ANDREW M. BAILEY, BRADLEY RETTLER,
AND CRAIG WARMKE

RESISTANCE MONEY

A Philosophical Case for Bitcoin

ROUTLEDGE

1

BITCOIN'S GENESIS

1.1 Welcome to bitcoin

Bitcoin is for criminals. It's a tool for terrorists, drug dealers, and hackers, and a plaything for degenerate speculators.

Bitcoin is for protestors. It's a tool for Alexei Navalny and other Russian dissidents. It's for Roya Mahboob and women under patriarchal rule. It's for underbanked Black Americans, North Korean and Ukrainian refugees, Venezuelan farmers suffering under hyperinflation, and whistleblowers like Julian Assange and Edward Snowden.

Bitcoin is resistance money.

Bitcoin is money. Though not created or maintained by any nation state, it has higher volume and more users than many national currencies.[1] But it's not just money. It's money for resistance. It's money for people on the margins. This doesn't necessarily make bitcoin good or bad. Resistance is itself neither good nor bad; it matters what's being resisted. We can resist bad things – that's good. But we can also resist good things – that's bad.

No doubt, bitcoin has empowered wrongdoers. That's why they've used it. But bitcoin also empowers those on the margins. In so doing, it serves as a check against the authority and overreach of corporations, states, and anyone else who would stand between people and their money.

Headlines about bitcoin fixate on price, often to the exclusion of all else. This book, by contrast, concerns the nature of bitcoin and its global consequences. We grant that bitcoin has some bad consequences. Even so, we suspect that after you finish this book, you'll prefer to live in a world with bitcoin – a world with resistance money – rather than without.

We begin with the basics – bitcoin's origin and purpose.
It starts with the cypherpunks.

1.2 The cypherpunk dream

Judith Milhon was a force of nature. She had issues with authority. Indeed, she was a criminal, arrested several times for organizing and participating in the 1960s civil rights protests. When St. Jude (as she was known) set her mind to a task, few could dissuade her. And if there wasn't a way, she made one.[2]

As a self-taught programmer, St. Jude became an early and powerful advocate for women in computing and hacking. "Girls need modems," she often said. In the emerging digital world, St. Jude's rebellious spirit found fresh expression. Like the do-it-yourself hippies of the 1970s, hackers in St. Jude's mold wouldn't rely on legacy institutions to accomplish their goals.[3] They would do it themselves – and pay little heed to any rules and rulers in the way.

St. Jude's advocacy and attitude were prescient.

In the 1980s and 90s, cyberpunk stories like *Neuromancer, Blade Runner*, and *Snowcrash* depicted a grim future where society has cut an unholy deal with digital autocrats. The autocrats supply channels for communication and commerce, ways to send and receive messages and money. Then, as we use their channels, the autocrats collect our personal information for power and profit. They can also kick us to the curb – at any time and for any reason. Many self-censor in both talk and trade to prevent the digital autocrats from censoring them first. Sound familiar? It's reality for many worldwide.

To counter these forces, some turn to politicians. They hope for regulatory solutions. They vote for a better world. They might even run for office. Others – the Unabomber types – resort to violence. And some retreat, hoping to find peace elsewhere. Senator, menace, or monk. Until recently, such were the posts in the nascent war against digital authoritarianism.

Those in St. Jude's mold forged another path. Decades before the iPhone, they began to meet regularly in the California Bay Area to discuss how they could avoid a world of digital autocrats with terrifying new powers. They thought cryptography could turn computers into engines of freedom rather than oppression. They didn't primarily rely on politicians, projectiles, or prayer.

Instead, they wrote code.[4] St. Jude dubbed them *cypherpunks*.[5]

The cypherpunks didn't just write code; they wrote *a lot* of code. You may have heard about some of it. The cypherpunks were responsible for Pretty Good Privacy, aka "PGP" (Philip Zimmermann and Hal Finney),

BitTorrent (Bram Cohen), and Wikileaks (Julian Assange), to start. Their work made possible the end-to-end encrypted messaging you might use in Signal or WhatsApp and anonymous internet browsing through Tor. The cypherpunks created pathways for private and secure communication, tore down the walls of intellectual property, fought for civil liberties, and revealed surveillance programs and war crimes to the world. But in our view, perhaps the most important cypherpunk creation is bitcoin.

We use money to express our values and preferences. Our transactions encode our dreams and desires. Money shapes the world. And as the world digitizes, so, too, does the money that makes it go 'round. Since digital money flows through financial institutions, they see every transaction and can stop any one of them. The digital money of banks and payment processors enables the dystopian future the cypherpunks feared.

To protect our privacy and autonomy, we need digital cash – money in the digital world that works like cash in the physical world. Physical cash resists surveillance and control. Unlike the digital money we more often use, physical cash requires no trusted intermediaries to hold and transfer funds. With cash, one party simply hands some bills over to the other. In software speak, cash is "peer-to-peer." So if you'd like to spy on a cash transaction in Chicago, you need eyes in Chicago. Or if you'd like to block one in Singapore, you must prevent the exchange in Singapore. The cypherpunks dreamed of a digital instrument with similar features – digital cash. Digital cash would preserve our privacy and autonomy even as we transact over the internet.

Serious obstacles stood in the way. The big one was the *double-spending problem*. Anyone would love to spend one and the same dollar bill twice – much like we'd love to have our cake and eat it too. But we can't for a couple reasons. First, we don't have a cheap and effective replicator. At least for now, we can't shove a dollar bill in a black box and then, for pennies, withdraw several perfect copies. Second, the Treasury's rules state that more than 50% of a bill must remain in exchange for new currency.[6] So thanks to the laws of physics and the power of a central authority, we can't expand the money supply with the cunning use of scissors.

Digital US dollars work differently, of course. We can't double-spend them because banks and other holders of digital money keep detailed financial records of who has which amounts. And like anyone who counterfeits physical dollars, anyone who cooks the digital books would face severe consequences. So we avoid dollar double-spends, whether physical or digital, with the help of central authorities.

The digital dollars in our bank accounts aren't digital cash because digital dollars aren't peer-to-peer. Truly digital cash, without central authorities, poses a major challenge. Digital cash would be, of course, digital – the

sort of thing that inhabits computers. But digital things are easy to copy and paste – just press CTRL+C/CTRL+V. That's a cheap and effective replicator in the digital realm. Few would use your digital trinkets as money if any 10-year-old could increase the supply with a few keystrokes. The marginal price of such a trinket would rapidly drop to zero.

To protect against digital counterfeiting, we might introduce a central authority to keep a ledger that tracks the ownership of each digital coin. Such an authority could block any attempt to spend one and the same coin twice. The authority could even provide significant privacy assurances. Thanks to advances in cryptography, the authority could block attempted double-spends without knowing the amounts or the parties involved.[7] But such designs reintroduce a trusted party, making the money much less cash-like and easier to block. Indeed, the system as a whole would have a single point of failure, the central ledger tracking all transactions. It would resemble traditional digital money more than digital cash.

Prior to bitcoin, *digital* seemed incompatible with *cash*. In *Digital Cash*, Finn Brunton captures the apparent paradox:

> The work of making cash digital means creating an object that is trivial to transact over networked computers and easy to verify – to prove that it is what it appears to be – but impossible to forge or duplicate, and that can carry the information about what it is and what it is worth, without generating any information about how it is used or by whom.
>
> This is a set of seemingly paradoxical and impossible demands: it must be available but scarce, unique and anonymous but identifiable and reliable, and easy to transmit but impossible to copy. It must have all these attributes in the context of technologies that were designed and built to make copies in their very functioning – costlessly, immediately, and perfectly.[8]

For several years and across various meetups and mailing lists, cypherpunks and their allies plugged away. Perry Metzger, one of the most prolific writers on the cypherpunk mailing list and a moderator of its successor, the cryptography mailing list, says that discussions about digital cash "percolated in the mailing lists more or less constantly for over 15 years."[9] Most attempts to make digital cash never launched. The ones that did, failed.[10]

And then there was bitcoin.

1.3 How bitcoin fulfills the cypherpunk dream

Cash is peer-to-peer. We can save it and spend it without depending on others. When it comes to money that isn't cash, we trust individuals and

institutions to provide financial services for us. When things go well, these providers take on certain roles and thus make our lives much easier. But they also bring risk. When these risks materialize, these providers make our lives much harder. To gain a better appreciation for digital cash, we'll focus on three functions or roles within the monetary domain and the risks associated with each: managing, mediating, and making money.[11]

1.3.1 Managers

Few store their life savings in cash under a pillow. Instead, we have others store our savings for us – managers. They usually have expertise, resources, and staff to provide security. Banks serve as managers most often. We entrust them with our funds because we think it's riskier to hold the funds ourselves.

Yet managers could lose our funds too. When banks hold funds, we trust them to keep funds safe from loss or theft. But banks usually don't store funds in vaults, physical or otherwise. They lend our money to others for profit. So by enlisting a bank to store our funds, we must also trust them to do so responsibly. If they do it irresponsibly, we might lose some or all of our funds.

1.3.2 Mediators

When using cash, you hand over some dollar bills, and the transaction is complete. No one else needs to know what happened, and no one else needs to cooperate for full settlement to occur. The handover is the settlement. In modern electronic payment systems, the "handover" often involves a complex web of trusted parties. These are the mediators.

With a tap of your Visa card, you can leave the store with Flintstone vitamins in hand. But the transaction isn't actually complete. *Provisional* settlement – a conditional and easily revocable state – occurs when Visa initially approves the transaction. But *final* settlement – unconditional and not easily revocable – typically takes days or weeks. In that time, money will travel through Visa, your bank, and the merchant's bank. It ultimately settles through master central bank accounts but might first wind through corresponding banks that facilitate inter-bank transfers.

Thanks to mediators, merchants themselves don't need to extend you credit or know who you are or where you live. But under the hood, mediators involve significant complexity. Your card has the Visa logo. The merchant trusts Visa. Visa trusts your bank. Your bank trusts you. Trust expands our financial powers and provides convenience. Thanks to mediators, we can also transact over great physical distances – good luck doing that with physical cash.

The system works only if mediators deal quickly, honestly, and with few mistakes. But each mediator is a potential point of failure. If they fail, convenience vanishes. You might get stuck in an infinite loop of Muzak and customer service representatives, hoping for someone to put Humpty back together again before dinnertime.

In the web of managers and mediators, some entities play both roles. Banks play both, for example. But whether service providers manage funds, facilitate transactions, or both, they know quite a bit about us. We provide personal information when we sign up for their services. And as we use those services, they collect even more personal information. So we have to trust that they'll steward this information responsibly – to protect it from prying eyes and to surrender it to authorities only with due cause.

Despite the overlap between mediators and managers, only when a provider serves as a mediator does it also serve as an *intermediary* between you and your counterparty in a financial transaction. That is, while both managers and mediators are *trusted parties* in the sense given earlier, mediators are also trusted *third* parties. To make this more vivid, imagine a cash transaction where you hand a dollar bill to a middleman, who then hands it to the merchant. Middlemen are often unnecessary for cash transactions. They are also risky: middlemen might delay or block the transaction or even take a cut for themselves. But modern electronic transactions require middlemen. When things operate smoothly, our trust and their trustworthiness together yield all manner of convenience.

1.3.3 Makers

Under the watchful eye of the Securities and Exchange Commission, American corporations create shares and sell them on the stock market. Corporations that issue stock are *makers*. And holding stock requires trust in its maker. A company that issues more units of stock may dilute the share of the company owned by shareholders, even if those shareholders continue to hold the same number of units. So issuing more stock also makes each unit less valuable.

Money has makers too. Even if you're unfamiliar with corporate finance, you've likely used the dollar, euro, or yen. Their makers are banks. How this happens varies across national boundaries and within them. Typically, *inside money* comes from commercial banks. Your bank account – which is *inside* the private sector – holds inside money. Your bank, in turn, ultimately has a balance at a bank for banks – the central bank, which is *outside* the private sector. Thus, this balance concerns *outside money*.

Inside money is an IOU for outside money.[12] For example, your personal bank account might show a dollar amount. But those aren't real

dollars. They are IOUs or claims on real dollars, the things represented by physical dollar bills or in balances that commercial banks hold at the central bank. Whereas commercial banks issue inside money through debt, central banks issue outside money through, well, decree. And either way, we trust banks to create money responsibly.

The most influential central bank in the world is the US Federal Reserve. It provides a monetary asset, the US dollar, around which billions of people coordinate their economic behavior. They carry out their mission by pushing and pulling various levers to help ensure that the US dollar maintains a stable price – or, what's the same, that goods and services enjoy a stable price in dollars.

The Federal Reserve is a trusted party in all three senses of maker, manager, and mediator – it is the monetary trinity. The Fed makes the dollar. The Fed manages the funds of other banks. And the Fed ultimately serves as the central mediator for digital dollar transactions through services like FedWire.

In sum, managers offer convenience and peace of mind. Mediators maintain financial plumbing. And makers enable economic stability and exchange through a common medium. Users of modern money trust these parties to do their jobs well. This is a tradeoff and involves risk. As cypherpunk Nick Szabo says, trusted parties are "security holes."[13] Managers sometimes fail, leaving their customers with pennies on the dollar. Mediators sometimes block lawful commerce. Makers also make mistakes. They might print too much money and, as inflation soars, put on the brakes too late. Then they might slam the brakes too hard and, as a recession looms, keep the brakes on for too long. Sometimes makers know which levels they'll pull and, as private citizens, execute a series of, let's say, well-timed trades in the stock market. This is insider trading, not with company stock, but with what company stocks trade against – a national currency.

As a group, these trusted parties can and sometimes do imperil our financial privacy, our funds, our freedom to use them as we'd like, and their value. Some will judge that the benefits of trusted parties outweigh the risk. They might be right. It might also be true that we would benefit from having options without one or more of these trusted parties so that participating in the economy doesn't force us into a single set of tradeoffs.

1.3.4 Minimizing trust: Cash and bitcoin

Traditional cash doesn't require users to trust managers and mediators. You can custody your own cash and transact without intermediaries. By being your own manager and mediator, you can enhance your financial privacy and freedom. But cash is subject to maker trust. Someone has to

print those bills. We trust them to print enough – but not too much – and with effective anti-counterfeiting measures.

Whereas traditional digital money requires trust in managers, mediators, and makers, and physical cash requires trust in makers alone, bitcoin requires trust in none. Or more cautiously, it was created to require trust in none. Here's how Satoshi Nakamoto, the pseudonymous creator of bitcoin, puts it:[14]

> I've developed a new open source P2P [peer-to-peer] e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust . . .
>
> The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.
>
> A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.
>
> It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.
>
> One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner. The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model. In its central

> position, the company can override the users, and the fees needed to support the company make micropayments impractical.
>
> Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle . . .
>
> The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.[15]

There's a lot going on here, including some technical vocabulary that we'll explain in Chapter 2. But even a cursory read will give you a sense of what bitcoin aspires to be: an electronic monetary system, with all the conveniences of modern money and without trusted parties – a system that enables peer-to-peer transfer, in other words. Or in two words: *digital cash*. The cypherpunk dream.

Does bitcoin make good on that promise? Did the dream come true? These are questions we'll take up in more detail in subsequent chapters. But for now, we'll make a few observations about how bitcoin's design matches the digital cash ideal.

Recall the risks associated with trusted parties: privacy leaks, blocked transactions, leakage (high fees extracted by intermediating parties), and irresponsible creation or management of monetary assets.

The cypherpunks feared a dossier society, a future where corporations and governments have the proverbial manila folder on each of us. Each of our digital dossiers would include the details of everything we've ever bought – when, where, and for how much. Despite the cypherpunks' warnings, we now live in a dossier society. When we sign up for credit cards or services like PayPal, we cough up our names and all sorts of personal information. Then everything we ever buy sticks to our real-life identities.

Trust – enabled by knowledge – is what makes the system work, and it goes both ways. To store your funds with a manager or transact using one or more mediators, you must register for an account and pass all manner of security or credit checks, visible and hidden. Your transactions are monitored and recorded, and each is attached to your name, your identity, and all the other information about you on file. Your passwords are on file, too, and these sometimes leak in unfortunate or even life-shattering ways.

Bitcoin, by contrast, requires no registration and collects no personal information. With little more than an internet-connected device, anyone can send or receive bitcoin to anyone else in the world. As with email, sending and receiving bitcoin requires both an address and a password. But unlike email, your bitcoin address and its password are meaningless

strings of symbols that bear no tell-tale connection to your real-life identity. Each serves as a pseudonym. You can use as many addresses as you like for as long as you like. Anyone who'd like to build your dossier from your bitcoin behavior has to work much harder to do so.

The previous paragraph is in need of qualification. Unlike the ledgers of typical commercial banks, the bitcoin ledger is open for anyone to read. Even so, bitcoin users can achieve significant levels of financial privacy. We'll explore this subject at much greater length in Chapter 6.

Bitcoin also provides enhanced monetary security. Credit card companies, banks, and payment processors often block transactions and close accounts. Governments sometimes seize money from the accounts of citizens. Although you own the funds in these accounts, you don't possess them. Trusted parties do. And trusted parties work for their own best interests, not ours. So although trusted parties provide valuable services like fraud prevention, they're also security holes. You have to trust them to behave well.

Bitcoin does away with mandatory managers and mediators. You can take custody of your own bitcoin, just as you do with cash. Doing so only requires that you store the relevant password. And since you can send bitcoin to anyone without funneling it through trusted intermediaries, you needn't pass security or credit checks.

Bitcoin also does away with makers in an important sense. The Federal Reserve updates its projections and policies frequently. On a near-monthly basis, millions tune in for the pronouncements from a single man at a podium to guide spending and investment – monetary groundhog day. Bitcoin has no CEO, no central bank, and therefore, no groundhog days. Its monetary policy is non-discretionary. It's also fixed and in two senses. In the first sense, the issuance schedule of bitcoin is planned forever. This is where the supply cap of 21 million bitcoin appears.[16] But some schedules are easier to change than others. And bitcoin's schedule is exceedingly difficult to change; this is how bitcoin's monetary policy is fixed in the second sense. A change in monetary policy would require near unanimity among network participants, an extraordinarily unlikely situation.

Bitcoin promises to combine the conveniences of modern money with the privacy and security assurances of cash but without the risk of makers. It's an enticing promise. So enticing, in fact, that it should also make you very skeptical.

We're skeptical too. Yet we will argue that bitcoin makes good on many of its promises. There are momentous tradeoffs along the way and qualifications aplenty. But fundamentally, bitcoin is what it says on the box: digital cash. And therein lies its power as a tool of liberation and resistance.

We'll say much more about how bitcoin works, its connection to the digital cash idea, and its costs and benefits in the chapters to come. But in what remains of this chapter, we'll describe our method and approach and then briefly preview the rest of the book.

1.4 How we'll proceed

In this book, we explain what bitcoin is and why we think you'd rather live in a world with it rather than without. We consider evidence, data, and arguments from a broad range of disciplines – computer science, law, ethics, finance, economics, climate science, history, international politics, and more. No one, so far as we know, has PhDs in all these areas. And most of these fall far outside our own core expertise in philosophy.

We'd forgive you for thinking that three philosophers aren't up to the task. Wouldn't a book on digital money better suit a computer scientist or economist? Or perhaps better yet, a computer scientist/economist? Maybe so. But not *this* book. Our big question is whether we would rather live in a world with or without bitcoin. To frame this question well, we must consider philosophical issues about bitcoin's nature, the nature of the worlds we're considering, the method for deciding, and the relevant values and moral principles in play.

We need philosophical tools not only to frame the question but to answer it. Now you might propose to answer the question by determining whether bitcoin helps or hurts more people overall. But this strategy treats everyone equally. Perhaps a welfare bump for the poor should trump the costs to the rich. The strategy also neglects the varying degrees to which Bitcoin helps or hurts different people. A person who saves Bitcoin privately to leave an abusive spouse outweighs a person who loses $1,000 in a bitcoin gamble. A full evaluation should also incorporate the degree to which bitcoin benefits and harms each person.

But that alone doesn't suffice either. Both present people and future people matter, not present people alone. Given the world's current state and trajectory, is it *better* that we continue with bitcoin or without? To answer this question, we'll reason from first principles about right and wrong, what money is and could be, which features of money are good features for a money to have, how to balance harm and happiness, and so on. Overall, we use the tool of philosophical argument. And the book revolves around a philosophically-motivated thought experiment to derive our conclusion: that very likely, you would prefer to live in a bitcoin world. So this particular bitcoin book needs philosophy.

We also need more than philosophy. We need the tools of computer science and cryptography to understand bitcoin's technical machinery. We

need tools from economics to understand bitcoin's incentives and the possible effects of its monetary policy. We need tools from physics and climate science to understand bitcoin's energy consumption. We also need to observe the world to see how bitcoin currently affects it and speculate reasonably about its future effects, given our current trajectory. We'll use data in the aggregate, as well as particular events. We'll use statistics about banking and finance, for instance, and examine real-world uses of bitcoin. Thus, unlike purely theoretical philosophy books, this one has two feet firmly planted in the concrete world. The task is enormous precisely because so many disciplines bear on it.

Herein lies the danger. Foreigners often get lost. And we are, in all fields except philosophy, foreigners. We are what Nathan Ballantyne calls *epistemic trespassers*, people who pass judgments in an area without having that area's evidence or skills.[17] No one can avoid this while working on the big questions about bitcoin. The questions are too expansive and multidisciplinary. To trespass responsibly, we've shored up our knowledge in other domains and consulted with a range of experts from other disciplines. Although the main argument channels evidence from other disciplines, it nonetheless remains philosophical overall.

This book focuses on the current state of the world, bitcoin's place in it, and the world's potential trajectories. We consider the people bitcoin helps, as well as those it harms. And besides individuals, we consider past, present, and future structural factors in the distribution of goods and power. We firmly believe that anyone who attends solely to bitcoin's benefits misses something, as does anyone who attends solely to its harms. A reasonable view about bitcoin requires considering both. In what follows, you'll find a framework for doing exactly that. And if you use it, you'll likely judge that bitcoin's benefits outweigh its costs.

1.5 Disclosures and denials

Let's clarify what the book doesn't do.

We don't prophesy. Though we'll argue in Chapter 5 that volatility is baked into bitcoin's design, the book makes no systematic bitcoin price predictions. The price of bitcoin will go up. But it will also go down. Up, down, all around. It might even drop to zero. But we care far more about bitcoin's use as resistance money than we do about bitcoin's price. So that's what this book is about.

We don't market. The book doesn't promote or encourage investment in bitcoin.[18] Imagine an overall positive philosophical assessment of the internet from the 1990s. At the time, detractors wouldn't have automatically

accused the authors of goading others to "buy the internet." This sounds silly because the main internet protocols were never monetized. But we often meet this sort of response to our work on bitcoin, and it's no wonder why. Bitcoin isn't just monetizable – it's money. And if you squint hard enough, defending anything that has a price resembles marketing. But this book isn't a pamphlet. We don't care whether you buy bitcoin. So we won't explain how to buy, hold, or spend it. We're philosophers. We care more about the truth than about bitcoin. We offer arguments about bitcoin but not arguments to buy bitcoin.

We don't preach – not to the choir, at least. Substantial portions of the book won't please many die-hard bitcoin enthusiasts. We argue for claims that many bitcoin enthusiasts reject or wouldn't say aloud in polite company – that bitcoin and the US dollar are symbiotic, that the world likely won't undergo "hyperbitcoinization" in our lifetimes (where bitcoin becomes the only money), that bitcoin can help ameliorate very real and human-caused climate issues, and so on. Although bitcoin enthusiasts have a diverse set of beliefs, as we discussed earlier, many influential bitcoin enthusiasts do endorse Austrian economics and some form of radical libertarianism or even anarcho-capitalism. We don't, however. And the book doesn't. We have few, if any, ideological arrows in our quiver. We argue from widely held beliefs.

We also acknowledge potential sources of bias. All three of us use bitcoin as money and hold modest amounts of it.[19] This could skew our judgment. We're human. We've all been fellows with the Bitcoin Policy Institute. One of us has also written for a bitcoin company. We appear on bitcoin podcasts, publish in bitcoin venues, and speak at bitcoin conferences. We have social ties across the bitcoin world. These all provide insight. But they also likely skew our judgment.

Some will call us grifters. Suppose we are. Still, our arguments stand or fall on their merits. We submit them for serious consideration. But really, we humbly submit that the grift critique gets things backwards. We advocate for bitcoin because we believe in it after years of study; we didn't study bitcoin for years because we own bitcoin. We've also taken on reputational risk. Academics, for the most part, still associate bitcoin with alt-right political views, gambling, and crime. Any academic who writes positively about bitcoin risks being labeled as a political radical or, yes, a grifter. Indeed, we know many academics who agree with us about bitcoin but who don't say so publicly for fear of reprisal. We've risked our reputations to say publicly what we've discovered privately – that bitcoin is likely overall good. This book is evidence of our skin in the game. We invite you to play, by considering the arguments themselves.

1.6 Audience

If you've made it this far and are curious about what comes next, this book is for you. Bitcoin is complex. But we'll equip you in the pages to come with just about everything you'll need to know to understand it, without fixation on unnecessary technical details.

The book is also for bitcoin skeptics. Skeptics keep us honest. They probe and poke and question. We're here for it. Although we view bitcoin positively, we'll draw throughout on premises that anyone can accept, not just die-hard friends of bitcoin. We'll also present and evaluate several dozen challenges to bitcoin along the way.

Few outsiders realize that crypto enthusiasts number among bitcoin's most ardent skeptics. We've also seen outsiders express surprise at the contempt bitcoin enthusiasts often have for the rest of the cryptocurrency space. Although we think bitcoin is special,[20] we wage no battles on this front. This is a bitcoin book, not an anti-crypto book. In our experience, crypto folk usually respect bitcoin. Some love it. But many such people hide their feelings to avoid bitcoin tribalists. If this is you, think of our book as a bridge back to bitcoin. Come on over for a bit; it's safe.

This olive branch might frustrate some bitcoin enthusiasts. And if they keep reading, we might frustrate them a bit more. As umpires of ideas, we call balls and strikes as we see them, even if we upset the home crowd. Standard pro-bitcoin arguments require significant qualification, and some should be rejected altogether. Tribalism, here as elsewhere, provides an unreliable outlook on the world. Tribes narrow and blur our vision.[21] Despite the hopes of many bitcoin diehards, it won't end war, restore the traditional family, or fix the real estate market. It won't improve nutrition, inspire a return to Renaissance-style art, or revive nineteenth-century architecture. Bitcoin does not fix everything. It fixes a few things – and even breaks some others. But what it does fix is of great consequence.

Many policymakers agree that bitcoin is consequential. Rarely do they treat bitcoin as they once did – as digital pogs or Dutch tulips, a passing fad among the young or degenerate. Even so, policy discussions often miss the mark. Many bitcoin-related policy recommendations would hurt more than they help. We think the main culprit here is ignorance. So policymakers would benefit from a deeper understanding of bitcoin and its global consequences. This book offers exactly that.

On the flip side, concerned voters hear that Governor so-and-so is pro-bitcoin or that Senator such-and-such is anti-bitcoin. We offer no advice about how to weigh political candidates on the basis of their bitcoin

stances. But the book will help readers understand bitcoin well enough to evaluate many policy proposals that touch on bitcoin.

Some crystal-ball readers suspect bitcoin is the future of money. And they wonder what the future holds as a result. They'll find valuable ingredients for their mental models in what follows.

Potential investors scrutinize bitcoin's value proposition. Although we would make crummy financial advisors, anyone who hopes to bet on bitcoin's success (or failure) would benefit from a deeper understanding of what bitcoin is and how it fits into the world.

Finally, we come to the philosophers. Our people. Understanding bitcoin requires some familiarity with several disciplines. But the big questions – the most controversial and interesting ones – are essentially philosophical. And this book is packed with controversy. There's some heterodox metaphysics in Chapter 2, unusually non-ideal political philosophy in Chapter 4, strident and liberal anti-censorship and pro-privacy arguments in Chapters 6 and 7, and a pro-bitcoin conclusion in Chapter 12. And then there's Chapter 11 – a compendium of anti-bitcoin arguments and responses to them. Food for thought: enjoy the meal.

1.7 Preview

The central question of the book is whether we ought to prefer a world with bitcoin to a world without bitcoin. So after explaining what bitcoin is and situating it among other cryptocurrencies, we introduce our preferred method of evaluation: the veil of ignorance. We ask the reader to forget who they are in the world and evaluate bitcoin from the supposition that they could turn out to be any actual person. We break the central question into five dimensions: monetary policies and institutions, privacy, censorship-resistance, financial inclusion, and security and energy use. Along each of these dimensions, we argue that bitcoin offers something valuable. With respect to monetary institutions, bitcoin brings the rule of law to the world of money and is an attractive alternative and opt-in money, especially for the billions who suffer under bad monetary rulers. With respect to financial privacy, we show how bitcoin's open architecture enables swapping, joining, and routing techniques that in turn enable privacy by obscurity – just like ordinary physical cash. With respect to censorship, we show that uncensorable money is a powerful tool in the fight against the authoritarian regimes under which half the world's population suffers. When it comes to financial inclusion, we discuss the reasons people are excluded from traditional monetary networks and show that bitcoin does not allow for systemic exclusion. We then turn our attention

to bitcoin's security and discuss bitcoin's energy use and the positive and negative externalities that energy use leads to. Having made a case for bitcoin due to the aforementioned features, we then offer and discuss all the best objections to bitcoin.

Where does this all leave us? We conclude with a cumulative evaluation of bitcoin that integrates the results of the previous chapters. If you didn't know who you'd be and were moderately risk averse, we think the balance of the evidence supports a net positive assessment of bitcoin behind the veil. There is room here, though, for reasonable disagreement, and our framework highlights the dimensions that matter, clarifies the fault lines that remain, and helps identify empirical, technical, and normative theses that deserve further attention. We conclude with a meditation on what bitcoin may yet do.

But before all that, you might want to know what bitcoin really is. That's where we turn next. But be warned that the next chapter is technical, especially Section 2.3 and following. Those who aren't interested in those technical details can skip ahead to Chapter 3.

Notes

1. Hazlett and Luther (2020).
2. Halvorson (2021).
3. Schrepel (2021).
4. Hughes (1993).
5. Bartlett (2016) and Levy (2001): Chapter 7.
6. We'll often speak of dollars, or US dollars, because that's a currency with which we and many others are familiar. In most cases, readers can substitute their own state-issued currency.
7. Chaum (1982).
8. Brunton (2020, p. 1).
9. Metzger (2022).
10. The preface to Narayanan et al. (2016) – "The Long Road to Bitcoin" – documents about a hundred cryptographic electronic payment systems, nearly all of which failed.
11. Each kind of trusted party can be found in an early post announcing the creation of bitcoin and explaining its contrast with conventional systems, quoted nearly in full later.
12. Lagos (2008).
13. Szabo (2001).
14. We'll drop the "Nakamoto" from here on out, refer to Satoshi as an individual (although the moniker may well have been operated instead by a collective), and use the pronouns that Satoshi apparently preferred. As for Satoshi's true identity, we'll not speculate on the matter here but refer interested readers to Frisby (2014): Chapter 6 and Appendix II.
15. Nakamoto (2009a). Notably, the post quoted here appeared on the website for the P2P foundation, "The Foundation for Peer to Peer Alternatives," further cementing disintermediated commerce as a central goal in bitcoin's design.

16. In fact, there will eventually be exactly 20,999,999.9769 bitcoin, 20,999,949.9769 of which will ever be spendable.
17. See Ballantyne (2019a, 2019b, p. 207).
18. For a book that takes up that task, see Edstrom (2019).
19. We have dollars too – American and Singaporean – and use them as money.
20. Bailey and Warmke (2023).
21. Kahan (2016).

RESISTANCE MONEY

Bitcoin isn't just for criminals, speculators, or wealthy Silicon Valley entrepreneurs – despite what the headlines say. In an imperfect world of rampant inflation, creeping authoritarianism, surveillance, censorship, and financial exclusion, bitcoin empowers individuals to elude the expanding reach and tightening grip of institutions both public and private. So although bitcoin is money, it isn't just money. Bitcoin is *resistance* money.

Resistance Money: A Philosophical Case for Bitcoin begins by explaining why bitcoin was invented, how it works, and where it fits among other kinds of money. The authors then offer a framework for evaluating bitcoin from a global perspective and use it to examine bitcoin's monetary policy, censorship-resistance, privacy, inclusion, and energy use. The book develops a comprehensive and measured case that bitcoin is a net benefit to the world, despite its imperfections. *Resistance Money* is intended for all, from the clueless to the specialist, from the proponent to the die-hard skeptic, and everyone in between.

Key Features:

- Provides a philosophical approach that makes use of multiple disciplines in its analysis
- Offers a clearly written, measured academic treatment of bitcoin, comprehensive in scope and free of ideological baggage
- Includes information on the financial, social, and environmental costs of bitcoin, how these costs are sometimes exaggerated, and how they might be mitigated
- Addresses the strongest arguments against bitcoin and shows how some succeed and most come up short.

Andrew M. Bailey is Associate Professor of Humanities at Yale-NUS College, Singapore.

Bradley Rettler is Associate Professor of Philosophy at the University of Wyoming in Laramie, Wyoming, USA.

Craig Warmke is Associate Professor of Philosophy at Northern Illinois University in DeKalb, Illinois, USA.