CHAPTER 10

OVERCOMING SHOWSTOPPERS:

TEN IMPLEMENTATION CHALLENGES

Lev Sergeyevich Termen was a gifted musician, but he preferred playing with physics. Born into Russian aristocracy before the turn of the twentieth century, Termen joined the Bolsheviks in dismantling the tsarist autocracy. One of his early missions was to create a device that could measure the electrical conductivity and capacity of various gases. He tried gas-filled lamps, he tried a high-frequency oscillator, and he even tried hypnosis.[1] The oscillator ended up working well, and so Termen's boss encouraged him to seek other applications for it. Two apps would become legendary. The more whimsical of the two started out as two metal terminals with nothing between them, like a lamp without the glass. Termen discovered that, if he infused this void with gas, he could gauge the gas's electrical properties. His design was brilliant: he substituted headphones for dials so that he could take acoustic rather than visual readings, monitoring the pitch of the signal that each gas produced. It was way ahead of its time, the stuff of Dr. Emmett Brown's garage in *Back to the Future*.

Devotees of TED talks and students of technological history already know the end of this story: Termen stumbled upon a means of making music out of thin air. Whenever he put his hands near the metal terminals, the pitch of the signal changed. He learned that he could manipulate the pitch by the precise position and motion of his hands. He called his device the "etherphone," known today as the theremin, an anglicized version of his name. The other app was a larger-scale version of this apparatus, one that was sensitive to movement within a radius of several meters. It was the first motion detector—sentry of the ether. He demonstrated both of these instruments at the Kremlin, playing his etherphone with abandon for Comrade Lenin. While Lenin delighted in the etherphone, he put the motion detector immediately to work in watching over the Soviet stashes of gold. If anyone crossed the electromagnetic line around the gold, they'd set off a silent alarm. Big Brother suddenly had electric eyes.

The moral of the story is simple: Termen's devices brought both light and darkness to the world. In a poignant talk, "Our Comrade the Electron," Maciej Ceglowski pointed out these two themes in all of Termen's inventions: as soon as they gave shape to airy nothing, they were usurped by dark forces. Lenin even co-opted electricity in his propaganda, equating communism with Soviet power plus the electrification of the country.[2] But it was Stalin who rounded up Termen and his peers, threw them into the Kolyma gulag, and forced them to invent instruments of tyranny.

We've heard bitcoin used with similar grandiosity in campaigns of all stripes. Like every revolutionary technology, the bitcoin blockchain has its upside and its downside. In the previous chapters, we've walked you through the many promises of this technology. This chapter shines a spotlight on ten showstoppers—problems and perils. Forgive us if some of these are technically complicated. We think it imprudent to supersimplify these issues: we need a certain level of detail for precision.

As well, after reading this section you may be tempted to dismiss these

blockchain innovators because they face serious obstacles. We encourage you to consider whether these are either "reasons the blockchain is a bad idea" or "implementation challenges to overcome." We think it's the latter, and we'd like innovators to view these as important problems to solve creatively as we transition to the second era of the Internet. For each challenge, we propose some solutions. In the final chapter, we present our thinking on what we can do overall to ensure the fulfillment of the blockchain's promise.

1. THE TECHNOLOGY IS NOT READY FOR PRIME TIME

As of this writing, most people have only a vague understanding of bitcoin the cryptocurrency, and very few have heard of blockchain the technology. You the reader are among the forward-thinking few. Bitcoin conjures images ranging from a pyramid scheme and a money Laundromat to a financial E-ZPass on the economic highway for value. Either way, the infrastructure isn't ready for prime time, so goes the argument.

The challenge is multifaceted. The first facet borrows from science fiction author William Gibson, that the future is here; its *infrastructure* is just unevenly distributed. Had Greek citizens known about bitcoin during their country's economic crash in 2015, they still would've been hard-pressed to locate a bitcoin exchange or a bitcoin ATM anywhere in Athens. They wouldn't have been able to transfer their drachmas into bitcoins to hedge against the plummeting fiat currency. Computer scientist Nick Szabo and information security expert Andreas Antonopoulos both argued that robust infrastructure matters and can't be bootstrapped during catastrophes. Antonopoulos said that Greece's blockchain infrastructure was lacking at the time of the crisis, and there was insufficient bitcoin liquidity for an entire population to move its troubled fiat currency into it.

On the other hand, the bitcoin blockchain isn't ready for Greece either. That's the second facet: it falls short on security controls for such a massive bump in usage. "The system lacks the *transactional capacity* to on-board ten million people. That would represent almost a tenfold increase in user base overnight," said Antonopoulos. "Remember what happened when AOL dumped 2.3 million e-mail accounts onto the Internet? We quickly discovered that the Internet wasn't ready, in terms of spam protection and Net etiquette, to absorb 2.3 million noobs who didn't have the culture. That's not good for an immature technology."[3] The blockchain would be susceptible to capacity problems, system failures, unanticipated bugs, and perhaps most damaging, the huge disappointment of technically unsophisticated users, none of which it needs at the moment.

That relates to the third facet of this showstopper, its *inaccessibility* to the average person. There's not enough wallet support, and many interfaces are user-*un*friendly, requiring a high tolerance for alphanumeric code and geekspeak. Most bitcoin addresses are simply strings of between twenty-six and thirty-five characters beginning with a one or a three, quite tedious to type. As Tyler Winklevoss said, "When you go to Google.com you don't type in a string of numbers. You don't type in an IP address. You type in a name, a word that you can remember. And the same goes with the bitcoin addresses. Bitcoin addresses shouldn't be exposed to the average user. Little things like that make a difference."[4] So there's much work to be done in basic user interface and experience.

Critics have also raised concerns about long-term *illiquidity* because bitcoin is finite in quantity—21 million by 2140—and mined at a diminishing rate. It's a rules-based monetary policy intended to prevent inflation triggered by arbitrary and discretionary monetary policies, a phenomenon

commonplace for many fiat currencies. Satoshi wrote, "It's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases. It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value."[5]

At the margin, coins stored in lost wallets or sent to addresses whose owners have lost their private keys are not recoverable; they just sit dormant on the blockchain, and so there will be fewer than 21 million in circulation. Early adopters have tended to hold on to bitcoin as they hold on to gold, hoping that its value will increase in the long run, and therefore treating bitcoin as an asset rather than as a medium of exchange. According to economic theorists, low or no inflation motivates holders to hoard rather than spend their bitcoin. Still, if more trusted bitcoin exchanges facilitate consumers' movement in and out of bitcoin, then the frequency and volume of trading could increase. If more merchants accept bitcoin as a medium of payment, then people who've been sitting on bitcoins may start to use their store for purchases, thereby freeing up more bitcoins. If merchants begin to issue bitcoin-denominated gift cards, then more people should be exposed to cryptocurrencies and become more comfortable transacting in bitcoin. And so, hypothetically, people will have fewer reasons to hoard bitcoin. Advocates of the bitcoin protocol argue that, because bitcoins are divisible to eight decimal places—the smallest unit is called a Satoshi, worth one hundredth of a millionth of a bitcoin—the smallest denominations will buy more if demand for bitcoin increases. There's also the possibility of tweaking the protocols to allow for greater divisibility, say, picopayments (trillionths of a bitcoin) and to remine stranded bitcoin after a period of dormancy.

A fifth dimension is *high latency*: for the bitcoin blockchain network, the process of clearing and settling transactions takes about ten minutes, which is far faster end to end than most payment mechanisms. But clearing transactions at the point of sale instantaneously is not the issue; the real problem is that ten minutes is simply too long for the Internet of Things where devices need to interact continuously. Core developer Gavin Andresen said solving for a trillion connected objects is "a different design space from bitcoin," a space where low latency is more critical and fraud is less of an issue or where parties could establish an acceptable level of trust without the bitcoin network. Ten minutes is also too long for financial transactions where timing matters to get an asset at a particular price, and where latency exposes traders to time-based arbitrage weaknesses such as market timing attacks.[6] The immediate solution for entrepreneurs has been to fork the bitcoin code base, that is, to modify the source code by tweaking a few parameters, and to launch a new blockchain with an altcoin in place of bitcoin as incentive to participate. Litecoin is a popular altcoin with a block time of 2.5 minutes, and Ripple and Ethereum are entirely reengineered blockchain platforms that have latency of seconds, not minutes.

A sixth dimension is *behavioral change* in a deeper sense than Netiquette. Today, many people count on their bank or credit card company, even talking with a real person, when they make an accounting error, forget their passwords, or lose their wallets or checkbooks. Most people with bank accounts aren't in the habit of backing up their money on a flash drive or a second device, securing their passwords so that they needn't rely on a service provider's password reset function, or keeping these backups in separate locations so that, if they lose their computer and all other possessions in a house fire, they don't lose their money. Without this discipline, they might as well stuff their mattress with cash. With greater freedom—better privacy, stronger security, and autonomy from third-party cost structures and system failures—comes greater responsibility. For those consumers who don't trust themselves to keep safe backups of their private keys, third-party storage providers could provide backup service.

A seventh dimension is *societal change*. Money is still a social construct

representing what a society values. It is endogenous to that society, it manifests because of human relationships, and it adapts to evolving human needs. "You can't take the social out of money," said Izabella Kaminska of the *Financial Times*. "A lot of these protocols attempt to do that by creating an absolutist and very objectified system. It just doesn't reflect the world as it is." She pointed to the euro system as an example of how one size—one set of protocols—doesn't fit all countries.[7] She echoed what Antonopoulos said about the very human need for societies to forgive and forget in order to move on. "There's a very long tradition in finance of obliterating records, because we as a society believe that it's wrong to persecute or discriminate against individuals for something they did ten or fifteen years ago. We have this whole debt jubilee-esque mentality because we think people should be given another chance. Creating a system that never forgets is slightly sociopathic," she said.[8]

That leads us to the eighth dimension, the *lack of legal recourse* in a world of irrevocable transactions and unvoidable smart contracts. According to legal scholars Primavera De Filippi and Aaron Wright, "People are, indeed, free to decide the particular set of rules to which they want to abide, but—after the choice has been made—can no longer deviate from these rules, to the extent that smart contracts are automatically enforced by the underlying code of the technology, regardless of the will of the parties."[9] This very high degree of certainty—mathematical certainty—as to the outcome of a transaction or a smart contract is unprecedented in society. It delivers greater efficiencies and effectively eliminates nonperformance risk because we have no choice of breach, no choice of damages. But that's also a downside. It allows no room for human beings. To Josh Fairfield of Washington and Lee University School of Law, that means "more messiness, not less. We're going to see more fights. 'You didn't actually renovate my house, I want my money back.' We're going to see more human messiness, but more human messiness doesn't mean the technology is bad."[10]

But will people actually take the counterparty to court? De Filippi estimated that, in the analog world, 80 percent of contract breaches aren't enforced because they're too costly to pursue in court, too expensive to go into proceedings. Why should those numbers improve in a blockchain world? When the code indicates that the contract has been fully executed rather than breached, except one party is dissatisfied with the outcome, will the dissatisfied party actually pursue a lawsuit? Will the courts recognize the case? Will the small business owner back away from the corporate legal team of Dewey, Cheatham, and Howe or—with his modest resources—even be able to identify his anonymous counterparty, so that he could file a lawsuit in the first place?

2. THE ENERGY CONSUMED IS UNSUSTAINABLE

In these primordial days of the bitcoin blockchain, the proof-of-work method described in chapter 2 has been critical to building people's trust. Years from now, we will look back and appreciate the genius of its deployment, from minting and allocating new bitcoins to assigning identity and preventing double spending. Pretty remarkable. And pretty unsustainable, according to critics of cryptocurrencies that use proof of work to keep the network safe and pseudonymous.

Hashing, the process of running pending transactions through the secure hash algorithm 256 (SHA-256) to validate them and solve a block, burns a lot of electricity. Some people in the blockchain ecosystem are making back-of-the-envelope calculations that become memes in the community. Estimates liken the bitcoin network's energy consumption to the power used

by nearly seven hundred average American homes at the low end of the spectrum and to the energy consumed by the island of Cyprus at the high end.[11] That's more than 4.409 billion kilowatt-hours,[12] a Godzilla-sized carbon footprint, and it's by design. It's what secures the network and keeps nodes honest.

In early 2015, *The New Republic* reported that the combined processing power of the bitcoin network was hundreds of times greater than the aggregate output of the world's top five hundred supercomputers. "Processing and protecting the more than $3 billion worth of bitcoins in circulation requires more than $100 million in electricity each year, generating a volume of carbon emissions to match." The article's author, Nathan Schneider, wrote what has been on our minds ever since: "All that computing power, which could be curing cancer or exploring the stars, is locked up in machines that do nothing but process bitcoin-type transactions."[13]

As citizens who care about our planet, we should all be concerned. There are two issues, one around the electricity used to run the machines and another around the energy used to cool them so that they don't fail. Here's a rule of thumb: for every dollar a computer burns up in electricity, it needs fifty cents to cool down.[14] The acute drought in California has raised serious concerns over using precious water to cool data centers and bitcoin mining operations.

As the value of bitcoin increases, the competition for mining new bitcoin increases. As more computing power is directed at mining, the computational problem that miners need to solve becomes more difficult. One measure of the total processing power of the bitcoin network is the hash rate. Gavin Andresen explains: "Let's say we have millions of transactions per block, each paying an average of a dollar transaction fee. Miners would be paid millions of dollars per block, and they would spend a little less than that in electricity to do that work. That's how the proof-of-work economics work out. It really is the price of bitcoin and however much reward is in a block that drives how much hashing is done."[15] The hash rate has been increasing considerably over the last two years, rising forty-five-fold in less than a year. And the trend is toward using more energy, not less.

"The cost for having no central authority is the cost of that energy," said Eric Jennings, CEO of Filament, an industrial wireless sensor network.[16] That's one side of the argument. *The energy is what it is,* and it's comparable to the cost incurred in securing fiat currency. "All forms of money have a relationship to energy," said Stephen Pair of BitPay. He revisited the gold analogy. "Gold atoms are rare on earth because an intense amount of energy is needed to form them." Gold is precious because of its physical properties, and those properties derive from energy. Pair mused that artificially manufacturing gold would require nuclear fusion.[17]

From one perspective, all this electricity consumption makes sense. Erik Voorhees, founder of the coin exchange ShapeShift, said critics were unfair in calling the energy spent on bitcoin mining a waste. "The electricity is being burned for a purpose. There is a real service being provided, the securing of these payments." He urged critics to compare it with the energy burned by the current financial system. Think of the big vaults, the bunkerlike architecture with majestic Grecian facades, HVAC systems pushing frigid air into bright lobbies, competing branches on every corner, and ATMs in between. "The next time you see a Brink's armored truck pumping black soot into the air, compare that to the burning of electricity in bitcoining. It is not quite clear which is worse," Voorhees said.[18]

The second energy-related issue is computer architecture itself. For backward compatibility with slower-changing legacy systems, your laptop or PC is likely a type of complex instruction set computer (CISC) that can run a wide range of math apps that the average person will never ever use. When engineers realized that they'd seriously overshot the market, they created the reduced instruction set computer (RISC). Your mobile device is likely an advanced RISC machine (ARM). What miners realized was that they could

also harness their graphics processing unit to increase processing speed. Because modern GPUs have thousands of computing cores on each chip, they are ideal for computations that can be done in parallel, such as the hashing done in bitcoin mining, There were some trade-offs, and estimating the machine's energy consumption got slightly more complicated, but for the most part GPUs could do the work.[19]

"If I can design a RISC computer to be oh-so-superfast and massively, near insanely parallel to try the billions of kazillions of codes simultaneously with little or no electricity, I will make money out of thin air,"[20] said Bob Tapscott, Don's CIO brother. That's what the BitFury Group has done: built a massively parallel bitcoin solver with application specific integrated circuits (ASICs) that are energy efficient and designed solely to mine bitcoins. Its founder and CEO, Valery Vavilov, argued the view that machines and mining operations overall will continue to get more energy efficient and environmentally friendly. Some of that depends on relocating to cold climates where energy is cheap and preferably renewable, such as hydro or geothermal, and where either Mother Nature handles the cooling or manufacturers figure out an efficient way to capture the heat. BitFury, for example, has two data centers—one in Iceland and another in the country of Georgia—with plans for additional centers in North America, and it acquired the Hong Kong–based start-up Allied Control, which specializes in immersion cooling technology.[21] And so BitFury is working to reduce the ecological impact of the bitcoin infrastructure.

Even if these initiatives limit mining's carbon footprint, we still have the rapid consumption and disposal of these continually upgraded devices. Miners who want to make a career of it must continually upgrade and specialize their systems. Most mining equipment has a useful life span of three to six months.[22] Bob Tapscott likened firms such as BitFury to those Yukon shopkeepers during the great gold rush: they made their real fortune by selling better and better shovels to the miners.[23] We found one miner's description of his Cointerra TerraMiner IV bitcoin with an ASIC chip that was so energy intensive that his home's electrical system couldn't handle it. "I am selling three units because my house is old and has substandard wiring. I do not want a fire." The starting bid was five thousand dollars.[24] Vendors such as MRI of Australia are applying new approaches to recycling, first disassembling rather than shredding all these computing components, and then managing resulting waste streams. Such creative processes are enabling them to reclaim precious metals and reuse up to 98 percent of product by weight.[25] Unfortunately, hardware recycling is still not widely available to most consumers.

For bitcoin's core developers, the concern is legitimate and worth solving: "If bitcoin really does become a global team network, I think we will need to slowly move away from proof of work as the only way it's secure," said Andresen. "In the very long run, maybe we will move away from proof of work as the way the network is secured, and we'll combine it with something else."[26]

That's what several altchains have done: explored alternative consensus algorithms such as proof of stake for securing the network while retaining decentralization. The open source nature of the bitcoin protocol makes it technically easy to do. Remember, the purpose of consensus algorithms is to distribute the right to decide what the state of the blockchain is to a decentralized set of users. To the mind of Vitalik Buterin, the visionary behind Ethereum, there are only three securely decentralized sets of users, and each set corresponds to a set of consensus algorithms: *owners of computing power*, with standard proof-of-work algorithm; *stakeholders*, with various proof-of-stake algorithms in wallet software; and *members of a social network*, with a "federated style" consensus algorithm.[27] Note that only one of those consensus mechanisms includes the word *power*. Ethereum version 2.0 will be built on a proof-of-stake model, whereas Ripple uses a federated model, a small controlled group akin to something like SWIFT, the global provider of secure financial messaging, where authorized groups reach consensus on the state of the blockchain.[28]

Those systems don't burn electricity as the bitcoin blockchain does. Bram Cohen, founder of Tor, has introduced a fourth way to address the energy waste, what he calls "proof of disk," where *owners of disk storage space*—people who have committed a chunk of computer memory to maintaining a network and performing network functions—defines the economic set of users. Of these alternatives to proof of work, Blockstream's Austin Hill cautioned against using alternative methods for securing consensus. "Experimentation with your proof-of-work algorithm is dangerous, and it's a new area of computer science."[29] It adds an additional dimension to innovation: not only must developers worry about whether their new features and functions will work in their own right, but they must also check how the choice of consensus algorithm keeps them secure and distributed to the most appropriate economic set.

Overall, the expression "If there is a will, there is a way" applies. The smartest technologists on the planet are working on creative solutions to the energy problem, with more efficient devices and use of renewable energy. Further, as computers become inexorably smarter, they will undoubtedly provide their own solutions. Bitcoin angel investor Roger Ver, nicknamed Bitcoin Jesus, said, "Say the smartest human has an IQ up close to 200. Imagine artificial intelligences with an IQ of 250, or say 500, or 5,000 or 5 million. There will be solutions, if we humans want them."[30]

3. GOVERNMENTS WILL STIFLE OR TWIST IT

To libertarians and anarchists, Satoshi Nakamoto wrote, "You will not find a solution to political problems in cryptography."[31] They would have to look elsewhere for a cure-all to big government. Satoshi viewed his experiment as a gain in a new territory of freedom, not a total upheaval. Where governments had succeeded in beheading centrally controlled networks like Napster, pure peer-to-peer networks like Tor were able to persist. Could the bitcoin blockchain network hold its own against mighty central authorities?

That might be the biggest unknown. What will legislators, regulators, and adjudicators around the world make of blockchain technologies? "The courts are going to get it wrong. They've already started to get it wrong, applying intellectual property rules to anything that is intangible. They think that physicality is the dividing line between virtual property and intellectual property, and it's not," said Josh Fairfield. "There's no intellectual property element, there's no part of a bitcoin that is intellectual property, there's no creative spark for copyright, there's no patentable idea, there's no patent, there's no trademark."[32] According to Stephen Pair of BitPay, "The biggest threat to bitcoin is that it becomes so heavily regulated at some point that a competitor that's more private and more anonymous shows up and everybody switches to that."[33] One thing's for sure: "Whatever the particular policy issue is, if you don't understand the technology and you don't understand the implications, you're setting yourself up for failure," said Jerry Brito of the bitcoin policy think tank Coin Center. "If you don't understand it, you can introduce law and policy that's going to harm the development of the technology. We just want you to understand what you're doing."[34]

So their challenge is formidable. They must oversee the unforeseeable. On the one hand, they must avoid stifling innovation by overreacting to worst cases—human trafficking, illicit drug trade, gunrunning, child pornography, terrorism, tax evasion, and counterfeiting, for instance. On the other hand, they must not twist new but unproven applications such as blockchain-based platforms for identity management to restrict civil liberties. There must be a stable approach to regulation, legislation, and the international negotiation of

treaties to minimize regulatory uncertainty, so that investors will continue to support the technology's global development.

Jurisdiction already matters when it comes to using bitcoin. Some governments have banned it or banned state banks from exchanging it, as China has done. Brito said, "In a typically Chinese way, it's not illegal, but it could be at any moment and everybody knows it."[35] China is allowing a serious professional mining community to flourish and those mining pools have become quite influential in debates over upgrades to the bitcoin protocol. What happens to blockchain security if China suddenly bans mining, too? Other jurisdictions have moved to define bitcoin narrowly, as the U.S. Internal Revenue Service has done. The IRS has labeled bitcoin as an asset for calculating taxes on the appreciation of value.

Legal frameworks also matter. Legal scholars De Filippi and Wright don't think the current one can handle the questions raised by smart property deployed globally at scale. Smart contracts both define and manage ownership rights. Their code makes no assumptions about the assignment of rights, and code can't arbitrarily seize, divest, or transfer these rights. For example, if during the process of land registration, government officials assigned the ownership of a parcel of land to someone who isn't the legal owner of that parcel, that person would have absolute sovereignty over the parcel, and the legal owner couldn't simply reverse the assignment.

Josh Fairfield focuses more on process: "The common law isn't affecting technology law; the common law *is* technology law. The common law is the process of adapting human systems to technological change . . . the real fight is how do we take old rules meant for old technology and adapt them rapidly and competently," so that they are recognizable when we start using them but iterated so that they're state of the art when the technology really hits.[36]

Last but not least, and this should be no surprise, identity matters big-time—or at least how we construct it on the blockchain matters. "People have a very simplistic view of identity," said Andreas Antonopoulos. "I am actually terrified of the implications of digital identity because I think people will take shortcuts. . . . If we transfer identity to the digital world where views are inflexible, we actually end up with a construct that does not resemble the social construct of identity, but is a terrifying, fascist copy of it."[37]

Combine a precisely coded version of personhood with a precisely coded version of society, and you get the stuff of science fiction novels and Arnold Schwarzenegger movies. Legal scholars De Filippi and Wright conjured images of "self-enforcing contracts, *walled gardens* or *trusted systems,* owned and managed by a sophisticated network of decentralized organizations that dictate what people can or cannot do, without any kind of constitutional safeguards or constraints." In other words, a machine-driven totalitarian regime.

Artificial intelligence expert Steve Omohundro threw this phrase at us: the *dictator's learning curve*, or how cave dwellers end up with space age technology. Think about all the AI labs out there staffed by the world's smartest PhDs with access to the world's most powerful computers. PhDs might fork the bitcoin code or write a smart contract that controls a drone's delivery of a package, where bitcoin is held in escrow until that exact moment when the package arrives. Let's say these PhDs post that software as open source code to the Internet, because that's what they do to move their ideas forward; they share ideas. So now ISIS doesn't need an AI lab, it doesn't need a software development team. It just needs to substitute a grenade for the package. That's the dictator's learning curve, and it's not steep. But don't blame the code or the culture of sharing. It's not necessarily what we do with the code; it's what we don't realize we're doing with it—the unintended consequences of a friction-free world.

4. POWERFUL INCUMBENTS OF THE OLD PARADIGM WILL USURP IT

Many of our concerns about the first generation of the Internet have come true. Powerful corporations have captured much of the technology and are using it in their vast private empires to extract most of the value. They have closed off opportunity and privatized much of our digital experience. We use proprietary stores to acquire and use new apps on our phones, tablets, and now watches. Search engines and marketing departments alike interrupt our content with advertising. Big companies that promote and prosper from consumer transparency are notoriously secretive about their activities, plans, technology infrastructures, and information assets. To be sure, some companies have opened up voluntarily, but many others have merely reacted to the sunlight of whistleblowers and investigative journalism. Such disclosures are dwarfed by efforts to hide operations and conceal information.

Simply put, they haven't been good stewards of the public trust.

Case in point: the banking industry. "Banks are traditionally secret keepers," according to Kaminska of the *Financial Times*. She explained that banks make good judgments about whom to lend to and how to process payments when they have good access to private information, and they get that information by promising to keep the secret. The more secrets they hold, the greater the information asymmetry and the greater their advantages, but those advantages have harmful systemic implications.[38] So what's to prevent huge corporations or powerful nation-states from capturing blockchain technologies for their own narrow interests? "Any consensus mechanism that you have is going to be susceptible to marketing—where powerful interests spend money trying to convince people to do a certain thing," said Pair of BitPay.[39]

To be clear, we are not suggesting that corporations and governments should leave this technology alone. After all, blockchain technology is emerging as an important global resource that could enable new capabilities. Moreover, society needs governments to deliver services for their citizenry and corporations to create jobs and wealth. But that's different from capturing a disruptive technology and its largesse in ways that limit its greater benefits to society.

Also consider what the core developers and blockchain companies are already doing to secure their networks, anticipating and responding quickly to worst-case scenarios. For example, in 2014, thieves stole eight million VeriCoins, a proof-of-stake cryptocurrency, from the MintPal exchange. Within days of the attack, VeriCoin developers released new code that forked the VeriCoin blockchain prior to the hack—in a sense, they rolled back time—and collaborated with exchanges to make sure it was adopted.[40] Similarly, "if money and power do try to capture the network, the miners would stop them by going to the real version of bitcoin and initiating a fork,"[41] according to Keonne Rodriguez, product lead at Blockchain.

What's to prevent China from aiming all its state processing assets and all its mining pools at the bitcoin blockchain to stage a 51 percent attack or at minimum destabilize the process? Let's say some wealthy despot has decided that bitcoin, like the Internet before it, has become so influential that it is eroding his power. This despot could seize all the mining power within reach and purchase the rest from countries that still tolerate his bad behavior, to put him over the 50 percent hash rate threshold. He could then decide which transactions to include in blocks and which to reject. With controlling interest, he could also decide whether to fork the code and introduce a few prohibitions, maybe blacklisting addresses associated with gambling or free speech. So do honest nodes adopt this centrally controlled fork or do they fork

over to a new code? Andrew Vegetabile, director of the Litecoin Association, said there was no escape from such a scenario because the despot controlled 51 percent of the network. And he needn't represent a government; he could be one of the world's wealthiest people or an executive of a highly profitable company with substantial purchasing power.[42]

A third scenario is that the incumbents will defend their territory, lobbying to make sure existing regulations for well-established firms apply to small start-ups, and suing any start-up that survives the regulatory inquisition. This litigate-not-innovate strategy may buy them time to sort out a strategy. Or it may simply drain the incumbent of whatever real value it contains. Think of those twin tyrants—legacy systems and active inertia. Academics have well documented the effects of lock-in and switching costs and have identified the challenges of postmerger systems integration. Organizations with huge technology investments in their installed base may be more likely to throw more money at their old system, sharpening their knives for the pistol fight rather than conducting strategic experiments on the blockchain.

5. THE INCENTIVES ARE INADEQUATE FOR DISTRIBUTED MASS COLLABORATION

Miners do have an incentive to maintain the bitcoin infrastructure because, if the network fails, all the unconverted bitcoin they'd earned (or could earn) through mining would be lost or worthless or otherwise at risk. Before we dig further into incentives, let's be clear about the service that miners provide: it is *not* transaction validation. Every full node can validate transactions. Rather, miners preserve the distribution of power—the power to decide which transactions to include in each block, the power to mint coins, the power to vote on the truth.

SO YOU WANNA BE A BITCOIN MINER?

As part of our research, we recruited Bob Tapscott—former bank CIO, management consultant at large, and Don's brother—to download the entire bitcoin blockchain stack and ledger in early 2015. The experiment was instructive in terms of the elapsed time, the effort required, the energy consumed, and the (lack of) payoff for hobby mining of bitcoin.

Bob dedicated his spare four-thread, two-core Windows PC to the task. Downloading took a full three days and consumed on average about 20 percent of the available processing power. Mining uses slightly more than 200 MB of memory and 10 percent of the CPU to stay current.

Although Bob's computer was hardly optimized for mining bitcoin, he entered it into a mining pool. In a 137-hour session, it mined 152.8 microbitcoin (μBTC), roughly three and a half U.S. cents at the time. But at ten cents per kilowatt-hour, Bob's computer used about fourteen cents of electricity. Bob concluded, "The days of mining bitcoins from your PC are now over."

So any design change to the original bitcoin protocol, whether through an altcoin or an upgrade, must keep in mind

appropriate economic incentives to sustain miner decentralization, so that the network gets good value from miners in exchange for the large sums of bitcoin. Bitcoin core developer Peter Todd likened this task to designing a robot that can buy milk at the grocery store. "If that robot doesn't have a nose, before long store owners are going to realize it can't tell the difference between unspoiled and spoiled milk, and you're going to get ripped off paying for a bunch of spoiled milk."[43] To Todd, that means that smaller miners in geographically dispersed locations should be able to compete nose to nose with larger miners that are geographically centralized, that is, large mining pools in Iceland or China.

The question is whether that's possible. Because the number of new bitcoins minted halves every four years, what will happen when the reward drops to zero? The mining cycle depends on the market price of bitcoin. When the price drops, some bitcoin miners park their supply, but they continue to play the lottery until the price increases. Other miners can't afford to park and play; they just dry-dock their mining rigs or divert their processing power to another altchain that might be more profitable. Still others join mining pools, pooling their computing power with nodes with the hope of increasing their odds and at least getting some fraction of the winnings rather than nothing at all. And then there's the industrial bitcoin mining complex. Valery Vavilov of BitFury estimated that his mining operation would have at least 200 megawatts' capacity by the end of 2016.

One answer is charging fees. Satoshi wrote, "There will be transaction fees, so [mining] nodes will have an incentive to receive and include all the transactions they can. Nodes will eventually be compensated by transaction fees alone when the total coins created hits the pre-determined ceiling."[44] So once all bitcoins have been minted, a fee structure will likely emerge. Think in terms of billions of nanopayments. Because each block has a fixed maximum size, there is a limit to how many transactions a miner can include. Therefore, miners will add transactions with the highest fees first, leaving those with low or zero fees to fight for whatever space might be left over. If your transaction fee is high enough, you can expect a miner to include it in the next block; but if the network is busy and your fee is too low, it might take two, three, or more blocks before a miner eventually records in the blockchain.

What does that mean for people who can't afford fees now? Won't levying fees lower the blockchain's advantage over traditional payment methods? According to venture capitalist Pascal Bouvier, the "fees reflect the marginal cost of verifying a transaction." Without fees to incentivize miners, as the block reward keeps halving, the hash rate would likely drop. If the hash rate drops, network security declines.[45]

That leads us back to the 51 percent attack, where a huge mining pool or a cartel of large mining pools controlled 51 percent of the hash rate. With that much firepower, they would constitute a majority vote of miners and could hijack block generation and force their version of the truth on the bitcoin network. They wouldn't necessarily get rich. Far from it. All they could do is to reverse their own transactions within a previous block, rather like a credit card chargeback. Let's say the attackers bought some big-ticket item from the same merchant, waited until it shipped, then attacked the network to get their money back. That wouldn't mean

tacking its own block to the end of the blockchain. That would mean going back and redoing the block that contained all their purchases as well as all subsequent blocks, even as the network continues to generate new blocks. When the cartel's branch became longer, it would become the new valid one. Satoshi bet on that being wildly more costly than mining new coins.

Where 51 percent attacks on proof-of-work models stem from concentrated mining power, attacks on proof-of-stake models come from concentrated coin control, and coin exchanges are typically the biggest stakeholders. In some jurisdictions, exchanges must be licensed and are under regulatory scrutiny. They also have reputation at stake, and so they have multiple incentives to protect the value of their brand and the value of the coins held in account wallets. However, with more coins in circulation, a greater diversity of value, and more strategic assets registered on PoW and PoS blockchains, an attacker may not care about any of these costs.

6. THE BLOCKCHAIN IS A JOB KILLER

At the 2015 World Economic Forum annual meeting in Davos, Switzerland, a panel of technology executives from Microsoft, Facebook, and Vodaphone discussed the impact of technology on jobs. All agreed that, although technological innovations may disrupt labor markets temporarily, overall they generate new and incrementally more jobs. "Why should this time be any different?" said Eric Schmidt, executive chair of Google.

The displacement of workers through automation is nothing new. Consider the Internet's impact on travel agents and music retailers. Uber and Airbnb have created income for drivers with extra time and home owners with spare rooms, but neither provides health insurance or other employee benefits, and both are displacing better-paid jobs in the travel and hospitality industries.

The blockchain is an extraordinary platform for radical automation, where computer code rather than humans do the work, managing assets and people. What happens when autonomous vehicles replace Uber drivers? Or digital currencies obviate Western Union's five hundred thousand points of sale around the world.[46] Or when a shared blockchain platform for financial services eliminates tens of thousands of accounting and IT systems management jobs? While there will be many new business and employment opportunities created through the IoT, will it drive further unemployment, especially in the relatively unskilled market for relatively routine tasks?

In the developing world, the blockchain and cryptocurrencies could enable entrepreneurs to raise capital, protect assets and intellectual property, and create jobs even in the poorest communities. Hundreds of millions could become microshareholders in new corporations and participate in economic exchange. The technology could radically improve the delivery and deployment of aid, increase government transparency, reduce corruption, and set the conditions for good government—a precondition for jobs in many parts of the world.

Even in the developed world the effects are not determinable. A global platform that drops transaction costs, in particular the costs of establishing trusted commerce and wealth creation, could result in more participants.

Even if this technology enables us to do more with fewer human resources, we still have no case to fear, delay, or halt its march. Ultimately, what matters is not whether new capabilities exist but the extent to which

societies turn these into social benefit. If machines are creating so much wealth, then maybe it's time for a new social contract that redefines human work and how much time we should all spend making a living.

7. GOVERNING THE PROTOCOLS IS LIKE HERDING CATS

How should we steward this new resource to fulfill its potential? Unlike the Internet, the bitcoin community does not yet have formal oversight bodies such as ICANN, the Internet Engineering Task Force, or the World Wide Web Consortium to anticipate development needs and guide their resolution—*and the community prefers it that way*. That presents uncertainty. People who want to keep the blockchain decentralized, open, and secure can't agree on a way forward. If we don't address governance, then the movement could collapse on itself as it disintegrates into warring factions.

There are countless issues. Bitcoin core developers Gavin Andresen and Mike Hearn have been advocating for an increase in block size from one megabyte of data to as large as twenty megabytes. Bitcoin is not "a token for rich people to trade back and forth. . . . It is a payment network," said Andresen.[47] They argue that if bitcoin is ever to compete seriously as a global payment mechanism, then it has to prepare for mainstream adoption. It couldn't grind to a halt one day when transaction flow suddenly surpassed blockchain capacity. Fees would skyrocket for people who didn't want to wait months or years for their transactions to settle. Or perhaps some central power would step in, in the interest of consumer protection, and process the overflow. In August 2015, they went ahead and launched Bitcoin XT, a fork of the blockchain that allows for eight-megabyte blocks. It is still a controversial compromise.

Opponents argue that people shouldn't be using bitcoin to buy their venti lattes at Starbucks. "Some developers want every single person in the world to be running a fully validating node that sees every single transaction and has absolutely no trust on anybody else," said Andresen. "The volunteer contributors who have been actually making the software work for the last few years are worried that they personally may not be able to handle larger blocks if transaction volume ramps up. . . . I don't have a whole lot of sympathy for that."[48] In other words, if the bitcoin blockchain is to scale and remain secure, then we can't have it both ways. Some nodes will run full protocols and process more transactions into increasingly larger blocks, and others will run simplified payment verification models and trust that 51 percent of full nodes get it right.

The biggest pushback against Bitcoin XT came from the mining pools in China. Serious bitcoin miners, like hard-core online gamers, need not only seriously powerful computers to find a correct hash but also seriously high-speed bandwidth to broadcast it quickly across the network. China is an exception to Nielsen's law of Internet bandwidth: bandwidth doesn't increase by 50 percent each year. If the block size increase is too large, it would put low-bandwidth Chinese miners at a disadvantage compared with miners in other parts of the world. Receiving new blocks to build upon would take longer; and when they did find a new block, they would take longer to send it out to the rest of the network. These delays would ultimately result in the network's rejecting some of their blocks. They would lose out to miners with more bandwidth whose blocks propagated faster.

"Trying to bootstrap or change a network protocol is just a monumental task," said Austin Hill. "You just don't want to be making changes ad hoc or very fast on an ecosystem that's managing anywhere from three to ten billion dollars' worth of people's wealth and assets."[49] At the end of the day, said

Andresen, "That governance model is driven very much by what code the people actually want to run, what standards people want to implement in the equipment they sell." He said that bitcoin, like the Internet, will "have a similar messy, chaotic governance process that will eventually come down to what codes the people choose to run."[50]

Again, we're not talking about regulating but about stewarding this resource for viability and success. Governance includes setting standards, advocating and adopting sensible policies, developing knowledge about the technology's potential, performing watchdog functions, and actually building out the global infrastructure. We discuss a multistakeholder governance model in the next chapter.

8. DISTRIBUTED AUTONOMOUS AGENTS WILL FORM SKYNET

There are highly distributed enterprises with a range of good and bad actors. Anonymous, a distributed affinity group of volunteers, consists of corporate saboteurs, whistleblowers, and watchdogs. With the blockchain, Anonymous could crowdsource bitcoin and hold these funds in a wallet. Let's say a group of French shareholders would like to give that money to a few assassins who would track down and kill off the unaccounted-for terrorists responsible for the Paris massacre. They'd need thousands of signatories to reach consensus and release the funds. In this scenario, who legally controls those funds? Who is responsible for the outcome of that transaction? If you've contributed one ten-thousandth of a vote, what is your legal liability?[51]

If vending machines are programmed to order the most profitable products, will they discover a supplier for illegal goods or drugs? (Hey, the candy machine is selling Ecstasy!) How should the law handle an autonomous vehicle that accidentally kills a human being? For *Wired* magazine, two hackers demonstrated how to hijack the control systems of a Jeep Cherokee on the highway. Chrysler responded by recalling 1.4 million vehicles and alarming drivers, manufacturers, and policymakers alike.[52] Could terrorists figure out how to hack smart devices so that they performed unwanted actions with devastating consequences?

There are other challenges with distributed models of the enterprise. How does society govern these entities? How can owners keep ultimate control? How do we prevent hostile takeovers of personless businesses? Let's say we own a decentralized Web hosting company where each of the servers has a say in company management. A human hacker or some malware could pretend to be a million servers and outvote the legitimate servers in the network. When such takeovers of traditional companies occur, the results can vary. With a DAE, the results will most likely be disastrous. Once that malevolent entity controls our distributed Web hosting company, it could cash out. Or it could release the private data from other servers or hold the data hostage until we human owners paid a ransom.

Once machines have intelligence and the ability to learn, how quickly will they become autonomous? Will military drones and robots, for example, decide to turn on civilians? According to researchers in AI, we're only years, not decades, away from the realization of such weapons. In July 2015, a large group of scientists and researchers, including Stephen Hawking, Elon Musk, and Steve Wozniak, issued an open letter calling for a ban on the development of autonomous offensive weapons beyond meaningful human control.[53]

"The nightmare headline for me is, '100,000 Refrigerators Attack Bank of America,'" said Vint Cerf, widely regarded as the father of the Internet. "That is going to take some serious thinking not only about basic security and privacy technology, but also how to configure and upgrade devices at scale," he

added, noting that no one wants to spend their entire weekend typing IP addresses for each and every household device.[54]

We do not recommend broad regulation of DAEs and the IoT or regulatory approvals. We do recommend that managers and entrepreneurs who are developing apps identify any significant public impacts—good, bad, or neutral—and alter source code and designs. We think they should consult with those likely affected by their creations to minimize risks in advance, identify alternative paths forward, and build support.

9. BIG BROTHER IS (STILL) WATCHING YOU

"There will be many attempts to control the network," said Keonne Rodriguez of Blockchain. "Big companies and governments will be devoted to breaking down privacy. The National Security Agency must be actively analyzing data coming through the blockchain" even now.[55] While blockchains ensure a degree of anonymity, they also provide a degree of openness. If past behavior is any indication of future intent, then we should expect corporations known for spying and countries known for waging cyberwarfare to redouble their efforts because value is involved—money, patents, access to mineral rights, the titles to land and national treasures. It's as if we've placed a big bull's-eye on top of the Internet. The good news is that everyone will be able to see the shenanigans. Some may be highly motivated to "out" spying, because they bet on the likelihood of a particular regime's attacking the blockchain in a prediction market.

What happens to privacy when the physical world starts collecting, communicating, and analyzing infinite data that could dog an individual forever? In a 2014 presentation at Webstock, Maciej Ceglowski ranted about Google's acquisition of Nest, a maker of luxury thermostats with sensors that collect data about rooms. His old thermostat didn't come with a privacy policy. This smart thermostat could report back to Google, maybe even eat his leftover pizza like a sketchy roommate.[56] Many of us are already uncomfortable with a social media environment that tracks our whereabouts and barrages us with personalized marketing messages wherever we go. In the blockchain world, we'll have better control over such, but will we be vigilant enough to manage our media diet?

None of these privacy challenges are true showstoppers. Continued Ceglowski: "The good news is, it's a design problem! We can build an Internet that's distributed, resilient, irritating to governments everywhere, and free in the best sense of the word," as we wanted it to be in the 1990s. Ann Cavoukian of the Privacy and Big Data Institute outlined seven principles for design that are "good for business, good for government, good for the public." The first is critical: make privacy the default setting. Reject false dichotomies that pit privacy against security; every IT system, every business practice, and all infrastructure should have full functionality. Leaders need to prevent rather than react to violations, maintain transparency in all operations, and subject their organizations to independent verification. Brands will earn people's trust by respecting user privacy, keeping users at the center of design, and ensuring end-to-end security of their data, destroying it when no longer needed. She said, "It really is a win-win proposition, rejecting zero-sum and embracing positive-sum."[57]

Said Ceglowski, "But it will take effort and determination. It will mean scrapping permanent mass surveillance as a business model, which is going to hurt. It will mean pushing laws through a sclerotic legal system. There will have to be some nagging. But if we don't design this Internet, if we just continue to build it out, then eventually it will attract some remarkable,

visionary people. And we're not going to like them, and it's not going to matter."[58]

10. CRIMINALS WILL USE IT

In its early days, naysayers often condemned bitcoin as a tool for laundering money or buying illicit goods. Critics argued that, because the technology is decentralized, lightning quick, and peer to peer, criminals would exploit it. Chances are, you've heard of Silk Road, the dark Web marketplace for illegal drugs. At its peak in October 2013, Silk Road had 13,756 listings priced in bitcoin. Products were delivered by mail with a guide to avoiding detection by authorities. When the FBI seized the site, the price of bitcoin plummeted and digital currencies became synonymous with crime. It was bitcoin's darkest hour.

But there is nothing unique to bitcoin or blockchain technology that makes it more effective for criminals than other technologies. Authorities in general believe that digital currencies could help law enforcement by providing a record of suspicious activities, maybe even solving a multitude of cybercrimes, from financial services to the Internet of Things. Marc Goodman, author of *Future Crimes*, argued recently, "There's never been a computer system that's proven unhackable."[59] Opportunities for crime have scaled with technology. "The ability of one to affect many is scaling exponentially—and it's scaling for good and it's scaling for evil."[60] So this falls under the category of human beings wanting to harm other human beings. Criminals will use the latest technology to do it.

However, bitcoin and blockchain technology could discourage criminal use. First, even criminals must publish all their bitcoin transactions in the blockchain, and so law enforcement can track payments in bitcoin more easily than cash, still the dominant payment medium for criminals. The old Watergate adage, "follow the money" to find the crook, is actually more doable on the blockchain than with other payment methods. Bitcoin's pseudonymous nature has regulators dubbing bitcoins "prosecution futures" because they can be tracked and reconciled more easily than cash.

After each mass shooting in America, U.S. representatives whose constituents and campaign funders are card-carrying members of the National Rifle Association are quick to say, "Don't blame guns for all the gun violence in America!" It would be very rich indeed if these same people banned blockchain technology because of the crimes some people might commit on it. Technology does not have agency. It does not want for anything or have an inclination one way or the other. Money is a technology, after all. When someone robs a bank, we don't blame the money that sits in the vault for the robbery. The fact that criminals use bitcoin speaks more to the lack of strong governance, regulation, advocacy, and education than to its underlying virtues.

REASONS BLOCKCHAIN WILL FAIL OR IMPLEMENTATION CHALLENGES?

So the obstacles are formidable. Looming in the distance is quantum computing, the cryptographer's Y2K problem. It combines quantum mechanics and theoretical computation to solve problems—such as cryptographic algorithms—vastly faster than today's computers. Said Steve

Omohundro, "Quantum computers, in theory, can factor very large numbers very rapidly and efficiently, and most of the public key cryptography systems are based on tasks like that. And so if they turn out to be real, then the whole cryptography infrastructure of the world is going to have to change dramatically."[61] The debate over technological innovation and progress is an ancient one: Is the tool good or bad? Does it advance the human condition or degrade it? As satirist James Branch Cabell observed, "The optimist proclaims that we live in the best of all possible worlds. The pessimist fears this is true."[62]

As the story of Lev Termen shows, individuals and organizations can use innovations for good and for evil, and that has been true across a broad range of technologies, from electricity to the Internet. Yochai Benkler, author of the seminal work *The Wealth of Networks,* told us, "Technology is not systematically biased in favor of inequality and structure of employment; that is a function of social, political, and cultural battles." While technology can change business and society dramatically and swiftly, Benkler believes it is "not in a deterministic way, one way or the other."[63]

In balance, the arc of technological history has been a positive one. Consider the many advances in food and medicine, from R&D to treatment and prevention: technology has made for greater human equity, productive capability, and social progress.

There is nothing to suggest blockchain couldn't fall into the same trap as the Internet did. It may be resistant to centralization and control; but if the economic or political rewards are great enough, powerful forces will try to capture it. Leaders of this new distributed paradigm will need to stake their claim and initiate a wave of economic and institutional innovation in order to ensure that everyone has the opportunity. This time, let's fulfill the promise. Which brings us to the issue of making all this happen.