Prologue

MONEY AND LIBERTY

> Anything that is in the world when you're born is normal and ordinary and is just a natural part of the way the world works. Anything that's invented between when you're fifteen and thirty-five is new and exciting and revolutionary and you can probably get a career in it. Anything invented after you're thirty-five is against the natural order of things.
>
> – Douglas Adams

On the third floor of the Time Warner Center in Manhattan, a glass-fronted mixed-use building that bifurcates as it rises into gleaming towers of luxury apartments, sat the upscale Italian restaurant A Voce. Like the 750-foot-tall building itself, completed in 2004, the restaurant was a symptom and symbol of post-9/11 New York City, the New York that three-term mayor Michael Bloomberg revitalized and sanitized. From the vantage point of someone high up in one of those extraordinary apartments, the green rectangle of Central Park – brown now, in late fall – spreads out northward in its manicured neatness like a welcome mat for money. It seemed laid out most of all for the new money – real-estate money, private equity money, technology startup money – that has poured into the city in recent years and set it gleaming, even as its middle-class residents have left in droves.

Like other restaurants of its kind, A Voce was routinely used

as a stage for client dinners, power lunches, and other indispensable set pieces of business theater. So it has ever been in New York. But the restaurant will enter history as the place where a small group of men have gathered in private to discuss the newest money of all. More than high-frequency trading, more than the Dodd–Frank Act, more than any new regulation, the subject at hand here, on this night, stands a better chance than anything else of unsettling the familiar world of finance. Past the hostess stand and coat check girl and through a door off the main dining room, a dozen or so men are drinking wine and snacking on hors d'oeuvres. It is 10 December 2013 and they are here to discuss Bitcoin, a digital currency and payment system that has grown rapidly from being the plaything of teenage anarchists to the talk of Wall Street.

The magic of Bitcoin is that it enables you to move money almost instantaneously from one side of the planet to the other without needing any bank, corporation, or government. Some of its proponents think it will alleviate poverty in developing nations, plugging everyone into the global economy. Others think it will make banks obsolete. Still others hope it will make governments obsolete.

In March 2013, Bitcoin's market capitalization – the total value of all bitcoins in existence – surpassed $1 billion for the first time. Now, two weeks before Christmas, it is $11.4 billion; units of the digital currency are trading at $948 each. With explosive growth has come intensified media scrutiny as well as greater enthusiasm from investors, hence the need for meetings like this one, to dispel rumors, fight the war of public perception, and spread the gospel. Inevitably, a few members of the press are here, making awkward, predinner small talk over glasses of pinot noir. Most of them are new to the subject, including a *Wall Street Journal* reporter who wrote his first column on Bitcoin less than a week earlier.

Tonight's master of ceremonies is Jeremy Allaire, a big, raw-faced man in a suit and open-collared shirt. He has flown in from Boston, where his new company, Circle Internet Financial, a Bitcoin startup, recently came out of stealth mode announcing

that it had raised $9 million of venture capital. Another star of the dinner is Barry Silbert, blond and boyish in his thirties, a brilliant investor and one of the youngest people ever to pass the Stockbroker's Exam. Six weeks ago, he launched a private Bitcoin fund now worth $63 million. Venture capitalist Jim Breyer, who led Facebook's first venture round, can be seen hobnobbing with reporters; so can a lawyer who represents Circle. His cuff links are coins that wink in the light.

Missing from the room, however, are any representatives of the very first wave of Bitcoin adoption, pioneers who risked their money, time, and freedom to build the early infrastructure of a new economy. The lucky ones have gotten rich. More than one, though, will soon find himself on the wrong end of a lawsuit or prison sentence. Two others live as expatriates in Panama. Yet another, a longtime resident of Japan, is preparing to renounce his American citizenship. Before spring, one chief executive will see his company – formerly the largest and most profitable Bitcoin exchange in the world – fall into ruin around him, and file for bankruptcy protection among accusations of incompetence and fraud. Others were disgraced long before.

Tonight, glass of wine in hand, looking out the window of the private dining room onto Columbus Circle where, high above the yellow taxis circling the roundabout, a thirteen-foot statue of Christopher Columbus stands on his pediment, I can't help but think of them, those absent pioneers, while talk of money, the invisible omnipresent animating force, goes on relentlessly around me.

When I first wrote about Bitcoin, in the summer of 2012, my editor at CNNMoney cautioned me not to treat it as anything more than a curiosity, at best a passing fad. By 10 December 2013, however, the computer network undergirding Bitcoin is more than 250 times faster than the combined processing power of the world's five hundred most powerful supercomputers. By the end of the year, the digital currency's value in US dollars will be fifty-six times higher than it was in January – the largest annual price growth, as far as anyone can tell, of any asset in history.

Why, then, one skeptic asks Allaire, shouldn't we dismiss it as

a scam or speculative bubble, as yet another Dutch tulip mania? The dramatic rise in value seems absurd, divorced from any fundamentals. 'I have a thesis,' Allaire tells him, 'which is that essentially the rising value of Bitcoin is a large put option, or a bet, that Bitcoin gets adopted as a medium of exchange.'

At bottom, that is, some people are willing to pay an exorbitant amount to own a single bitcoin, just as they would a single bar of gold or a single share in a highly valuable company, because they believe either that its value will increase over time or that it will be a stable store of value.[1] The total supply of bitcoin is finite, so the more that merchants and consumers use the currency, and the more they come to appreciate its benefits, the more desirable – and valuable – it will tend to become. Less than a week before the dinner, Bank of America currency strategists praised Bitcoin's potential for online commerce and estimated its maximum market cap at $15 billion, or about $1,300 per bitcoin.

Some economists and commentators have been scoffing at the idea that a digital currency – a form of commodity money that exists only online, with no central bank or government backing – could ever be widely adopted as a method of payment, much less replace a national currency like the Argentine peso. Worse, to many institutions Bitcoin looks like reputational poison. It may well be the biggest development in finance since the banknote, but it has already weathered more than its fair share of scandal. In late 2013, the biggest headlines it has yet garnered connect it intimately to the online black market Silk Road.

But to others, Bitcoin looks like what money has always aspired to be: a means of exchange that is endlessly divisible and instantly transferable; a store of value that is less like gold than like the essence of gold, the value itself apart from the dead metal, stateless, rootless, weightless, capable of traversing the whole earth as easily as a mile, moving capital to where it is most needed, like a man in Nantucket flinging out a handful of seeds to make flowers bloom in the African desert. Bitcoin looks like money's dream of itself. 'We're talking about a global currency here,' Allaire says at the dinner. 'We're not talking about what's interesting as a speculative investment.'

In fact, Bitcoin is a triple threat to established markets, because it can function as a store of value, like gold; as a method of payment for online commerce, like credit cards or PayPal; and as a global transaction network, like Western Union or MoneyGram. There are about $7 trillion dollars' worth of gold in the world today. E-commerce is a $1.2 trillion industry. And remittances – the practice of workers, usually recent immigrants, sending a portion of their pay back home to their families in another country – are a big source of revenue for many countries, including India and China. According to the World Bank, a total of $542 billion in remittances flowed to nations around the world in 2013. India alone received $70 billion, more than the $65 billion earned from exporting the software services for which the country has become known.

Barry Silbert, who has a knack for spotting investment opportunities at just the right time, knows what it would mean if the digital currency were to claim even a small percentage of any of these markets, never mind all three. Earlier in December, a pair of analysts at Wedbush Securities made an even more dramatic prediction than Bank of America's strategists, estimating that a single bitcoin could one day be worth $98,500. Bitcoin's current price, they thought, reflected only 'a peak penetration of one percent of total potential demand in ten years'. Barry, meanwhile, has been meeting with Wall Street guys – hedge fund executives, forex traders at large financial institutions, portfolio managers, and others – who have already invested personally in Bitcoin, whether through Barry's own fund or by some other means. It appears to be only a matter of time before their firms follow suit. 'We're three to six months away from Wall Street dollars moving into Bitcoin in a big way,' he tells us. In fact, the move is already beginning. But few of the assembled journalists seem to pay much attention to his words. The *New York Times* reporter has already left. As for me, though, I'm hooked. There is nowhere else I would rather be.

AT THE TIME OF THAT dinner, I was a staff editor at *Entrepreneur*, and I became convinced that the remarkable Bitcoin entrepreneurs I had met were at the forefront of something revolutionary. Each

of them was a fascinating character in his own right, and each had his own agenda for Bitcoin. Even in the collegial early days, when Bitcoiners gathered on online forums to share news and gossip, to philosophize, announce their startups, and encourage each other in what they often couched as a collective effort to build a new financial paradigm – even then it was obvious that there were differences of opinion, some of them markedly divergent, and it wasn't long before those differences began to express themselves in business ventures.

One leader who emerged, Roger Ver, was already a millionaire by the time he discovered Bitcoin in 2011. He soon became one of its biggest boosters, investing in more than a dozen startups and turning a huge amount of his personal wealth into digital currency. When its value soared, so did his net worth. A hardcore libertarian, he saw Bitcoin as an antidote to government coercion and taxpayer-funded wars.

Charlie Shrem, a middle-class Jewish kid from Brooklyn who dreamed of joining the tech boom, cofounded one of the most successful early Bitcoin startups – the first to receive more than $1 million in venture capital. But he couldn't handle its rapid growth, and later found himself charged with laundering drug money for users of Silk Road. His right-hand man, Erik Voorhees, made a pile of cash by selling a Bitcoin gambling website and went on to operate another digital currency startup down in Panama. But he got in trouble with the US Securities and Exchange Commission (SEC) for selling unregistered securities.

A later pioneer, Nic Cary, one of Erik Voorhees's old college fraternity brothers, was recruited by Roger Ver to be the chief executive of a tiny Bitcoin startup whose main competitor had the backing of one of Silicon Valley's most prestigious venture capital firms. He saw Bitcoin as a tool of financial inclusion – a means of plugging people in developing countries into the global economy. He fought like hell and turned his underdog company into one of the fastest-growing startups in the world, outsmarting regulators along the way.

Barry Silbert, too, had to reckon with unfriendly regulations.

A former investment banker, he could have been a billionaire if his ethics hadn't gotten in the way. For him, Bitcoin looked like a life raft in a world awash in debt. And it offered a chance to save his brokerage firm, in the process making digital currency a mainstream asset class.

The deeper I dug into the subject, the more obvious it became that, just as the digital currency revolution promised to make itself felt around the world, so the story of Bitcoin intersected with some of the largest issues and events of our time: the financial crisis and Great Recession, the reining in of Wall Street, the Silicon Valley startup culture that now informs global capitalism, and the rise of the digital economy which has occurred alongside, in the developing world, a continuing lack of financial inclusion and, in developed nations, a government criminalization of business that hobbles entrepreneurs at every turn.

If Bitcoin's early proponents were united by anything, it was a fierce vision of progress. More than most technologies, Bitcoin starkly illuminates competing ideas of money and liberty, competing visions of – as the title of a book by Ludwig von Mises, a favorite economist of early Bitcoin advocates, would have it – human action. Like the Internet, which also invited mockery in its early years, Bitcoin enlarges the scope of what is possible. With its advent, contrarian theories about privately issued currencies, cross-border trade, and economic justice – theories which were, however, politically impossible to put into practice – could finally be tested.

If Bitcoin is a financial innovation deserving serious consideration, it is also a sign of the deep weirdness of which the Web is capable. The Bitcoin software is open-source, meaning that anyone can inspect the code that makes it function, unlike the software created by most for-profit companies. Satoshi Nakamoto, Bitcoin's pseudonymous creator, designed it that way, and the practice has been continued by the developers who took over from Satoshi when he walked away for good. They are continually alert for bugs that need fixing, improvements that should be made. Consequently, Bitcoin is a living, breathing piece of technology. And it is, in some senses, a grand experiment, still in beta testing.

Consequently, at the dinner in December 2013, it dawned on me that not even the men in that room could say with certainty what Bitcoin would look like in a few years. Indeed, we have now arrived at a point where partisans on all sides are in open conflict over the future of Bitcoin, distributed networks, and money itself. The stakes are high enough that *The Economist* has taken notice, reporting that a 'civil war' has broken out between 'two competing camps of developers and Bitcoin companies . . . One side wants to keep Bitcoin smallish and pure; the other is pushing for it to grow rapidly, even if this means turning it into something more like a conventional payment system.'[2]

This conflict will likely be resolved in time. But larger differences will remain. Some Bitcoiners see digital currency as a business tool, a way to grease the wheels of globalization. Others see it as a way to ensure the financial rights of individuals, or a weapon to wield against the Federal Reserve. Still others treat it merely as electronic cash for buying all kinds of contraband – drugs, guns, and worse.

By 2016, many technologists who were uncomfortable with Bitcoin's checkered reputation were doing their best to change the conversation, speaking more generally of 'cryptocurrency' or 'blockchain', the technology underlying Bitcoin's payment system. To be clear, however, there is only one cryptocurrency that has become a household name. In the late spring of 2016, following a slow rise in value after a sustained period of lower prices, the price of Bitcoin went on a tear, hitting $720 and again boosting the currency's market cap above $11 billion. Few would be arrogant enough to claim that they know what it will do next. But to date, Bitcoin has proved its resiliency many times over.

Critics have pointed to its extreme price volatility, perceived drawbacks in its technology, and its use by criminals as reasons it will eventually fail or be regulated out of existence. Others are more optimistic. 'If Bitcoin has attributes that cause its downfall, for whatever reason, then I guarantee that the next batch of cryptocurrencies will not have that problem,' says Adam Levine, the host of a popular Bitcoin podcast, 'because the prize for creating the

thing that becomes the next Bitcoin is unfathomable.' Satoshi Nakamoto, whoever he was, created billions of dollars of value out of thin air.

But how was this possible? And, for that matter, why was an apparent outsider like Satoshi able to achieve this breakthrough when it had eluded the world's biggest technology firms as well as other cryptographers and coders? How did an invention that a few years ago was taken seriously by practically nobody come to be on the lips of people as different as 50 Cent and Bill Gates, the latter of whom, in October 2014, called it 'exciting' and said it was 'better than currency' for moving money around?

For that matter, just how large an effect will Bitcoin have? Already the companies founded upon it are growing by leaps and bounds. After ignoring it for the first few years of its existence, major investors – venture capital firms, Goldman Sachs, the New York Stock Exchange, and billionaires like Richard Branson and Peter Thiel – have decided to risk more than $1 billion of investment capital on digital currency businesses. And the innovations it has inspired are proliferating. The impact of cryptocurrency, it now seems clear, will not be confined to the worlds of finance and commerce but will be felt also in the realms of digital identity, citizenship, taxation, property rights, surveillance, privacy and contract law, and corporate governance. And yet, even as its users reap the benefits, it is making them – and the global economy – vulnerable in new ways, helping cybercriminals to reap hundreds of millions of dollars a year in profits from victims all over the world.

This is the story of how a niche technology gained global attention, and what happened to the pioneers who took it up and used it to advance their own agendas, altruistic or otherwise; a story about a handful of smart people risking everything – their livelihoods, professional reputations, homes, and liberty – to gamble on something they thought would change the world.

This book is also an attempt to reckon with what the future might hold for the rest of us. After all, not only vast sums of money but our ideas about money itself may be at stake. The

public Internet has been with us for barely more than one generation, and already there are people who believe that broadband access is tantamount to a human right, so necessary has the Web become as a source of information and economic opportunity. If money is a form of speech, and the US Supreme Court decision in *Citizens United v. Federal Election Commission* holds that it is, then it may be only a matter of time before access to the best form of money – the most effective means of monetary communication – is also considered a fundamental right. Then Bitcoin, or whatever takes its place, will have been fully assimilated into the social contract.

But it was a renegade ideology that got there first, long before any Wall Street banker or Washington regulator had seen the potential (or the potential danger); it was a bunch of outlaws who broke open the frontier on which so many warring parties now want to stake their claims. Bitcoin began not in the unobjectionable light of day but in the shadows, among cryptographers, hackers, Free Staters, ex-cons and drug dealers, teenage futurists and entrepreneurs – heterodox thinkers all, dissenters from consensual reality, holders of grudges against big government and big banks, people committed to stoking the fires of creative destruction. Hephaestus fires: able to melt down and forge anew. It is because of them that any of us have heard the word 'Bitcoin'. For a long time, Bitcoin was their world. We've just moved into it.

Chapter 1

MAKING MONEY

> A feeble man can see the farms that are fenced and tilled, the houses that are built. The strong man sees the possible houses and farms. His eye makes estates, as fast as the sun breeds clouds.
>
> – Ralph Waldo Emerson

Bitcoin came into the world fully formed, like Athena from the head of Zeus. It was announced on an Internet mailing list for cryptographers in the fall of 2008 by somebody calling himself Satoshi Nakamoto – an event that some day, if Bitcoin endures, may rank in the annals of invention alongside that moment on 10 March 1876 when a former teacher of deaf children, Alexander Graham Bell, who had already helped his father to disprove the commonly held belief that the deaf could not learn to speak, followed this miracle by forcing electric current to carry the sound of a human voice.

Like Bell, Bitcoin's pseudonymous creator must have spent years on his invention, working long hours against long odds to give people something they didn't even know they wanted. He did it all backwards, writing the code in order to convince himself that it was possible, that it wasn't just a pipe dream, before writing the paper that laid out the concepts realized by the code. When a famous cryptographer, Hal Finney, asked him to provide a detailed explanation of the Bitcoin protocol, complete with algorithms and

details of the data structures involved, Satoshi said it would take less time simply to release the first version of the software. Like everyone else, he had seen earlier attempts to create electronic cash go nowhere, or hit a dead end. So enough with theory and spec papers, he figured. He didn't just want to tell them it *could* work. He wanted to show them it would.

'I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party,' Satoshi's announcement began. It was 2:16 P.M. Eastern Standard Time on the first day of November and he was telling everyone on the mailing list that he had figured out how to do for money what the Internet had already done for information – set it free as bits and bytes, without gatekeepers, making financial transactions as painless as email. He wanted his peers to know before anyone else.

To explain his invention, Satoshi had prepared a white paper, in which he outlined the features of Bitcoin that were technical advancements on earlier forms of electronic money. It would be decentralized, meaning that a network of people running the Bitcoin software would assume the dual role of a mint, producing the currency, and a central clearinghouse, reconciling and recording transactions. This arrangement was revolutionary. Until the invention of Bitcoin, nobody had managed to overcome without a trusted third party the central stumbling block of electronic cash, which was known as the 'double-spending problem'. With physical cash – US dollars, say – it is easy to prevent someone from spending the same bill twice. If you hand your friend a $10 bill, everyone can plainly see that she, not you, now possesses the ten dollars. You have spent it and can't spend it again. Moreover, cash transactions are irreversible: once you have given your $10 away, you can't get it back without your friend's consent, unless you take it by force. Because cash has a socially agreed-upon value, and because cash transactions are final, it allows two parties who don't trust each other to do business – making it useful for criminals and other untrusting types.

Electronic money, on the other hand, is like any other electronic data; it can be copied and distributed ad infinitum. This is

advantageous when you want to send an important file to your boss while retaining the original on your own computer, but it's absolutely ruinous when you want to establish a payment system. Imagine sending $10 of digital money to someone to settle a debt. Because you still have a perfect copy on your computer, what would prevent you from spending the same $10 again and again? It would be like counterfeiting, only worse, because each copy would be identical to the original. Like a man who, much to the chagrin of his genie, has cannily wished for infinite wishes, the bearer of electronic cash would be the richest man alive – if only his digital wealth weren't worthless, since nobody in their right mind would accept payment under these terms.

Before Bitcoin, the solution to the double-spending problem was simple, though with unfortunate side effects: employ a trusted third party. This is the role played today by PayPal, Venmo, and every other online payment processor. The company acts as an authority to verify transactions, debiting a balance from one customer's account and crediting it to another's account, and keeping track in its central ledger of where the money goes. Users trust these services to keep an accurate record of transactions, so that no double payments are possible. In so doing, users give up control over their money. The third party – PayPal, say – can choose to reverse any transaction at any time, and can even freeze customer funds if it finds cause. The final judgment call rests with PayPal, just as credit card chargebacks are at the discretion of the credit card company. Worse yet, the security and integrity of the entire payment network depends on the company operating it. Even as the once-novel idea of 'online shopping' gave way to a booming global e-commerce sector, then, there was still no way to replicate over the Internet the direct, ancient, peer-to-peer experience of money changing hands, finally and irrevocably.

Satoshi Nakamoto devised a way for people to spend digital cash permanently, and for everyone else to be able to check the validity of each transaction. Each bitcoin, as it passes from one person to another, is digitally signed by the person transmitting it. A coin therefore becomes, in Satoshi's phrase, 'a chain of digital

signatures' – a record of ownership, like a logbook signed by each person who has ever held the coin. When you wish to transfer to your friend a coin you received from Satoshi, your friend can verify that you truly own the coin by checking that Satoshi's signature on the previous transaction is legitimate.

But this on its own, Satoshi knew, would not be enough to solve the double-spending problem without relying on a bank or other central authority. He went further, requiring that all transactions be publicly broadcast to the entire network running the Bitcoin software, so that anyone with an Internet connection, at any time, might check an enduring record of every transaction that had ever taken place. One could even, at least in theory, trace every single coin back through all its transactions to the moment when it was first created. (This would be difficult for a layman, and actions could be taken to obfuscate the source, but it would be possible.) It was in the rules of Bitcoin creation – a process known as mining – that Satoshi pulled off his most impressive feat, simultaneously establishing a decentralized mint for the cryptocurrency and nailing the lid shut on double payments.

When one person sends bitcoins to another, that transaction is broadcast to every node of the network, spreading worldwide from its point of origin. Each node that receives the transaction broadcasts it still further, amplifying the signal, as it were, so that in a very short time the transaction has been acknowledged by the entire network. If that person were to attempt to spend the same bitcoins twice, the second transaction would likewise be beamed out to the network, but the first would have such a huge head start on the second that it would be all but impossible for the fraudulent transaction ever to catch up, like a runner trying to win the hundred-meter dash after giving his opponent a fifty-meter lead.

But now suppose that a minority of judges are unable to see the first runner, the one who is in the lead. They might think the second-place runner deserves the gold medal. Just so, it is entirely possible that some nodes on the network will receive the second transaction first and broadcast it as being legitimate. By then, however, a majority of nodes will have already accepted the

original spend and begun processing it into a batch of transactions known as a block. When that block is completed, it is added to the public ledger – the blockchain – and everyone begins processing the next block. Each block builds on all the blocks that came before. Even if some computers are processing a competing block that contains the fraudulent transaction, the blockchain containing the original spend will end up being longer, because it has a majority of the network's processing power building it. Soon, the entire network will accept the longer blockchain as the true blockchain. As long as honest miners control at least fifty-one percent of the network's processing power, Satoshi wrote, 'the honest chain will grow the fastest and outpace any competing chains.' The judges with imperfect vision can accept the majority decision of the other judges as to the winner of the race.

Processing and verifying transactions requires tremendously difficult computer calculations, analogous to factoring prime numbers. To reward those dedicating computer resources to the difficult process of verifying transactions, Satoshi decided that whoever solved the complex math problems required should be given new bitcoins. It would be a winner-takes-all race by every active node of the Bitcoin network. Every ten minutes, the race would begin anew. Like oil or gold, bitcoins have a limited rate of production and an upper limit on their supply. Every ten minutes, a new block of transactions is added to the blockchain; every ten minutes, a new batch of coins is created mathematically, like gold dug out of the ground. But where gold miners use manual labor and heavy equipment, with Bitcoin miners, wrote Satoshi, 'it is CPU time and electricity that is expended.' The ultimate limit is twenty-one million coins, though each coin is divisible to eight decimal places, or one hundred millionth of a bitcoin. Like an oil well running dry, the supply of bitcoins will one day be depleted. As with other commodities, Satoshi knew, this scarcity would tend to drive up the price over time, assuming people found it worth using. Through cryptography, he had found a way to emulate the properties of a physical commodity. In the words of *The New*

Palgrave Dictionary of Economics, Bitcoin 'allows for the first time the final transfer, not the mere copying, of digital assets in a way that can be verified by users without trusting other parties'. Those who understood it at its inception were astounded. Here at last was the solution to a problem that had bedeviled computer scientists for years.

So far, so elegant. But if all transactions are public, what then becomes of financial privacy? Here Bitcoin is counterintuitive. With a bank, privacy depends not on hiding the fact that you have an account at Wells Fargo or Chase but on keeping to yourself the amount of money stored there. Bitcoin reverses the relationship. Anyone can see how much money is being held at a given address, but nobody knows to whom the money belongs. This works because Bitcoin addresses are strings of random letters and numbers, with no identifying personal information attached. This, too, was revolutionary, allowing people who neither knew nor trusted one another to do business over the Internet without revealing their identities. Anonymous donations to nonprofits would be possible; so would hard-to-trace drug deals. Even if it were necessary to reveal some personal information in the course of a transaction, say in order to take delivery of a physical product ordered online, the customer could simply generate a new Bitcoin address for each new transaction. With no single address revealing their purchase history, and nothing to link their several addresses to each other, they could maintain their privacy.

Cryptographers spend their professional lives studying and creating techniques to keep communications private even when they are being spied on. Their field sits at the intersection of computer science, mathematics, and electrical engineering. The best of them are not easily impressed. Before introducing Bitcoin to his peers, Satoshi was surely braced for criticism. But he may not have expected the chorus of disbelieving voices that rose up to shout him down. 'I've noticed that cryptographic graybeards tend to get cynical,' one member of the mailing list would later relate. 'When Satoshi announced Bitcoin on the cryptography mailing list, he got a skeptical reception at best.'

One of the earliest respondents voiced doubts that Bitcoin could scale up to meet the needs of a large population. But the writer prefaced his critical remarks in a way that made it clear he hoped to be proven wrong. 'We very, very much need such a system,' he told Satoshi.

A resident of the San Francisco Bay Area, who uses the name Ray Dillinger in computer programming circles and has a background in software quality assurance, accused Satoshi of failing to account for the increase in mining power that improved computer hardware would bring over time. A well-known computer science principle, known as Moore's Law, says that computer processing power tends to double approximately every two years. Faster computers would mine more coins than expected, leading to a glut of new money, driving down the value of the existing supply. (It is worth noting that the same thing happens when central banks such as the Federal Reserve increase the money supply, which is why $40,000 in 1975 had the same purchasing power as $176,221 in 2015.) An annual inflation rate of thirty-five percent for Bitcoin 'is almost guaranteed by the technology', Dillinger wrote.

But Satoshi had accounted for that. He explained that his system was designed to keep coin production constant by linking people's efforts to mine new bitcoins to the difficulty of the mining function itself. The more processing power miners brought to bear – in order to crunch the numbers quickly and produce higher yields – the more difficult it would become to solve the math problems that generated the bitcoins. Moreover, the difficulty was designed to increase over time no matter what, keeping pace proportionally with improvements in computer hardware predicted by Moore's Law. That was how Satoshi could be confident not only of the total number of bitcoins that would ever be created – twenty-one million – but of the number of new coins that would be created every year in the future, with the last fraction of a coin being mined in the year 2140.

'The fact that new coins are produced means the money supply increases by a planned amount, but this does not necessarily result in inflation,' he told Dillinger. 'If the supply of money increases

at the same rate that the number of people using it increases, prices remain stable. If it does not increase as fast as demand, there will be deflation and early holders of money will see its value increase.' That last statement was particularly important because, almost like a pyramid scheme, it gave people an incentive to buy into the idea as early as possible. And it would prove to be prophetic.

Another objection was more fundamental. Satoshi, whoever he was, appeared to have built a financial weapon against central banking, against the ability of governments to issue money and regulate their economies, and was explaining to his peers, in a calmly confident way, its destructive potential. Who did he think he was, to act as if a mere 31,000 lines of code could cut a Gordian knot that had persisted for decades? And even if Bitcoin *was* a game-changing invention, was it right of him to have invented it? After all, Satoshi didn't put Bitcoin to a vote. Like other creators in the Internet age, he simply wrote the code and released it into the digital scrum of the Web, where it would flourish or not to the extent that people found it worthwhile. 'You will not find a solution to political problems in cryptography,' one correspondent admonished.

It was a charge that would be echoed in various forms and in various forums over the next several years, and one that Satoshi had surely anticipated. Bitcoin, he replied, would at least allow its users to 'win a major battle in the arms race and gain a new territory of freedom for several years'. He had noticed that governments and entrenched corporate interests were quick to demolish any threat to their monopolies, just as the music industry had prosecuted Napster, the early music file-sharing service. But how do you stop a leaderless network whose members are spread across the globe? No one knew who Satoshi was. If there was no central, identifiable figure to serve with a lawsuit, or to arrest and imprison, the government would be at a loss for how to stop Bitcoin.

By the fall of 2008, the folly of launching an alternative currency seemed obvious to most people. Although developed nations were moving steadily toward a cashless future, alternative currencies, much less true digital cash, anonymous and stateless, seemed like

science fiction. The field was littered with the bodies of those who had tried and been cut down.

ELECTRONIC MONEY IS ALREADY HERE; in fact, it has been around for decades. Most of the money in the world now exists in electronic form. Although digital currency as conceived by Satoshi Nakamoto and his predecessors is a radical invention, banks were not slow to adopt electronic money. By the mid-1990s, the Clearing House Interbank Payments System, or CHIPS, a clearinghouse for large transactions denominated in US dollars, was moving $1 trillion a day in electronic payments.[1] Owned and used exclusively by big banks, CHIPS makes it easy for American Express, Santander, Deutsche Bank, and other financial institutions to settle their accounts without ever touching cash.

Consumers aren't privy to CHIPS, but they have access to electronic money through debit cards, prepaid phone cards, metro passes – to say nothing of mobile payment options offered by Apple and Samsung. By 1994, the Japanese phone company NTT had already sold 330 million prepaid phone cards.[2] While useful, not to say increasingly ubiquitous, however, these forms of payment have what some consider serious downsides. Electronic money is linked, by law, to a huge amount of identifying information – typically in the United States a person's name, date of birth, Social Security number, geographic location, and transaction history. The government can access this information, and banks sell it to advertisers. Card companies also hold this information on their customers. That means the familiar oligopoly of Visa, MasterCard and, in the US, American Express, present huge targets for cyber theft; hackers stalk them like big-game hunters hoping to bag a lion.

Having millions of people's financial information held by a handful of corporations would be worrying enough. But in fact every retailer that processes card transactions is a possible site of identity theft. The system requires consumers to trust retailers and websites of all kinds, some of which have minimal security, to safeguard their information. Add to that many consumers' habit of using weak, easy-to-remember passwords for their personal