

‘You need to read *Cryptocurrency* today’

NIALL FERGUSON, AUTHOR OF *THE ASCENT OF MONEY*

PAUL VIGNA AND MICHAEL J. CASEY

CRYPTO CURRENCY



**How Bitcoin and Digital
Money are Challenging the
Global Economic Order**

Contents

	<u>Cover</u>
	<u>About the Book</u>
	<u>About the Authors</u>
	<u>Dedication</u>
	<u>Title Page</u>
	<u>Introduction: Digital Cash for a Digital Age</u>
	<u>1. From Babylon to Bitcoin</u>
	<u>2. Genesis</u>
	<u>3. Community</u>
	<u>4. Roller Coaster</u>
	<u>5. Building the Blockchain</u>
	<u>6. The Arms Race</u>
	<u>7. Satoshi's Mill</u>
	<u>8. The Unbanked</u>
	<u>9. The Everything Blockchain</u>
	<u>10. Square Peg Meets Round Hole</u>
	<u>11. A New New Economy</u>
	<u>Conclusion: Come What May</u>
	<u>Notes</u>
	<u>Acknowledgments</u>
	<u>Index</u>
	<u>Copyright</u>

About the Book

The system that governs how money works, with its brokers and middlemen, has stayed roughly the same for centuries. Now there's an alternative, and it puts us on the cusp of a revolution that could reshape our world.

At the heart of this lie cryptocurrencies, a technology with the transformative potential of the printing press or the internet. They bypass the elites and cut out the gatekeepers. Unlike traditional money they're peer-to-peer, they don't have a nationality, they're digital and democratic. They are also lawless.

For the Afghani woman denied a bank account by a repressive society, or any of the world's 2.5 billion unbanked individuals, cryptocurrencies open new possibilities. What would a world without banks or credit cards or even national currencies look like for all of us?

From Silicon Valley to the streets of Beijing, this is a book about a revolution in the making, a story of human invention, and a guide to the future.

About the Authors

Paul Vigna is a markets reporter for *The Wall Street Journal*, covering equities and the economy. He writes for the popular MoneyBeat blog, and is the anchor of the daily, live show of the same name. Before that post, he wrote and edited the Market Talk column for Dow Jones Newswires.

Michael J. Casey is a senior columnist at *The Wall Street Journal*. Casey's work has appeared in publications as diverse as *Foreign Policy*, *The Huffington Post*, *The Far Eastern Economic Review*, *The Financial Times*, *The Washington Post* and *The Boston Globe*. He is the author of *The Unfair Trade: How Our Broken Financial System Destroys the Middle Class*.

For Elizabeth

—PV

For Mum and Dad

—MC

Cryptocurrency

*How Bitcoin and Digital Money are
Challenging the Global Economic Order*

PAUL VIGNA

and

MICHAEL J. CASEY



THE BODLEY HEAD
LONDON

Introduction

DIGITAL CASH FOR A DIGITAL AGE

Money won't create success, the freedom to make it will.

—*Nelson Mandela*

Even though Parisa Ahmadi was in the top of her class at the all-girls Hatifi High School in Herat, Afghanistan, her family was initially against her enrolling in classes being offered by a private venture that promised to teach young girls Internet and social-media skills—and even pay them for their efforts. “Here in Afghanistan a woman’s life is limited by her room’s walls and school,” she wrote in an e-mail.¹ In Afghanistan, girls are not exposed to the Internet, not at home and not at school. That’s the way it might have stayed, too, if Ahmadi hadn’t persisted. She was a top student, and she wanted to take even more classes. In her mind, that was reason enough. She pressed her family, by her own admission, “a lot.”

The venture backing these classes is the Film Annex, a U.S.-based arts group that uses social media and an online site to pay the three hundred thousand bloggers and filmmakers who contribute their work. Film Annex ended up in Afghanistan by way of its direct affiliation with the Women’s Annex, a digital literacy program set up in conjunction with Afghan businesswoman Roya Mahboob, which now educates fifty thousand girls in schools across Afghanistan. Mahboob is something of a celebrity; named one of the one hundred most influential people in the world by *Time* magazine, she runs a software company called Afghan Citadel, is one of the few female CEOs in Afghanistan, and has made education for Afghan women

her central cause. The Women's Annex sets up its classrooms in local high schools, and the classes are taught by women. Because of this last feature, Ahmadi's family finally relented and let her sign up.

Ahmadi started taking classes in 2013. She and her classmates were learning about the World Wide Web, social media, and blogs. A movie lover who also loved to write about the movies that moved her, she began posting on a blog, and its members responded positively to her reviews, earning her the first real income of her young life.

Still, one of the other things most girls don't have in Afghanistan is a bank account. If the Afghan teen ever had any money, she had to transfer it into her father's or brothers' bank accounts, and that's simply the way it is for most girls where she lives. In this sense, she was lucky—for many women from her background male family members block them from access to their funds and treat the money as their own.

Ahmadi's luck would change in early 2014. The Film Annex's New York-based founder, Francesco Rulli, aware of the difficulty faced by women like Ahmadi and frustrated by the transaction costs he incurred in sending relatively small amounts of money around the world, implemented a sweeping change to the Film Annex's payment system.² He would pay his bloggers in bitcoin, the digital currency that had seemed to come out of nowhere in 2013, with a small, fiercely dedicated band of tech-minded, libertarian-leaning digital utopians acting as its standard-bearers, and swearing to anybody who'd listen that it was going to change the world.

Rulli, driven by a philosophy that's a sort of bootstrap capitalism, soon "got" bitcoin and gleaned the advantages it could have for people like Ahmadi, who was one of more than seven thousand young Afghan women listed as paid contributors to the Film Annex. Bitcoins are stored in

digital bank accounts or “wallets” that can be set up at home by anyone with Internet access. There is no trip to the bank to set up an account, no need for documentation or proof that you’re a man. Indeed, bitcoin does not know your name or gender, so it allows women in patriarchal societies, at least those with access to the Internet, to control their own money. The importance of this cannot be overstated. These women are building something that is theirs, not their fathers’ or brothers’. While not a panacea, this blast of cutting-edge, twenty-first-century technology offers real promise as a way to help unshackle an entire swath of the human population.

Many Film Annex contributors in the United States, the United Kingdom, Italy, and other rich countries grumbled about the inconvenience of the digital currency. Few businesses, online or otherwise, accepted it for payment, and to many the whole thing seemed dodgy. The complaints aren’t unique to Film Annex contributors; to many people bitcoin seems like a half-baked scam, some scheme to sucker fools out of their money. Moreover, Ahmadi contends with the same issues related to bitcoin that her peers in other countries had grumbled about, in particular that the options for spending it are still limited, especially in an economy as underdeveloped as Afghanistan’s. To deal with such problems, the Film Annex set up an e-commerce site in 2014 allowing its members to trade bitcoins for gift cards from global sites such as Amazon that will ship to Kabul, Herat, and other Afghan cities. In effect, Film Annex is creating its own self-enclosed bitcoin economy, an approach it reinforced by changing its trade name to BitLanders.

Ahmadi used her bitcoins to buy a new laptop. Only a few years ago, this would have been impossible. She credits bitcoin with “teaching us how to be independent and how to decide by our own, and best of all, how to stand on our own feet.” It’s allowed her to ponder a future in which she

isn't merely an appendage to the men in her life, a future in which she can chart her own course. "I see myself an educated and active female doctor in the future," she said.

You don't typically read stories like Ahmadi's in press coverage of bitcoin. Most of it has focused on the roller-coaster ride of what's seen as a suspect monetary concept. Ask people on the street what they know about bitcoin, and if they can answer anything at all, they'll likely cite the most prominent of those press reports. They'll say something about drug dealers who were busted using bitcoin on the illicit Silk Road Web site. Or they'll refer to volatile price movements and utter the word *bubble*. Or they might recall the sudden vanishing of a large number of bitcoins from a thing with the Dr. Seuss-esque name of Mt. Gox, knowing little more than that it was an obscure online exchange in Tokyo. Perhaps they know of the search for Satoshi Nakamoto, the shadowy figure who created bitcoin.

All of these elements of the circus sideshow that has arisen around bitcoin are both colorful and important to understanding its story. But to dismiss it as a con because of them is to turn your back on something that may well change your life. Bitcoin is a groundbreaking digital technology with the potential to radically change the way we conduct banking and commerce, and to bring billions of people from the emerging markets into a modern, integrated, digitized, globalized economy. If it works—and that's still a big if—an awful lot of things that today seem like part of the natural state of the world are going to look as antiquated as Gutenberg's printing press.

The system we use now for managing exchanges of currency and assets dates back to the time of the Medici family of the Florentine Renaissance, when banks first assumed dominance in the monetary economy of Europe. These guys were the ultimate technological disrupters, radical thinkers who discovered a vital need in society and

then filled it. In essence, they figured out how to intermediate between savers and borrowers, bringing in the excess capital of the former and parceling it out to those among the latter who needed it—all for a fee. This was a dramatic version of what a Silicon Valley investor would these days call a network efficiency. By bringing society's myriad debts and claims into the central ledger of a single bank, the bankers created a powerful, new centralized system of trust. With the help of their specialized intermediating services, strangers that previously had no way of trusting each other enough to do business could now do so. In effect, the Medici created a high-powered system of money creation—money being not a physical currency but a system for organizing, expanding, and sharing society's debts and payments. It made way for an explosion in mercantile trade, which in turn created the wealth and capital that would finance the projects from which great civilizations would grow and conquer the world.

But ... by creating this centralized system of trust and then putting themselves in the middle of it, banks became extremely powerful—eventually, too much so. Since strangers could not do business with each other without the banks, the world's increasingly complex and interconnected economies became utterly dependent on the bankers' intermediation. The ledgers they kept inside their institutions became the vital means through which societies kept track of the debts and payments that arose among their citizens. Thus the banks created the ultimate rent-seeking business, positioning themselves as fee-charging gatekeepers, managers of the financial traffic that made economies tick. Anyone sitting at the sending or receiving end of that traffic had no choice but to deal with a bank—much as Parisa Ahmadi did before the Film Annex changed its payment policy. As this new finance business grew and became more complex, other rent-seeking

middlemen installed themselves as specialized providers of intermediated *trust*—from early bond and securities brokers, to insurance agents, to financial lawyers, to the payment processors and credit-card companies of our modern day. As it currently works, our high-charged global economic system would collapse if these middlemen stopped doing what they do. All of this has simply made the banks at the center of it all even more powerful, so much so that eventually a system that first empowered people has fostered a dangerous dependence upon them. This is what gave rise to the behemoths of Wall Street, which would ultimately take the world to the brink of disaster in 2008.

Enter cryptocurrency—the category to which bitcoin belongs. The simple genius of this technology is that it cuts away the middleman yet maintains an infrastructure that allows strangers to deal with each other. It does this by taking the all-important role of ledger-keeping away from *centralized* financial institutions and handing it to a network of autonomous computers, creating a *decentralized* system of trust that operates outside the control of any one institution. At their core, cryptocurrencies are built around the principle of a universal, inviolable ledger, one that is made fully public and is constantly being verified by these high-powered computers, each essentially acting independently of the others. In theory, that means we don't need banks and other financial intermediaries to form bonds of trust on our behalf. The network-based ledger—which in the case of most cryptocurrencies is called a blockchain—works as a stand-in for the middlemen since it can just as effectively tell us whether the counterparty to a transaction is good for his or her money.

By eliminating middlemen and their fees, cryptocurrency promises to reduce the costs of doing business and to mitigate corruption inside those intermediating institutions as well as from the politicians who are drawn into their

prosperous orbit. The public ledgers used by cryptocurrencies can bring into the open the inner workings of an economic-political system that was previously hidden within impenetrable, centralized institutions. Indeed, the technology's potential as a force for transparency and accountability goes far beyond money and payments, as it can strip out information-controlling middlemen from many other forms of human exchange—in elections, for example, where cryptocurrency enthusiasts see the capacity to end vote-rigging. At its core, this technology is a form of social organization that promises to shift the control of money and information away from the powerful elites and deliver it to the people to whom it belongs, putting them back in charge of their assets and talents.

If we listen to Mike's neighbor, Scott Robbins—the same Scott of Pelham, New York, whose Middle American skepticism toward globalization also helped ground the introduction to *The Unfair Trade*—it's clear that many middle-class Westerners struggle to grasp how all this might improve their own lives. "I just don't understand why I should give a damn about bitcoin," Scott said one evening. And sure, if we focus narrowly on, say, the 2 or 3 percent savings that bitcoin offers on each credit-card transaction fee—a benefit that would typically go to merchants—it's hard to get excited about a "cryptocurrency revolution." But when we consider that world economic output runs to \$87 trillion a year, and think of how much of that is hived off by the same banks and financial toll-collectors that cryptocurrencies bypass, it's possible to imagine many trillions of dollars in savings. Each of us can stake a claim on those funds, indirectly via the employment and income opportunities that businesses might create with what they save on financial costs, or directly via the lower interest rates, bank fees, and transaction charges by our bank and credit-card accounts.

The day you started earning and spending money is the day you began repeatedly handing over slices of that money to these middlemen, often adding up to millions of dollars over a single person's lifetime. Cryptocurrency promises to stop that outflow and put the money back in your pocket. This, in the most basic way, is bitcoin's value proposition—the “Why should I care?” that Scott was looking for.

Cryptocurrency is certainly not without flaws and risks. Some fear that if we follow bitcoin's model, its mechanism for incentivizing computer owners to maintain and manage the public ledger—which drives them to compete for batches of newly issued bitcoins every ten minutes—could encourage a politically disruptive concentration of computing power. So, even as bitcoin aims to decentralize monetary power, capitalism's innate monopolizing tendencies could lead some players to accumulate enough computing power to seize control of the network and revert a trustworthy, decentralized system back to one where self-interested, centralized institutions are in control. Bitcoin is not currently under such a threat, and many believe it would never arise because computer owners who profit from owning bitcoins have no interest in destroying it. Still, the threat cannot be fully eliminated.

Also, bitcoin and crime have been associated, as seen in the Silk Road case, where users sought to exploit the digital currency's anonymity to sell drugs and launder money. Some worry, too, that bitcoin could foment economic crises because it strips government policymakers of the capacity to adjust the money supply and to offset people's instinct to hoard it at times of mass panic. We will examine these important concerns and show how the community of people working on bitcoin is already addressing them.

There's no getting around that cryptocurrency is a highly disruptive technology. All else being equal, technological disruption makes an economy more efficient and creates

more wealth overall. But it is never painless. That will clearly be evident if cryptocurrency takes hold. It will unleash political tensions as millions who've made their living from the old system wake up to find their jobs are at risk. That backlash is already building, even before the technology is properly established, as we'll witness in the struggles and debates that arise in the chapters to follow. The political conflict is not only between those who cling to the old system and those who support the new one, but also within the ranks of the latter group, as idealists, pragmatists, entrepreneurs, and opportunists compete to control cryptocurrency's future.

When disruption is driven by a technology associated with money, these clashes can be especially intense. However, when the knives are out—metaphorically; we're not yet aware of any bitcoin-related assassinations—it's often a good sign that something big is happening.

Former U.S. treasury secretary Larry Summers has grasped this. "If you think about what a modern economy is all about, it basically involves ever more exchange," he told us.³ "And exchange, unless it can be literally simultaneous, always has real issues of trust. So, what the breakthrough in communications and computer science represented in bitcoin does is to support deeper exchange at lower price. And that matters both within countries for the traditionally excluded and it also matters across international borders."

The "issues of trust" to which Summers refers are the core problem that the Medici bankers first sought to solve, the dilemma that strangers face when they seek to do business with each other. When Summers talks of "the traditionally excluded," he's making an oblique reference to the "unbanked," the Parisa Ahmadis of the world, the roughly 2.5 billion people from Afghanistan to Africa to even America who have been shut out of the modern finance system, who don't have bank accounts with

verifiable balances, or credit histories, or any of the requirements banks impose for us to do business through them.⁴ Without access to banking, they are essentially shut out of the modern economy.

At its core, cryptocurrency is not about the ups and downs of the digital currency market; it's not even about a new unit of exchange to replace the dollar or the euro or the yen. It's about freeing people from the tyranny of centralized trust. It speaks to the tantalizing prospect that we can take power away from the center—away from banks, governments, lawyers, and the tribal leaders of Afghanistan—and transfer it to the periphery, to We, the People.

So, what exactly is bitcoin? It gets a little confusing because people refer to two different things when they talk about bitcoin. The first is the feature that has got the most attention: *bitcoin the currency*, the digital units of value that are used by people in exchange for goods and services or other currencies, and whose price tends to swing wildly against traditional government-issued currencies. But that narrow definition distracts from a broader one that captures bitcoin's far more important contribution, and that is *bitcoin the technology*—or, as some prefer to write it in text, *Bitcoin*, with a capital *B* (with the currency always referred to with a lower-case *b*).^{fn1}

At its core, *bitcoin the technology* refers to the system's protocol, a common phrase in software terminology that describes a fundamental set of programming instructions that allow computers to communicate with each other. Bitcoin's protocol is run over a network of computers that belong to the many people around the world that are charged with maintaining its core *blockchain* ledger and monetary system. It provides those computers with the operating instructions and information they need to keep track of and verify transactions among people operating

within the bitcoin economy. The system employs encryption, which lets users key in special passwords to send digital money directly to each other without revealing those passwords to any person or institution. Just as important, it lays out the steps that computers in the network must perform to reach a consensus on the validity of each transaction. Once that consensus has been reached, a payee knows that the payer has sufficient funds—that the payer isn't sending counterfeit digital money.

Now, here's what gets techies, economists, and futurists most excited about bitcoin the technology. They see its open-source protocol as a foundation on which to develop new tools for doing commerce and for managing exchanges. You can think of it as an operating system. (Because it's based on open-source software, we'd use the analogy of Linux for PCs or Google's Android for smartphones rather than Microsoft's Windows or Apple's iOS.) The difference is that bitcoin's operating system is not providing instructions to a single computer on how to run itself but to a network of computers on how to interact with each other. Its core features are its decentralized model of "trustless" proof and an automatically generated database that contains every transaction ever completed, is made available to everyone in real time, and can never be tampered with. Just as mobile-app makers are busy building applications on top of Android, developers are building specialized applications on top of bitcoin that exploit those key features. These applications might merely make exchanges of bitcoin the currency more fluid and user-friendly, such as the mobile digital-wallet apps that allow smartphone users to zap digital money to each other, or their objectives might be much more expansive. The bitcoin protocol's rules for sharing information allow these developers to fashion a set of software-based instructions to manage decision-making across companies, communities, and societies. Because it comes with a fully

verifiable, transparent record of ownership that requires no centralized registry, this “trustless” system allows people to exchange all sorts of digitized items of value and any manner of useful data with confidence that the information is accurate. This all comes without the costly intervention of banks, government agencies, lawyers, and the many other intermediaries required to make our current, centralized system function. That’s the power of bitcoin the technology.

Because of its rapid price rise, high-profile missteps, and passionate, occasionally messianic legions of believers and critics, bitcoin has inspired volumes of heated debate that have tended to overwhelm serious efforts to explain it and its potential. This book is an effort to restore balance to the subject in a way that will allow readers of various levels of expertise and understanding to get a grip on what it is, how it works, and what it might mean for all of us.

We’re journalists, not futurists. Our intent is not to outline some definitive case for what the future will look like. But if we’ve learned anything since the arrival of the Internet, it’s that technology does not wait for us to catch up. From threshing machines and power looms to electricity and assembly lines to mainframe computers and e-mail, individuals and governments who haven’t paid significant attention to new technologies have been in for a nasty shock. We believe bitcoin, and more specifically the breakthroughs that have made it and other cryptocurrencies particularly effective tools for monetary exchange, have the potential to be an important force in finance. Just consider this: control of a currency is one of the most powerful tools a government wields; ask anybody in Ireland, Portugal, Greece, or Cyprus who lived through those countries’ recent financial crises. Bitcoin promises to take at least some of that power away from governments

and hand it to people. That alone augurs significant political, cultural, and economic clashes.

You see hints of those clashes to come in the fervor of the pro and con crowds. The bitcoiners we spoke to in researching this book and talked to during our day jobs at *The Wall Street Journal* have a passion that borders on fervor. Bitcoin takes on the look of a religious movement: the meetups that are reminiscent of church socials, the cultlike crowds that sing bitcoin's praises on social forums such as Reddit and Twitter, the movement's evangelists—people such as Barry Silbert, Nicolas Cary, Andreas Antonopoulos, Charlie Shrem, and Roger Ver (whose nickname is Bitcoin Jesus). At the top of it all, ensconced firmly in a creation myth that inspires and nurtures the faithful, is Satoshi Nakamoto, the godhead of bitcoin.

But cryptocurrencies could flame out entirely—like the Betamax video format (for those of you old enough to remember it). Or they could have only marginal real-world application, much as the once heavily hyped Segway has had. No less a dedicated bitcoiner than Gavin Andresen, the software engineer whom Satoshi Nakamoto effectively appointed to become the lead developer of bitcoin's core software, articulates it this way: "Every time I give a talk, I emphasize that bitcoin really is still an experiment; every time I hear about somebody investing their life savings in it, I cringe."⁵ And that's the guy responsible for keeping the whole thing running. More convinced in their doubt are mainstream business leaders such as JP Morgan Chase's chieftain, Jamie Dimon, who called bitcoin "a terrible store of value," and legendary investor Warren Buffett, who called it simply a "mirage."^{6, 7}

These are not unusual reactions, actually. Most people, we found, react about the same way when they first start to think about bitcoin and cryptocurrencies. Some get past the initial gut reaction, some don't. We expect you'll go

through a sort of Kübler-Ross model of cryptocurrency recognition before this book is over. It would go something like this:

Stage One: Disdain. Not even denial, but disdain. Here's this thing, it's supposed to be money, but it doesn't have any of the characteristics of money with which we're familiar. It's not tangible. It's not issued by a government or forged from precious metal.

Stage Two: Skepticism. You read the paper every day, and enough stories have appeared to convince you that bitcoin is real, that some entrepreneurs, including the Winklevoss twins of Facebook fame, expect to make a lot of money from it. But the details don't add up. You get it by doing math problems? No? By having your computer do math problems? How can that possibly work? At this stage, phrases like *Ponzi scheme* and *tulip mania* enter your mind.

Stage Three: Curiosity. You've kept reading. It becomes clear that many people, even some seemingly sensible people such as Internet pioneer Marc Andreessen, people with a track record for being right about this stuff, are genuinely excited by it. But why all the fuss? Okay, it's digital money, it may work, but what difference is that going to make to regular people? And why are people so heated up about it?

Stage Four: Crystallization. This is the critical one. Choose whatever metaphor you like—call it the jaw-drop moment, the lightbulb moment, the mind-now-officially-blown moment—it is a point of realization that hits just about everybody who spends any time around digital currencies, even if they remain skeptical about the hurdles to their acceptance. Some people we spoke with talked about being unable to sleep for days, scouring every word they could find on bitcoin. In one fell, digitized swoop, an entire new way of doing things crystallizes in your mind.

Stage Five: Acceptance. It's not an easy thing to get your head around, but big ideas never are. The bottom line is

that even if bitcoin doesn't keep growing, even if none of the other "altcoin" cryptocurrencies catch on—and several hundred of these bitcoinlike cryptocurrencies with their own features and quirks exist—we've seen a way of doing business that is faster and cheaper, that cuts out the middleman and the rentier, brings in millions of "unbanked" people, and gives everyone a measure of control over his or her finances and businesses that has not existed before. Once you see this, there is no way to unsee it.

For sure, reasons exist to doubt the success of this grand experiment. Bitcoin tends to attract headlines about scandals and security breaches, and while these are not yet as big as those occurring within the dominant, bank-centric system of finance and credit-card payments, they create an image problem. Imagine the PR blow if reports emerge that bitcoin has been used to finance a major terrorist attack. Public anxiety over such risks could prompt an excessive response from regulators, strangling the project in its infancy. This legal reaction could be especially restrictive if officials sense that bitcoin is starting to impinge on governments' capacity to control their monetary and payments system—which is the stated goal of many of its more impassioned, libertarian-minded supporters. The first serious regulatory efforts are now under way as officials in Washington, New York, London, Brussels, Beijing, and various other financial and political capitals formulate rules for users of digital currencies to follow. If well designed, these could bolster cryptocurrencies by making people feel better protected from their more dangerous elements. But the bureaucrats may go too far and quash innovative start-ups' ability to make full use of this technology's potential to empower individuals, break down monopolies, and reduce cost, waste, and corruption in our financial system.

Meanwhile, other emerging technologies could evolve to provide better competition. For example, in China, people currently have few incentives to use it in payments because ubiquitous new mobile smartphone-based applications already allow them to make renminbi-denominated payments without the risk of bitcoin's volatility. The legacy systems that are coming under attack will surely work to improve the services they offer, lower their costs, and support regulation designed to dull bitcoin's competitive advantage.

The biggest wild card in all of this is people. Cryptocurrency's rapid development is in some ways a quirk of history: launched in the throes of the 2008 financial crisis, bitcoin offered an alternative to a system—the existing financial system—that was blowing itself up and threatening to take a few billion people down with it. Within a few years, an entire counterculture movement formed around cryptocurrencies, and it has continued to revolve around them. Without that crisis painfully exposing the flaws of the world's financial system, it's hard to say where bitcoin would be today. As that crisis recedes, will the impetus to adopt a digital currency recede with it?

No one can claim to know how all of this will shake out. So, while we won't be making predictions, we will speculate on the prospects for cryptocurrency, examining *what might be* while recognizing and detailing reasons why it might *not* be.

You may be skeptical. That's fine; we were, too. We both started covering the markets in the 1990s. We saw the dot-com boom, and the dot-com bust. We saw the housing boom, and the housing bust. We saw the financial crisis, and the global recession, and the euro crisis, and Lehman Brothers, and Long-Term Capital Management, and Cyprus. We interviewed any number of true believers from the tech

world who thought they had the next big thing. You go through enough of that, and you're instinctively skeptical.

So we were both doubters when we first heard of bitcoin. Money that isn't backed by a government? That's crazy! (In our experience, that is the single biggest sticking point for most doubters; they simply can't get past it.) But our curiosity got the better of us. We started writing about it, and talking to people about it, and writing some more. Eventually, the enormity of bitcoin's potential became apparent to us, and in some ways this book mirrors our own trip through the world of cryptocurrencies. It's an extension of our curiosity.

We are telling the story of bitcoin, but the thing we're really trying to do is to figure out exactly where cryptocurrencies fit into the world, to put this big puzzle together. It's a big story, one that spans the globe, from the high-tech hub of Silicon Valley to the streets of Beijing. It includes visits to the mountains of Utah, the beaches of Barbados, schools in Afghanistan, and start-ups in Kenya. The world of cryptocurrencies comprises venture-capital royalty, high school dropouts, businessmen, utopians, anarchists, students, humanitarians, hackers, and Papa John's pizza. It's got parallels with the financial crisis, and the new sharing economy, and the California gold rush, and before it's all over, we may have to endure an epic battle between a new high-tech world and the old low-tech world that could throw millions out of work, while creating an entirely new breed of millionaires.

Are you ready to jump down the bitcoin rabbit hole?

^{fn1} In some cases, bitcoin will refer to both the currency and the technology. But for convenience and consistency with the style at *The Wall Street Journal*, we stick with lowercase in all references. To a large extent, context will clarify the distinction being made.

One

FROM BABYLON TO BITCOIN

The eye has never seen, nor the hand touched a dollar.

—*Alfred Mitchell Innes*

For any currency to be viable, be it a decentralized cryptocurrency issued by a computer program or a traditional “fiat” currency issued by a government, it must win the *trust* of the community using it. For cryptocurrency advocates, as we’ll learn in the chapters ahead, the whole point is to offer an alternative model for that trust. They tout a system of payments in which the payee no longer has to trust “third-party” institutions such as banks or governments to assure that the payer can deliver the agreed-upon funds. Instead, cryptocurrency systems imbue trust in an inviolable, decentralized computer program that is, in theory, incapable of defrauding people. None of this, however, gets cryptocurrencies off the hook. They, too, must win people’s trust if they are to become relevant.

Trust is at the core of any system of money. For it to work, people must feel confident that a currency will be held in the right esteem by others. So before we get into bitcoin’s dramatic arrival on the scene and its bid to change the way we think about such things, we need to explore that notion of trust in more depth as it has evolved through history. This chapter will take us on a journey through the evolution of money, one of society’s most remarkable yet poorly understood inventions.

Let’s start with some basic questions. What is money? What does it represent? How did society come to develop such a system for exchanging goods and measuring their

value? As is the case in any field of study, figuring out how something functions is often best approached by examining cases where the system hasn't worked.

One contemporary example of failure is in Zimbabwe, whose defunct multibillion-denominated notes now sit on the desks of financial reporters and currency traders as reminders of how unhinged things can become with money. But the strongest lesson Western societies have learned comes from farther back: the 1920s Weimar Republic. The German government then, unwilling to court military conflict with its European neighbors but also reluctant to upset the public by raising taxes, instead printed money to cover its debts and sent the German mark into an uncontrollable downward spiral. As inflation soared beyond anything anyone could imagine, children would arrange stacks of worthless 50-million-mark notes into playhouses. The greatest caution from all this comes from the knowledge that this monetary and governmental chaos opened a door to Adolf Hitler.

Germany was eventually converted into a functioning, generally peace-loving nation, showing that it's possible for democratic societies to restore order after a bout of financial and political chaos. The same goes for Brazil, which, through tough monetary-policy reforms, put the 30,000-plus percent inflation rates and the dictatorship of the 1980s behind it. But some places live with monetary dysfunction almost permanently, and for this they pay a formidable price. We learn from their experience that the core problem is not irresponsible policy decisions by money-printing central banks, though this is the mechanism through which hyperinflation is created. Rather, the problem stems from a deep-seated breakdown of trust between the people who use a currency and the monetary authority that issues it. Since those monetary authorities are ordinarily national governments, this breakdown reflects a society's flawed relationship with its

government. It's an instructive way to think about what a cryptocurrency, with its "trustless," math-based system of monetary exchange, offers as an alternative.

If citizens don't trust a government to represent their interests, they won't trust its currency—or better put, they won't trust the monetary system around which their economy is organized. So when given a chance, they will sell that currency and flee it for something they regard as more trustworthy, whether it's the U.S. dollar, gold, or some other safe haven. When this dysfunction is entrenched, such beliefs are self-fulfilling. The loss of value in its currency depletes the government's financial resources, which leaves money-printing as the only means to pay its debts and ensure political survival. Pretty soon, the excess money in circulation further undermines trust, which can give way to a vicious cycle of spiraling inflation and plummeting exchange rates.

Argentina has lived with this broken relationship for a long time. A century of failure to resolve the trust problem explains why Argentina has been through many, many currency crises and why it has fallen from the world's seventh-richest country at start of the twentieth century to rank around eightieth in mid-2014.^{[fn1](#)} That puts Argentina, which for many years portrayed itself as a beacon of European sophistication in a continent of New World backwardness, more or less on par with Peru.

Mike knows a thing or two about Argentina. He picks up the story from here:

My family and I spent six and a half happy years in Buenos Aires. Sunshine, steak, Malbec wine, all rounded out the experience. The best part was the friends we made, people who would give you bear hugs, who would always go out of their way to help you, and who thought nothing of taking a four-hour lunch to engage in intense conversation about the state of the world.

But mine was a love-hate relationship with their country. For all of Argentines' passionate embrace of friends and family, their society is in permanent war with itself. This is manifest in the dog feces littering Buenos Aires' sidewalks, the graffiti defacing the city's once-beautiful Parisian architecture, and the interminable traffic jams caused by drivers' unwillingness to yield. The country's bitterly divided politicians espouse competing, outdated ideologies, but in truth their loyalty lies with a unifying, corrupt political machine installed by Juan Domingo Perón half a century ago. Peronism's system of Machiavellian power has trapped Argentine politics in a vicious cycle of shortsightedness and corruption, a failure that has left Argentines with zero faith in their governments. Skipping taxes is the norm—why, people reason, would you pay crooks who will steal your money? In this environment, self-interest constantly asserts itself, and the country's deep pool of natural resources is squandered. Bucketloads of money will be made in short multiyear bursts by those savvy enough to ride the pump-and-dump schemes that masquerade as policies, but that only means the economy rushes toward an oncoming cliff every ten years or so.

I arrived in Argentina in early 2003, right when the last such crisis was barely subsiding. Banks, which were still keeping people's savings frozen in accounts that the government had forcibly converted from dollars to devalued pesos, had enclosed their downtown branches in steel plates to protect their windows from the barrages of bricks hurled by protesting depositors. When I left, in 2009, the next crisis was brewing. Inflation was pushing toward 30 percent a year, but the government was openly lying about it, an act of bad faith that only made Argentines mistrust their currency further and led businesses to hike prices preemptively in a self-reinforcing cycle. People were slowly withdrawing pesos from banks again, and the government was putting restrictions on purchases of

foreign currencies, which, predictably, further undermined confidence in the national currency. This cat-and-mouse game, as Argentines knew too well, was destined to end badly.

It also complicated our departure. A year after we left, we finally sold the lovely apartment we'd bought in the leafy Buenos Aires suburb of Palermo. But when I returned to the city to close the deal, it was now difficult to get our money out of the country.

Residential property in Argentina has historically been sold in dollars—literally, physical greenbacks. History has made Argentines wary not only of their own currency but also untrusting of checks, money orders, and anything else that requires the provision of credit. Cold, hard dollar notes can cut through all that. That's what our buyers wanted. Reluctant to wire money to our U.S. bank account, they wanted to do things in that old, traditional way. They suggested we complete the deal at a *casa de cambio* in Buenos Aires' financial district, one of numerous exchange houses that help Argentines manage their complicated financial affairs. The *casa* would take our newly obtained cash and credit our U.S. bank account. Easy. What could possibly go wrong?

With shiny lobbies, Victorian-style insignia, and names conveying integrity and security, these exchange houses can look similar to bank branches, but they operate outside the banking system. In addition to swapping dollars for pesos, they manage a network of accounts to shift money overseas at lower costs than bank wires. Now that the government was placing strict constraints on offshore bank wires, these places were in demand as convenient, extra-official money transmitters.

I was uncomfortable with this seemingly shady option, but Miguel, my closest friend in Buenos Aires, told me that this *casa de cambio* handled his business weekly in fully legal transactions with his associates overseas. He trusted

them fully and I trusted him. This was the way things worked in Argentina: you trusted whom you knew, and to resolve your business affairs you frequently leaned on those relationships more than you relied on the legal protection of a corrupt judicial system.

To be certain, however, I had an initial meeting with the *casa de cambio*, in which I was assured that the overseas transfer would be fully verifiable and legal since we would have the real estate contract as backing documentation. Satisfied, I agreed to the buyers' plan. Days later, eight people gathered in one of the firm's sealed rooms to complete the closing: two staff members; the couple buying our apartment; one of their fathers, who was paying for it; an official *escribano*, or notary public, required by law to authenticate the settlement; Miguel; and I.

A man entered carrying ten or so stacks of bills and gave them to me. I'd never had my hands on so much cash, but was still struck by how small \$280,000 packed down to. It was counted by staff from the *casa de cambio*, after which the signing of the transfer papers began. Once the *escribano* had ascertained that all was aboveboard and fair, he and the father bid their farewell, and arrangement of the international transfer began.

Suddenly, a staff member rushed in, hurriedly yelling, "You can't do it! This has to go through the banking system!" I looked at Miguel and it sank in. The staff had misunderstood a key documentation requirement under the ever-changing Argentine foreign-exchange laws. Or perhaps—the conspiratorial Argentine in me was now kicking in—we'd been set up. Why did this happen after the *escribano* had left and signed over the property? Either way, we were stuck.

These were my options: I could gather up the money, our life savings, and take them across town—in what? A backpack? In my socks?—and hope the local bank branch at which I'd maintained a mostly inactive account to pay my

electricity bills would happily accept a massive stack of dollars, convert them into pesos for a fee and at a confiscatory exchange rate, and then immediately convert them back into dollars for another fee and at another expensive exchange rate before wiring the money to my bank for a bigger fee. We were facing security risks and some \$15,000 more in costs, assuming the plan would fly with the bank's compliance officers. Or, the *casa de cambio* offered, I could complete the deal with them but without the documentation I'd been promised. The institution would take my money, and an agent overseas would deposit the equivalent amount in our account—but I would receive no paper record of ever having handed over any money. I would have to trust—*that word again*—that twenty-four hours later I could call my bank and ascertain that the money was en route to my account, although it would take three days before the credit actually registered.

I thought hard about it. Tens of thousands of Argentines did such transactions every day. To them, it was, ironically, a more trustworthy method of exchanging value than dealing with a banking system that had repeatedly robbed them of their savings. More important, Miguel, the man I trusted more than anyone else in Argentina, trusted this group of people to look after his accounts. He did so in a more transparent, aboveboard way than I was contemplating, but he dealt with them regularly. Indeed, the *casa de cambio* needed to maintain Miguel's trust. The confidence of their customers was the foundation of their business. On the other hand, I was unlikely to be a repeat customer.

I reluctantly agreed to the unofficial transaction. All the exchange house could give me as a "record" was a cutoff piece of ticker tape from a basic, receipt-printing calculator that simply showed numbers in text: the total amount transferred, minus the fee, and nothing else. I misplaced it that very evening.