


The full text of this book is available online at:

whycryptocurrencies.com

 This is a self-published book and if you're curious about the creation process I wrote a few blog posts about it:

[REDACTED]

Cover art by Brad Lark 

[REDACTED]

Copyright © 2021 Jonas Hietala.

All rights reserved.

[REDACTED]

To Veronica, who lights my way in darkness.

Acknowledgements

As usual, there is a great woman behind every idiot.

John Lennon

I'm ~~sometimes~~ an idiot, but it's clear that I have a great woman in Veronica that supports me, and without her this book would've never seen the light of day.

A big thanks to Filip Strömbäck, who proof-read everything and provided me with tons of good feedback.

And thanks to all others who gave me supportive comments, feedback, pull requests and donations. I'm forever grateful.

About the book

A perspective beyond the hype

What value does cryptocurrency add? No one's been able to answer that question to me.

Steve Eisman

Whenever the topic of cryptocurrencies—where Bitcoin and Ethereum are the most known—come up in conversations they're almost always misunderstood or dismissed.

If you're a cryptocurrency skeptic I honestly can't blame you. All you ever hear about it on the news is how Bitcoin rallies^[1] and then how Cryptocurrencies are about to become worthless^[2]. Maybe you'll see claims that it's an environmental disaster^[3] or only used for illegal purposes^[4].

Curiously enough they don't explain what cryptocurrencies are or what they can be useful for. But it's to be expected as news today focuses on eye-catching stories; it's why unsettling events like murder gets a disproportional amount of focus.

Maybe this is why most people—even cryptocurrency fans—only see cryptocurrencies as a form of investment? After all there are few things as exciting as the possibility of becoming rich very quickly.

It's interesting when the news handles something you have a good understanding of—they're often completely wrong. Makes you wonder, how wrong are they about things you're not familiar with?

Schneier brings an interesting perspective and he's right about one very important aspect: contrary to popular belief cryptocurrencies don't remove **all** trust.

To counter his point that "cryptocurrencies are useless" all you have to do is provide one counterexample where they're useful. This book is full of them.

Beanie Babies is a type of fluffy toy that people used to speculate with. It **become** a mania where people would sell—and buy—these toys at 10x, 100x or even 1000x their original price. The mania managed to make the creator, Ty Warner, one of the richest men in the world before it crashed (he's still insanely rich though).^[6]

If you're looking for the digital version of Beanie Babies then look no further than CryptoKitties, a blockchain game running on Ethereum. There someone spent \$114,000 on a virtual kitten.^[7]

Tulip mania is one of the first recorded speculative bubbles which occurred 1636–1637 in Netherlands. There people speculated on tulip bulbs which reached spectacular prices before crashing down abruptly.^[8]

But please take care and do your research, there are **many** scams out there.

What hope does average Joe have when even the famous security technologist Bruce Schneier concludes that:

Honestly, cryptocurrencies are useless

Bruce Schneier, "Blockchain and Trust"^[5]

It's almost a universal phenomena. I've heard these arguments from students, co-workers, friends, family and in highly technical online communities:

- 1 It's a scam.
- 2 It's just a speculative bubble and cryptocurrencies are really worthless. Here many draw parallels to Beanie Babies or the Tulip mania. **And to** be fair cryptocurrencies have displayed bubble behavior—several times.
- 3 They don't do anything better than other payment systems like PayPal or VISA.
- 4 There's no legal use case.
- 5 They don't do anything valuable.

It seems everyone has an opinion but few are capable of explaining what they are or what they do differently. Of course most aren't dismissive but simply don't understand what it's all about. Many are curious and want to learn more.

With this book I hope to show how cryptocurrencies can be useful, what use cases exist and how they can help people. I'll briefly go over how they work in a more conceptual level and I might throw in some historical notes here and there. I'm not trying to make anyone a cryptocurrency fan. I just hope to bring some nuance and **to** help answer some common questions.

And I must admit I'm also being selfish—writing a book is on my bucket list.

What this book is

This book tries to describe what value cryptocurrencies have using several examples. In particular I'll argue that:

- 1 Cryptocurrencies aren't just scams.
- 2 It's more than just a speculative asset.
- 3 They do many things better than any alternative.
- 4 There are legal use cases.
- 5 They have valuable use cases.

Of course everything new brings positive and negative aspects with it. It's up to you to decide where on the global spectrum of good and bad cryptocurrencies lie.

What this book isn't

This isn't a deep dive on a technical level and we won't focus on a single implementation. Bitcoin is the first cryptocurrency but there are hundreds more.

Although there are hundreds and perhaps thousands, most are just copies or outright scams.

There are many problems with cryptocurrencies as they exist today, for instance:

- Why aren't cryptocurrencies used more?
- Bitcoin uses a public ledger where all payments are visible—what about privacy?
- How can a cryptocurrency scale globally?
- What about Bitcoin's energy usage?

I don't dismiss these problems, and I discuss them in more detail in the chapter *Challenges for cryptocurrencies* (p.191), but the focus of this book isn't to explain them or to look at how we might address them.

A problem-centric view is great for an engineer or a problem solver but it also limits foresight. For example the computer had many problems and drawbacks when first introduced, but today we ridicule statements like these:

I think there's a world market for maybe five computers

Thomas Watson, president of IBM, 1943

There is no reason anyone would want a computer in their home

Ken Olsen, founder of Digital Equipment Corporation, 1977

Instead of putting on blinders and getting stuck at these problems—which I believe can be addressed—we'll focus on the potential cryptocurrencies have. Only with this vantage point can we see if the problems are worth working on, or if we instead should scrap the whole idea.

And of course none of this is investment advice.

Well, the only advice I'll give is to understand what you're investing in, and my hope is that this book can help with that.

Why cryptocurrencies in five minutes

ELI5 - what is the inherent values of cryptocurrencies?

While cryptocurrencies are mostly seen as speculative assets or get rich quick schemes, they have valuable properties and valuable use cases. For example:

- **Excellent monetary properties**

Cryptocurrencies have better monetary properties (p.41) than anything else in history. In contrast to the fiat money we use today, cryptocurrencies have a limited supply and compared to gold cryptocurrencies are much more portable, are easier to divide into small parts and cannot be counterfeit.

At first glance, this may seem insignificant, but money affects everything and even small improvements can have a massive effect.

- **Cheaper payments**

Merchants have to pay a 1–4% fee for every credit card transaction, while cryptocurrency transactions only come with a small fixed fee (p.50).

- **Irreversible digital transactions**

You receive money in under an hour (p.52) and after that the money is yours, while it may take days to receive other digital payments that can also be reversed weeks or months later.

This means merchants don't have to worry about having a purchase reversed, which usually means they have to swallow the loss.

If you've heard about the ridiculously high Bitcoin fees then don't worry—it's the exception not the rule. Please read the chapter *Cheaper & faster* (p.49) for more info.

This is known as *charge back fraud* or *friendly fraud* (p.52) and is a big problem for merchants.

Please note that Bitcoin (and most other cryptocurrencies) are only *pseudo-anonymous*. There are others—like Monero—that improve the situation. Please see *the privacy and fungibility challenge* (p.193) for more information.

- **For anyone and anything**

Cryptocurrencies can be used by anyone. It's for businesses who cannot accept credit cards (p.55), for people without a bank account (p.73), and people in dysfunctional countries. You can use it for truly uncensorable donations (p.63) and you don't have to worry that your payment processor or bank will freeze your account (p.59).

Nobody can prevent you from sending or receiving cryptocurrencies.

- **Financial privacy**

Banks, credit card companies and payment processors have all your financial transactions on record. Cryptocurrencies allows you to reclaim some of your privacy (p.109) as they work like a swiss bank account in your pocket (p.133).

- **An alternative financial system**

The traditional financial system rewards behavior that caused the 2008 financial crisis (p.83) and relies on being able to predict the unpredictable (p.91). Cryptocurrencies represent an alternative without a central authority that can manipulate the money supply, and they can be used to truly separate money from state (p.151).

- **Extensions**

You can build applications on top of cryptocurrencies, such as provably fair gambling (p.169) or a timestamping service based on mathematics instead of social proof (p.157).

Of course cryptocurrencies don't solve everything perfectly and there are many difficulties—both technical and social—that need to be overcome. And as with all new technology they will be associated with positive and negative change.

If you want to learn more and see more examples just continue reading. You can also jump to whatever chapter interests you—they're supposed to be self-contained.

Part II

What is a cryptocurrency?

Peer-to-peer electronic cash

Bitcoin is the beginning of something great: a currency without a government, something necessary and imperative.

Nassim Nicholas Taleb

If we're going to talk about cryptocurrencies, we need to know what they are. Otherwise, how can we tell what value—if any—they have? And I think the best description of what a cryptocurrency is can be found in the title of the original white paper: *Bitcoin: A Peer-to-Peer Electronic Cash System* (p.189). It's like cash, but in digital form.

In this part, we'll begin by looking at the properties cryptocurrencies have, which lay the foundation for the use-cases described in the book, and we'll take a closer look at how cryptocurrencies work. Technical understanding isn't required to see their usefulness, but it helps us navigate the cryptocurrency space and to see through misleading information.

Then I'll try to back up my claims that cryptocurrencies are like cash by discussing what money is, the properties of money, and if it's fair to classify cryptocurrencies as money. Not only will I say that cryptocurrencies are money, but that they're potentially the best money we've ever seen, although they're held back by volatility and low adoption.

The white paper is a good read. I recommend you look it up. If you prefer an annotated version or a podcast, there are those as well. (p.189)

Chapter 1

Properties of a cryptocurrency

Trustless and permissionless

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

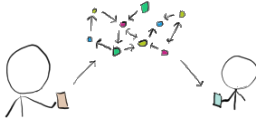
Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”

These are the most important properties of cryptocurrencies as I see it:

- No more third parties
- No counterfeiting
- Predetermined emission rate
- Irreversible transactions
- Private
- Large and small amounts behave the same
- Borderless

They highlight the difference between cryptocurrencies and other payment systems and ultimately they're what makes cryptocurrencies useful.

Technically, you don't interact with each other directly but with a distributed ledger. You trust the system as a whole, not one particular entity.



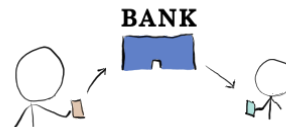
No more third parties

The important difference between a cryptocurrency and digital payments we have today is the removal of a third party. Payments are *peer-to-peer* just as if you gave someone a dollar bill or a gold coin.

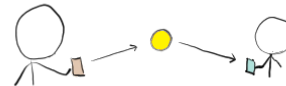
Sending money to people via your bank isn't peer-to-peer as you rely on your bank to send it for you. VISA, PayPal, Swish, Apple Pay and other digital payments have the same problem, all except cryptocurrencies.



Cash is given directly from hand to hand.



Regular digital payments are sent through a bank or different payment processors.



Cryptocurrencies are sent directly from device to device.

Transfers are therefore *trustless* and *permissionless*.

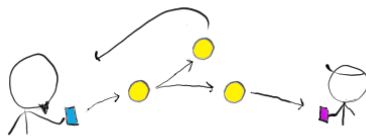
Trustless means you don't have to rely on a third party to make or confirm the transfer for you and permissionless means you don't have to worry about your transactions being blocked. Nobody can freeze your account (p.59) or prevent you from opening one (p.55). Cryptocurrencies are *uncensorable*.

You also don't have to trust a third party to hold your money like you do when you have money in a bank. What you really have is an IOU from the bank where they promise to give you your money when you ask for it. With cryptocurrencies you can write down the keys to your wallet and you alone have access to it.

No counterfeiting

Problems with counterfeit coins and bills go far back. From biting coins to test their hardness to today's advanced techniques, counterfeit prevention has always been an important feature for cash.

With cryptocurrencies anyone can independently verify the integrity of the coins you send and receive. Details on how is in the next chapter but I assure you no biting is needed. You cannot counterfeit coins and you cannot send the same coin to multiple people (*double spend*). This is what allows cryptocurrencies to operate without a trusted third party.



A double spending occurs when someone sends the same coin both to a merchant and back to himself.

Some will be quick to point out that transfers aren't trustless. You need to trust your wallet, the OS, the hardware etc. Which is true. The context here is not having to trust a third party to handle transfers for you, not eliminating trust of all kinds—which is impossible.

You can let a third party hold them if you want and it's probably a good choice for many.

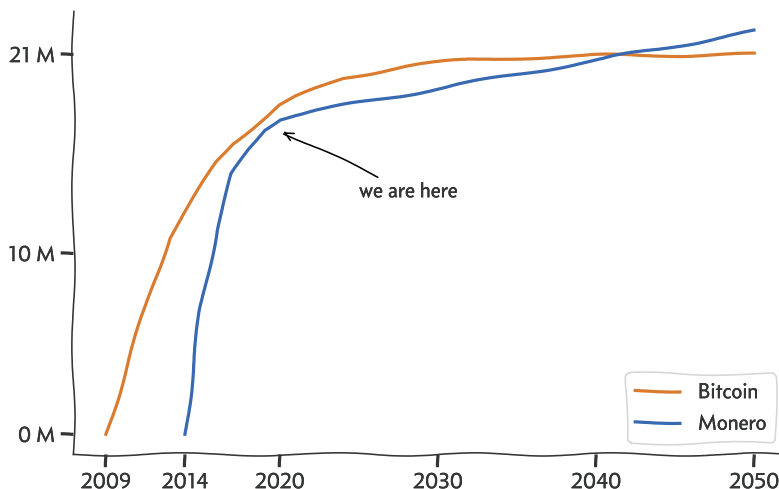
But please make sure to encrypt your seed (a human-readable representation of your keys) (p.208) otherwise a thief can easily steal your coins if he finds it.

The new coins are rewards for miners who secure the network, but more on that in the next chapter.

Predetermined emission rate

As there's no trusted third party, there's no single entity who controls the creation of new money and the inflation. Instead, new coins are minted following predetermined rules.

Circulating supply



The emission rate in Bitcoin approximates the rate gold is mined. In Monero, the tail emission is there to replace lost coins and to make sure rewards for miners don't run out.

If you're curious about Austrian Economics, which most cryptocurrencies follow, I can recommend the Bitcoin.com podcast with Jeffrey Tucker^[11]. It's not something you hear about often, but it presents an interesting viewpoint and shouldn't be dismissed.

The book *Thinking, Fast and Slow* is fantastically thought provoking.

Bitcoin has a hard limit of 21 million bitcoins, while in Monero new coins will always be created.

If inflation is good or bad depends on who you ask. Keynesian economists argue inflation is good^[9] while the Austrian school argues inflation is bad^[10].

I sure don't know who's right. It's probably best to be skeptical of both camps—economics operate in an extremely complex and irregular environment. Economic theories are difficult, or impossible, to verify.

acquisition of skills requires a regular environment, an adequate opportunity to practice, and rapid and unequivocal feedback about the correctness of thoughts and actions.

Daniel Kahneman, *Thinking, Fast and Slow*^[11]

Either way, it's not an argument against cryptocurrencies in general, as they can be made either inflationary or deflationary (although all I know of becomes deflationary).

Irreversible transactions

Just like with cash, cryptocurrency transfers are irreversible. This means if you've sent someone coins, you can only get them back if they agree to give them back. It prevents *charge back fraud* (p.52) but it makes theft worse.

Private

Commonly used payment systems, like credit cards for example, asks you to give up your privacy as all payments are recorded, and they require you to tie your identity to them. But cryptocurrencies can be used privately—there's no need to disclose your identity or your transaction history—making them similar to cash in this respect.

Large and small amounts behave the same

In contrast to cash or gold where large amounts can be cumbersome to handle, there's no difference between large or small transfers in a cryptocurrency. Transaction costs are the same for small transfers as for large transfers, and they are just as secure, and wallets can store as much as you're comfortable with.

It's also easy to split coins into small parts. In fact, you don't have to think about dividing at all, you use a wallet just like a credit card—a transfer is always exact.

Borderless

Cryptocurrencies are inherently global. They're usable wherever you are as long as you have an internet connection. You can even send to wallets which are offline, but to retrieve them you need to access the internet. Technically, you could do transfers completely offline—on paper—but they would be unconfirmed and might not be valid when you do want to use them.

It's possible to reverse transfers... If everyone agrees. Ethereum famously altered their rules in the DAO hard fork. Many agreed but not everyone, so Ethereum split into two coins where Ethereum Classic kept the old rules.^[12]

Bitcoin, like most cryptocurrencies, do record all transactions in a public ledger. So, it's a little misleading to say that cryptocurrencies are inherently private, but some cryptocurrencies like Monero tries to solve this problem (p.193).

For example, one bitcoin can be divided into one hundred million parts—called satoshis. But there's no real technical limit, only a usability concern.

An offline wallet with no computer contact like a *paper wallet* is called *cold storage*. It's an excellent way to store large amounts you're not planning to use for some time.

Chapter 2

How do cryptocurrencies work?

Decentralized consensus

Price is the least interesting thing about bitcoin.

Roger Ver

This is my attempt to explain how a standard cryptocurrency like Bitcoin works. Other cryptocurrencies may diverge on various points but the fundamentals are the same.

As stated in the introduction the focus isn't on technical details, but it's a **hard** balance to make between keeping it simple and explaining how cryptocurrencies work. If this chapter is too technical you can safely skip to the next chapter or just read the summary—it's not required knowledge.

For example, Ethereum adds Turing complete smart contracts (p.155) and CryptoNote protocols like Monero hides transaction details (p.193).

Summary

The *blockchain* is a ledger that stores balances. The crucial problem is deciding between double spends (using a coin twice). Cryptocurrencies like Bitcoin use *proof-of-work* which makes miners expend energy and compete for rewards. This competition between miners is used to resolve double spends and to secure the chain, allowing the winner to extend the blockchain with new transactions that don't double spend.

What makes it all work is the incentives for the miners to work in the best interest of the network as it's the most profitable option. The security assumption is that most of miners are honest and work for profit, otherwise the security model fails and transactions can be reversed.

The ledger

If you want to create a digital currency, you only really need to keep track of how many coins everyone has. For example, your bank might have entries in a ledger like this:

Person	Swedish krona
Sneaky Steve	7 000 SEK
Honest Harry	1 000 SEK

When Sneaky Steve wants to send 500 SEK to Honest Harry, the bank simply updates the ledger:

Person	Swedish krona
Sneaky Steve	6 500 SEK (-500 SEK)
Honest Harry	1 500 SEK (+500 SEK)

Cryptocurrencies work this way as well. In fact, the ledger in a cryptocurrency, often referred to as the *blockchain*, contains the balance of all addresses.

Your keys, your coins

To be able to create a transaction, you need to have the *private keys* to the address you want to send from. Think of it as a secret password that unlocks your account. This prevents anyone else from stealing your coins, unless, of course, they steal your private key!

It uses *public-key cryptography* (p.204), which allows you to prove you control the private key without sharing the private key itself. Compare it to credit card numbers which act as both a private and public key. See *A hitchhiker's guide to cryptography* (p.201) for more details, but low-level cryptographic understanding isn't required to understand how cryptocurrencies work.

It's a slight simplification to say the blockchain stores balances. It actually stores all transactions from which you can calculate all balances.

To lighten the load, you can run your software in a pruned mode which discards the transactions after validation and only keeps the balances.

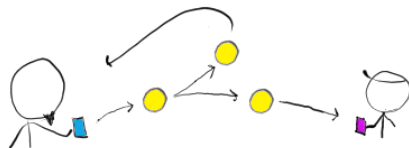
Copying a coin & double spending

So far cryptocurrencies don't do anything new. The hard problem is how do you prevent someone from copying a coin and sending the copies the different receivers? Couldn't you just copy the hard drive to copy your coins?

For example Sneaky Steve wants to buy a computer from Honest Harry and wants to pay with Bitcoin. The computer costs 1 BTC and the Bitcoin ledger looks like this:

Address	Bitcoin
Sneaky Steve 1	1 BTC
Sneaky Steve 2	0 BTC
Honest Harry	0 BTC

What Sneaky Steve tries to do is send 1 BTC to the merchant Honest Harry and then send a copy of 1 BTC to his other address Sneaky Steve 2. (It's possible to have as many addresses as you want—a consequence of the permissionless nature of Bitcoin.)



Sneaky Steve sends a digital coin both to Honest Harry and himself.

If we didn't prevent this the ledger might look like this:

Address	Bitcoin	Diff
Sneaky Steve 1	-1 BTC	(-2 BTC)
Sneaky Steve 2	1 BTC	(+1 BTC)
Honest Harry	1 BTC	(+1 BTC)

We copied our coin and printed 1 BTC out of thin air, so now the ledger contains a negative balance. This is a form of *double spending*—spending the same coin twice.

This isn't really a problem with physical cash since you can't just copy gold coins or paper notes. It's not a problem for banks either since the bank can just deny one or both of the transactions. But this is a hard problem for a digital currency that tries to remove the central authority. This is why before Bitcoin no decentralized digital currency existed.

Decentralization is a common term used to refer to the lack of trusted third party. Instead multiple unrelated entities come together and decide as a group.

There are different types of decentralization in a cryptocurrency to consider. For example:

1. Mining decentralization
2. Development decentralization
3. Node decentralization

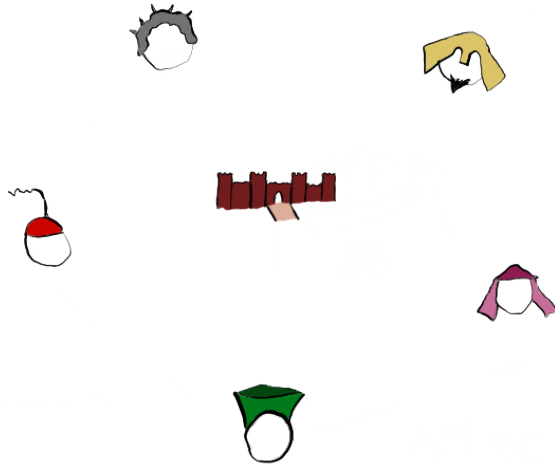
The one we're interested in here is who decides which transactions to approve, which is the miners' job.

The Byzantine Generals Problem

To resolve double spending it's enough to choose one of double spending transactions. But how do you do that when there are many unrelated people—some who want to cheat?

This is the same problem as the *Byzantine Generals Problem*^[13]. Here's my description of a simple variation:

In the Eastern Roman Empire, also referred to as the Byzantine Empire, a couple of generals surround an enemy city:

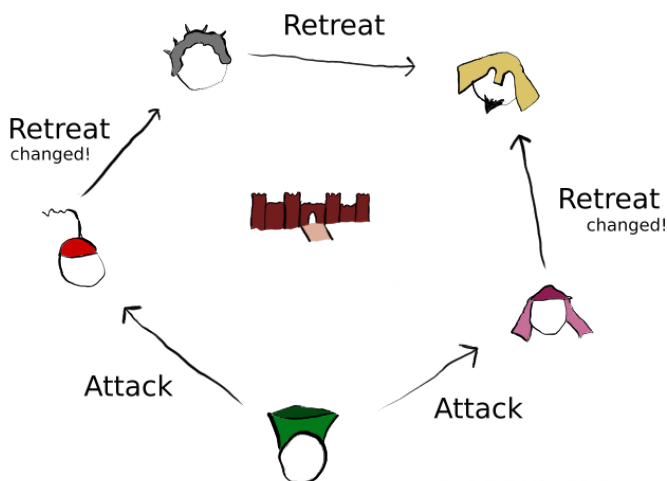


The five generals surround a well defended enemy city. They don't have direct contact and instead need to communicate by sending messengers.

The city is very well defended and if they attack individually they will get crushed. They will have to work together and coordinate to attack at the same time or to retreat as a unit. Doing nothing is not an option either as they have limited food supply and the city is waiting for reinforcements.

If they try to act without a majority they will for sure get defeated—they must coordinate.

This would be very easy if they could trust each other. Unfortunately they cannot trust the messages—either the messenger or the message itself could be replaced—and even some of the generals could be traitors.



One countermeasure to corrupt messengers is to *encrypt* messages (p.204). Unfortunately it doesn't protect against a traitor who knows the code, like one of the generals. Also in ancient times encryption weren't very advanced and could possibly be broken, see the *Caesar cipher* as an example.

One general sends out messengers declaring his intent to attack to the generals next to him, who then sends messengers of their own, and so on until all generals have received the message. However, two of the messengers are traitors and change the message from "attack" to "retreat".

In this simple example three of the generals now believe they will attack while two are preparing to retreat. In a more complex scenario they might receive conflicting messages and notice something is amiss, but they don't know what's real and what's not and cannot decide what to do.

To relate it back to cryptocurrencies the choice between "attack" and "retreat" is similar to choosing between two transactions in a double spend. You know there are bad actors, but who can you trust?

The resistance to this kind of problem is called *Byzantine fault tolerance (BFT)*. There's a big difference between systems with known actors and systems with unknown actors, like with cryptocurrencies, but they both fall under the BFT umbrella.