in one line." The chapters stand alone and can be read in any order, but reading them in sequence shows how the argument evolved from 2013 to 2016.

Note: the figures and examples the author cites (the number of unbanked people, remittance volumes, fee levels) reflect the years in which the talks were given, and some have changed since. The arguments themselves, however, have lost none of their force.

Contents

Eleven chapters

1	What is Bitcoin?	Athens · 2013	3
2	Peer-to-Peer Money in a Historical Context	Rotterdam · 2015	4
3	Privacy, Identity, Surveillance and Money	Barcelona · 2016	5
4	Innovators, Disruptors, Misfits and Bitcoin	Detroit · 2014	6
5	Dumb Networks, Innovation and the Festival of the Commons	San Francisco · 2015	7
6	Bitcoin and the Coming Infrastructure Inversion	Zurich · 2016	8
7	Money as Language & the Multi-currency Future	Toronto · 2014	9
8	Bitcoin Design Principles	Boston · 2015	10
9	Money as a Content Type and the Grand Arc of Technology	Queenstown · 2014	11
10	Bitcoin: Elements of Trust	Berlin · 2016	12
11	Will Bitcoin Fail to Scale?	Prague · 2016	13
·	Volume recap: The threads that tie the chapters together	Appendix	14
·	Sources and license	Appendix	15

Page numbers are as shown in the page footer; the cover is unnumbered.

1

Chapter One

What is Bitcoin?

Disrupt conference, Athens · November 2013 · 20 minutes

This is Antonopoulos's best-known short talk, and it opens the book because it puts every idea on the table at once. He begins with a line he returns to in every chapter: **Bitcoin is digital money, but it is much more than that**, just as the internet is not a "fancier telephone" or "email." Money is only the first application.

The problem Satoshi solved

In 2008 Satoshi Nakamoto published a paper claiming to have solved an old problem in computer science: how can a decentralized network agree on a single truth without a central authority? This is the "Byzantine Generals' Problem," which had gone unsolved since it was described in 1982. Everyone ignored him or laughed at him. Three months later he released the software and the network started running.

Bitcoin is not a company or an institution; it is a standard protocol, like TCP/IP. Every ten minutes the network agrees on which transactions took place and who owns what, through something like an electronic election that no central party runs. That solution matters more than the currency itself: currency is the first application, but voting, asset registration, notarization and applications we have not yet imagined are all possible on a distributed consensus system.

Ignore the price, understand the technology

Antonopoulos explicitly asks the audience to ignore the price. If the currency fails, another one can be launched, but the technology cannot be "uninvented." What matters most to him are the two billion people who are online but have no bank account, and the six and a half billion who are entirely outside the international financial system. They do not need a bank; they need an app.

Neutrality and permissionless innovation

The most important lesson of the internet is **neutrality**: the network makes no distinction between CNN and an Egyptian blogger. Bitcoin, likewise, is neutral toward the sender, the recipient and the value of the transaction. The result: anyone can innovate in money the way they innovate on the internet, without anyone's permission. "You can become Citibank." The old system achieves its security by restricting access; Bitcoin turns that on its head with a flat network in which every node is equal.

If we wreck the money, we can simply launch another currency. But Bitcoin as a technology cannot be uninvented.

Paraphrased from the talk

The idea in one line

Bitcoin is not a currency but an internet of money: a neutral network that anyone can build on without permission, with currency as merely the first application.

2

Chapter Two

Peer-to-Peer Money in a Historical Context

Reinvent Money conference, Erasmus University, Rotterdam · September 2015

How old is the technology of money? Most people answer hundreds, or a few thousand, years. The truth is that we have never discovered a single civilization without money. In fact, money is **older than writing**: the earliest inscriptions we have found, hieroglyphic or cuneiform, were ledgers. Money may be as old as language itself, because at its core it is a **language**: a way of communicating value between people. Even monkeys learn to use pebbles as currency, and the first thing they “invent” after that is armed robbery.

Five revolutions in the history of money

- **Barter**: exchanging goods that have consumption value (goats for bananas).
- **The first abstraction**: shells, feathers and beads, things you cannot eat but that represent value.
- **Precious metals**: scarce, portable and divisible; then nothing new for thousands of years.
- **Paper**: a note that says “I have gold in the vault.” It took about four hundred years to be accepted, and people thought anyone who accepted it was crazy.
- **Plastic cards** sixty years ago, then **Bitcoin**: a shift as radical as the move from metal to paper, and perhaps more so.

From institutions to platforms to protocols

Bitcoin did not happen in a vacuum. The internet turned closed, hierarchical institutions into platforms with interfaces, and then into protocols that need no permission: TCP/IP works everywhere without your having to open an account with anyone. Bitcoin is **the first form of money based on a network and a protocol**, with no institutional context. Every node in it is equal; there are no “special nodes.”

Who is the slave?

The harshest passage in the talk. When you put your money in a bank you do not “have money in the bank”; you have lent the bank your money for next to no interest, and it lends it to your neighbor at twenty-four percent. In computer science, a relationship in which one side holds a weak, meaningless copy is called “master/slave.” If the old money is built this way, the uncomfortable question is: who is the slave? The people of Cyprus, Greece, Venezuela and Argentina learned the answer the day they went to the bank and it would not give them their money.

In Bitcoin, nobody owes anybody anything. It is absolute ownership of an abstract token: **whoever holds the keys owns Bitcoin, and whoever does not hold them does not**. No one can freeze it, seize it or censor it.

They will tell you they are worried that criminals will use Bitcoin. The truth is they are far more terrified that the rest of us will.

Paraphrased from the talk

The idea in one line

Money is older than writing and has been transformed only a handful of times in history; Bitcoin is the next transformation: from money based on debt to money based on absolute ownership.

3

Chapter Three

Privacy, Identity, Surveillance and Money

Fab Lab, Barcelona · March 2016

Antonopoulos defines his politics with a single word of his own invention: “disruptarian.” Every thirty or forty years, power in settled systems accumulates and centralizes, and with centralization comes corruption. And no power is more absolute than the power of money. Banks freed money from kings after the fifteenth century, then became centralized in their turn. It is time for disruption again.

Structure, not villains, produces the outcomes

Most of the problems of centralized money do not arise because people are evil. Bankers are mostly decent people who want to pay off their mortgages. The problem is that the **structure** of hierarchical institutions produces exclusionary outcomes by its very nature, and that hierarchical systems reward those with a sociopathic drive to climb to the top. Although the internet has made communication global, financial inclusion is in **retreat**: there are systems for small amounts and others for large ones, all of them carved up by borders and jurisdictions.

Network neutrality and “spam transactions”

The internet’s real strength is not speed but **neutrality**: no discrimination by source, destination or content. Bitcoin is the first neutral financial network. That is why Antonopoulos rejects the term “spam transaction” outright: if you paid the fee, your transaction is legitimate by definition, because the market, not a committee, is what decides.

Privacy for the weak, secrecy for the powerful

Since the 1970s, digitizing currencies has been a dream of states: watching every transaction between every human being. The result is a global, totalitarian system of financial surveillance, and billions shut out of banking in the name of “identity verification.” WikiLeaks was cut off from the financial system without trial or conviction, through pressure on just four companies.

He then draws the distinction he counts among the most important things in the book: **privacy** is the right of billions not to be watched, and **secrecy** is the privilege of the few to escape accountability. Our world is upside down: our transactions are completely transparent and the money of the powerful is completely opaque. Bitcoin sets it right side up again. One of his favorite words is “sousveillance”: watching from below instead of surveillance from above, seven and a half billion people staring at a few hundred thousand.

Attack breeds immunity

Bitcoin is a living, evolving system. Attack its privacy and it becomes more private; attack its resilience and it becomes more decentralized. The internet used to go down for days under denial-of-service attacks; today Google absorbs gigabits of attack traffic and reroutes it. The attacks never stopped; the system became immune. And Bitcoin is a “honeypot” with a reward of billions for whoever breaks it, and no one has claimed the prize yet.

Privacy is a human right. Secrecy is a privilege of power. We need a world with strong privacy for the billions, and fragile, easily pierced secrecy for the powerful.

Paraphrased from the talk

The idea in one line

On January 3, 2009, the states’ dream of a totalitarian financial system died; Bitcoin restores privacy to individuals and strips secrecy from the powerful, and every attack on it makes it stronger.

4

Chapter Four

Innovators, Disruptors, Misfits and Bitcoin

Maker Faire, Detroit · July 2014

A talk aimed at makers and hobbyists, so he speaks about Bitcoin from the angle of the “misfits”: those who see the elegance in a technology that does not yet work well, and who spot innovation decades before everyone else.

Bitcoin is like Wikipedia, Linux and the internet: **it doesn’t work in theory, but it works in practice.**

Whitewashed history

We rewrite the history of technology so that it looks bright and smooth. In reality the press mocked the automobile for two full decades: dirty, noisy machines, slower than horses. In Britain the hysteria went as far as the “Red Flag Laws”: every vehicle needed a driver, an engineer and a man running ahead of it with a red flag to warn pedestrians. The result? Britain, which had been leading the automobile race, lost it entirely. Electricity, too, was described as something that “will burn houses down” and as a toy for the rich. The very same line is used about Bitcoin today.

Criminals first... then everyone

The first users of any technology are often criminals: cars for getaways, the telephone for conspiracy, the telegraph for fraud. The reason is economic, not moral: criminals operate in a high-profit, high-risk environment, so adopting a new technology costs them nothing. Decades later, the same technology becomes mainstream. Bitcoin is already past that stage.

Kodak, Nokia and Linux

When dominant industries see a disruptive technology, they first ignore it, then mock it, then try it, and then comes the stampede... and by then it is too late. Kodak lost a twelve-billion-dollar industry within three years to a company that does not make cameras, called Nokia. IBM was unshakable; then a Finnish student wrote an operating system in his room, and it came to run eighty percent of the world’s phones.

Why will Bitcoin win?

Not because it is better, and not because the banks are “run by crooks.” It will win because it is **open**, and open wins in a world of tinkerers. Every financial network achieves its security by excluding “bad actors”; in 2008 we discovered that the bad actors already own the banks. Bitcoin is different not because it found the most honorable people, but because it does not depend on that: its security is math and incentives, a game of Sudoku won by whoever plays by the rules. In 2014 more than \$250 million in investment flowed in, with more than a thousand companies building “the next application,” at a faster pace than the internet of 1995.

It’s not about the first billion

Bitcoin is not for the billion who have international accounts, but **for the other six billion**. On top of \$550 billion in annual remittances sit companies that take a 15% cut from the poorest people. The day a migrant discovers he can send a hundred dollars instead of eighty, everything will change. And a cheap Nokia phone on the roof of a mud hut can become a bank.

First they ignore you, then they laugh at you, then they fight you, then you win. We are still in the laughing stage, and that’s fine.

Paraphrased from the talk

The idea in one line

Every great technology was mocked for decades before its history was rewritten; Bitcoin will win not because it is better but because it is open, and open wins.

5

Chapter Five

Dumb Networks, Innovation and the Festival of the Commons

O'Reilly Radar Summit, San Francisco · January 2015

He opens with a small correction: the Canadian Senate said he “literally wrote the book on Bitcoin,” but he wrote it with more than 150 contributors on GitHub and published it under a Creative Commons license so that any developer in the developing world could read it for free. This is no passing preamble; it is the idea of the whole talk in miniature: openness.

Dumb network or smart network?

The most important decision in designing any network: do you build a smart network that serves dumb devices, or a dumb network that serves smart devices? The telephone network was smart: the phone itself was four electronic parts, and all the features (caller ID, call waiting) lived in the network. The fatal flaw: innovation happens only at the center, with permission, and only when millions of subscribers need it.

The internet is a dumb network: it moves data from A to B without knowing whether it is a Skype call or a web page, or whether the device is a phone or a refrigerator. That is why an application with five users can work: the intelligence is at the edges. **Bitcoin is a dumb network that serves smart devices.** It does not care whether an address belongs to a millionaire, a device or a smart contract, nor about the size of the amount or the location. It moves value according to a simple locking script. Write your application, run it at your edge, and the network will route it, because it is dumb.

Compare that with the banks: very smart networks, controlled so as to deliver specific applications to very dumb endpoints. The best online banking service is an HTML page with a set of services they decided to grant you.

From the tragedy of the commons to the festival of the commons

In economics we know the “tragedy of the commons”: a shared pasture where everyone grazes without limit until it becomes a mud pit. The old financial networks suffer from a form of it: when Visa innovates, Visa alone wins. Bitcoin, by contrast, is a shared resource that **grows more valuable with use** and excludes no one. If a company builds an open-source feature, the whole system benefits from it. The investment comes back multiplied, to everyone. This is not a tragedy but a **festival of the commons**.

His example: 2014 was Bitcoin’s “worst year” if you look only at the price, yet it saw the spread of multisignature and hierarchical deterministic wallets, the fruit of research done two years earlier, and hundreds of companies received \$500 million. “Give us two years,” and you will see what ten thousand developers can do.

And if Goldman Sachs builds its own currency?

Let them build it. If it is open and decentralized, they have proved the idea, and we all walk away declaring victory. If it is closed, it will freeze up within months while we accelerate, feeding on one another’s inventions.

Innovation without permission. Innovation without central approval. Innovation without upgrading the whole network. That is the power of the internet, and that is the power of Bitcoin.

Paraphrased from the talk

The idea in one line

Bitcoin is a deliberately “dumb” network that pushes intelligence to the edges, letting anyone innovate without permission; and because it is open, every improvement benefits everyone: a festival of the commons, not a tragedy.

6

Chapter Six

Bitcoin and the Coming Infrastructure Inversion

Bitcoin Meetup Switzerland, Zurich · March 2016 · the best-known talk in the book

Many consider this chapter the best thing in the book, and it was remade in visual form in 2020. The idea: every disruptive technology is forced, in its early years, to **live on top of the infrastructure of the technology it is replacing**, so it looks like a slow failure. Then things flip: infrastructure is built for the new technology, the old technology runs on top of it with ease, and applications that were never possible before are born.

The car on horse roads

The first person to drive a car drove it on rutted mud roads designed for horses, with no signals and no rules. A horse has four feet and is balanced; the first car had two driving wheels. So it got stuck in the mud, with no gas station in sight. "This will never work." Then the roads were paved, and horses were comfortable on asphalt too; what is more, bicycles, scooters and skateboards appeared, things that could not have existed before paving. That is infrastructure inversion.

Electricity on gas pipes

When electricity was exhibited at the Paris exposition, it was called "a fad that will end when the Eiffel Tower is taken down." Homes were lit by gas, and gas infrastructure does not carry electricity. Anyone who put "lightning in his walls" was a madman whose house would burn down. People also said: there is not enough of a distribution network to create customers, and not enough customers to justify the network. Then the wires were laid, and they lit and heated better than gas, and along came fans, blenders and hair dryers.

The internet on the phone line

His favorite example: the sound of the modem. The phone line was a dirt road designed for a narrow band around one kilohertz, and we were trying to push data through it. Two machines "singing" to each other through a straw. The phone companies hated it, and in Athens they would cut the line if they detected a modem, just as banks today close the accounts of Bitcoin companies. They said: nobody needs broadband. Then the companies became internet providers, then their backbone became data, then all calls came to be carried over the internet. The ultimate irony: "comfort noise generation," a device that whispers artificial noise into your ear because the digital line is so clean you would think the other party had hung up.

A Formula One car on the banks' mud

Today we are driving the Formula One car of finance on the mud roads of 1970s banking: exchanges, bank accounts, IBAN transfers. And the banks point and say: look, it doesn't work. His prediction: over 15 to 20 years the banks will resist, then adopt, then run their systems alongside Bitcoin, then **run traditional banking as an application on top of a decentralized ledger**. Emulating the old banks on Bitcoin is trivially easy: take its capabilities and slow them down. "An app that settles your transaction in three to five business days for five dollars": comfort noise for those who are afraid of fast finance.

Enabling the future on top of your old system is very hard. But once you invert the infrastructure, emulating the past on top of the network of the future becomes extremely easy.

Paraphrased from the talk

The idea in one line

The car on horse roads, electricity on gas pipes, the internet on the phone line: everything new looks like a failure on top of the old infrastructure, until things flip; and Bitcoin is the greatest infrastructure inversion the world will witness.

7

Chapter Seven

Money as Language & the Multi-currency Future

Bitcoin Expo, Toronto · April 2014

A philosophical talk, given at a conference where Ethereum had a striking presence, so one question kept coming up: does Ethereum threaten Bitcoin's future? Antonopoulos answers that the question itself is the child of an **old paradigm**: we have all lived in a world where currency is imposed by monopoly and determined by geography, so we do not choose our currency; it is an "accident of birth," like skin color. He was born in Greece and inherited the drachma just as he inherited everything else. In that world currency is the flag and the state, and competition is zero-sum: one currency wins when another loses.

When any child can create a currency

There is a website that lets you create a currency through a web form. Think about it: children in school invent currencies on their own, with rubber bands, Pokémon cards and popularity tokens. What if a five-year-old could launch "JoeyCoin" to compete with "MariaCoin" in a popularity contest? At that point the question "How many currencies will there be?" becomes like the question "How many bloggers will there be on the internet?" The answer: **all of us**. There will not be hundreds, but hundreds of thousands and then millions, most of them with no economic value but with cultural value.

Authority shifts from the issuer to the user

Before the internet, the authority of an opinion came from owning a printing press the size of a stadium and a name like The New York Times. Then anyone could publish, so we had to judge an opinion by its content rather than its publisher, and an Egyptian blogger was publishing the truth while the Times was publishing what pushes a nation into war. The same thing has happened to currency: authority no longer comes from the sovereignty of the issuer, but from who uses it, how much they use it and why. Picture a village a decade from now trading one currency with a Japanese dog on it and another with "an old lady named Elizabeth" on it; no one remembers who issued either of them; what matters is that it buys eggs. The only difference: one of them has a predictable, algorithmic money supply.

Currency as an app, and the unified wallet

Email was the internet's killer app; then came chat, Twitter and Facebook. Do you worry that Twitter will "destroy" email? No: each has its purpose, and we build interfaces that move us smoothly between them. Money is the same: one wallet with a hundred and fifty currencies. You pay for the house in Bitcoin, register the domain in Namecoin, pay for the contract in ether and tip in Doge, and the interface converts automatically. And perhaps an "index currency" that is never traded at all but expresses overall purchasing power, the way the S&P 500 index does.

Currency is politics, and currency is sovereignty

When you choose a currency you choose a community and a politics: you believe in a 21 million cap, or in an inflationary currency, or in a currency that sets aside a share for carbon capture. This is "politics by algorithm." More important still: for a thousand years, **sovereignty created currency**. After 2008, **currency creates sovereignty**: the internet, the largest and most populous economy and the first transnational one, now has its own currency, and with it purchasing power and economic freedom that cross borders.

Did you stop learning your mother tongue because English is widespread? There will be no single world currency, just as there is no single world language.

Paraphrased from the talk

The idea in one line

Money is a language, not a flag, and currencies will coexist like languages, not like empires; after 2008 the equation flipped: currency creates sovereignty, and the internet has become a sovereign with a currency of its own.

8

Chapter Eight

Bitcoin Design Principles

IDEO Lab, Boston · June 2015 · to an audience of designers, not programmers

The designer's job here is exceptionally hard: designing an experience for the oldest technology in the world (money), which nobody really understands. Try explaining money to a four-year-old; within four questions you will arrive at "go clean your room." Money is a **shared cultural illusion**: pieces of cotton with green ink on them, on which we build our relationships. Bitcoin is simply the latest layer of abstraction, and every time, society panics just as it panicked over paper.

Every metaphor in Bitcoin is broken

In design, a metaphor sets expectations, and it is dangerous when misused. In Bitcoin, all the terms are wrong:

"Wallet"

It holds keys, not money, and the right name is "keychain." A key can be copied, and whoever has a copy opens the door without your permission.

"Coin"

The most abstract form of money was named after the most physical one. There are no "coins" in Bitcoin, only divisible transaction outputs.

"Balance" and "account"

Addresses have no balance, only outputs that you control; there is no "account," no "sender" and no "recipient" in the code.

The gold coin image

The most detestable metaphor of all: a pile of gold coins stamped with the letter B at the top of every article, so people buy metal replicas thinking they have "joined the revolution."

Star Trek without money

Disruptive technologies are harder to understand because the most important things they do have no precedent: Star Trek predicted mobile phones but did not imagine the internet, and there is no money in its world at all. Bitcoin's real innovations will appear once adoption is dense enough, just as Wikipedia was not possible in 1992.

Innovation in the gaps

The internet cut the cost of moving information to nearly zero, and millions of applications were born; Bitcoin cuts the cost of verifying rules without a third party. The clearest example: **legal personhood**. Every financial system assumes that the owner of money is a person; Bitcoin does not care, so a program can own money. Combine Bitcoin, Uber and self-driving cars and you get a taxi that owns itself and pays for its own insurance and fuel, or an autonomous charity that distributes donations without a board of directors.

Don't try to be a bank

Bitcoin ATMs are an example of bad design: they imitate a bank teller machine for a user who does not know what Bitcoin is and has no wallet. Had he designed one himself: in the neighborhood grocery store, in Spanish, its first function "Send money to Mexico City," and a big "Talk to a human" button. His advice: win over the young before they open a bank account, because when they hear "three to five business days" they will say: what is a business day?

We don't need to sell Bitcoin hard for it to beat the banks. We only need someone to use it for a week, and then the bank takes care of the rest.

Paraphrased from the talk

The idea in one line

Bitcoin badly needs designers: all of its metaphors were designed by engineers and all of them are broken, and the right design is the one that gets "my mom" to use it without it looking like a bank.

9

Chapter Nine

Money as a Content Type and the Grand Arc of Technology

Bitcoin South, Queenstown, New Zealand · November 2014

The central idea: Bitcoin **separated money from the transport medium** and turned it into a content type of its own. A Bitcoin transaction is a signed data structure; it does not need the Bitcoin network to carry it, it only needs to reach a miner. Nothing in it is sensitive.

The credit card is broken by design

When you pay with your card you are sending **the secret key itself**: the number, the date and the verification code, through a chain of intermediaries, each of whom has to encrypt it and store it. If the encryption fails at any link, your whole account is exposed. Target and Home Depot lost tens of millions of cards, and JPMorgan 75 million accounts. Not because they are careless; quite simply, “there are two kinds of companies: those that have been hacked and those that will be.”

A Bitcoin transaction is the opposite: a signed authorization message that points to an unspent output and a new destination. It contains no secret at all. Print it on a billboard, shout it from the rooftop, or send it by carrier pigeon or smoke signals; there is nothing in it to steal.

Emoji and shortwave radio

Can an authoritarian government block transactions? No. Skype has an alphabet of 128 emoji, that is, a base-128 encoding, so a 250-byte transaction becomes a string of emoji. A two-line Python script. Ban Skype and I use Facebook, then Craigslist, then a review on TripAdvisor, then a comment on Wikipedia, then the background of a vacation photo. And with no internet at all? A shortwave transmitter with a USB port, an antenna made from a clothesline or a fence wire, the push of a button and twenty-five seconds of transmission, and then you vanish into the woods. “How do you stop that? You don’t.”

The medium is the message

When the medium is expensive, it limits the range of expression: Gutenberg’s press printed only Bibles. Then comes the descent: television, then cinema, then theater, with every generation sneering at the next medium as trivial and “vulgar”; even Aristotle complained that the young preferred theater to philosophy. Twitter took the cost of publishing to zero, so we got “SMH,” but also the tweets of the Cairo revolution, which CNN was reading on air. Gatekeepers confuse the cost of their production with the value of their message, and think that control is quality.

The grand arc: from grandeur to grandparents

The old financial networks segment money by size and by recipient: for small amounts and large ones, for companies and governments... and no network from consumer to consumer. I cannot send twenty cents across the world. Bitcoin frees the entire range: from a satoshi to a nation’s oil bill. And in the grand arc of technology, every “grand” medium ends up with the grandparents: the first checks financed the East India Company, and today a grandmother pulls one out in the supermarket line and everyone groans. The banks will cling to their domed halls and their empty vaults, which will become bars serving cocktails.

We have separated the message from the medium. Money is now a content type. And we are never going back.

Paraphrased from the talk

The idea in one line

A Bitcoin transaction contains no secret, so it can travel over any medium, even emoji or radio; money has become a content type freed from its medium, and the gatekeepers of the old medium are at the end of their arc.

A talk with no slides ("I brought a beer as a visual aid"). Antonopoulos recounts his first encounter with Bitcoin: it looked like a familiar banking system, with block explorers showing "sender," "recipient" and "account." Then, as a programmer, he opened the source code and found none of those words. No balance, only unspent outputs; no sender, only inputs. He discovered that Bitcoin has an **atomic nature**.

There is no such thing as copper

In chemistry we talk about copper, iron and helium, but beneath chemistry lies a simpler layer: atomic physics. Copper is not a "thing"; it is a pattern of protons and neutrons, and the very same proton could just as well be part of helium. A handful of particles make a hundred elements with utterly different properties. Bitcoin is the same: its elements are the components of a transaction and the script language, mathematical and cryptographic properties (does this hash equal that one? does the signature match?). The "transaction" you see is merely a **composition** of those elements that looks like a bank, to help you understand at the beginning.

Lego and the red fire truck

His favorite toy as a child was Lego, but he never built what was on the box. If the cover showed a red fire truck, he built a dragon or a "hippo-giraffe." Had he been given a smooth, molded plastic truck, it would have been perfect, but it would only ever be a fire truck, and he would be bored with it in twenty minutes. Lego is messy and has sharp edges, but it unleashes creativity. Bitcoin is a box of Lego with a picture of a "payment system" on the cover, and when we show it to the banks they say: your truck has sharp edges and is made of silly pieces.

Cooking and McDonald's

Then cooking: a perfect blend of science and art. If you understand how ingredients react to salt and heat, you can make anything. Bitcoin is ingredients and recipes, not a finished result. We take the ingredients and make a burger (a payment system), and the banks say: McDonald's makes one in 45 seconds and sells a billion of them, so why do you need a chef? But they are missing the point: we do not want a billion copies of a poor product; we want to unleash the creativity of an entire generation. People recombine the ingredients: atomic transactions and digital signatures give you a crowdfunding platform; a two-party signature with timelocks gives you a payment channel that bills for streaming video by the second; link the channels with hash-locked contracts and you get the Lightning Network. Recipes no one has ever seen before. And when the banks say "the fees are high and scaling is impossible," what they are saying is "your burger is slower than McDonald's."

The factory that makes nothing but red trucks

The red-truck factory tells you that 95% of children want a red truck, that it was tested in focus groups, and that it costs three cents with a little lead paint. But it cannot make anything else. That is how the financial system built itself: it serves a small elite segment, with totalitarian surveillance "the Stasi would envy" and borders that do not allow commerce, and it can block a donation to WikiLeaks while you can still donate to the Ku Klux Klan. It is the most efficient in the world at one thing: exclusion and surveillance. As for "our crazy little mixture," it may be slow and inefficient, but it grants freedom and unleashes creativity.

We are not trying to sell a billion burgers in 45 seconds. We are trying to unleash the creativity of an entire generation.

Paraphrased from the talk

The idea in one line

Bitcoin is not a payment system but a platform of trust made of atomic elements that can be recombined, like Lego, chemistry and cooking; its value lies not in efficiency but in freedom and creativity.

Will Bitcoin Fail to Scale?

Paralelní Polis, Prague · March 2016 · at the height of the block size debate

Delivered at the height of the “block size war,” yet it approaches scaling from a historical angle rather than a technical one. In 1989 the internet was dial-up even at its backbone, and there was “Usenet”: discussion groups whose messages spread from node to node over phone calls, arriving 24 to 48 hours later. As Usenet grew, the “experts” calculated that one day’s worth of messages would take 26 hours to carry, and a day has only 24. Therefore the internet would collapse.

A chain of gradual, successful failure

- **Email:** messages arriving within two hours instead of a day; “the internet will collapse.” Solved.
- **Attachments:** ten times the size of text. It will collapse. Solved.
- **Voice over the internet:** the phone companies ran campaigns about how impossible it was, then started carrying their own calls over it.
- **Video:** had we launched Netflix in 1992, it would have melted the internet. And today, Netflix.

Networks do not scale. Some of them simply **fail to scale gracefully for decades**, and those are the networks that succeed. Scale is not a goal you reach; it is a definition of what you can do with the network today. No sooner does capacity increase than someone invents an application that fills it, and the network fails all over again.

Bitcoin fails gracefully too

The very arguments once made about email, voice and video are being made now: “It will never reach Visa’s scale; it will collapse under adoption.” There is a website that collects the “Bitcoin obituaries” published every three to six months since 2009, and it has become the best recruiting tool there is: people hear that Bitcoin has died, then four months later they hear about a new application and ask, “Bitcoin is still around?”

When the network filled up during a stress test, transactions were delayed and newcomers panicked, thinking their money was “in transit,” when in fact there is no in-between state at all. Some wallets raised their fees from four cents to seven, and the press pronounced Bitcoin dead. What actually happened: wallets were built that are smarter at calculating fees, and flooding the network became expensive for the attacker and nearly free for the genuine user.

There is no such thing as a “spam transaction”

There are two ways to deal with congestion: a paternalistic, top-down decision about what is “legitimate,” which breaks the network’s neutrality and confines its future to the applications we can imagine today; or letting the market set the minimum fee through supply and demand. Whoever pays the fee has a legitimate transaction by definition. There are no spam transactions; there are transactions that were mined and others that did not pay enough.

There is no president of Bitcoin

And the governance crisis is not a crisis; it is simply the fact that Bitcoin is hard to change, because there is no one who can say, “I’m the president, end of discussion.” That is not a flaw but the most important feature. Democracy is noisy; its opposite is twelve men with cigars meeting to cut interest rates for the 101st time without a single dissent. As for the banks, they cannot adopt Bitcoin; it is the “poison pill” for global finance, and what they are building is an intranet, not an internet.

The internet has been failing to scale gracefully for twenty-five years. In Bitcoin, let’s keep failing gracefully too. Bitcoin is not dead yet.

Paraphrased from the talk

The idea in one line

Scaling is not a problem to be solved but a moving frontier that keeps being pushed; the networks that succeed are the ones that fail to scale gracefully for decades, and every Bitcoin “obituary” recruits new believers.

The threads that tie the chapters together

Eleven talks over four years, yet they revolve around a handful of ideas that recur in different wording. If you forget all the details, these are the ideas Antonopoulos wants to stay with you.

The idea	What it means	Where it appears
Currency is only the first application	Bitcoin is a neutral platform of trust, and money is the first thing built on it, just as email was the internet's first application.	Chapters 1, 3, 5, 10
Neutrality and permissionless innovation	The network does not distinguish between sender and recipient, or between large and small, so anyone can build on it; innovation happens at the edges, not at the center.	Chapters 1, 3, 5, 11
Money is a language, not a flag	Money is a way of expressing value, older than writing, and currencies will coexist like languages, not like empires.	Chapters 2, 7, 8
Absolute ownership, not debt	Your money in the bank is a loan. In Bitcoin, whoever holds the keys owns the money, with no intermediary able to freeze or seize it.	Chapters 2, 10
Privacy for individuals, transparency for the powerful	Our system is upside down: our transactions are exposed and the money of those in power is secret. Bitcoin restores the balance.	Chapters 3, 9
Every great technology was mocked	The car, electricity and the internet were ignored, then mocked, then fought. Bitcoin is in the mockery stage; afterward, history gets rewritten.	Chapters 4, 6, 11
Infrastructure inversion	The new first lives on top of the old infrastructure and looks like a failure; then things flip and the old runs on top of the new with ease.	Chapter 6
The other six billion	Bitcoin is not for the billion who have international banks, but for those who have a cheap phone and no bank.	Chapters 1, 4, 8
The banks cannot swallow it	A "blockchain without openness" is like an "internet without neutrality": a boring intranet. What makes Bitcoin strong is exactly what the banks do not want.	Chapters 2, 5, 6, 11
Failing to scale gracefully	Scaling is not a problem to be solved but a frontier that keeps being pushed, and every new bit of capacity is filled by a new application.	Chapters 5, 11

What sets this volume apart from the two that follow?

Volume One was written (or rather, delivered) in the years when Bitcoin was still being treated as a joke or a threat. That is why its tone is both defensive and evangelistic: it explains what Bitcoin is and answers "it will die," "criminals use it" and "it won't scale." Volume Two (2017) shifts to a broader critique of the financial system and of money as a tool of control, and Volume Three (2019) to financial surveillance and the currencies of corporations and states. But the whole foundation is here.

Where this summary came from

This summary is based on the recorded talks that make up the book *The Internet of Money, Volume One* by Andreas M. Antonopoulos, published by Merkle Bloom in 2016. The talks are published on the author's YouTube channel under a **Creative Commons Attribution (CC BY)** license, which permits reuse, translation and summarization provided the source is credited.

The quoted lines in this summary are paraphrases of what the author said in the talks; they are not verbatim and are not taken from the text of the printed book. Any error in summarizing is the summarizer's, not the author's.

The original talks

Chapter	Talk	Venue and date
1	What is Bitcoin?	Disrupt, Athens — November 2013
2	Peer-to-Peer Money in a Historical Context	Reinvent Money, Rotterdam — September 2015
3	Privacy, Identity, Surveillance and Money	Fab Lab, Barcelona — March 2016
4	Innovators, Disruptors, Misfits and Bitcoin	Maker Faire, Detroit — July 2014
5	Dumb Networks, Innovation and the Festival of the Commons	O'Reilly Radar, San Francisco — January 2015
6	Bitcoin and the Coming Infrastructure Inversion	Bitcoin Meetup, Zurich — March 2016
7	Money as Language & the Multi-currency Future	Bitcoin Expo, Toronto — April 2014
8	Bitcoin Design Principles	IDEO Lab, Boston — June 2015
9	Money as a Content Type and the Grand Arc of Technology	BitcoinSouth, Queenstown — November 2014
10	Bitcoin: Elements of Trust	Blockchain Meetup, Berlin — March 2016
11	Will Bitcoin Fail to Scale?	Paralelní Polis, Prague — March 2016

Links

- Playlist of the Volume One talks on YouTube: youtube.com/playlist?list=PLPQwGV1aLnTvCuQXCZ3RBvdICnqstTirl
- The author's channel: youtube.com/@aantonop
- The book (print, ebook and audiobook): theinternetofmoney.info
- Mastering Bitcoin, free in several languages: bitcoinbook.info

Summary by Turki Alsharari — @Alshs0b · This summary may be shared freely with attribution.

Summary by

Turki Alsharari



X account

[@AlshtsOb](#)



Website

The Bitcoin power law

[btclaw.io](#)