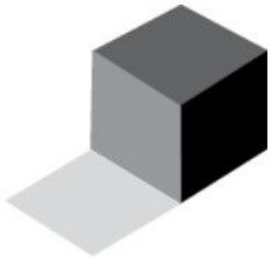
PART I



SAY YOU WANT A REVOLUTION

CHAPTER 1

THE TRUST PROTOCOL

It appears that once again, the technological genie has been unleashed from its bottle. Summoned by an unknown person or persons with unclear motives, at an uncertain time in history, the genie is now at our service for another kick at the can—to transform the economic power grid and the old order of human affairs for the better. If we will it.

Let us explain.

The first four decades of the Internet brought us e-mail, the World Wide Web, dot-coms, social media, the mobile Web, big data, cloud computing, and the early days of the Internet of Things. It has been great for reducing the costs of searching, collaborating, and exchanging information. It has lowered the barriers to entry for new media and entertainment, new forms of retailing and organizing work, and unprecedented digital ventures. Through sensor technology, it has infused intelligence into our wallets, our clothing, our automobiles, our buildings, our cities, and even our biology. It is saturating our environment so completely that soon we will no longer "log on" but rather

go about our business and our lives immersed in pervasive technology.

Overall, the Internet has enabled many positive changes—for those with access to it—but it has serious limitations for business and economic activity. *The New Yorker* could rerun Peter Steiner's 1993 cartoon of one dog talking to another without revision: "On the Internet, nobody knows you're a dog." Online, we still can't reliably establish one another's identities or trust one another to transact and exchange money without validation from a third party like a bank or a government. These same intermediaries collect our data and invade our privacy for commercial gain and national security. Even with the Internet, their cost structure excludes some 2.5 billion people from the global financial system. Despite the promise of a peer-to-peer empowered world, the economic and political benefits have proven to be asymmetrical—with power and prosperity channeled to those who already have it, even if they're no longer earning it. Money is making more money than many people do.

Technology doesn't create prosperity any more than it destroys privacy. However, in this digital age, technology is at the heart of just about everything—good and bad. It enables humans to value and to violate one another's rights in profound new ways. The explosion in online communication and commerce is creating more opportunities for cybercrime. Moore's law of the annual doubling of processing power doubles the power of fraudsters and thieves—"Moore's Outlaws"[1]—not to mention spammers, identity thieves, phishers, spies, zombie farmers, hackers, cyberbullies, and datanappers—criminals who unleash ransomware to hold data hostage—the list goes on.

IN SEARCH OF THE TRUST PROTOCOL

As early as 1981, inventors were attempting to solve the Internet's problems of privacy, security, and inclusion with cryptography. No matter how they reengineered the process, there were always leaks because third parties were involved. Paying with credit cards over the Internet was insecure because users had to divulge too much personal data, and the transaction fees were too high for small payments.

In 1993, a brilliant mathematician named David Chaum came up with eCash, a digital payment system that was "a technically perfect product which made it possible to safely and anonymously pay over the Internet. . . . It was perfectly suited to sending electronic pennies, nickels, and dimes over the Internet."[2] It was so perfect that Microsoft and others were interested in including eCash as a feature in their software.[3] The trouble was, online shoppers didn't care about privacy and security online then. Chaum's Dutch company DigiCash went bankrupt in 1998.

Around that time, one of Chaum's associates, Nick Szabo, wrote a short paper entitled "The God Protocol," a twist on Nobel laureate Leon Lederman's phrase "the God particle," referring to the importance of the Higgs boson to modern physics. In his paper, Szabo mused about the creation of a be-all end-all technology protocol, one that designated God the trusted third party in the middle of all transactions: "All the parties would send their inputs to God. God would reliably determine the results and return the outputs. God being the ultimate in confessional discretion, no party would learn anything more about the other parties' inputs than they could learn from their own inputs and the output."[4] His point was powerful: Doing business on the Internet requires a leap of faith. Because the infrastructure lacks the much-needed security, we often have little choice but to treat the middlemen as if they were deities.

A decade later in 2008, the global financial industry crashed. Perhaps propitiously, a pseudonymous person or persons named Satoshi Nakamoto outlined a new protocol for a peer-to-peer electronic cash system using a cryptocurrency called bitcoin. Cryptocurrencies (digital currencies) are

different from traditional fiat currencies because they are not created or controlled by countries. This protocol established a set of rules—in the form of distributed computations—that ensured the *integrity* of the data exchanged among these billions of devices *without going through a trusted third party*. This seemingly subtle act set off a spark that has excited, terrified, or otherwise captured the imagination of the computing world and has spread like wildfire to businesses, governments, privacy advocates, social development activists, media theorists, and journalists, to name a few, everywhere.

"They're like, 'Oh my god, this is it. This is the big breakthrough. This is the thing we've been waiting for,'" said Marc Andreessen, the cocreator of the first commercial Web browser, Netscape, and a big investor in technology ventures. "'He solved all the problems. Whoever he is should get the Nobel Prize—he's a genius.' This is the thing! This is the distributed trust network that the Internet always needed and never had."[5]

Today thoughtful people everywhere are trying to understand the implications of a protocol that enables mere mortals to manufacture trust through clever code. This has never happened before—trusted transactions directly between two or more parties, authenticated by mass collaboration and powered by collective self-interests, rather than by large corporations motivated by profit.

It may not be the Almighty, but a trustworthy global platform for our transactions is something very big. We're calling it the Trust Protocol.

This protocol is the foundation of a growing number of global distributed ledgers called blockchains—of which the bitcoin blockchain is the largest. While the technology is complicated and the word *blockchain* isn't exactly sonorous, the main idea is simple. Blockchains enable us to send money directly and safely from me to you, without going through a bank, a credit card company, or PayPal.

Rather than the Internet of Information, it's the Internet of Value or of Money. It's also a platform for everyone to know what is true—at least with regard to structured recorded information. At its most basic, it is an open source code: anyone can download it for free, run it, and use it to develop new tools for managing transactions online. As such, it holds the potential for unleashing countless new applications and as yet unrealized capabilities that have the potential to transform many things.

HOW THIS WORLDWIDE LEDGER WORKS

Big banks and some governments are implementing blockchains as distributed ledgers to revolutionize the way information is stored and transactions occur. Their goals are laudable—speed, lower cost, security, fewer errors, and the elimination of central points of attack and failure. These models don't necessarily involve a cryptocurrency for payments.

However, the most important and far-reaching blockchains are based on Satoshi's bitcoin model. Here's how they work.

Bitcoin or other digital currency isn't saved in a file somewhere; it's represented by transactions recorded in a blockchain—kind of like a global spreadsheet or ledger, which leverages the resources of a large peer-to-peer bitcoin network to verify and approve each bitcoin transaction. Each blockchain, like the one that uses bitcoin, is *distributed*: it runs on computers provided by volunteers around the world; there is no central database to hack. The blockchain is *public*: anyone can view it at any time because it resides on the network, not within a single institution charged with auditing transactions and keeping records. And the blockchain is *encrypted*: it uses heavy-duty

encryption involving public and private keys (rather like the two-key system to access a safety deposit box) to maintain virtual security. You needn't worry about the weak firewalls of Target or Home Depot or a thieving staffer of Morgan Stanley or the U.S. federal government.

Every ten minutes, like the heartbeat of the bitcoin network, all the transactions conducted are verified, cleared, and stored in a block which is linked to the preceding block, thereby creating a chain. Each block must refer to the preceding block to be valid. This structure permanently time-stamps and stores exchanges of value, preventing anyone from altering the ledger. If you wanted to steal a bitcoin, you'd have to rewrite the coin's entire history on the blockchain in broad daylight. That's practically impossible. So the blockchain is a distributed ledger representing a network consensus of every transaction that has ever occurred. Like the World Wide Web of information, it's the World Wide Ledger of value—a distributed ledger that everyone can download and run on their personal computer.

Some scholars have argued that the invention of double-entry bookkeeping enabled the rise of capitalism and the nation-state. This new digital ledger of economic transactions can be programmed to record virtually everything of value and importance to humankind: birth and death certificates, marriage licenses, deeds and titles of ownership, educational degrees, financial accounts, medical procedures, insurance claims, votes, provenance of food, and anything else that can be expressed in code.

The new platform enables a reconciliation of digital records regarding just about everything in real time. In fact, soon billions of smart things in the physical world will be sensing, responding, communicating, buying their own electricity and sharing important data, doing everything from protecting our environment to managing our health. This Internet of Everything needs a Ledger of Everything. Business, commerce, and the economy need a Digital Reckoning.

So why should you care? We believe the truth *can* set us free and distributed trust will profoundly affect people in all walks of life. Maybe you're a music lover who wants artists to make a living off their art. Or a consumer who wants to know where that hamburger meat really came from. Perhaps you're an immigrant who's sick of paying big fees to send money home to loved ones in your ancestral land. Or a Saudi woman who wants to publish her own fashion magazine. Maybe you're an aid worker who needs to identify land titles of landowners so you can rebuild their homes after an earthquake. Or a citizen fed up with the lack of transparency and accountability of political leaders. Or a user of social media who values your privacy and thinks all the data you generate might be worth something—to you. Even as we write, innovators are building blockchain-based applications that serve these ends. And they are just the beginning.

A RATIONAL EXUBERANCE FOR THE BLOCKCHAIN

For sure, blockchain technology has profound implications for many institutions. Which helps explain all the excitement from many smart and influential people. Ben Lawsky quit his job as the superintendent of financial services for New York State to build an advisory company in this space. He told us, "In five to ten years, the financial system may be unrecognizable . . . and I want to be part of the change."[6] Blythe Masters, formerly chief financial officer and head of Global Commodities at JP Morgan's investment bank, launched a blockchain-focused technology start-up to transform the industry. The cover of the October 2015 *Bloomberg Markets* featured Masters with the headline "It's All About the Blockchain." Likewise, *The Economist* ran an

October 2015 cover story, "The Trust Machine," which argued that "the technology behind bitcoin could change how the economy works."[7] To *The Economist*, blockchain technology is "the great chain of being sure about things." Banks everywhere are scrambling top-level teams to investigate opportunities, some of these with dozens of crackerjack technologists. Bankers love the idea of secure, frictionless, and instant transactions, but some flinch at the idea of openness, decentralization, and new forms of currency. The financial services industry has already rebranded and privatized blockchain technology, referring to it as *distributed ledger technology,* in an attempt to reconcile the best of bitcoin—security, speed, and cost—with an entirely closed system that requires a bank or financial institution's permission to use. To them, blockchains are more reliable databases than what they already have, databases that enable key stakeholders—buyers, sellers, custodians, and regulators—to keep shared, indelible records, thereby reducing cost, mitigating settlement risk, and eliminating central points of failure.

Investing in blockchain start-ups is taking off, as did investing in dot-coms in the 1990s. Venture capitalists are showing enthusiasm at a level that would make a 1990s dot-com investor blush. In 2014 and 2015 alone, more than $1 billion of venture capital flooded into the emerging blockchain ecosystem, and the rate of investment is almost doubling annually.[8] "We're quite confident," said Marc Andreessen in an interview with *The Washington Post,* "that when we're sitting here in 20 years, we'll be talking about [blockchain technology] the way we talk about the Internet today."[9]

Regulators have also snapped to attention, establishing task forces to explore what kind of legislation, if any, makes sense. Authoritarian governments like Russia's have banned or severely limited the use of bitcoin, as have democratic states that should know better, like Argentina, given its history of currency crises. More thoughtful governments in the West are investing considerably in understanding how the new technology could transform not only central banking and the nature of money, but also government operations and the nature of democracy. Carolyn Wilkins, the senior deputy governor of the Bank of Canada, believes it's time for central banks everywhere to seriously study the implications of moving entire national currency systems to digital money. The Bank of England's top economist, Andrew Haldane, has proposed a national digital currency for the United Kingdom.[10]

These are heady times. To be sure, the growing throng of enthusiasts has its share of opportunists, speculators, and criminals. The first tale most people hear about digital currencies is the bankruptcy of the Mt. Gox exchange or the conviction of Ross William Ulbricht, founder of the Silk Road darknet market seized by the Federal Bureau of Investigation for trafficking illegal drugs, child pornography, and weapons using the bitcoin blockchain as a payment system. Bitcoin's price has fluctuated drastically, and the ownership of bitcoins is still concentrated. A 2013 study showed that 937 people owned half of all bitcoin, although that is changing today.[11]

How do we get from porn and Ponzi schemes to prosperity? To begin, it's not bitcoin, the still speculative asset, that should interest you, unless you're a trader. This book is about something bigger than the asset. It's about the power and potential of the underlying technological platform.

This is not to say that bitcoin or cryptocurrencies per se are unimportant, as some people have suggested as they scramble to disassociate their projects from the scandalous ventures of the past. These currencies are critical to the blockchain revolution, which is first and foremost about the peer-to-peer exchange of value, especially money.

ACHIEVING TRUST IN THE

DIGITAL AGE

Trust in business is the expectation that the other party will behave according to the four principles of integrity: honesty, consideration, accountability, and transparency.[12]

Honesty is not just an ethical issue; it has become an economic one. To establish trusting relationships with employees, partners, customers, shareholders, and the public, organizations must be truthful, accurate, and complete in communications. No lying through omission, no obfuscation through complexity.

Consideration in business often means a fair exchange of benefits or detriments that parties will operate in good faith. But trust requires a genuine respect for the interests, desires, or feelings of others, and that parties can operate with goodwill toward one another.

Accountability means making clear commitments to stakeholders and abiding by them. Individuals and institutions alike must demonstrate that they have honored their commitments and owned their broken promises, preferably with the verification of the stakeholders themselves or independent outside experts. No passing the buck, no playing the blame game.

Transparency means operating out in the open, in the light of day. "What are they hiding?" is a sign of poor transparency that leads to distrust. Of course, companies have legitimate rights to trade secrets and other kinds of proprietary information. But when it comes to pertinent information for customers, shareholders, employees, and other stakeholders, active openness is central to earning trust. Rather than dressing for success, corporations can undress for success.

Trust in business and other institutions is mostly at an all-time low. The public relations company Edelman's 2015 "Trust Barometer" indicates that trust in institutions, especially corporations, has fallen back to levels from the dismally low period of the 2008 great recession. Edelman noted that even the once impregnable technology industry, still the most trusted business sector, saw declines in the majority of countries for the first time. Globally, CEOs and government officials continue to be the least credible information sources, lagging far behind academic or industry experts.[13] Similarly, Gallup reported in its 2015 survey of American confidence in institutions that "business" ranked second lowest among the fifteen institutions measured; fewer than 20 percent of respondents indicated they had considerable or high levels of trust. Only the U.S. Congress had a lower score.[14]

In the preblockchain world, trust in transactions derived from individuals, intermediaries, or other organizations acting with integrity. Because we often can't know our counterparties, let alone whether they have integrity, we've come to rely on third parties not only to vouch for strangers, but also to maintain transaction records and perform the business logic and transaction logic that powers commerce online. These powerful intermediaries —banks, governments, PayPal, Visa, Uber, Apple, Google, and other digital conglomerates—harvest much of the value.

In the emerging blockchain world, trust derives from the network and even from objects on the network. Carlos Moreira of the cryptographic security company WISeKey said that the new technologies effectively delegate trust—even to physical things. "If an object, whether it be a sensor on a communications tower, a light bulb, or a heart monitor, is not trusted to perform well or pay for services it will be rejected by the other objects automatically."[15] The ledger itself is the foundation of trust.[16]

To be clear, "trust" refers to buying and selling goods and services and to the integrity and protection of information, not trust in all business affairs. However, you will read throughout this book how a global ledger of truthful information can help build integrity into all our institutions and create a more secure and trustworthy world. In our view, companies that conduct some or all of their transactions on the blockchain will enjoy a trust bump in share price.

Shareholders and citizens will come to expect all publicly traded firms and taxpayer-funded organizations to run their treasuries, at minimum, on the blockchain. Because of increased transparency, investors will be able to see whether a CEO really deserved that fat bonus. Smart contracts enabled by blockchains will require counterparties to abide by their commitments and voters will be able to see whether their representatives are being honest or acting with fiscal integrity.

RETURN OF THE INTERNET

The first era of the Internet started with the energy and spirit of a young Luke Skywalker—with the belief that any kid from a harsh desert planet could bring down an evil empire and start a new civilization by launching a dot-com. Naïve to be sure, but many people, present company included, hoped the Internet, as embodied in the World Wide Web, would disrupt the industrial world where power was gripped by the few and power structures were hard to climb and harder to topple. Unlike the old media that were centralized and controlled by powerful forces, and where the users were inert, the new media were distributed and neutral, and everyone was an active participant rather than a passive recipient. Low cost and massive peer-to-peer communication on the Internet would help undermine traditional hierarchies and help with the inclusion of developing world citizens in the global economy. Value and reputation would derive from quality of contribution, not status. If you were smart and hardworking in India, your merit would bring you reputation. The world would be flatter, more meritocratic, more flexible, and more fluid. Most important, technology would contribute to prosperity for everyone, not just wealth for the few.

Some of this has come to pass. There have been mass collaborations like Wikipedia, Linux, and Galaxy Zoo. Outsourcing and networked business models have enabled people in the developing world to participate in the global economy better. Today two billion people collaborate as peers socially. We all have access to information in unprecedented ways.

However, the Empire struck back. It has become clear that concentrated powers in business and government have bent the original democratic architecture of the Internet to their will.

Huge institutions now control and own this new means of production and social interaction—its underlying infrastructure; massive and growing treasure troves of data; the algorithms that increasingly govern business and daily life; the world of apps; and extraordinary emerging capabilities, machine learning, and autonomous vehicles. From Silicon Valley and Wall Street to Shanghai and Seoul, this new aristocracy uses its insider advantage to exploit the most extraordinary technology ever devised to empower people as economic actors, to build spectacular fortunes and strengthen its power and influence over economies and societies.

Many of the dark side concerns raised by early digital pioneers have pretty much materialized.[37] We have growth in gross domestic product but not commensurate job growth in most developed countries. We have growing wealth creation and growing social inequality. Powerful technology companies have shifted much activity from the open, distributed, egalitarian, and empowering Web to closed online walled gardens or proprietary, read-only applications that among other things kill the conversation. Corporate forces have captured many of these wonderful peer-to-peer, democratic, and open technologies and are using them to extract an inordinate share of value.

The upshot is that, if anything, economic power has gotten spikier, more concentrated, and more entrenched. Rather than data being more widely and democratically distributed, it is being hoarded and exploited by fewer entities that often use it to control more and acquire more power. If you accumulate

data and the power that comes with it, you can further fortify your position by producing proprietary knowledge. This privilege trumps merit, regardless of its origin.

Further, powerful "digital conglomerates" such as Amazon, Google, Apple, and Facebook—all Internet start-ups at one time—are capturing the treasure troves of data that citizens and institutions generate often in private data silos rather than on the Web. While they create great value for consumers, one upshot is that data is becoming a new asset class—one that may trump previous asset classes. Another is the undermining of our traditional concepts of privacy and the autonomy of the individual.

Governments of all kinds use the Internet to improve operations and services, but they now also deploy technology to monitor and even manipulate citizens. In many democratic countries, governments use information and communications technologies to spy on citizens, change public opinion, further their parochial interests, undermine rights and freedoms, and overall to stay in power. Repressive governments like those of China and Iran enclose the Internet, exploiting it to crack down on dissent and mobilize citizens around their objectives.

This is not to say that the Web is dead, as some have suggested. The Web is critical to the future of the digital world and all of us should support efforts under way to defend it, such as those of the World Wide Web Foundation, who are fighting to keep it open, neutral, and constantly evolving.

Now, with blockchain technology, a world of new possibilities has opened up to reverse all these trends. We now have a true peer-to-peer platform that enables the many exciting things we've discussed in this book. We can each own our identities and our personal data. We can do transactions, creating and exchanging value without powerful intermediaries acting as the arbiters of money and information. Billions of excluded people can soon enter the global economy. We can protect our privacy and monetize our own information. We can ensure that creators are compensated for their intellectual property. Rather than trying to solve the problem of growing social inequality through the redistribution of wealth only, we can start to change the way wealth is *distributed*—how it is created in the first place, as people everywhere from farmers to musicians can share more fully, a priori, in the wealth they create. The sky does seem to be the limit.

It's more Yoda than God. But this new protocol, if not divine, does enable trusted collaboration to occur in a world that needs it, and that's a lot. Excited, we are.

YOUR PERSONAL AVATAR AND THE BLACK BOX OF IDENTITY

Throughout history, each new form of media has enabled mankind to transcend time, space, and mortality. That—dare we say—divine ability inevitably raises anew the existential question of identity: Who are we? What does it mean to be human? How do we conceptualize ourselves? As Marshall McLuhan observed, the medium becomes the message over time. People shape and are shaped by media. Our brains adapt. Our institutions adapt. Society adapts.

"Today you need an organization with endowed rights to provide you with an identity, like a bank card, a frequent flyer card, or a credit card,"[18] said Carlos Moreira of WISeKey. Your parents gave you a name, the state-licensed obstetrician or midwife who delivered you took your footprint and vouched for your weight and length, and both parties attested to the time, date, and place of your arrival by signing your birth certificate. Now they can record this certificate on the blockchain and link birth announcements and a college fund

to it. Friends and family can contribute bitcoin to your higher education. There, your data flow begins.

In the early days of the Internet, Tom Peters wrote, "You are your projects."[19] He meant that our corporate affiliations and job titles no longer defined us. What is equally true now: "You are your data." Trouble is, Moreira said, "That identity is now yours, but the data that comes from its interaction in the world is owned by someone else."[20] That's how most corporations and institutions view you, by your data contrail across the Internet. They aggregate your data into a virtual representation of you, and they provide this "virtual you" with extraordinary new benefits beyond your parents' happiest dreams.[21] But convenience comes with a price: privacy. Those who say "privacy is dead—get over it" are wrong.[22] Privacy is the foundation of free societies.

"People have a very simplistic view of identity,"[23] said blockchain theorist Andreas Antonopoulos. We use the word *identity* to describe the self, the projection of that self to the world, and all these attributes that we associate with that self or one of its projections. These may come from nature, from the state, from private organizations. We may have one or more roles and a series of metrics attached to those roles, and the roles may change. Consider your last job. Did your role change organically because of changes in the work that needed to be done or because of revisions to your job description?

What if "the virtual you" was in fact owned by you—your personal avatar—and "lived" in the black box of your identity so that you could monetize your data stream and reveal only what you needed to, when asserting a particular right. Why does your driver's license contain more information than the fact that you have passed your driving test and demonstrated your ability to drive? Imagine a new era of the Internet where your personal avatar manages and protects the contents of your black box. This trusty software servant could release only the required detail or amount for each situation and at the same time whisk up your data crumbs as you navigate the digital world.

This may sound like the stuff of science fiction as portrayed in films like *The Matrix* or *Avatar*. But today blockchain technologies make it possible. Joe Lubin, CEO of Consensus Systems, refers to this concept as a "persistent digital ID and persona" on a blockchain. "I show a different aspect of myself to my college friends compared to when I am speaking at the Chicago Fed," he said. "In the online digital economy, I will represent my various aspects and interact in that world from the platform of different personas." Lubin expects to have a "canonical persona," the version of him that pays taxes, obtains loans, and gets insurance. "I will have perhaps a business persona and a family persona to separate the concerns that I choose to link to my canonical persona. I may have a gamer persona that I don't want linked to my business persona. I might even have a dark web persona that is never linkable to the others."[24]

Your black box may include information such as a government-issued ID, Social Security number, medical information, service accounts, financial accounts, diplomas, practice licenses, birth certificate, various other credentials, and information so personal you don't want to reveal it but do want to monetize its value, such as sexual preference or medical condition, for a poll or a research study. You could license these data for specific purposes to specific entities for specific periods of time. You could send a subset of your attributes to your eye doctor and a different subset to the hedge fund that you would like to invest in. Your avatar could answer yes-no questions without disclosing who you are: "Are you twenty-one years or older? Did you earn more than $100,000 in each of the last three years? Do you have a body mass index in the normal range?"[25]

In the physical world, your reputation is local—your local shopkeeper, your employer, your friends at a dinner party all have a certain opinion about you. In the digital economy, the reputations of various personas in your avatar will be portable. Portability will help bring people everywhere into the digital economy. People with a digital wallet and avatar in Africa could establish the

reputation required to, say, borrow money to start a business. "See, all these people know me and have vouched for me. I am financially trustworthy. I am an enfranchised citizen of the global digital economy."

Identity is only a small part of it. The rest is a cloud—an identity cloud—of particulates loosely or tightly linked to your identity. If we try to record all these into the blockchain, an immutable ledger, we lose not only the nuance of social interaction but also the gift of forgetting. People ought never be defined by their worst day.

A PLAN FOR PROSPERITY

In this book, you'll read dozens of stories about initiatives enabled by this trust protocol that create new opportunities for a more prosperous world. Prosperity first and foremost is about one's standard of living. To achieve it, people must have the means, tools, and opportunities to create material wealth and thrive economically. But for us it includes more—security of the person, safety, health, education, environmental sustainability, opportunities to shape and control one's destiny and to participate in an economy and society. In order to achieve prosperity, an individual must possess, at minimum, access to some form of basic financial services to reliably store and move value, communication, and transactional tools to connect to the global economy, and security, protection, and enforcement of the title to land and other assets they possess legally.[26] This and more is the promise of the blockchain. The stories you will read should give you a sense of a future where there is prosperity for everyone, not just more wealth and power for the wealthy and powerful. Perhaps even a world where we own our data and can protect our privacy and personal security. An open world where everyone can contribute to our technology infrastructure, rather than a world of walled gardens where big companies offer proprietary apps. A world where billions of excluded people can now participate in the global economy and share in its largesse. Here's a preview.

Creating a True Peer-to-Peer Sharing Economy

Pundits often refer to Airbnb, Uber, Lyft, TaskRabbit, and others as platforms for the "sharing economy." It's a nice notion—that peers create and share in value. But these businesses have little to do with sharing. In fact, they are successful precisely because they do not share—they aggregate. It is an aggregating economy. Uber is a $65 billion corporation that aggregates driving services. Airbnb, the $25 billion Silicon Valley darling, aggregates vacant rooms. Others aggregate equipment and handymen through their centralized, proprietary platforms and then resell them. In the process, they collect data for commercial exploitation. None of these companies existed a decade ago because the technological preconditions were not there: ubiquitous smart phones, full GPS, and sophisticated payment systems. Now with blockchains, the technology exists to reinvent these industries again. Today's big disrupters are about to get disrupted.

Imagine instead of the centralized company Airbnb, a distributed application—call it blockchain Airbnb or bAirbnb—essentially a cooperative owned by its members. When a renter wants to find a listing, the bAirbnb software scans the blockchain for all the listings and filters and displays those that meet her criteria. Because the network creates a record of the transaction on the blockchain, a positive user review improves their respective reputations and establishes their identities—now without an intermediary. Says Vitalik Buterin, founder of the Ethereum blockchain: "Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains

automate away the center. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly."[27]

Rewiring the Financial System for Speed and Inclusion

The financial services industry makes our global economy hum, but the system today is fraught with problems. For one, it is arguably the most centralized industry in the world and the last industry to feel the transformational effect of the technological revolution. Bastions of the old financial order such as banks go to great lengths to defend monopolies and often stymie disruptive innovation. The financial system also runs on outmoded technology and is governed by regulations dating back to the nineteenth century. It is rife with contradictions and uneven developments, making it sometimes slow, oftentimes insecure, and largely opaque to many stakeholders.

Distributed ledger technology can liberate many financial services from the confines of old institutions, fostering competition and innovation. That's good for the end user. Even when connected to the old Internet, billions of people are excluded from the economy for the simple reason that financial institutions don't provide services like banking to them because they would be unprofitable and risky customers. With the blockchain these people can not only become connected, but more important become included in financial activity, able to purchase, borrow, sell, and otherwise have a chance at building a prosperous life.

Similarly incumbent institutions can transform themselves around blockchain technology, if they can find the leadership to do it. The technology holds great promise to revolutionize the industry for the good—from banks to stock exchanges, insurance companies to accounting firms, brokerages, microlenders, credit card networks, real estate agents, and everything in between. When everyone shares the same distributed ledger, settlements don't take days, they occur instantly for all to see. Billions will benefit, and this shift could liberate and empower entrepreneurs everywhere.

Protecting Economic Rights Globally

Property rights are so inexorably tied to our system of capitalist democracy that Jefferson's first draft of the Declaration of Independence listed the inalienable rights of man as life, liberty, and the pursuit of *property*, not happiness.[28] While those aspirational tenets laid the groundwork for the modern economy and society we enjoy in much of the developed world, to this day much of the world's population does not reap their benefits. Even though some progress has been made in the departments of life and liberty, a majority of the world's property holders can have their homes or their bit of land seized arbitrarily by corrupt government functionaries, with the flick of a software switch in their centralized government property database. Without proof of property ownership, landowners can't secure a loan, get a building permit, or sell the property and they can be expropriated—all serious impediments to prosperity.

Peruvian economist and president of the Institute for Liberty and Democracy Hernando de Soto, one of the world's foremost economic minds, suggests that as many as five billion people in the world are barred from participating fully in the value created through globalization because they have a tenuous right to their land. Blockchain, he argues, could change all that. "The central idea to blockchain is that the rights to goods can be transacted, whether they be financial, hard assets or ideas. The goal is not merely to record the plot of land but rather to record the rights involved so that the rights holder cannot be violated."[29] Universal property rights could lay the

groundwork for a new agenda of global justice, economic growth, prosperity, and peace. In this new paradigm, rights are protected, not by guns or militias or minutemen, but by technology. "Blockchain is for a world that's governed by real things instead of fictitious things. And I think that's good,"[32] said de Soto. And it's decentralized. No central authority controls it, everybody knows what's happening, and it remembers forever.

Ending the Remittance Rip-off

Just about every report, article, or book reviewing the benefits of cryptocurrencies discusses the opportunity of remittances. And for good reason. The largest flow of funds into the developing world is not foreign aid or direct foreign investment. Rather, it is remittance money repatriated to poor countries from their diasporas living abroad. The process takes time, patience, and sometimes courage to travel each week to the same wire transfer office's seedy neighborhood, fill out the same paperwork each time, and pay the same 7 percent fee. There is a better way.

Abra and other companies are building payment networks using the blockchain. Abra's goal is to turn every one of its users into a teller. The whole process—from the funds leaving one country to their arriving in another—takes an hour rather than a week and costs 2 percent versus 7 percent or higher. Abra wants its payment network to outnumber all physical ATMs in the world. It took Western Union 150 years to get to 500,000 agents worldwide. Abra will have that many tellers in its first year.

Cutting Out Bureaucracy and Corruption in Foreign Aid

Could blockchain solve problems with foreign aid? The 2010 Haiti earthquake was one of the deadliest natural disasters in recorded history. Somewhere between 100,000 and 300,000 people perished. The government in Haiti proved itself a liability in the aftermath. The global community donated more than $500 million to the Red Cross, a known brand. An after-action investigation revealed that funds were misspent or went missing altogether.

The blockchain can improve the delivery of foreign aid by eliminating the middlemen who take the aid before it reaches its destination. Second, as an immutable ledger of the flow of funds, blockchain holds institutions more accountable for their actions. Imagine if you could track each dollar you gave to the Red Cross from its starting point on your smart phone to the person it benefited. You could park your funds in escrow, releasing amounts after the Red Cross reached each milestone.

Feeding the Creators of Value First

Under the first generation of the Internet, many creators of intellectual property did not receive proper compensation for it. Exhibit A was musicians and composers who had signed with record labels whose leaders failed to imagine how the Internet would affect their industry. They failed to embrace the digital age and reinvent their own business models, slowly ceding control to innovative online distributors.

Consider the major labels' reaction to Napster, the peer-to-peer music file-sharing platform launched in 1999. Incumbents in the music industry teamed up to sue the new venture, its founders, *and eighteen thousand of its users*, dismantling the platform by July 2001. Alex Winter, director of a documentary on Napster, told *The Guardian*, "I have a problem with black-and-white thinking when it comes to big cultural changes. . . . With Napster, there was an enormous amount of grey" between the 'I can share everything I've paid for' position and the 'You're a criminal even if you share only one of

the files you've purchased' point of view."[31]

We agree. Cocreating with consumers is usually a more sustainable business model than suing them. The whole incident turned a huge hot spotlight on the music industry, exposing its outdated marketing practices, gross distribution inefficiencies, and what some interpreted as antimusician policies.

Very little has changed since then. Until now. We look at the new music ecosystem emerging on the blockchain, led by British singer-songwriter Imogen Heap, cellist Zoë Keating, and blockchain developers and entrepreneurs. Every cultural industry is up for disruption, and the promise is that creators get fully compensated for the value they create.

Reconfiguring the Corporation as the Engine of Capitalism

With the rise of a global peer-to-peer platform for identity, trust, reputation, and transactions, we will finally be able to re-architect the deep structures of the firm for innovation, shared-value creation, and perhaps even prosperity for the many, rather than just wealth for the few. This doesn't mean smaller firms in terms of revenue or impact. To the contrary, we're talking about building twenty-first-century companies, some that may be massive wealth creators and powerful in their respective markets. We do think enterprises will look more like networks rather than the vertically integrated hierarchies of the industrial age. As such there is an opportunity to distribute (not redistribute) wealth more democratically.

We'll also take you on a stroll through the mind-boggling world of smart contracts, new autonomous economic agents, and what we call distributed autonomous enterprises where intelligent software takes over the management and organization of many resources and capabilities, perhaps displacing corporations. Smart contracts enable the creation of what we call open networked enterprises based on a new set of business models, or old business models with a blockchain twist.

Animating Objects and Putting Them to Work

Technologists and science fiction writers have long envisioned a world where a seamless global network of Internet-connected sensors could capture every event, action, and change on earth. Blockchain technology will enable things to collaborate, exchange units of value—energy, time, and money—and reconfigure supply chains and production processes according to shared information on demand and capacity. We can attach metadata to smart devices and program them to recognize other objects by their metadata and to act or react to defined circumstances without risk of error or tampering.

As the physical world comes to life, everyone can prosper—from small farmers in the Australian outback who need electrical power for their businesses to home owners everywhere who can become part of a distributed blockchain power grid.

Cultivating the Blockchain Entrepreneur

Entrepreneurship is essential to a thriving economy and a prosperous society. The Internet was supposed to liberate entrepreneurs, giving them the tools and capabilities of big companies without many of the liabilities, such as legacy culture, ossified processes, and dead weight. However, the high-flying success of dot-com billionaires obfuscates an unsettling truth: entrepreneurship and new business starts have been steadily declining for thirty years in many developed economies.[32] In the developing world, the Internet has done little to lower the barriers of would-be entrepreneurs who

Cultivating the Blockchain Entrepreneur

Entrepreneurship is essential to a thriving economy and a prosperous society. The Internet was supposed to liberate entrepreneurs, giving them the tools and capabilities of big companies without many of the liabilities, such as legacy culture, ossified processes, and dead weight. However, the high-flying success of dot-com billionaires obfuscates an unsettling truth: entrepreneurship and new business starts have been steadily declining for thirty years in many developed economies.[32] In the developing world, the Internet has done little to lower the barriers of would-be entrepreneurs who must suffer deadening government bureaucracies. The Internet has also not liberated the financial tools essential to starting a business available to billions of people. Not everyone is destined to be an entrepreneur, of course, but even for the average person trying to earn a decent wage, the lack of financial tools and the prevalence of government red tape make doing so challenging.

This is a complex issue, but blockchain can help supercharge entrepreneurship and therefore prosperity in many important ways. For the average person living in the developing world to have a reliable store of value and a way to conduct business beyond his community, all he needs now is an Internet-enabled device. Access to the global economy means greater access to new sources of credit, funding, suppliers, partners, and investment opportunities. No talent or resource is too small to monetize on the blockchain.

Realizing Governments by the People for the People

Buckle up for big changes in government and governance too. Blockchain technology is already revolutionizing the machinery of government and how we can make it high performance—better and cheaper. It's also creating new opportunities to change democracy itself—how governments can be more open and free from lobbyist control, and behave with the four values of integrity. We look at how blockchain technologies can change what it means to be a citizen and participate in the political process, from voting and accessing social services to solving some of society's big hairy problems and holding elected representatives accountable for the promises that got them elected.

PROMISE AND PERIL OF THE NEW PLATFORM

If there are six million people in the naked city,[33] then there are six million obstacles to this technology fulfilling its potential. Further, there are some worrisome downsides. Some say the technology is not ready for prime time; that it's still hard to use, and that the killer applications are nascent. Other critics point to the massive amount of energy consumed to reach consensus in just the bitcoin network: What happens when thousands or perhaps millions of interconnected blockchains are each processing billions of transactions a day? Are the incentives great enough for people to participate and behave safely over time, and not try to overpower the network? Is blockchain technology the worst job killer ever?

These are questions of leadership and governance, not of technology. The first era of the Internet took off because of the vision and common interests of its key stakeholders—governments, civil society organizations, developers, and everyday people like you. Blockchain requires similar leadership. We discuss at greater length in the book why leaders of this new distributed paradigm will need to stake their claim and unleash a wave of

economic and institutional innovation, to ensure this time that the promise is fulfilled. We invite you to be one of these.

This book grew out of the $4 million Global Solution Networks program at the Rotman School of Management at the University of Toronto. Funded primarily by large technology corporations along with the Rockefeller and Skoll foundations, the U.S. State Department, and Industry Canada, the initiative explored new approaches to global problem solving and governance. We were both involved in running the program. (Don founded it; Alex led the project on cryptocurrencies.) In 2014, we launched a one-year initiative on the blockchain revolution and its implications for business and society, culminating in this book. In it, we have attempted to put the promise and the peril of the new platform into perspective.

If business, government, and civil society innovators get this right, we will move from an Internet driven primarily by the falling costs of search, coordination, data collection, and decision making—where the name of the game was monitoring, mediating, and monetizing information and transactions on the Web—to one driven by the falling costs of bargaining, policing, and enforcing social and commercial agreements, where the name of the game will be integrity, security, collaboration, the privacy of all transactions, and the creation and distribution of value. That's a 180-degree turn in strategy. The result can be an economy of peers with institutions that are truly distributed, inclusive, and empowering—and thereby legitimate. By fundamentally changing what we can do online, how we do it, and who can participate, the new platform may even create the technological preconditions to reconciling some of our most vexing social and economic challenges.

If we get this wrong, blockchain technology, which holds so much promise, will be constrained or even crushed. Worse, it could become a tool powerful institutions use to entrench their wealth or, if hacked by governments, a platform for some kind of new surveillance society. The tightly related technologies of distributed software, cryptography, autonomous agents, and even artificial intelligence could get out of control and turn against their human progenitors.

It is possible that this new technology may be delayed, stalled, underutilized, or worse. The blockchain and cryptocurrencies, particularly bitcoin, already have massive momentum, but we're not predicting whether or not all this will succeed, and if it does, how fast it will occur.[34] Prediction is always a risky business. Says technology theorist David Ticoll: "Many of us did a bad job of predicting the full impact of the Internet. ISIS type bad phenomena are among what we missed, and some big optimistic predictions turned out wrong." He says, "If the blockchain is as big and universal as the Net, we are likely to do a comparably bad job of predicting both its upsides and downsides."[35]

So rather than predicting a blockchain future, we're advocating for it. We're arguing that it should succeed, because it could help us usher in a new era of prosperity. We believe that the economy works best when it works for everyone, and this new platform is an engine of inclusion. It drastically lowers the cost of transmitting such funds as remittances. It significantly lowers the barrier to having a bank account, obtaining credit, and investing. And it supports entrepreneurship and participation in global trade. It catalyzes distributed capitalism, not just a redistributed capitalism.

Everyone should stop fighting it and take the right steps to get on board. Let's harness this force not for the immediate benefit of the few but for the lasting benefit of the many.

Today, both of us are excited about the potential of this next round of the Internet. We're enthusiastic about the massive wave of innovation that is being unleashed and its potential for prosperity and a better world. This book is our case to you to become interested, understand this next wave, and take action to ensure that the promise is fulfilled.

So hang on to your seat and read on! We're at one of those critical junctures in human history.