THE SATOSHI REVOLUTION: THE REVOLUTION OF RISING EXPECTATIONS
by Wendy McElroy

ACKNOWLEDGEMENTS

First and foremost, I wish to thank Roger Ver for the confidence he placed in *The Satoshi Revolution* and for the generosity with which he treats me and everyone else with whom he works. He is the rarest sort of visionary; one who translates his vision into reality.

Too many people at Bitcoin.com assisted in the serialization of an early version of *The Satoshi Revolution* for me to list them all, but some cannot go without mention. Mate Tokay is a masterful coordinator for all things Bitcoin.com and for preserving both the wider context of the operation as well as its minutia. Editor-in-Chief Nanok Bie's decades in journalism was invaluable. Marcel Chou is a patient editor who has become a trusted friend and sounding board. What I've come to call "the Bitcoin Guys" never once tried to influence the theories being tested and hypotheses floated in print. I thank them all.

Jeff Tucker, author of the Preface, has been a highly valued associate of mine for many years; he could not have been more encouraging about the articles as they appeared. To his credit, Jeff caught on faster than I did to the extraordinary implications cryptocurrency has for freedom. My evolution to understanding also owes a debt to other people too numerous to list. The most prominent among them are noted intellectual-property attorney Stephan Kinsella and President of the Satoshi Nakamoto Institution Michael Goldstein.

I had another great stroke of fortune during *The Satoshi Revolution.* Out of the blue, Dr. Peri Dwyer-Worrell emailed me with an offer to proof my articles. I have always been cavalier about matters such as the placement of commas in the belief that only the ideas are important. Peri proved me wrong and, in the process, she made me a better writer. I am grateful for finally coming to care about punctuation and for knowing this fine woman.

No dedication is complete without an expression of my ever-enduring thanks to Bradford, my husband, who is the indispensable framework for all I do.

TABLE OF CONTENTS

INTRODUCTION

PREFACE

by Jeffrey A. Tucker

The world has needed this book to give the big picture of the revolution taking place, and Wendy McElroy is exactly the person to write it. Her work has been steeped in the history of liberty and the struggle against authoritarian control. She has tracked that struggle from the 19th century to the present, having written pioneering articles and books on the full range of human experience. In *The Satoshi Revolution*, she has turned her attention to what I'm convinced is one of history's most momentous innovations: cryptocurrency and related services and assets. She explains how, in our own time, this technology portends fundamental changes, great changes, in the relationship between the individual and the state. In the last ten years—historians of the future will note this—we've observed the creation of a new monetary and financial architecture that could serve as a replacement for everything that's been known and used in the lifetime of every living person.

We've experienced a useful and secure money that works all over the world, is not connected to the state, and doesn't need the existing banking system. This same system can serve as a replacement for all existing payment systems that use national monies. This money is a purely market creation that adds to traditional accounting and store-of-value functions one additional feature: it is also a global peer-to-peer means of payment.

A decade ago, even high-level theorists said this couldn't happen. Then it did happen.

We've seen the creation of smart contracting systems that can manage a vast number of human deals, commitments, and interactions. Even people who accepted that Bitcoin was real doubted that Ethereum could achieve this. But it happened anyway.

We've even observed how this system has become a tool for raising capital and replacing traditional lending functions. Three years ago, this was merely a

speculative idea. Then it became a one-hundred billion dollar reality, and new forms of capital being raised through tokenization.

Seemingly out of nowhere, we have now an entire suite of technology that could conceivably displace and even replace national money, traditional payment options, and even regulated capital markets, and bring something new.

You are reading this and thinking: here we go again with crypto-utopianism. But here's the thing. It's not just theory anymore. These technologies exist in real time, even if only in their beginning stages. This is why there are so many Bitcoiners out there who speak so exuberantly about the future. They have already experienced it. They are drivers of Maseratis on roads filled with Model Ts and they know it. An improvement over the status quo that is this impressive won't be suppressed.

You might not have used any of these new technologies. That's fine. With all the failings of the current system, the old structures do get the job done. So long as there is no great crisis in the system, people are confident in it. There is no strong reason to switch, even if the new system is more secure, faster, more democratic, more inclusive, less risky, and less compromising of personal privacy. Still, the old system enjoys the momentum that comes from the network effect. Everyone else uses it, so you keep doing so.

Regulation Is Key

There is another factor that is holding back the switch from old to new. Regulations are trying to force the new technology to behave like the old technology. In the US, to buy Bitcoin or any cryptocurrency, you are required to comply with know-your-customer regulations, giving up every detail about your person. Any money you make from upward price movements in your new asset must be reported and you must pay taxes on it. Companies that want to assist in onboarding and offboarding crypto to fiat have to register with government as money exchanges. And with the capital-raising functions of blockchain technology, the regulators are threatening to shut them all down and make them behave like traditional securities.

I've watched as these regulations, gradually imposed and arbitrarily enforced, have introduced an element of fear in a fearless technology, distorting the sector and making it less innovative and competitive. Every time a new use of distributed networks is revealed and begins to catch on, some bigwigs emerge from on high to warn about compliance with decades-old laws designed for a different technology.

Consumers are scared and the end-user experience is not improved as much as it might have been in the absence of huge compliance costs. I've seen how legal uncertainty has caused merchants and consumers to lose access to a variety of services. I've seen entrepreneurs put their plans on hold pending some administrative edict coming from Washington, DC.

How much further along we would be in the absence of these interventions? It’s impossible to see the innovations we have not experienced. We only know that things would be different. But once you consider just how different, the reality becomes something beyond awesome. And yet it is not to be.

How Long the Delay?

Consider what happens when power is deployed to stop the progress of a new technology. Does it really ever work over the long term? To answer the question, we have to engage in counterfactuals.

Imagine if governments in Europe had cracked down to stop the printing press. What if cities around the world had banned the automobile? What would have been the fate of railroads, domestic electric lighting and indoor plumbing if special interests had suppressed them in order to favor prevailing technologies?

We can only guess because none of this really happened. It’s true that not everyone welcomed the printing press. Scribes in monasteries worried about the future of their talents. Some people wondered if the old faith could survive people having access to the ancient texts. But for the most part, the advent of printing was seen as a welcome innovation. So too with internal combustion, lighting, and plumbing. Some people were slow to adopt it, to be sure, but governments mostly let the innovation happen.

What if they had not? Does anyone really believe that these innovations could have been stopped and not merely slowed? I don’t think so. There are cases in history when grants of government monopolies delay competitors from going to market with improvements. This happened with the steamship in England, airplanes in the US, and some software applications in the last decades. But these delays are temporary; patents expire and history moves forward.

Regulations are different. Entrepreneurs have to innovate around them. Gray and black markets emerge. Risk takers deal with running afoul of the authorities. But eventually, something gives. Consider, for example, the results if every Lord and Baron in Europe in the 12th century had banned the horseshoe. Do you think that would have stopped the implementation of that technology for centuries? Highly doubtful, and the reason is fundamental: ideas are more powerful than governments. Eventually the costs of enforcement vastly exceed the benefits to the existing ruling class.

A Cryptoized World

In light of what we’ve seen over ten years, here's a thought experiment I've been toying with. It occurred to me while daydreaming as my tax attorney was going on at length about the taxable events in the regular dealings with crypto. I was considering just how incompatible these impositions are with a technology that emerged from and operates within a framework of perfect freedom.

Some legislatures have come to understand this. Wyoming, for example, has exempted crypto from all taxation, defined certain tokens in a way that make them exempt from securities law, and made special provisions for corporate forms that are distributed, among other changes. The legislature did its best to make the state attractive to this new industry.

Now let us enter into the realm of fantasy. Let's say that the U.S. Congress passed legislation that exempted all cryptocurrencies, cryptotrading, and cryptoassets from all taxation and regulation. The legislature establishes complete laissez faire in this sector, while everything else in the regular world (the dollar, the Fed, the SEC, the Treasury, and everything else we know) stayed the same.

What would you expect to happen? Ten years ago, had Congress done the same thing, not much would have changed, obviously. The technology didn't exist, and we didn't really know that it could exist.

What would happen today if all interventions around this technology were repealed? You are no longer punished for buying and selling in crypto, floating new tokens, putting out new applications in smart-contracting platforms, innovating new payment systems and so on. Companies could tokenize rather than float stock. Businesses could pay in crypto and do their accounting in crypto and face no penalties. Consider carefully: you could keep a third more of your just earnings merely by switching to a better technology.

How long would it take before crypto economics mostly replaced everything else? If this legislative change actually happened—and no it obviously will not—we might observe the wholesale displacement of old-world economic and financial systems with 21st century systems, and maybe it would happen much sooner than anybody would expect, perhaps 12 to 48 months, provided the crypto infrastructure could scale in time to meet the new demand.

Forcing the Present Into the Past

Now, if this thought experiment is correct, there are some mighty implications. It suggests that the financial and monetary world as it exists today is really being held together by force that is holding us to old forms. This force is imposing limitations and inefficiencies; it is literally keeping a vast infrastructure in place that otherwise would cease to dominate or even exist, and forestalling the onset of a new way of living. And this new way is not just about buying and selling. So central to our public lives are nationalized money and regulated capital markets that the advent of a cryptoized world would fundamentally change the relationship of the individual to the state.

Am i wrong to be slightly in awe of this realization?

Keeping a vast system alive solely by force does not strike me as sustainable over the long term. If you have a massive suite of technology that is waiting to take

over and is only being held back by purely artificial means, that does not bode well for the likelihood that the past can be forever preserved. The future cannot be forever put off even by the world's most powerful governments. Eventually ideas win out.

Wendy McElroy, from her past studies of history and her current deep dive into crypto-technology, understands the power of ideas. Bitcoin and all that is related to it is among the most revolutionary ideas in history. She demonstrates how they are going to transform for the better the structure of economics, politics, and human relationships generally. Getting from here to there is going to require the broadest possible understanding of what is happening. McElroy is the expert and erudite guide we've been waiting for.

JEFFREY A. TUCKER is Editorial Director for the American Institute for Economic Research and a former Director of Content for the Foundation for Economic Education. He is a managing partner of Vellum Capital: Blockchain Financial Management, the founder of Liberty.me, Distinguished Honorary Member of Mises Brazil, economics adviser to FreeSociety.com, research fellow at the Acton Institute, policy adviser of the Heartland Institute, founder of the CryptoCurrency Conference, member of the editorial board of the Molinari Review, an advisor to the blockchain application builder Factom. He is the author of many thousands of articles in the scholarly and popular press and eight books in 5 languages, most recently The Market Loves You. He speaks widely on topics of economics, technology, social philosophy, and culture.

INTRODUCTION

> You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete.
> —R. Buckminster Fuller

The revolution of 2009 went unnoticed by most people because it was peaceful, orderly, and technologically arcane. In 2009, Satoshi Nakamoto released open source software by which peer-to-peer transfers of digital wealth, called bitcoins, flashed over an immutable and transparent ledger, called the blockchain.

The familiar model of revolution is the toppling of an oppressive government by a popular uprising. But the bitter reality of history is that another government almost inevitably arises as a replacement—one as elite and brutal as its predecessor. The Satoshi model of revolution is different. It peacefully renders the old system irrelevant by out-competing it through a new technology and a private currency unlike anything seen before. Cryptocurrency moves seamlessly through a world without states or borders, obeying only the commands of individuals who choose to deal with each other. Transfers are pseudonymous with substantial privacy provided by encryption algorithms and hash functions. The blockchain is immutable and visible to all which makes it immune to corruption. Resistant to manipulation and inflation by government, crypto does not serve powerful elites at the expense of average people. bitcoin, or crypto in general, is the people's

money. (Note: The capitalized Bitcoin denotes both the currency and the blockchain; bitcoin denotes the currency.)

In an instant, with the first flash of transfer, the world changed forever.

Liberty Versus Power

Individuals suddenly had the weapon of self-defense that had been missing from their arsenal—a weapon that was necessary to win what the Austrian economist Murray Rothbard calls, “the great conflict which is eternally waged between Liberty and Power.” Individuals had a viable, private currency that allowed them to control their own wealth and become their own banks—to self-bank. At last, there was a practical path away from the manipulated fiat and the corrupt financial institutions that formed the basis of state power. (The words “state” and “government” are used interchangeably in this book.)

Bitcoin came at the right moment. Just two years before, the monetary monopoly had caused the devastating financial crisis of 2007-2008 across the globe. Bitcoin and the blockchain offered individuals a better system—one that served their needs, not those of the elite, and it promised the financial independence and control that is foundation of autonomy.

In his massive work *Conceived in Liberty* (Volume 2), Rothbard presents a broader view of why this freedom is essential. It is not only “a great moral good in itself” but also “the necessary condition for the flowering of all the other goods that mankind cherishes: moral virtue, civilization, the arts and sciences, economic prosperity.” Without a private currency and banking system based on Liberty, not Power, human potential was crippled.

Until Bitcoin, however, few prerequisites of liberty received as little attention from modern political activists as the need for a private currency and a private banking system that is accessible to everyone. Freedom fighters have marched and died under banners reading FREEDOM, TRUTH, and JUSTICE. No banner I know of has read PRIVATE MONEY, SELF-BANKING, even though these mechanisms are essential to fulfilling most other goals in life.

(Note: Money has three traditional uses. It is a medium of exchange, a store of value, and a unit of account. Crypto can serve all three functions, but the discussion here is limited to currency—the money in circulation as a medium of exchange.)

Economic autonomy is the bedrock of freedom without which other rights become problematic. Freedom of speech is irrelevant to a starving man. Freedom of association rings hollow to a woman who must endure physical abuse to feed her children. Due process is irrelevant to someone who cannot afford the medicine required to live another day. The fundamental need of every human being is to provide for his own survival. Only then can freedom follow, along with “moral virtue, civilization, the arts, and sciences.”

For years, the political vision of the individual or the team known as Satoshi Nakamoto flew under the public radar. Developed by crypto-anarchists and not backed by government decree or media attention, state authorities took no notice of the phenomenon; those who did notice sneered at it. They notice now, and the smirk has dropped from their faces. Banks and businesses now eagerly adopt and adapt the blockchain because they recognize its incredible power as a tool. There is a rush for patents in what used to be an open-source community. Traders are arrested for not being licensed. Exchanges are raided for not filing required paperwork on customers. Governments clamor to regulate the currency to control not only its profits but also the danger it poses to their monopoly on money.

Rothbard observes, "[L]iberty has always been threatened by the encroachments of power, power that seeks to suppress, control, cripple, tax, and exploit the fruits of liberty and production." Power is also threatened by liberty because the two dynamics enjoy an inverse relationship; that is, as one grows, the other shrinks.

No wonder Satoshi's vision of individual freedom through financial autonomy is under assault. The attacks include:

- Cryptocurrencies are said to be merely financial instruments and nothing about which to get politically excited. Calling them tools of self-defense in a battle between Liberty and Power is considered "anarchistic nonsense," and discussion of the subject does not even occur.
- Only criminals need financial privacy, it is claimed. Crypto users are drug dealers, tax evaders, sex traffickers and the like. Otherwise, why would they resist reporting to government? The accusation intimidates some users into remaining silent for fear of being considered a criminal a priori.
- Without regulation, massive fraud is said to be inevitable. This claim diverts attention from the massive fraud of fiat and central banking.

The preceding statements are examples of the sticks that are used to beat up and discredit crypto. None are valid but many are widely believed. And public belief tends to be translated into law whenever it benefits the state to do so.

The most dangerous attack on crypto, however, is the carrot—the promise of respectability. Even the crypto community is susceptible to this lure. Advocates want the blockchain and crypto to be as widely accepted as possible. The core advocates want acceptance to expand on an individual-by-individual, business-by-business basis, with all interactions being voluntary and extralegal. Others are less concerned with voluntaryism; they believe their holdings and investments will soar in value if governments and other monopoly institutions become users or guarantors of security. To these users, respectability is the key to increased profits, and profits are everything. They view advocates who run on about freedom as obstacles, fools, or both.

Unfortunately, "respectable" is often seen as a synonym for "state sanctioned," when the two terms should be antonyms. Bitcoin was needed precisely because

government and crony institutions, like central banks, are shameful; they loot average people down to rags and bones through currency manipulation, inflation, obstructive regulation, taxes, and other financial sleights of hand. The elites shut the people out of prosperity through licensing, patents, artificial credit, investment restrictions, monopolies, and other self-serving obstacles.

Governments are the problem, they are not the solution, and they never will be. “State sanctioned” should mean “disgraceful,” not “respectable.”

An added insult to seeking state sanction is the clear implication that freedom is *not* respectable, that freedom and respectability are in some way antagonistic and require the state as a referee. This is a false, dangerous dichotomy because the opposite is true, and it gives the state a foothold from which to expand, as it always does. Nothing is more respectable than the sight of human beings dealing peacefully with each other to mutual advantage. What governments inject into a free society is violence or the threat of violence, which is the end of freedom and civil society.

The stakes are high, both for Liberty and for Power. For Liberty: Privatizing their own wealth means individuals privatize their lives and determine the terms upon which they live. For Power: Governments and financial institutions lose their monopoly on money and wealth without which they are impotent.

It is in the nature of Power to tighten its grip whenever threatened. Power will attempt to centralize, regulate, ban, or otherwise dominate digital currencies and the blockchain. The attempts will fail, in part because of the decentralized nature of the technology, but a great deal of harm can be inflicted by a failing state. The technology cannot be stopped, but some of the individuals who use it can be persecuted, imprisoned, and broken. The victims’s surest protection is to keep Satoshi’s original vision of crypto clearly in sight and not to swerve from it.

The Bloodless Revolution

It is the quintessential image of political revolution. Starving peasants storm the Bastille because oppression has driven them beyond the limits of human endurance. But what if this image is wrong? Or woefully incomplete? What if the most revolutionary forces in the world are not hunger and despair, but hope and opportunity?

The phrase and dynamic that captures the latter vision is called “the revolution of rising expectations”; it describes the hardcore promise of the Satoshi revolution. The term became popular after World War II had destabilized governments across the globe, with old regimes and political systems collapsing. Politics abhors a vacuum. Especially in what was then called the Third World, average people began to believe their lives could improve through their own efforts. The “revolution of rising expectations” refers to a situation in which an increase in prosperity and freedom makes people believe they can create a better life for themselves and their families. They not only act to do so, but they also demand

the political breathing room to achieve more. They hunger for independence and prosperity. Rising expectations becomes an engine of “populism” in the best sense of the word.

Authorities have long known that downtrodden people obey because they believe there is no viable alternative. They believe no act of resistance can better their lives, so they maintain the status quo, however bleak it may be. Greyness, conformity, and fear are the friends of totalitarian regimes that want to quash any flare of nonconformity or creativity because the sparkle expresses individual choice and innovation. The sparkle cannot be controlled. The same is true of hope. Hopeful people act to control their own lives because they glimpse the possibility of freedom and prosperity—two sides of one coin. The 19th-century sociologist Alexis de Tocqueville observed that the French Revolution was strongest in areas of France where the standard of living had been steadily improving. It was strongest there because people believed in the possibility of continuing improvement. They hoped and they demanded.

The concept of “rising expectations” also explains why social revolt often brews in places of opportunity rather than those of oppression. Revolution flows from privileged university students, for example. Revolutionary leaders notoriously come from the upper or middle classes, from the intelligentsia, and they do not share the victimhood of the truly oppressed whom they claim to represent. In fact, the downtrodden often refuse to work for social change. Marx referred to this category of society as the “lumpenproletariat”—the proletariat, especially criminals, vagrants, and the unemployed, who lacked awareness—and he scorned them for not understanding or caring about their own class interest. Instead of hoping for change, perhaps they were doing the best they knew how.

Most revolutions end badly. Some begin badly with violence and an eruption of anger that seems to aim more at revenge than at justice. Even initially peaceful revolutions tend to dissolve into violence and be commandeered by leaders with personal agendas—a lust for power, ideology, greed, or all of the above. When the smoke clears and corpses are removed from the streets, the new regime is cheered by the populace. It quickly reveals itself to be no less tyrannical than the tyrants just toppled, however.

The Satoshi revolution does not run this risk. The blockchain is intrinsically peaceful, with no ability to commit violence. Crypto does not directly confront governments, behead monarchs, or storm oppressive bastions. It sidesteps and obsoletes them with ruthless efficiency. To those steeped in the barricade-erecting version of revolution, the preceding statement may seem tame. But by providing people with financial freedom—even an incomplete freedom—crypto is incendiary. The flow of trade and commerce produces freedom because it produces independence and choice. It establishes a revolution of rising expectations that is not based on ideology but upon people’s rational self-interest. Nothing is more powerful.

What is the engine that drives the Satoshi revolution?

The Power of Peer-To-Peer

Crypto's political brilliance rests on one fact; it solves the "trusted third party problem." (Here the word "trusted" means the inverse of its literal definition.) Understanding this concept is essential to understanding how a free society functions. Yet it was missing from the lexicon of freedom.

The absence was odd. After all, the state's core dynamic is to force people to use the trusted third parties of bureaucracies and crony associates as a way to control them. If people wish to conduct daily life, they have no choice but to deal with the monopoly agencies of the state, including regulators, tax agents, central banks, and law enforcement. Trusted third parties are the enforcement arm of the state. And this is where the "problem" part of the concept arises. The intermediate layer between the state and the people—the layer of trusted third parties—is where corruption and control thrives. By mandating the use of these parties, the state cements its authority and exploits the average person. Without trusted third parties, the state has no means of enforcement. The absent concept is key to political science.

Modern society seems to require trusted third parties, especially the central banking system. Otherwise, it is argued, human beings will return to the direct exchange of barter which is clumsy and severely limited in the geographical range of commerce and the variety of goods exchanged.

Crypto and the blockchain were game changers. Satoshi's original white paper, "Bitcoin: A Peer-to-Peer Cash System" (October 2008), explains, "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." This is Bitcoin's raison d'être.

A note of perspective, however. There is a proper role—a free-market role—for trusted third parties. It is to facilitate the transactions of individuals by providing services, such as the verification of identity provided by a notary. Such trusted third parties are subordinate to the free market that they exist to serve. But even free-market trusted third parties present problems. One is inherent. The word "trusted" implies it is not always possible to verify if the third party is reliable. If verification were possible, then the need to trust would not even arise as an issue; the term would be "verified third party." This risk arises in private dealings as well as public or state-serving ones. Does a lawyer operate clandestinely on behalf of himself rather than on behalf of his clients, for example? Trusting another person with your wealth is a risky business, even if you know the person well. When the third party is an impersonal institution without legal accountability and paid by the state, such as law enforcement, the risk soars astronomically.

All institutions function according to their own self-interest and preservation. In the free market, the self-interest of a business is to serve its customers in order to profit and to avoid losing them to the competition. This is a powerful incentive to

establish a sound reputation and to maintain satisfied clientèle. Government and its monopoly third parties have no similar incentive or constraint because people *must* deal with them. The state regulates all aspects of the financial world, for example, which forces those who wish to bank or trade to interact with state-regulated institutions. There is no competition to which monopolies can lose customers, and the monopolies that address basic human needs will never lack for floods of coerced clientèle. If someone needs a bank account or a credit card to function, then he must accept whatever terms of service the banking system requires. It is no wonder that those terms benefit the bank, not the customer.

Those who work for statist third parties are not necessarily bad people, but their intentions and character do not matter to the outcome. Bureaucrats, civil servants, and bankers may truly believe that their work promotes the public good. They may smile pleasantly, be conscientious at work, and even be helpful to those who use their services. This does not influence the content of what they produce—namely, a mandated monopoly through which the state controls the wealth and behavior of society. A well-meaning bureaucrat is akin to a man who works at a tuna cannery and announces one day that he intends to make candy instead of canned fish. As long as he follows the cannery's rules and uses its machinery, he will produce a can of tuna and not a chocolate bar. His intentions do not matter because the machinery and protocol of the factory is what determines the final product. The same is true of state agencies. A policeman may sincerely announce his intention to protect individual rights against state aggression but, as long as he follows the rules and mechanisms of law enforcement, the resulting product will violate individual rights and sustain the state. This is an important point because an attack on the state should not become an attack on human beings who could become fellow travelers.

The dilemma: Modern commerce and international finance require intermediaries, such as a system of interconnected banks that transmits money across great distance. Again, people's need for commerce leaves them open to exploitation and control by the state that appropriates wealth and information by dominating the intermediaries.

Satoshi elegantly solved this problem. Crypto allows people to transfer wealth on a peer-to-peer basis that requires no intermediary, no trusted third party. The transfers cannot be arbitrarily reversed or altered, so the two parties need not trust or know each other; intentions are irrelevant. The best aspect of barter is maintained—direct exchange—while the worst aspects fall away—geographical barriers and a limited diversity of goods. Since people can maintain their own wallets, the need to rely upon a storage facility or transfer agent is also eliminated. Each user can function as a self-banker with wallets secured by private keys that prevent prying eyes and prying fingers.

The implications for personal freedom are profound.

The Necessity of Decentralized Money

For average people to rise above barter and embrace the prosperity of modern commerce, a means of exchange is necessary—that is, a currency is needed.

Economists scrutinize the characteristics that a desirable means of exchange possesses, such as broad acceptance, durability, and fungibility. But a crucial aspect of a sound currency is often ignored; who controls it? Who issues the currency and decides the rules by which it circulates? A currency is only as sound as the rules it plays by. On the extreme ends of the social continuum, there are two possible answers. The currency is under the centralized control of an authority or the decentralized control of each person using it. In other words, the currency either expresses the power of the state or the freedom of the individual.

In a primitive society, the question of what constitutes a valid currency is determined by the people who trade; they might decide upon sea shells, for example. To an outside observer, the dynamic could resemble a centralized consensus because most people would find it convenient to choose the same currency and to abide by the same evolved rules. The currency actually expresses decentralization, however, because every individual can withdraw his participation at any time and offer another means of exchange. That's the defining feature of decentralization; the individual freely renders or withdraws his consent.

Modern society is said to need centralization because its complexity requires massive coordination. Advanced societies, it is argued, demand decisions to be coordinated by a government that creates the currency, defines its circulation, and eliminates fraud. Besides the moral objection to a currency monopoly—namely, it is wrong to compel peaceful individuals to use or do anything—at least two other objections exist. The first was sketched earlier. Government and its allied institutions act for their own enrichment and preservation, not in the interest of the individuals forced to use its "services."

The second objection is utilitarian. In his 1974 Nobel Memorial Lecture "The Pretense of Knowledge," the classical-liberal economist Friedrich Hayek explains:

> The recognition of the insuperable limits to his knowledge ought…to teach the student of society a lesson in humility which should guard him against becoming an accomplice in men's fatal striving to control society—a striving which makes him not only a tyrant over his fellows, but which may well make him the destroyer of a civilization which no brain has designed but which has grown from the free efforts of millions of individuals.

No one has enough information about the billions of transactions that happen every minute to centralize or control them. Even if it were possible to do so for a frozen moment in time, which it is not, human preferences and circumstances are unpredictable and would change in the next moment. What was true yesterday will not be true today. In short, Hayek believed social engineering crippled rather than created society because it imposed ignorance and prevented individuals

from acting in their own self-interest. A healthy society is the result of human action but not of human design.

One argument for centralization inevitably arises. If every individual pursues his own self-interest, then chaos is said to be the inevitable outcome, especially when an endeavor involves many individuals. The opposite is true. The 19th-century English philosopher Herbert Spencer argues persuasively against the notion that social order was manufactured by coordination through law. Instead, he believed order sprang naturally from “the spontaneous cooperations of men pursuing their private ends.”

Spencer contrasts two forms of order: ranks of soldiers marching in tandem (military society) and spontaneous order (industrial society). The latter can resemble chaos but it is actually a seamless form of coordination. Consider a large department store during the Christmas shopping rush. A person looking down on the scene with a God-like perspective would see people rushing about in different directions, sometimes bumping into each other or looking lost. Shoppers pick up items only to put them down again before darting off in different directions. They unfold clothing only to leave them in a clumsy heap on top of a teetering stack. Announcement of a flash sale causes them to stampede toward the bargain. Harried store clerks race back and forth to answer questions or to cash people out. The scene would appear “anarchistic” in the chaos sense of the word.

What the observer sees, however, is a sophisticated version of spontaneous order by which all parties peacefully achieve their own goals without centralized coordination. It is a microcosm of the free market at work. The store wants to sell its goods; the employees want to keep their jobs; the customers want gifts. What appears to be the scurrying of an ant hill is the conscious and goal-oriented behavior of individuals who unintentionally benefit each other while satisfying their own needs. Without Christmas shoppers, the store might go bankrupt; the store clerks could lose their jobs; the shoppers would have no packages under the tree. The apparent chaos is the free market working to satisfy the needs of people without central planning, without coordination. And all are satisfied.

Crypto’s dynamic is similar. Its free-market decentralization depends upon a consensus from which everyone is free to withdraw without punishment. The participants do not require knowledge of transactions other than their own, and they come at the blockchain from all directions for different purposes. What looks like chaos is a sophisticated form of order that advantages everyone.

The Primacy of Privacy

Crypto’s privacy is imperfect, although technological improvements are being made. It provides pseudonymity—a state of disguised identity that allows confirmation of a user without disclosing his legal identity. Nevertheless, crypto offers a strong layer of protection against state abuse and other threats that arise from intrusive eyes. Tools like mixers can further increase crypto’s protection of people’s identity, of their True Name. (More on this concept.)

Privacy and freedom are intimately connected. Imagine a world in which income is not reported. How could taxes be collected or bank accounts confiscated when the government doesn't know what you have or where you have it? If the recording of life events like birth or school attendance are private, how can your children be drafted? If permission is not required to open a business, how could regulations be enforced? The machinery of government is paralyzed without information about who you are and what you have. That's why its appetite for data is voracious. Knowledge is power. (Note: the words "government" and "the state" are being used interchangeably.)

Employment, finances, medical history, military eligibility, education, residency, marital status, telephone records, travel habits, internet use, automobile ownership, and a blizzard of other data is either stored by government or easily accessed by it. Crypto provides a rare privacy haven based on algorithms and pseudonymity. When one wallet sends payment to another, the key of the sender is decoded by the key of the recipient. The encryption shields the transaction from meddling or theft. Its privacy shields people's lives from the state.

This is Satoshi Nakamoto's vision: a peer-to-peer, decentralized, and pseudonymous system of commerce and self-banking through which the individual avoids the corruption of the current system by avoiding trusted third parties. Individuals privatize their own lives. Short of Gutenberg's printing press, few inventions have created such freedom and opportunity for freedom.

This will remain true, however, only if the original vision is sustained and not compromised by those who seek "respectability" and equate this word with state sanction.

Conclusion

The introduction has focused on crypto's contribution to the power and freedom of the individual, but crypto's benefit to civil society is immense. Perhaps no other author better captured the benefits of uncoordinated self-interest to society than the French Enlightenment philosopher Francois-Marie Arouet de Voltaire.

In his *Letters Concerning the English Nation,* Voltaire asks why there was so much religious tolerance in England as compared to France, which had been torn apart by brutal conflicts between Catholics and Protestants. It was not due to laws or history. British laws strongly favored the Church of England and past persecution had been severe enough to prompt the Pilgrims to make a treacherous voyage to a New World. The key difference between England and France, Voltaire concludes, was the relatively free network of commerce through which ordinary people dealt with each other solely for financial self-interest. The difference was the rise of a commercial middle class that earned England the nickname of "a nation of shopkeepers." Financial freedom bred tolerance and a civil society.

Voltaire declares:

> Go into the Exchange in London, that place more venerable than many a court, and you will see representatives of all the nations assembled there for the profit of mankind. There the Jew, the Mahometan, and the Christian deal with one another as if they were of the same religion and reserve the name of infidel for those who go bankrupt. There the Presbyterian trusts the Anabaptist, and the Church of England man accepts the promise of the Quaker. On leaving these peaceable and free assemblies, some go to the synagogue, others in search of a drink; this man is on the way to be baptized in a great tub in the name of the Father, by the Son, to the Holy Ghost; that man is having the foreskin of his son cut off, and a Hebraic formula mumbled over the child that he himself can make nothing of; these others are going to their church to await the inspiration of God with their hats on; and all are satisfied.

By enabling the free flow of commerce and wealth, crypto enriches not only individuals but also civil society because financial interaction is a cornerstone of tolerance. It breaks down racial, ethnic, and class barriers. As well as encouraging a healthy society, crypto offers diversity of choice for the individual. Some users will choose anonymity, while others may advertise their identities. Some will be rugged individualists and anarcho-capitalists, while others may prefer socialism. Differences of ideology, religion, or lifestyle are irrelevant to blockchain transactions because they are blind to such niceties. They recognize only consent.

A thriving society is one in which people come together for their own profit whether the profit is defined in monetary terms or cultural ones. They come together in independence and freedom. They part ways when they want to move on. And all are satisfied.

SECTION ONE: THE TRUSTED THIRD PARTY PROBLEM

CHAPTER ONE: Listening to the Past

> The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.—Satoshi Nakamoto

The trusted third party problem has haunted modern financial systems and centralized exchanges because people require an intermediary to make them work. The third party’s good or bad motives become a defining aspect of the transaction, and the those who use the institutions are at the mercy of those intentions. This is especially true of the current system of state-issued money and central banking.

A trustless system avoids intermediaries and does not depend upon the intentions of participants; that is, the system functions in the same manner regardless of anyone's intentions. The blockchain, with a transparent and immutable peer-to-peer protocol, is called trustless because there is no corruptible intermediary upon whom exchanges must depend.

On a small scale, the trusted third party problem may always exist because a middleman is useful or necessary in some situations. If third parties offer competitive services on a free market, however, the damage of dishonesty or incompetence is limited. People can take their business elsewhere, report a swindler to watchdogs, warn others, and file a lawsuit.

An occasionally dishonest third party is not the problem Satoshi addresses. He speaks to the institutionalized corruption of government and central banks from which the average person could not escape by using a competitor or by suing. Almost everyone who works over the table, runs a business, buys or sells goods, accepts government benefits or pays taxes has had to accept a fiat that constantly plunges in value due to inflation. Almost everyone who uses credit, accepts checks, takes out loans, conducts commerce or does business abroad has needed to go through banks that steal like drunken muggers.

For average people, the situation used to seem hopeless because no legal, practical, and private alternative existed for transferring funds across considerable distance, including borders. Attempts to reform or remove the system also seemed doomed because it was inherently corrupt and self-serving. In fact, fiat and central banking were serving the purpose for which they had been established: financial control by elites. People's need for money and exchange became their straitjackets.

Then Satoshi. Then the blockchain and crypto. A new concept of money was created in a form that cannot not be inflated; the number of bitcoins is fixed at 21 million divisible units. The supply can only decrease when coins are lost, as inevitably happens. Satoshi notes, "Lost coins only make everyone else's coins worth slightly more. Think of it as a donation to everyone." Bitcoin solved the fiat problem.

A new concept of financial transfer solved the third party problem, especially with regard to banks. Although peer-to-peer transactions involve a middleman or miner, no trust is required since the transaction is released only when "proof of work" is rendered, which consists of solving a complicated math problem. Arriving at a solution may be costly in computer power and time, but the solutions themselves are easy to verify. Satoshi comments, "With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless." The soundness and propriety of the blockchain's protocol itself is assured by the use of open source that is visible to all and verifiable. The political outcome: A private currency and method of exchange freed people from financial oppression.

The idea of private currency itself is hardly new, however.

Precedent in Radical Individualist Theory

The late Friedrich Hayek is the most respected Austrian economist of the 20th century. His book *The Denationalisation of Money: An Analysis of the Theory and Practice of Concurrent Currencies* argues vigorously for private and competitive currencies to displace government-issued ones. Hayek ponders a key question. "When one studies the history of money one cannot help wondering why people should have put up for so long with governments exercising an exclusive power over two thousand years that was regularly used to exploit and defraud them. This can be explained only by the myth" that government money was necessary "becoming so firmly established that it did not occur even to the professional students of these matters…ever to question it. But once the validity of the established doctrine is doubted its foundation is rapidly seen to be fragile."

Governments reap incredible profits from debasing the currency, but the rigged game works only if people have no alternative but to play it. The political purpose of legal tender and banking laws is to grant a monopoly to the state, which permits the redistribution of wealth and power from average people upward to the elite of society. Fiat money and banking remains fragile, however, because the system relies on people either not understanding the dynamics or not having a choice. Hayek wonders why public understanding is so elusive. Why was "a government monopoly of the provision of money…universally regarded as indispensable" and what would happen "if the provision of money were thrown open to the competition of private concerns supplying different currencies?"

With eerie prescience, Hayek argues for currencies developed by entrepreneurs who innovate new forms of money just as they innovate in other areas. One of the drawbacks of government's monopoly is that it imposes a freeze on the sort of invention that now runs free in crypto. The voluntaryist historian Carl Watner observes, "No one can tell in advance what form these monies might take because no one can know for sure what choices individuals would make or what new technologies might be discovered. Laws forcing people to use the Federal Reserve System money have frozen monetary developments at a certain stage...Just imagine if Congress had protected the Post Office by passing laws that would have prevented people from communicating via the internet. We would never have experienced the marvels of e-mail."

The late Austrian economist Murray Rothbard also wrestles with the question of "why do people so vigorously resist private currencies?" His book *For a New Liberty: The Libertarian Manifesto* advances an explanation. "If the government and only the government had had a monopoly of the shoe manufacturing and retailing business, how would most of the public treat the libertarian who now came along to advocate that the government get out of the shoe business and throw it open to private enterprise?" Rothbard predicts that the skeptics would attack the libertarian for depriving them of the only possible source of shoes—the

government. People are thoroughly indoctrinated to believe that daily life cannot function without the state and fiat.

Hayek and Rothbard are unusual among free-market economists in their embrace of private money and monetary systems. Even laissez-faire zealots rarely champion free-market currencies or private banking. Instead, they debate marginal issues such as fractional reserve and other reforms they think will improve the existing system. Or they argue for the restoration of a gold standard as though it were a panacea. But if a gold standard were applied to fiat, the system would still require people to trust the government and banks. This means trusting both institutions to act against their own interests, which they have historically neglected to do.

The modern neglect of free-market money and banking is odd because 19th-century radical individualists focused intensely on the importance of private money and private banking to personal freedom. They placed a primal emphasis on the right of every individual to create his own currency and to function as his own bank. It was a natural right as important as freedom of speech or of religion. The pivotal individualist Benjamin Tucker believed that the right to issue private currency was so important that it could destroy the State all by itself. His reasoning: The money monopoly, including control of credit, was how the State sustained itself and robbed average people not merely of wealth but also of economic opportunity.

Two specific events sculpted the approach that the early individualist-anarchists adopted toward the monetary monopoly. One was the Panic of 1837 that tipped the United States into recession until the mid-1840s. Commonly cited causes of the Panic include a collapsing land bubble and a sharp fall in cotton prices. Blame is also placed at the feet of President Andrew Jackson for vetoing the recharter of the Second Bank of the United States and precipitating an unfortunate chain of economic events. Drawing on the work of Professor of Economics Peter Temin, Rothbard disputes this interpretation.

> First, he [Temin] points out that the price inflation really began earlier, when wholesale prices reached a trough of 82 in July 1830 and then rose by 20.7 percent in three years to reach 99 in the fall of 1833. The reason for the price rise is simple: The total money supply had risen from $109 million in 1830 to $159 million in 1833, an increase of 45.9 percent, or an annual rise of 15.3 percent. Breaking the figures down further, the total money supply had risen from $109 million in 1830 to $155 million a year and a half later, a spectacular expansion of 35 percent. Unquestionably, this monetary expansion was spurred by the still-flourishing Bank of the United States, which increased its notes and deposits from January 1830 to January 1832 from a total of $29 million to $42.1 million, a rise of 45.2 percent. Thus, the price and money inflation in the first few years of the 1830s were again sparked by the expansion of the still-dominant central bank.

Arguably, the Panic began in May 1837 when banks in New York City announced they would not redeem commercial paper for specie at full face value. Of the approximately 800 banks in America, all but six ceased at one point or another to redeem banknotes and deposits for gold or silver coins. Suspicion and hatred of traditional banks and government-issued money soared, with radicals scrutinizing alternate systems.

The other event dramatically to impact the radical fever from monetary reform was the Civil War for which the North financed its fighting through Legal Tender Acts and the National Banking Act of 1863.

The radicals did not merely theorize; they experimented with private currencies and new economic models. Their efforts are fascinating, but they are also cautionary tales. A major problem for 19th-century individualist-anarchism was the movement's general acceptance of a link between sound money and the labor theory of value. This theory states that the true value of a good or service is based on the labor required to produce it rather than the price at which a seller and buyer are willing to exchange. In short, a good has intrinsic and not subjective value. (More on this in the section on the Regression Theorem.) Happily, their main economic goal was the abolition of the "money monopoly." The term referred to three different but interacting forms of monopoly: banking, the charging of interest, and the privileged issuance of currency. The abolition of state power over currency was the focus, and they eschewed the use of force to implement their own schemes.

Josiah Warren provided a real-world example of what was meant by a currency that rested on the labor theory of value. Credited with being the first American anarchist, Warren tested his specific solution to the money monopoly through a Time Store from which he issued "Labor Notes." In 1827, the business opened with $300 worth of groceries and dry goods that were offered at a 7 percent mark-up from Warren's own costs in order to cover expenses such as overhead. This was before groceries were prepackaged or preweighed, and it was usual for buyers to bargain with the shopkeeper rather than pay a posted price. One of Warren's innovations was to post prices, which drove costs lower because transactions consumed less time. The customer paid in traditional money for the goods and paid with a Labor Note to compensate Warren for his time. The Labor Note obliged the customer to provide Warren with an equivalent amount of his time. If the buyer was a seamstress, for example, the Labor Note committed her to render to Warren X units of time to produce clothing. Warren's goal was to establish an economy—or to establish a proof of principle, at least—in which profit was based on the exchange of time and labor. The Labor Notes were circulated and traded widely with in the community.

To some degree, Warren succeeded. People traveled from a hundred miles away to avail themselves of the Time Store's low prices. After a few years, he declared the experiment to be a success and closed the store. Whether the Labor Notes *were* a success is questionable, however. The store itself may well have succeeded due to its low prices, not to the Notes. Whichever explanation is true, it

is difficult to see how this novel currency could function in dense populations or on a grander scale of commerce. Few people today would be convinced of the viability of private money based on the Time Store experiment.

What could convince the public and economists that private currencies work as well or better than government-issued ones? Going back a bit further in American history is a good place to start because the future is always based on the past.

America is Born into Private Currency

Colonial America teaches powerful lessons about private currencies.

The British colonies naturally used British currency, but the homeland's dubious monetary policies created a voracious appetite for alternative monies as well. Rothbard explains in *A History of Money and Banking in the United States: The Colonial Era to World War II*, "Great Britain was officially on a silver standard….However, Britain also coined gold and maintained a bimetallic standard,,,,In 17th- and 18th-century Britain, the government maintained a mint ratio between gold and silver that consistently overvalued gold and undervalued silver in relation to world market prices." Britain's policies created a robust market in substitutes for its own money.

Gresham's law ruled colonial money in the same way it rules all currencies. The law: If two monies are officially valued at the same price or a fixed ratio and the market value of one goes higher, then the more valuable money will disappear from general circulation and be used in another manner, such as hoarding or paying off foreign debts. This is the meaning of the axiom "bad money drives out good." Full-bodied silver coins began to disappear from circulation within the colonies, which turned to lighter silver, commodity-based money, or foreign and privately-minted coins. These monies functioned as fully parallel currencies, with Spanish pieces of eight being particularly popular.

The first privately-minted American coin seems to be the Granby or Higley Token, which was struck by Dr. Samuel Higley of Connecticut in 1737. After Samuel's death, his brother John produced the copper coins from 1737 to 1739 inclusive. Valuing the tokens at three pence each, John reportedly spent most of them at the local bar, until the barkeeper refused to accept any more. Then he cast coins with one side reading "Value Me as You Please" and the other side declaring "I Am Good Copper." No value was stamped on the coin, which was common practice in those days. They circulated widely for many years even after John ceased to mint them, because they were a reliable alloy with which goldsmiths made jewelry. Later metallurgical analysis of the Granby found the coins to be 98-99% pure copper.

Another lesson: The 18th-century New York City goldsmith Ephraim Brasher demonstrated a method by which privately-minted coins could circulate widely and without doubts about their purity or weight. Many private minters had good reputations within their own communities, but circulation of their coins was often

limited to those environs. Brasher offered a solution. He became renowned for testing coins upon which he stamped “EB” if they proved to be sound. Backed by his reputation, stamped coins migrated far and wide.

This is a great advantage crypto has over earlier private currencies; its coins do not have the same need to be backed by verification. Unlike physical coins, bitcoins cannot be shaved down, counterfeited, diluted by alloys, or negated by the bad acts of the miners or of users. A bitcoin is a bitcoin is a bitcoin, and no one can alter the fact. This sidesteps the verification of purity or weight.

How and Why Government Outlawed Private Money

How did ratification of the United States Constitution in 1788 affect private money?

People assume the United States Constitution grants Congress a monopoly “right” to issue money. The assumption comes from Article 1, Section 8, Clause 5 of the Constitution that delegates to Congress the power “[t]o coin money, regulate the value thereof, and of foreign coin, and fix the standard of weights and measures.” This is assumed to be a monopoly right. In his pamphlet “The Unconstitutionality of the Laws of Congress Prohibiting Private Mails” (1844), the legal scholar and private-money advocate Lysander Spooner explains otherwise:

> [T]he powers of Congress…’to coin money’, are in reality exclusive, only as against the State governments….The constitutional prohibition upon individuals, to coin money, extends no farther than to prohibitions upon ‘counterfeiting the securities and current coin of the United States’. Provided individuals do not ‘counterfeit’ or imitate ‘the securities or current coin of the United States’, they have a perfect right, and Congress has no power to prohibit them, to weigh and assay pieces of gold and silver, mark upon them their weight and fineness, and sell them for whatever they will bring, in competition with the coin of the United States.

The Constitution does address the regulation of “foreign coin,” but private domestic coins remained popular, especially one called the Bechtler.

The 19th century saw a wave of gold rushes in North America. In the late 1820s, both Georgia and North Carolina experienced huge rushes and an accompanying dilemma. There was no government mint in the area. Shipping gold to the main mint in Philadelphia was problematic because it cost a great deal to transport and to insure. A local paper explained the miner’s plight:

> Since the State Bank has limited her issues and is drawing into her vaults the notes which have been loaned to our citizens, in the settlement of her outstanding accounts, great inconvenience has been let in business transactions with the Bank, and also for the common purposes of commerce. How far this scheme [having a private mint] will succeed in effecting these objects, we have yet to learn. The risk and expense of

> sending gold to the [Philadelphia] mint is such that the owners of the mines often find it difficult to dispose of the products of the mines at a fair value, as things now are. The urgent petition to Congress for the establishment of a branch of the US Mint in the 'gold region' having failed, and the gold produced being in a fair way to entirely disappear from the country and fall into the rusting hoards of Europe, this scheme has been resorted to.

Gold miners approached the well-respected watchmaker and goldsmith Christopher Bechtler Sr. for a private solution. Because he was also a metallurgist and an honest man, Bechtler was a perfect candidate to start striking coins. The first Bechtler gold coin issued in 1831, followed by advertisements declaring that Bechtler would mint any miner's gold for 2½ percent of the bullion.

Government's reaction to competition can be judged by the fact that the United States Treasury lost little time in testing the new coins, probably in the hope of discrediting them. Alas for the Treasury, the Bechtlers were purer than government issue. Indeed, the Federal Mint bought $294,000 worth of Bechtlers and used them to pay debts and to trade with Europe. Suddenly, the government was motivated to open its own Federal mint in Charlotte, North Carolina, which was about 80 miles from the Bechtler one. The Federal Mint began to produce gold coins in 1838.

By the time of Bechtler Sr.'s death, considerably more than one million Bechtlers circulated widely in America, particularly in the southeast. Thereafter, however, the relatives who assumed the business were either incompetent or dishonest. Consistency and purity declined, and the market responded by walking away. The mint closed a few years later because it lived or died on its reputation.

The original Bechtlers continued to circulate, however. They were so popular that, during the American Civil War (1861-1865), the monetary obligations of the Confederacy were specified as being payable in Bechtler gold, not Confederate or other government-issued currency.

The Bechtler coin is both an inspiring tale and a warning. It speaks to the free-market consequences of integrity and of debasement, both of which are non-issues for crypto because it is trustless and the coins cannot be altered. The Bechtler story also demonstrates how the free market outperforms government in terms of moving swiftly into an empty niche and producing quality. As they do today, free-market currencies outcompete government issue. If they cease to do so, the currency fails due to Gresham's Law. As it did in the past, the government today uses private currencies, such as gold and crypto, while trying to undercut the competition they represent through laws.

Government resistance to competition did not begin or end with the Bechtlers, of course. In his essay "Hard Money in the Voluntaryist Tradition," Watner traces the course of a mint in San Francisco during the California gold rush: Moffat & Co. "Moffat & Co. was apparently the most responsible of the private concerns minting money," for when, "the businesses of San Francisco placed an embargo

on all private gold coinage" the exception was Moffat. "The remainder of the private issues were soon sent to the U. S. Assay Office to be melted down or else were passed only for their bullion content in trade."

Initially, Moffat issued gold ingots in direct competition with the U.S. federal Assay Office because no state Assay Office then existed. According to the reference site *Coinfacts*, "The official government assay of these ingots proved them to be worth more than the amount stamped on them." Moffat outcompeted the government.

The ingots' denomination was too large for normal trade, however, and merchants demanded smaller coins. Moffat had contracted with the U.S. Assay Office and now asked for the authority to strike coins, as well as the larger ingots. When permission was not forthcoming, Moffat began minting coins under its own mark and authority in 1849. The firm's high reputation and its policy of redeeming all coins at face value meant that their issue became a popular circulating currency.

Government obstruction did not stop with a refusal to authorize coinage. On April 20, 1850, the State Assayer, Melter, and Refiner of Gold of California was established by law. A companion bill was passed at the same time with the goal of reining in private minters. Along with an earlier measure on April 8th, the bill represented a compromise. *Coinfacts* explained the original position the government had taken toward minters such as Moffat.

> It was during the first part of 1850 that there was serious agitation against private coinage. The California Legislature considered a bill…which would have branded private coiners as counterfeiters, and which urged subjecting 'the makers or passers of such coin to the penalty imposed upon coiners and counterfeiters'. The bill would also have forced the private mints to redeem their coins in 'lawful money'. The *Alta California* printed the proposed bill along with a supportive editorial. The editor further pointed out the inability to use private coins in payment of customs.

The next day, the *Alta California* ran an open letter from Moffat himself through which he appealed to the people of San Francisco. He acknowledged that the state could not legally issue coins due to Constitutional restrictions, but private individuals had no similar constraint. He pointed to the Bechtler mint that continued to strike coins even though the business was only 80 miles from the federal government's Charlotte branch. Moffat powerfully reminded San Francisco that no one had ever been defrauded by purchasing or accepting his coins.

The first compromise bill of early April prohibited the private issuance of gold pieces weighing less than four troy ounces. Again, this was an awkward size for normal commerce and almost guaranteed a limited circulation. By contrast, the state Assay Office was allowed to cast gold ingots of two troy ounces. *Coinfacts* observed, "The State Assay Office of California was a unique institution in our nation's history. It was the only mint to operate in this country under the authority of a state, after 1789. Its issues (though never challenged in the courts) may have been illegal under the United States Constitution, which forbade any state to issue

coins or currency.” The state used the sleight of hand of striking ingots which were not mentioned in the Constitution but which circulated as the equivalent of coins.

The April 20th companion bill further hobbled private minters by requiring them to redeem their coins at face value for government issue. A complicated back and forth between Moffat and both the state and federal assay offices ensued. Moffat received a coining contract with the state and sought federal permission to strike smaller coins; it was denied. Eventually, Moffat resumed issuing its own coins in smaller denominations, whereupon the government granted the firm permission to issue official $10 and $20 coins for the Assay Office.

The federal government changed tactics in 1852. The U.S. Customs House suddenly refused to accept Moffat’s $50 ingots even though they had been issued under the direct authority of the U.S. Assay Office. Paying customs was a primary use of the ingots, but federal law abruptly required duties to be paid in coins of 900/1000 fineness rather than the California standard of 884/ to 887/1000. The Treasury Department took the remarkable step of refusing to accept coins issued by its own Assay Office. It invalidated its own coinage.

The history of Moffat & Co. is significant not merely because it illustrates how private money can and will fulfill public needs but also because it lays bare the government’s absolute resolve to eliminate competition in currency and the tactics it used to do so. The tactics remain the same to this day. One is to prohibit the currency by criminalizing it as the California legislature attempted to do through the accusation of counterfeiting. Another is to absorb and control the competition as the Assay Office did by contracting with Moffat. A third strategy is to place huge obstacles in the path of free currencies, which amount to a de facto ban and give a decided advantage to government money.

The government strategy worked. Watner explains, “By October 1856, the Federal mint was apparently able to meet all demands for coins in domestic circulation and for export, so that private issues of gold coin quietly passed out of existence. There is no record of any further private minting in California after this time.”

The history of private minting in early America is deep, pervasive, and intimately tied to the nation’s economic success. Fraud was certainly present but meticulous honesty and solutions to fraud were as well. The mints with high reputations and good business sense succeeded, and they often outperformed their government counterparts, reducing them to the use of force (law) to gain the upper hand.

Government did not act on behalf of the public. If it had, it would not have attacked honest firms that provided desperately needed services to miners, merchants, and purchasers; the public need for currency was ignored by the Treasury Department. Nor does the Act explain why some governments themselves preferred to use private coins on occasion. One explanation makes sense; the government wanted to eliminate the competition not because it was fraudulent but because it could win on a free market. Government acted on its own behalf to line its pockets and strengthen its power.

On June 8, 1864, Congress passed An Act to punish and prevent the Counterfeiting of Coin of the United States. It read, in whole:

> That if any person or persons, except now authorized by law, shall hereafter make, or cause to be made, or shall utter or pass, or attempt to utter or pass, any coins of gold or silver, or other metals or alloys of metal, intended for the use and purpose of current money, whether in the resemblance of the coin of the United States or foreign countries, or of original design, every person so offending shall, on conviction thereof, be punished by fine not exceeding three thousand dollars, or by imprisonment for a term not exceeding five years, or both, at the discretion of the court, according to the aggravation of the offence.

The private minting of currency effectively ceased in America.

The Act was undoubtedly sold to the public as being necessary to protect against fraud. Without excusing whatever fraud existed or suggesting that the crime should not be punished, a caveat emptor or "buyer beware" policy should have applied instead; the buyer is responsible for checking the quality of goods before a purchase. A great deal of fraud could have been avoided if people had not relied on government guarantees but learned to assess quality for themselves. An entire and valuable category of business was criminalized because some participants were dishonest and some customers incautious. These were excuses. The main motivation was for the government to eliminate competition.

Mark Twain reputedly said, "History does not repeat itself, but it rhymes." To some, private coinage in early America may seem to have little in common with crypto, but there is a common theme. Government is threatened and wants to monopolize or regulate a new private money through a mixture of banning, hoisting obstacles, absorption, and punishment. History is beginning to rhyme loudly.

Ultimately, the viability of crypto and other private currency comes down to two factors. Can the free-market provide a competitive money? And will the state allow private money to exist without regulation?

A large obstacle to the acceptance of crypto in free-market circles has been the conviction that it is not and cannot be a valid money.

The Regression Theorem

The example of the Granby coin that continued to circulate due to its value in making jewelry illustrates a principle that has created debate about whether crypto can be viewed a currency at all. The concept is the Regression Theorem.

The Regression Theorem is an economic proposition that is most associated with Ludwig von Mises. It applies the subjective theory of value to the purchasing

power or objective value of money. The theorem does so by tracing objective-exchange values through “the subjective theory of value, whereby the values are traced to the ultimate subjective-use values of the marginal consumers who value such goods and services for their objective-use values which they expect to consume.” In other words, the objective-use value of money goes back to the point at which people valued its non-monetary uses. This raises a problem for fiat that is not consumed as gold or silver can be. Instead, with fiat, “the subjective and objective use values of money coincide and are equal to its objective-exchange value, the estimated value of the goods and services for which it can be exchanged.”

Economics Professor Jeffrey Rogers Hummel unpacks the concept further as it applies to fiat. Today’s purchasing power of money “draws on yesterday’s, and yesterday’s…and so on….How far back does the regression…go? Logically, Mises explained, for a commodity money it goes back to the day before the commodity first started being used as a medium of exchange. On that day it had an exchange value or purchasing power due only” to its importance “as an ordinary commodity (for consumption or for use as a productive input) and not for use as a medium of exchange. For…the U.S. dollar that became a fiat money by terminating the redeemability of what had been a claim to a commodity money…the historical chain goes back to the day before termination, and thence back to the day before that commodity became a medium of exchange. Application of the logic to a new fiat money” means applying an official rate of redemption to an established fiat money.

The theorem has been very influential because it elegantly interweaves the purchasing power of money with the theories of subjective theory and marginal utility. The subjective theory of value argues that no good or service is inherently valuable; it has no built-in value due to the labor required to produce it, for example. Instead, its value is determined by how important the good or service is to the specific individuals who sell and consume it. But this value does not remain constant even for those individuals because of marginal utility. Marginal utility refers to the additional satisfaction a person receives from consuming one more unit of a good or service, as measured in ordinal numbers. A starving man would probably value a plate of food as #1 on the list, whereas an overweight person on a strict diet might give same plate a negative rating. After eating his fill, the starving man is likely to devalue the marginal utility of more food and prioritize finding shelter for the night. All economic value is subjective and in flux.

The Regression Theorem needs to be carefully weighed if only because many Austrian and other free-market economists reject crypto on the grounds that it violates the circumstances in which valid money must originate; these people should be natural allies of the crypto community, not critics. Meanwhile, most crypto enthusiasts react in one of four ways to hearing the Regression Theorem objection. They don’t care. They assume the attitude of “if a dog eats it, it is dog food”; that is, if something buys goods and services, it is money. They claim the theorem does not apply to the digital age. Or they insist it *does* apply to crypto in a manner that is misunderstood. The latter two approaches show promise toward

resolving what seems to be a tension between Mises and crypto. Both sides could benefit from clarification.

An initial point: A theorem is a general proposition that is not self-evident but needs to be proven by a chain of reasoning. It has been called “a truth established by means of accepted truths.” It is not an axiom, and it is vulnerable to changing circumstances or additional reasoning. This means the proposition is malleable.

The economist Robert P. Murphy provides another path to explain how bitcoin emerged as a medium of exchange without being tied to a commodity or redeemable in a fixed amount of an established fiat. His article “Why Misesians Need to Tread Cautiously When Disparaging Bitcoin” argues, “[T]he very first people to trade for it did so because it provided them with direct utility because they knew there was at least a chance that it would serve to chafe the governments of the world.…[T]he early adopters of Bitcoin were doing it for ideological reasons, not for pecuniary reasons.” To Murphy, freedom is the commodity or service value of bitcoin.

Crypto-enthusiast Jeffrey A. Tucker takes a different tack. In a *Foundation for Economic Education* article entitled “What Gave Bitcoin Its Value?,” he points to the purpose that the theorem had originally served; it helped answer the question of why certain commodities emerged as currencies while others did not. The emergence of salt as a currency, rather than sea weed, was due to salt’s direct utility and durability, for example.

Tucker then links crypto not to a hard good but to a hard service that fills a deep need and has direct utility—namely, the blockchain as a payment system.

> Bitcoin is both a payment system and a money. The payment system is the source of [non-monetary] value, while the accounting unit merely expresses that value in terms of price. The unity of money and payment is its most unusual feature, and the one that most commentators have had trouble wrapping their heads around…This wedge between money and payment has always been with us, except for the case of physical proximity. If I give you a dollar for your pizza slice, there is no third party. But payment systems, third parties, and trust relationships become necessary once you leave geographic proximity. That’s when companies like Visa and institutions like banks become indispensable.

To Tucker, the non-monetary value of crypto is as a payment system that does not require a trusted third party and has no geographical limitations. The blockchain is what causes crypto to emerge as a medium of exchange. In this manner, the Regression Theorem is applied to bitcoin, but the theorem needs to be updated in order to focus upon the unique services—functioning as de facto goods—that are available in the digital age.

The last word on Regression Theorem belongs to Satoshi. In a post entitled "Bitcoin does NOT violate Mises' Regression Theorem" on the bitcointalk forum that he founded, Satoshi states:

> As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties:—boring grey in colour—not a good conductor of electricity—not particularly strong, but not ductile or easily malleable either—not useful for any practical or ornamental purpose and one special, magical property:—can be transported over a communications channel If it somehow acquired any value at all for whatever reason, then anyone wanting to transfer wealth over a long distance could buy some, transmit it, and have the recipient sell it. Maybe it could get an initial value circularly as you've suggested, by people foreseeing its potential usefulness for exchange. (I would definitely want some) Maybe collectors, any random reason could spark it. I think the traditional qualifications for money were written with the assumption that there are so many competing objects in the world that are scarce, an object with the automatic bootstrap of intrinsic value will surely win out over those without intrinsic value. But if there were nothing in the world with intrinsic value that could be used as money, only scarce but no intrinsic value, I think people would still take up something. (I'm using the word scarce here to only mean limited potential supply).

Even if crypto is a valid currency, it must be able to compete with fiat and other money if it is to thrive. What makes a money competitive? This leads to the more fundamental question of "What is money?"

Currency Can Create Freedom and Civilization…or Oppression

> Historically, money was one of the first things controlled by government, and the free-market 'revolution' of the eighteenth and nineteenth centuries made very little dent in the monetary sphere. So it is high time that we turn fundamental attention to the life-blood of our economy—money.—Murray Rothbard, *What Has Government Done to Our Money?*

I was seven years old when I realized my parents did not understand some of the most important dynamics of life. I was in the back seat of our car with a bag of candy that had been purchased from a roadside store in the hope of keeping me quiet. It didn't work. A thought tumbled out of my mouth. "Why do we pay for anything? Why don't people just go into stores and take what they need?"

My mother replied, "It is wrong to steal."

I explained, "I don't mean stealing. I mean why do we give people money instead of just sharing everything?" My parents fell silent.

When I asked again, my mother shot back over her shoulder, "Don't ask stupid questions!"

They didn’t know the answer; I recognized this immediately. And their inability to explain why we needed money disturbed me because they discussed money constantly. Was there enough to repair the car *and* pay the mortgage? Could they afford to replace the roof? What was the spending cap on Christmas this year? Money ran as a theme through every aspect of their lives and yet my parents didn’t know how to answer the basic question of why we need it.

“Money is how the world works,” my father finally explained, “because it lets people buy the things they need to live.” This was a non-answer because it returned me to not understanding why we bought things instead of simply sharing them. At a childish level, I was trying to understand monetary theory, and I’ve been struggling with it ever since.

Nothing has been more beneficial in this quest than the short book *What Has Government Done to Our Money?* by Rothbard. He did not use the term “trusted third party” or its equivalent in the book or elsewhere in his writing, as far as I know. Murray was a friend and mentor, however, which gives me some confidence in predicting what his probable reaction to the entire Satoshi hypothesis would have been. I suspect he would not have viewed the need to trust a financial intermediary as a problem because private banks could offer guarantees such as reputation, redemption in gold, and audits. To Murray, the dilemma of modern money seemed to begin with government fiat as the problem, and it ended with the free market as the solution that allowed private financial institutions and currency issued by individuals, should they choose to do so. Murray’s name for his own hypothetical currency was “the Rothbard.”

What Has Government Done to Our Money? belongs to the preBitcoin years, but it offers significant contributions to crypto. It explains the origins of money in clear terms, as well as highlighting money’s pivotal role in establishing freedom and civilization. The book provides a context in which to appreciate the immense liberation that is crypto and the immense oppression that is fiat. The book is a deceptively simple exposé of the world’s greatest swindle: inflation. The scam is only possible when people need a trusted third party in financial matters and government usurps that role through law and central banking.

Understanding inflation requires a common-sense grasp of what money is and what it should be. This is no small feat. Modern monetary theory creates a haze of complexity that ensures average people are left speechless when confronted by basic questions—even by ones that deeply impact their lives. This could be avoided easily. Schools could teach practical economics; government and financial institutions could be transparent rather than brick walls; fiscal policy could be presented in English rather than bureaucratese with impenetrable statistics and math.

This won’t happen by itself. The lack of public awareness benefits the state’s monetary monopoly, and tax-funded public schools are not prone to teach revolution against the hand that feeds them.

A Brief Tour of the Basics

Every society exchanges goods and services because trade is a human need. It is the engine of economic life, a wellspring of prosperity, and the basis of survival. Trade is not a zero-sum game, as some economists argue. That is to say, if a person trades a fish for a loaf of bread, one trader's profit does not cancel out that of the other. Trade is a win-win situation because the exchange only occurs when one person values the bread more than the fish and vice versa. Each one gains from the exchange or else it does not occur. In the process, the traders also establish cooperation and, perhaps, a level of good will that aids commerce in the future. This makes free exchange a main building block of civil society.

Human beings are so magnificently varied that a diverse range of skills exist even within a small group of individuals. Trading these skills increases the odds of survival for both the group and each member in it, but direct exchange or barter is severely flawed, as Rothbard explains. "The two basic problems are 'indivisibility' and 'lack of coincidence of wants'." "Indivisibility" means a barter good, like a plow, may be difficult or impossible to divide into many parts, which keeps it from being bartered for several things with several people. So no trade occurs. "A lack of coincidence of wants" means Smith has eggs and Jones has shoes, but Smith wants butter. So no trade occurs.

Indirect exchange resolves the barter problem…to a degree. Smith trades his eggs for Jones's shoes because the latter can be traded to a third person for something Smith *does* desire. This mitigates the lack of coincidence of wants. More importantly for monetary theory, however, indirect trading naturally encourages a medium of exchange to emerge. Why? Traders will favor barter items that are highly desirable and will be accepted by many people. Highly tradable goods tend to share characteristics, including divisibility, durability, fungibility, and transportability. Not coincidentally, these same characteristics often describe good money, and they apply to crypto.

According to Mises's theorem, the desirable barter item is first valued for its use value. Rothbard lists some commodities that became currencies. "[T]obacco in colonial Virginia, sugar in the West Indies, salt in Abyssinia, cattle in ancient Greece, nails in Scotland, copper in ancient Egypt, and grain, beads, tea, cowrie shells, and fishhooks." The demand for a good generates a "reinforcing spiral: more marketability causes wider use as a medium which causes more marketability, etc. Eventually, one or two commodities are used as general media —in almost all exchanges—and these are called money."

Commonly accepted currencies eliminate the need for both barter and indirect exchanges, which can be clumsy, time consuming, and geographically limited. Currencies create a complex free market that allows billions of people who do not know each other to consume products from around the world. In short, money catapults human beings from survival into a prosperity that allows the luxury of time to think, to create art, to enjoy deep relationships, and to take care of their health. A medium of exchange is a foundation of civilization.

Enter government. Currency had played a defining role in freeing and civilizing human beings. Now it would be used to enslave them.

Inflation, the Greatest Theft of All

Government does not produce goods and services in the marketplace to sell to customers who desire them. Individuals do this. The state steals wealth from so-called customers by forcing them to pay for “goods” and “services” such as the military whether they want to do so or not. Taxation is the most visible form of stealing. But it is far from the only engine of theft. By crippling competitors who would provide for society’s needs on the free market, government also steals opportunity and unrealized profits from the productive class of people.

The most powerful tool of public theft, however, is the state’s monopoly on issuing money or fiat. Rothbard explains, “The emergence of money, while a boon to the human race, also opened a more subtle route for governmental expropriation of resources.…[I]f government can find ways to engage in counterfeiting—the creation of new money out of thin air—it can quickly produce its own money without taking the trouble to sell services or mine gold. It can then appropriate resources slyly and almost unnoticed, without rousing the hostility touched off by taxation.”

The “almost unnoticed” part of the foregoing analysis is key. Everyone understands taxation because it comes with forms to fill out, deductions from a paycheck, imprisonment for evasion, scary agents who audit, and a painful premium on goods at the cash register. Almost everyone resents taxation; outbreaks of resistance, rebellions, and calls for repeal are common themes throughout history; the American Revolution is an example. Predictably, government wants to reduce the presence of enraged mobs protesting its policies in the street. Yet it needs that wealth.

By contrast, a complex and arcane spiral of inflation rarely enrages the average person who does not notice it until the effects are ruinously apparent and inescapable. If taxation is the equivalent of theft with a gun pointed at people’s heads, then inflation is a cat burglar who strips their homes in the dead night. Inflation is also difficult to avoid because government monopolies have embedded fiat and the central banking system at the core of modern commerce. Perhaps the well-know saying should be “nothing is inevitable except death and inflation.”

What is inflation? Inflation is an increase in the supply of money and credit. It is usually associated with government, and justly so, but it can occur with free-market money as well. The supply of gold could increase for various reasons, including huge mineral finds or a massive release of a bank’s reserve. But a crucial difference between state and free-market inflation is that gold fulfills many non-monetary uses. If the supply increases, then consumption for those uses would increase as well since the cost of gold would fall. This means an inflation in the available units of gold would be a good thing for some people—specifically for

those who use gold in a non-monetary manner. In turn, the increased demand for non-monetary gold would both absorb the “excess” supply and drive the monetary value back up. Free-market inflation is self-adjusting and it is accompanied by a social benefit, including an increase in the value of competing private currencies such as silver.

By contrast, fiat’s only use is as money. This means there is no self-adjusting mechanism. World markets may devalue an egregious fiat if other fiats are not even worse. In that circumstance, however, the government with devalued currency can crank up its printing press and create a vicious circle of further inflating the money supply. Fiat inflation is neither self-adjusting nor does it provide a benefit to anyone except the elite class who receive the freshly printed money first.

For the average person, the word “inflation” is a synonym for “a rise in prices,” but the rise is a consequence of inflation, not a synonym for it. As noted previously, inflation is simply an increase in the supply of money and credit. The difference between these two meanings is much more than semantic. Viewing inflation as rising prices misses much of the great harm inflicted by inflation because it implies that all of society faces the same disadvantage: omnipresent higher prices. The opposite is true. Inflation is a class weapon that redistributes wealth from average people upward to the elite in society. This happens because new fiat is initially valued at the same rate as the old units that are already in circulation. Doubling the money supply overnight would eventually collapse the buying power of each unit in circulation, but the operative term is “eventually.” First users enjoy the preinflation value because the damage trickles down slowly throughout the economy. These first users include the state, bureaucracy, financial institutions, and crony businesses that receive favorable loans. The end user is the average person who receives diluted fiat that has lost buying power as it spread through the economy. The average person bears the brunt of inflation by having the value of his wealth and income sink while the cost of living soars. Meanwhile, the upper class enjoys increased prosperity at his expense.

With legal-tender laws and without the gold standard, little prevents government from pumping up money and credit at will, using interest rates for fine tuning. The incentives are all on the side of inflation. It is hugely profitable to the state and mostly invisible to the public, especially in its early stages. The economic villain of free-market advocates, John Maynard Keynes, knew this well. His pivotal book *The Economic Consequences of Peace* declares:

> Lenin is said to have declared that the best way to destroy the Capitalist System was to debauch the currency. By a continuing process of inflation, government can confiscate, secretly and unobserved, an important part of the wealth of their citizens. By this method they not only confiscate, but they confiscate arbitrarily; and while the process impoverishes many, it actually enriches some. As the inflation proceeds and the real value of the currency fluctuates wildly from month to month, all permanent relations between debtors and creditors, which form the ultimate foundation of

> capitalism, become so utterly disordered as to be almost meaningless; and the process of wealth-getting degenerates into a gamble and a lottery.
>
> Lenin was certainly right. There is no subtler, no surer means of overturning the existing basis of society than to debauch the currency. The process engages all the hidden forces of economic law on the side of destruction, and does it in a manner which not one man in a million is able to diagnose.

The harms of inflation scroll on. Rothbard emphasizes a less-discussed one:

> It distorts that keystone of our economy: business calculation. Since prices do not all change uniformly and at the same speed, it becomes very difficult for business to separate the lasting from the transitional, and gauge truly the demands of consumers or the cost of their operations. For example, accounting practice enters the 'cost' of an asset at the amount the business has paid for it. But if inflation intervenes, the cost of replacing the asset when it wears out will be far greater than that recorded on the books. As a result, business accounting will seriously overstate their profits during inflation—and may even consume capital while presumably increasing their investments.

Central banks bear massive blame for the theft and distortions of inflation; the state is ultimately to blame. A central bank is a clearing house for national currency; it is a middleman for a nation's financial policies. It enjoys monopoly control over the production and distribution of a nation's money and credit. Typically, it also sculpts monetary policy through mechanisms, such as setting interest rates, and it polices member banks.

The American Federal Reserve System is sometimes called "private." For one thing, the regional Reserve Banks are private corporations owned by their member banks. The label is illusory. The Federal Reserve was established by an act of Congress in 1913 and derives its core power from a government-granted monopoly to issue legal tender. The system may mimic a private agency in some ways but, as Rothbard explains, the system of banks are "always directed by government-appointed officials, and serve as arms of the government."

The Federal Reserve enables inflation. It does so in two root ways: by removing checks on inflation and by directing inflation itself. Rothbard sketched an early deployment of the first tactic. "[T]he Federal Reserve Act compels the banks to keep the minimum ratio of reserves to deposits and, since 1917, these reserves could only consist of deposits at the Federal Reserve Bank. Gold could no longer be part of a bank's legal reserves; it had to be deposited in the Federal Reserve Bank." Rothbard illustrates the second tactic of directing inflation. "By controlling the banks' 'reserves'—their deposit accounts at the Central Bank. Banks tend to keep a certain ratio of reserves to their total deposit liabilities, and in the United States government control is made easier by imposing a legal minimum ratio on the bank. The Central Bank can stimulate inflation, then, by pouring reserves into

the banking system, and also by lowering the reserve ratio, thus permitting a nationwide bank credit-expansion."

To the extent that government tightens its grip on money is the extent to which freedom and civilization are weakened. Traditional private money confronts and outcompetes government fiat. But as long as the state can dominate and manipulate money, it can own the financial system down to individual bank accounts, bonds, and the other stored wealth of individuals. It can own your future wealth by diluting it through inflation. Until crypto, anarchism stumbled and fell over the trusted third party problem of the state and banks. Until crypto, the state seemed to have an unshakable grip on currency.

Civil Liberties and Central Banks

The central banking system should be rejected not merely on economic grounds but also on civil liberty ones. (Note: I make no distinction between economic and civil rights. They are both expressions of self-ownership; this is the moral jurisdiction every human being has over his own body and peaceful actions simply by virtue of being human. But economic versus civil rights is a common distinction.)

The central banking system is a vehicle of monetary control and funding for anyone in power. According to the *Financial Times*, "Leading central banks now own a fifth of their governments' total debt." The six key central banks "that have embarked on quantitative easing over the past decade—the US Federal Reserve, the European Central Bank, the Bank of Japan and the Bank of England, along with the Swiss and Swedish central banks—now hold more than $15tn of assets according to analysis by the FT of IMF and central bank figures, more than four times the precrisis level." Quantitative easing occurs when a central bank purchases securities, usually government ones, in order to lower interest rates and increase the money supply. This artificially fuels the economy by driving down borrowing costs for households and businesses. But it is unsustainable.

Governments and central banks are not independent. History reveals that collusion between them is inherent and intimate, not accidental. The Swedish Riksbank is widely regarded as the first central bank. Opened in 1668, Riksbank was technically a private, joint-stock bank, but it functioned under strict royal authority; the king mandated the rules of operation and appointed the bank's management. The entire purpose of the Riksbank was to lend funds to the government and to be a clearing house for commerce.

In 1694, the Governor and Company of the Bank of England was created by Royal Charter. It is a model upon which most modern central banks draw. The Bank of England emerged because King William III's credit was drek. The joint-stock company provided a path for the king to rake in the public funds that allowed him to continue waging war. William III was at military odds with Ireland, Scotland, and North America, all of which were in various stages of rebellion. More importantly,

however, the Nine Years' War (1688-1697) with France had devastated England's navy. No financial institution would risk the £1.2M required to reconstruct it.

Accordingly, English law established artificial incentives to encourage loans to the king. Those assisting in the process became incorporated as joint owners of the Bank of England. Lenders gave the king cold cash in return for which they received exclusive access to the government's finances. The bank also became the only limited-liability corporation allowed to issue banknotes, using government bonds as collateral. In other words, the Bank of England extended a loan to a recipient no one else would touch; it acquired bonds from the king—the untouchable recipient; based on the bonds, the bank issued money that was lent out again. Without legal privilege, the central bank would not have attracted investors or finance. With legal privilege, the £1.2M was raised in less than two weeks.

Government and central banks are two hands washing each other.

Financial gain is not the only motive for herding people toward the trusted third party of central banks. There is also the hunger for power. War is the ultimate flexing of power through which governments maintain, assert, and expand themselves. War requires money—a lot of it. The question is always how to get enough. There is outright theft, of course. The economy can be looted, but the looted individuals might object and rebel. Such a rebellion had led to the Magna Carta in 1215; a contemporary commentator warned King John, "With occasions of his wars he pilleth them [the people and nobles] with taxes and tallages unto the bare bones." John was forced to sign the Magna Carta, presumably under threat of death. He pledged to cease pillaging the economy to pay for his wars. More subtlety in plundering was required.

When a government declares war, it does so on at least three fronts: the opposing government, the people of the opposing nation, and the dissenters within its own population. Some internal dissenters agitate on principle, but their ranks are swelled by those who object to the taxes and other civil liberty violations committed in the name of war. For government, the tricky question is how to extract as much money as possible without incurring a backlash? How can it sidestep the tendency of people to assert their civil liberties and resist?

An under-discussed aspect of central banks and currency manipulation is their impact on civil liberties. Direct taxes, confiscations, and regulations are visible. People understand a hand that reaches directly into their pockets or throws them in jail for refusing to pay taxes for war. By contrast, confusing and non-transparent monetary policies are invisible. People do not understand nor do they immediately feel the impact of quantitative easing, for example. It does not drive them into the streets with picket signs. Instead, people go about their daily lives and simply assume the burden of an indirect tax they do not quite grasp.

To restate this point through a parallel: Inflation is a hidden tax that people tolerate even though they would rebel against a direct one. The inflation is

comparatively unseen and not understood, however. People who would protest a pro-war tax tolerate central bank policies, without which the waging of war would be impossible. Those who are anti-war should call, first and foremost, for the dissolution of the Federal Reserve and of all other central banks. But the role of central banks in financing war is unseen, which permits the government to sidestep a confrontation with anti-war activists. People do not assert their civil rights for no other reason than that they do not know those rights are being violated. The role of central banks in social control remains largely unrecognized because it is arcane.

CHAPTER TWO: Technology Meets Anarchy and Both Profit

> Bitcoin is the catalyst for peaceful anarchy and freedom. It was built as a reaction against corrupt governments and financial institutions. It was not solely created for the sake of improving financial technology. But some people adulterate this truth. In reality, Bitcoin was meant to function as a monetary weapon, as a cryptocurrency poised to undermine authority. Now it is whitewashed. It is seen as a polite and unassuming technology in order to appease politicians, banksters, and soccer moms. Its purpose is sometimes concealed in order to make the tech palatable to the unwashed masses and power elite. However, no one should forget or deny why the protocol was written.—Sterlin Lujan

Crypto was created to make a political difference not to make a profit. If the core developers wanted to reap a fortune, then they would not have employed open source software and eschewed the patents that would have made them billionaires. Profiting from crypto and the blockchain are laudable by-products for some, and those who accumulated riches on the free market should be applauded. This is especially true because the manner in which they made money did not interfere with anyone else's privacy and financial freedom. Equally, the blockchain was not forged to make banking more efficient but to render it obsolete. Anyone who believes Bitcoin was designed for financial gain is not paying attention to its history or to the idealism built into its algorithms. Bitcoin was conceived as a vehicle for creating political and social change by empowering individuals and impoverishing government. The developers were revolutionaries. Bitcoin was their opening volley.

Not a moment too soon. The Internet gave the government an incredible weapon against the privacy of individuals, which would have been radically reduced without cryptography—the art of secret communication.

The History of Bitcoin

The history of Bitcoin is sometimes traced back to the engineer and scientist Timothy C. May. May's "Crypto Anarchist Manifesto" (1988) first appeared by being distributed to a few techno-anarchists at the Crypto '88 conference. The six-paragraph manifesto calls for a computer technology based on cryptographic

protocols that would “alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation…The technology for this revolution—and it surely will be both a social and economic revolution—has existed in theory for the past decade…But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable.”

The manifesto concludes with a cry to arms. “Arise, you have nothing to lose but your barbed wire fences!”

Even in 1988, May could draw upon a rich crypto history. In the mid-1970s, cryptography ceased to be the nearly exclusive domain of military and intelligence agencies, which operated largely in secrecy. By contrast, the academic research that later surged forward was openly shared. One event in particular broke government’s grip on the field. In 1975, computer guru Whitfield Diffie and electrical engineering professor Martin Hellman invented public-key encryption and published their results the next year in the essay “New Directions in Cryptography.” (Arguably, the public key was a re-invention as the British had developed such encryption earlier, but they had been silenced on the subject by government.) In 1977, cryptographers Ron Rivest, Adi Shamir, and Leonard Adleman created the RSA encryption algorithm, which was one of the first practical public-key systems.

Public-key encryption hit the computer community like an explosion. Its brilliance is its simplicity. Every user has two keys—a public and a private one—both of which are unique. The public key scrambles the text of a message that can be unscrambled only by the private key. The public key can be thrown to the wind but the private one should be closely guarded. At the time, the result was close to impenetrable privacy.

Diffie was inspired by the trusted third party problem. The book *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (1996) quotes him as saying, “You may have protected files, but if a subpoena was served to the system manager, it wouldn’t do you any good. The administrators would sell you out, because they’d have no interest in going to jail.” His solution was to remove the need for trust through a decentralized network in which each individual possesses the mathematical key to his own privacy—the right most threatened by digital society. Public-key encryption also removed the tension of sending secure information over insecure channels. It excluded “Eve”; this is the name cryptographers call an unwanted eavesdropper who could be the state or a common criminal. Importantly, public-key encryption was free to all because a successful revolution requires nothing so much as participation.

Government was not amused. The National Security Agency (NSA) could no longer eavesdrop at will because its domestic monopoly on encryption was suddenly ripped away. The journalist Steven Levy commented in a *Wired* article, “In 1979, Inman [then head of the NSA] gave an address that came to be known as ‘the

sky is falling‘ speech, warning that ‘non-governmental cryptologic activity and publication...poses clear risks to the national security’.”

A later statement by cryptographer John Gilmore captured the rebellious response.

> Show us. Show the public how your ability to violate the privacy of any citizen has prevented a major disaster. They’re abridging the freedom and privacy of all citizens to defend us against a bogeyman that they will not explain. The decision to literally trade away our privacy is one that must be made by the whole society, not made unilaterally by a military spy agency.

What could be called “the first crypto war” erupted when the NSA tried to curtail circulation of Diffie’s and Hellman’s ideas. The agency informed publishers that the two rebels and anyone who published them could face jail time for violating laws restricting the export of military weapons. One of Hellman’s outlets, the Institute of Electrical and Electronics Engineers (IEEE), received a letter that read, in part, “I have noticed in the past months that various IEEE Groups have been publishing and exporting technical articles on *encryption and cryptology*—a technical field which is covered by Federal Regulations, viz: ITAR (International Traffic in Arms Regulations, 22 CFR 121-128).” Gag orders were issued. Legislation was proposed. The NSA attempted to control funding to crypto research and considered requiring people to escrow their private keys with a third party who would be vulnerable to a judge’s order or to the police. This would have returned the trusted third party problem that public-key encryption was intended to avoid. In reaction, Electronic Frontier Foundation co-founder John Perry Barlow declared, “You can have my encryption algorithm…when you pry my cold dead fingers from my private key.”

The NSA failed. Powerful encryption became a public good that offered extraordinary privacy to individuals.

Arise Cypherpunks

In the late 1980s, cypherpunks emerged as something akin to a movement. The deliberately humorous label was coined by hacker Judith Milhon who blended “cipher” with “cyberpunk.” The cypherpunks wanted cryptography to defend against both surveillance and censorship by the state. They also sought to build a counter-economic society as an alternative to existing bank and financial systems. As defined by its exemplar and anarcho-capitalist Samuel E. Konkin III, counter-economics is the study and practice of all peaceful human action that is forbidden by the state.

The cypherpunks’ vision was facilitated by the pioneering work of computer-scientist David Chaum, nicknamed the “Houdini of crypto.” Three of his papers were particularly influential.

- "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms" (1981) lays the groundwork for research into and development of anonymous communications based on public-key cryptography.
- "Blind Signatures for Untraceable Payments" (1983) states, "Automation of the way we pay for goods and services is already underway…The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy, as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns." The essay calls for digital cash.
- "Security without Identification: Transaction Systems to Make Big Brother Obsolete" (1985) further describes anonymous digital cash and pseudonymous reputation systems.

A typical cypherpunk distrusted and disliked government, especially the federal variety; the NSA's crusade against unclassified encryption only strengthened this response. Most cypherpunks also embraced the counterculture with its stress on free speech, sexual liberation, and the freedom to use drugs. In short, they were civil libertarians. One of the earliest portraits of the coding radicals was the Levy *Wired* article previously mentioned. Levy called them "techie-cum-civil libertarians." They were idealists who "hope for a world where an individual's informational footprints—everything from an opinion on abortion to the medical record of an actual abortion—can be traced only if the individual involved chooses to reveal them; a world where coherent messages shoot around the globe by network and microwave, but intruders and feds trying to pluck them out of the vapor find only gibberish; a world where the tools of prying are transformed into the instruments of privacy." The stakes? "The outcome of this struggle may determine the amount of freedom our society will grant us in the 21st century." The ideal is not to be granted freedom, of course, but to take it as a natural right.

In 1991, Phil Zimmermann developed Pretty Good Privacy (PGP), which became the world's most popular email encryption software. He viewed PGP as a human rights tool and believed in it so deeply that he missed five mortgage payments and almost lost his house to design it. The original version was called "a web of trust." Zimmermann describes this protocol in the manual for PGP version 2.0.

> As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.

PGP was initially distributed for free by being posted on computer bulletin boards. Zimmermann explained, "[l]ike thousands of dandelion seeds blowing in the wind" PGP spread around the globe. Government noticed, and Zimmermann was

targeted in a three-year criminal investigation based on the possible violation of U.S. export restrictions on cryptographic software.

Fast forward to 1992. May, Milhon, Gilmore and Eric Hughes formed a small group of coding zealots who met every Saturday in a small office in San Francisco. A *Christian Science Monitor* article describes the group as "all united by that unique Bay Area blend: passionate about technology, steeped in counterculture, and unswervingly libertarian."

The group grew rapidly. An electronic posting forum called The List became its most active aspect, with the "people's algorithms" drawing staunch support from the likes of Julian Assange and Zimmermann. The *Christian Science Monitor* article comments, "Radical libertarians dominated the list, along with 'some anarcho-capitalists and even a few socialists'. Many had a technical background from working with computers; some were political scientists, classical scholars, or lawyers." Eric Hughes contributed another manifesto to the movement. "A Cypherpunk's Manifesto" opens, "Privacy is necessary for an open society in the electronic age." It continues, "for privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society."

The group quickly encountered an objection that would come to dominate the government's attack on private encryption; "bad actors," it was argued, will use anonymity to commit crimes. During a 1992 interview, a skeptic confronted May. "Seems like the perfect thing for ransom notes, extortion threats, bribes, blackmail, insider trading and terrorism," he challenged. May replied, "Well, what about selling information that isn't viewed as legal, say about pot-growing, do-it-yourself abortion? What about the anonymity wanted for whistle blowers, confessionals, and dating personals?" What about the "good actors" who would be penalized by the removal of private encryption?

Cypherpunks believed public-key encryption actually made society *less* dangerous, *less* criminal because it reduced or removed at least two major sources of violence. The first was the state; its criminal intrusion into the personal lives of individuals could be largely neutralized by effective privacy. If financial exchanges were invisible, for example, the theft of taxation or confiscation would be impossible. The second source of violence was the risk attached to victimless crimes such as drug use ,which were not viewed by the cypherpunks as crimes at all. Public-key encryption reduced or removed this risk. Ordering drugs online, for example, was safer than buying them in a back alley of a bad neighborhood at midnight.

Without question, public-key encryption could shield activities that *did* violate rights, just as paying by cash could do so. This prospect was largely irrelevant, however, as encryption was a reality that would spread in spite of unpleasant side effects. Cypherpunks argued that technology or community could evolve solutions to real online crime.

The Crypto Wars Continue

One incident captured the core of the crypto wars between cypherpunks and the state. Gilmore determined to save and spread the information in documents being threatened by NSA censorship. He distributed a paper by a cryptographer whose work the NSA had been instrumental in suppressing. After Gilmore posted it on the Internet, the paper went viral. In 1992, Gilmore filed a Freedom of Information Act (FOIA) request to acquire the declassified parts of a four-volume work by William Friedman, who is sometimes called the father of American cryptography. The manuals were decades old. Gilmore also requested the declassification of Friedman's other books.

While NSA dragged out its response to the FOIA, Gilmore heard fascinating news from a cypherpunk friend. Friedman's personal papers had been donated to a library after his death and they included the annotated manuscript of a classified book. The friend simply lifted the book off the library shelf and Xeroxed it for Gilmore. Another of Friedman's classified books was found on microfilm at Boston University. Gilmore notified the judge in what had become a FOIA appeal that the so-called classified documents were publicly available in libraries. Before he did so, however, Gilmore made several copies of the material in question and hid them in obscure places, including an abandoned building.

The NSA reacted with extreme prejudice. They raided libraries and reclassified documents that had been publicly available. The Justice Department called Gilmore's lawyer to say that his client was close to violating the Espionage Act, which could bring a prison term of ten years. The violation: he showed people a public library book.

In turn, Gilmore contacted technology reporters in the press. The NSA feared publicity, and the cypherpunks knew it. Articles critical of the NSA began to flow, including one in the *San Francisco Examiner*. Two days later, the *New York Times* stated, "The National Security Agency, the nation's secretive electronic spy agency, has abruptly retreated from a confrontation with an independent researcher over secret technical manuals he found in a public library several weeks ago.…[I]t said that the manuals were no longer secret and that the researcher could keep them." The *Aegean Park Press*, a California publisher, quickly printed the books.

The early cypherpunks were prototypes who set the attitude, technology, and political context in which much of the next generation of crypto zealots operated. The goals were disobedience to unjust authority, counter-economics, personal freedom, and the disruption of a corrupt system through cryptography.

Cautionary Tales From Earlier Digital Cash

> There are 3 eras of currency: commodity based, politically based, and now, math based.—Chris Dixon

Versions of digital cash and online transfer systems existed decades before Bitcoin. DigiCash and e-gold are among the better-known, but neither one could shake the dogged trusted third party problem. Both lacked the essential vehicle of privacy and self-banking created by Satoshi: the blockchain. The early systems are useful as cautionary tales, however, and they spotlight the elegance of Bitcoin.

DigiCash: Its Lessons.

In 1983, the renowned cryptographer David Chaum introduced the idea of digital cash in a path-breaking research paper. In 1989, he founded an electronic money corporation named DigiCash, which, in turn, established the electronic payment system e-cash. (The actual currency was dubbed DigiCash.) E-cash has been called “technically perfect.” It built upon an earlier system designed by Chaum: Blind Signature. This is a digital signature in which the content of a message from one person is disguised so that it is not seen by a second person who authenticates the message.

The process is often described by an analogy. A voter wants his ballot to remain secret. To be counted, however, it must be signed by an election official who verifies the voter’s eligibility. The solution: the voter writes his credentials on the outside of an envelope, wraps the marked ballot in carbon paper, and places it inside the envelope. The official verifies the credentials and signs the envelope, thereby transferring his signature to the ballot inside; he verifies the ballot without knowing its contents. The voter puts the now-authorized ballot into a new unmarked envelope that is slipped into a box of ballots waiting to be counted. The tabulator verifies the authenticating signature and the vote is recorded. The vote counter has no idea of who cast any particular ballot, however. Neither the content of the vote nor the ballot itself can be linked back to an individual voter. This is the essence of a blind signature.

In simple terms, the Chaumian e-cash uses blind signatures as follows. At a bank that handles e-cash, you have an account with $20 to which a password gives access. To withdraw e-cash in sums of $1 each, you use software to generate 20 unique, random numbers of sufficient length that it is highly unlikely anyone else will also produce them. The problem: you need the bank to verify that each number represents $1 in value, but you don’t want the bank to know which $1 is which because then the currency could be tracked. If nothing else, the bank could match outgoing and incoming data, allowing it to know where you shop, what you buy, your lifestyle, and other information that you wish to remain private.

You maintain privacy by “blinding” each request with special encryption. The bank then receives a scrambled request upon which it signs off with a private key for $1; this affirms both value and authenticity. The bank’s stamp converts the number into the equivalent of a $1 coin that can be used only by you. It is anonymous; the bank knows how many $1 units it stamped for you, but it cannot

distinguish between those 20 units or recognize them from any other $1 unit it has ever authenticated.

To spend the cash, you unblind the number. This results in a valid signed message that can be verified by the bank's public key. The $1 units are stored on your computer, waiting to be sent to anyone who accepts e-cash. To do so, you send the person a decrypted, signed number, and they take it to the bank. The signature is verified; the serial number is recorded; the amount is redeemed. Recording the number allows the bank to reject any attempt at double-spending. But the bank cannot connect the transaction to your account, and the $1 recipient has no idea who you are unless you choose to reveal your identity.

The process is as anonymous as cash. It stands in stark contrast to online credit-card use, which involves telling a company and a recipient who you are, where you are, and what you are purchasing. DigiCash is also safe from malicious people who are trying to steal identities. It has an extra advantage. Because it is highly divisible, it accommodates micro-payments—payments under $10, for which transaction costs make credit cards impractical. E-cash was perfect for transferring e-nickels and e-quarters over the Internet.

DigiCash Inc. made quite an impact on the financial community. The first bank to adopt it was the Mark Twain Bank in St. Louis, Missouri, but others soon followed. By 1998, e-cash was available through Deutsche Bank in Germany, Credit Suisse in Switzerland, and several other powerful outlets. But, in 1998, DigiCash Inc. filed for Chapter 11 bankruptcy and subsequently sold its assets, including patents.

What happened? Explanations vary and all may contain some truth.

In a 1999 interview, Chaum claimed DigiCash was an idea before its time because e-commerce had not been firmly established. *Forbes* had another explanation: "A brave new currency for a brave new world, with only one problem: No one wanted it–not banks, not merchants and, most important, not consumers. Electronic commerce is flourishing, but it turns out Visa and MasterCard–not digital cash–are the currency of choice." Most governments were among those who did not like the untraceable money because it could be used to avoid taxes and commit other "crimes," usually against the state.

A fascinating anonymous piece in *Next!* magazine advanced an entirely different theory. Cryptographers, it explains, are generally paranoid. And Chaum is a GREAT cryptographer. The internal workings of DigiCash depicted in the article sound like a psychiatric ward, not a tech company. Chaum also seemed to be an abysmal businessman. One example:

> ING Investment Management was interested. This deal was about twenty million guilders [$10 million USD at the time]. The plans were all laid out. ING Barings together with Goldman Sachs would also bring DigiCash to the stock market within two years. 'The day we were all set to sign, David didn't want to', tells Stofberg [the man responsible for DigiCash's financial affairs].

> ‘He was so paranoid, that he always thought something was wrong. There were 8 people from ING, including the CEO, and David simply refused to sign‘!

A more interesting approach than psychologizing is to look at some of weaknesses of the e-cash and DigiCash systems, which contributed to its failure and to contrast them with the success of bitcoin and the blockchain.

> • Chaum believed in patent and copyright, both of which he applied to his designs. This severely restricted access and co-operative development by a global community of brilliant minds. Putting a price-tag on the product hindered broad public acceptance. By contrast, Bitcoin is patent-free and open-source, which gives unrestricted access and allows development to sprint forward.
> • E-cash did not get around the trusted third party problem because it needed an authorizing blind signature from a financial institution. Moreover, its growing alliance with prominent central banks indicated a growing presence of trusted third parties. Peer-to-peer bitcoin eliminates trusted third parties altogether because acceptance by the blockchain *is* the authorization, and each participant is a self-banker.
> • E-cash required a centralized issuer such as a bank. Bitcoin is decentralized down to the individual level.
> • E-cash preserved the existing banking system. Bitcoin renders the current system irrelevant.
> • E-cash was vulnerable to the personality flaws of one man. The Bitcoin community is haunted by internal conflicts, but no one personality can destroy it because no one owns the system. Besides which, it is always possible to create an alternate crypto to compete with one that is subpar in some manner.
> • E-cash was not designed for financial freedom. The essay “Untraceable Electronic Cash,” co-authored by Chaum, stated, “Generating an electronic cash should be difficult for anyone, unless it is done in cooperation with the bank.” The anarchists and idealists who sculpted Bitcoin wanted to empower the individual against banks and the state and needed no one’s permission to do so.

No wonder corporations showed immediate interest in e-cash. They have only recently shown interest in Bitcoin, which they now hope to patent, dominate, and tame for their own purposes.

E-gold: Its Lessons.

E-gold was a digital gold currency system that was operated between 1996 and 2009 by Gold & Silver Reserve, Inc. In 2000, G&SR restructured and a new company, e-gold Ltd., assumed the administration of e-metal issuance and transfers. The digital currency was linked to gold, with the typical unit of account being grams or troy ounces. Like early U.S. gold certificates, e-gold represented units of gold for which it could be redeemed on demand from stored metal.

Customers with accounts on the e-gold website could also make instant transfers of precious metals to other accounts.

It was one of the first payment systems to allow complex global exchanges outside the traditional banking system. A critic of fiat currency and conventional banking, co-founder and libertarian Douglas Jackson had a mission; he wanted to forge a private alternative to the financial mire caused by governments. In the book *A History of Digital Currency in the United States: New Technology in an Unregulated Market* (2016), the publisher of *Digital Gold* magazine P. Carl Mullan quoted Jackson as saying that such a "task required large-scale computational capacity, data storage and secure global means of communication." The costs were prohibitive, except for national governments. That is, until the Internet.

With the Internet, e-gold pioneered several breakthroughs. In 1999, for example, the company introduced wireless mobile payments using a web-enabled cellphone. This was seven years before PayPal offered a similar service. A less laudable innovation came in 2000 when the company required customers who wished to add value to their accounts to have a trusted and independent third party who could exchange e-gold for fiat and vice versa. Within a year, several dozen businesses and individuals filled that niche; a new industry was born.

According to e-gold Ltd., the number of accounts grew from 1 million in 2003 to 5 million in 2008. E-gold users had a variety of motives. Some were gold bugs who devoutly believed e-gold was superior to fiat. Others were economic anarchists who thought government had no proper role to play in money. Still others wanted to evade taxes or the risks of other victimless crimes.

Many more flooded into the emerging High Yield Investment Programs, some of which used e-gold as a payment platform. These programs offered unrealistically high returns that could be maintained only by redirecting the wealth of new investors; the Ponzi schemes led to an e-gold rush on an international level. Fraud artists took advantage of e-gold features such as the fact that all transactions were final and never charged back. The scammers opened e-gold accounts and urged prospective investors to do the same. Then they milked investors and buyers for all they could.

By this time, e-gold offered a wide range of services from online casinos and auctions to metals trading and donations to non-profits. The company was rife with possibilities for scammers. Unfortunately, defrauded customers often made no distinction between the ethical e-gold itself and the con artists who ripped them off with faux investments or non-existent goods. Some disillusioned users complained to government authorities.

In 2007, the U.S. Federal Government accused e-gold of money laundering and violating 18 U.S. Code § 1960, which prohibits businesses from transmitting money without a license. Several exchanges attached to e-gold were closed down. The publicity and disrupted exchanges caused a steep drop in the number of e-gold customers; the difficulty of exchanging e-gold for fiat caused potential

recipients of e-gold to shy away. Many customers were trapped with accounts they could not liquidate.

E-gold vigorously fought the charges, to no avail. In April 2008, the judge in *United States of America v. E-gold, Ltd.* ruled against the company and in doing so dramatically increased the Treasury Department's range of authority. The law now defined a "money transmitter" as a business that transferred any stored value from one person to another, even if the transfer involved cash. This was a blank check on future prosecutions.

The company's three directors pleaded guilty and entered into an agreement by which e-gold would comply with the legal requirements for a money-transmitting business, including being licensed. Jackson received 300 hours of community service, 3 years of supervision, and a $200 fine. He could have received 20 years and a $500,000 fine. The two other directors received the same sentence, with heavier fines.

Then came a bitter irony. The guilty pleas precluded the directors from acquiring a license anywhere in the U.S. This put all of e-gold in lock-down because returning money to customers would involve transmitting money without a license, which violated the plea agreement. In 2010, the government finally allowed e-gold to return the monetized value of their accounts to customers.

The Treasury's expanded and vague definition of "money transmitter" has clear implications for bitcoin. The success of e-gold and the court case against it changed the way government handled online-payment systems. Now it had the legal precedent to act against crypto.

The parallels between bitcoin and e-gold are clear. E-gold was highly divisible into micropayments as tiny as one ten-thousandth of a gram. It maintained an open ledger in which daily transactions were published live and in transparent form. Like bitcoin, e-gold was not a complementary currency. A complementary currency is one that does not compete with a national currency; an example would be private money issued as a promotion by a business to customers, which could be used to purchase merchandise in the store. E-gold was intended as a replacement for fiat and for the banking system, with the added advantage of being a hedge against inflation.

The differences between bitcoin and e-gold are as important as the parallels.

- E-gold embodied the trusted third party problem, as the customers stranded by legal proceedings found out. It is difficult to blame e-gold for the circumstances, of course, but dishonesty or inefficiency are not the only risks of trusting others with your money. Bitcoin eliminates this problem.
- Arguably, e-gold introduced a trusted-fourth-party problem when it insisted customers use exchanges to convert into and out of fiat.
- E-gold and the exchanges were points of centralization and easy targets for regulation or prohibition. They were also choke points at which to gather

customer information. When e-gold restructured in 2000, OmniPay formed as the company's exchange system. OmniPay used three methods to verify the identities of customers: universal postal verification; payment by bank wire only; and, safeguards to detect incoming third-party payments. In e-gold's plea agreement years later, the government almost certainly gained access to that information. Peer-to-peer bitcoin is pseudonymous.
• E-gold's insistence on "membership for use" restricted the spread of its services. Bitcoin is open to all.

The riskiness of a trusted third party exchange like OmniPay is a warning bell for crypto users. A centralized exchange is usually the first target of government regulation because it is visible, vulnerable, and constitutes a cache of valuable data on otherwise elusive users. Exchange owners are likely to comply with government demands because non-compliance means being closed down, imprisoned, or both. In short, centralization encourages even honest third parties to obey laws and regulations that harm customers.

CHAPTER THREE: Discovering Satoshi

> Companies like Visa, Dun and Bradstreet, Underwriter's Laboratories, and so forth connect untrusting strangers into a common trust network. Our economy depends on them. Many developing countries lack these trust hubs and would benefit greatly from integrating with developed world hubs like these. While these organizations often have many flaws and weaknesses–credit card companies, for example, have growing problems with fraud, identity theft, and inaccurate reports, and Barings recently went belly up because their control systems had not properly adapted to digital securities trading–by and large these institutions will be with us for a long time.—Nick Szabo

The greatest financial threat to people's wealth and freedom is the trusted third party system that does not serve customers but rushes, instead, to comply with government regulations such as reporting requirements.

Anonymity is a powerful tool for privacy, but individuals also need to eschew state channels that counter confidentiality. Modern data collection is voracious, and surveillance is accelerating. If you play the state's game by following the financial paths it directs you down, then the state has written the rulebook, and it has the home advantage. It will not play fair. So do not play at all. To repeat Buckminister Fuller, "You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete." Walking away from the state and simply living gives freedom the home advantage. Until recently, however, walking away meant a massive sacrifice of economic opportunities and quality of life because the state had a lock on what Nick Szabo calls "trust hubs."

Satoshi and Buckminister Fuller

The brilliance of Bitcoin: It is the new model of which Fuller spoke. Blockchain users are able to walk away from trusted third parties without deep sacrifice. The blockchain either performs the valid services of a trusted third party or it obviates the need for them. Decentralized exchanges—peer-to-peer exchanges—increasingly provide sophisticated services such as buying and selling crypto as speculation.

Satoshi's "White Paper" and the step-by-step "Bitcoin Whitepaper: A Beginner's Guide" spell out how the blockchain replaces trusted third parties. The paper defines "an electronic coin as a chain of digital signatures." The coins travel over a distributed digital ledger, called the blockchain, by which they are recorded in a transparent, chronological, and immutable fashion. These are the basic steps in a coin's journey:

1. An individuals broadcasts a new transaction to all nodes or computers in the network.
2. The nodes collect the new transaction into a block. A block is akin to a single page in the ledger of the blockchain, and it contains information on a specific transfer, as well as processing data.
3. The controller of each node—called a "miner"—performs a proof of work for the block. Proof of work is a computer calculation that is difficult to produce in terms of processing power and time, but it is easy for others to verify.
4. When a node has a proof of work, it broadcasts the completed block to all other nodes.
5. Nodes accept the block only if the transaction is valid and the coin has not already been spent. Unique timestamps, which are included in every block, prevent double spending.
6. The nodes express acceptance of the block by proceeding to work on the next one in the chain, using the hash of the previously accepted block to build a seamless continuity of information. A hash is a function that converts an input into an alphanumeric string of fixed size. Each block has a unique hash value.

Trusted third parties originally arose because they provided valid functions to customers. The functions included verification of a transaction, ease and security of a transfer, preservation of privacy, prevention of double spending, mediation of disputes, and provision of a record. Today's trusted third parties have perverted these valuable services to customers into assaults upon them. Bitcoin returns these services to individuals without attendant attacks.

Verification of a transaction. A valid trusted third party authenticates a transaction. A bank may compare the signature on a check with one that's kept on file, or it may verify that money is not counterfeit. These services have value. But a staggering amount of authentication performed by banks today is a *dis*value to customers. The exhaustive verification of a customer's identity, for instance,

violates his privacy to satiate the government's appetite for data, which is often used to damage the customer.

The blockchain verifies transactions without intruding upon users. The transfer is authenticated, not the participants. The transaction is verified by miners through a proof of work conducted on a block. A coin is authenticated when the proof of work is completed, and the block is accepted by the blockchain. Since the blockchain is an open public ledger, everyone can trace the history of a coin and be assured of a transaction's accuracy without knowing the identity of those involved. The government is able to browse the blockchain, but the ledger is far more of a barrier than an aid to surveillance.

Ease of transfer. As global commerce gallops forward and the Internet encourages instant gratification, the speed and ease of transfers become increasingly important—that is, to the customer. With a virtual monopoly on international transfers, however, banks set terms that advantage them and disadvantage customers. Banks impose direct and indirect costs. One direct cost is the fee attached to each transfer, which can be substantial. Three indirect costs: the currency conversion, if necessary; the personal information required; and the considerable time a transfer can take to clear. The clearing period is called the "float." Float is money in the banking system that is counted twice in the process of transferring a payment—once when the it is deposited in the payer's bank, and once when it is received by the payee's bank. Since the payer's bank receives interest on the floating money, it has incentive to make the process longer than necessary.

By contrast, the blockchain does not recognize distance in the transfer of wealth or information. Two computers in the same household can be as close or far away from each other (in terms of transmission time) as two computers on different continents. Miners charge a fee for their service, but the fees are known and have no hidden gotchas. If the fee for transfer of one crypto is unsatisfactory, then there are many other cryptos to choose from. By contrast, bank fees tend to be standardized. Most transfers occur quickly—at least, compared to banks—and there is no float. The blockchain has no self-interest or hidden agenda.

Security of transfer. Even honorable banks can be hacked, robbed, and compromised in transmissions. Although much is made of crypto exchanges losing or stealing wealth from their accounts—and this is an undeniable problem—banks are as vulnerable. There is one huge difference between the two regarding security, however. Every over-the-table financial institution delivers customer information to the government, which utilizes the data to tax, confiscate, fine, and arrest customers.

The blockchain is decentralized and resists hacking attacks; it cannot be corrupted by bad intentions because it is inanimate. The widely publicized loss of coins through theft occurs when a person moves from the peer-to-peer transfers that he controls and deposits his coins into an exchange, especially a centralized

one. The crypto community needs to reduce the risks in this category of crypto use. The work is underway.

Meanwhile, no personal information is surrendered to government. The ledger is transparent to all, including the state, but it is relatively easy to mask an identity and to scramble transfers through services such as mixers or tumblers. The blockchain is currently the most secure method by which to transfer funds online. The main threat to security is if government attempts to control the entire Internet. If this is possible to do and if alternatives did not quickly arise, then all methods of online transmission are threatened, not merely crypto.

Preservation of privacy. The type of privacy once notoriously offered by Swiss banks is long gone, even in Switzerland. Financial institutions are choke points at which a customer's personal data are collected and shared with authorities. The only true privacy is the secrecy with which banks inform on a customer, without the customer's knowledge or consent.

Maintaining privacy on a transparent blockchain seems to be a contradiction in terms. The "Bitcoin Whitepaper: A Beginner's Guide" explains why it is not. "With the peer-to-peer network, privacy can still be achieved even though transactions are announced. This is accomplished by keeping public keys anonymous. The network may be able to see payment amounts being sent and received, but transactions are not linked to identities."

If a user decides to reveal public keys, then a common privacy strategy is pseudonymity. A peer-to-peer transfer does not require information beyond the crypto addresses of the sender and the recipient, which are privately generated by each participant's wallet. Nevertheless, when a person joins the blockchain, he becomes vulnerable to network analysis that searches for patterns of transfers in order to piece together a user's profile. That is why some users generate a different address for every transaction, which creates multiple pseudonyms. Satoshi explains, "When you generate a new bitcoin address, it only takes disk space on your own computer (like 500 bytes). It's like generating a new PGP private key, but less CPU intensive because it's ECC. The address space is effectively unlimited. It doesn't hurt anyone, so generate all you want."

Other standard privacy practices: create multiple wallets to isolate a transaction or a type of transaction from being associated in a pattern; cloak an IP address by going through an anonymizing tool such as Tor; and go through a mixing service.

Prevention of double spending. Double spending is when the same unit of money is spent in more than one transaction even though it can be spent legitimately only once. Satoshi describes how traditional payment systems prevent double spending, "A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double spent. The problem with this solution is that the fate of the entire money system depends on the company

running the mint, with every transaction having to go through them, just like a bank.” The solution places the money supply in the hands of a trusted third party, or even a trusted fourth party, which makes it a *non*-solution.

In theory, crypto is susceptible to double spending. Two transactions with the same coin could be transmitted in rapid succession so that the first is not publicly recorded before the second one is submitted. Satoshi’s solution is elegantly simple. Every transaction is not only public but also adopted by all network participants in one time line to assure that the order of the chain is the same for everyone. Each transaction is timestamped. If a second transaction with the same coin occurs, then the earliest timestamp is counted, and the later one discarded.

Mediation of Disputes. Physical money has had an advantage over other forms of payment; the exchange is irreversible except with consent or through a lawsuit. Most online payment systems have a built-in procedure for reversing or contesting a transaction. This service increases the overall fees of the payment system, as well as placing a practical limit on the minimum size of a transaction. It also increases the payment system’s hands-on involvement in transactions.

Blockchain transfers are irreversible. Funds can be returned only on a peer-to-peer basis if a recipient agrees to do so. This obviates a fee and enables micropayments. If the traditional guarantee of “money back” is desired, then some services provide escrow for an extra fee.

Provision of a record. Financial institutions maintain records, but their content may or may not be provided to the customer. A bank’s interaction with a tax agency, for example, will almost certainly be withheld from an account holder. This means that many records are kept for the benefit of the bank and the government only, not for the customer.

The blockchain itself is the record. It is an immutable, transparent ledger of every transfer that has occurred since the original Genesis block. No concealed interaction can harm a user.

In summary, crypto provides both the services of an honest third party and additional advantages.

Is Satoshi a Libertarian and Anarchist?

Part of exploring the dynamic of trusted third parties and the importance of bypassing them is to ask, “Why was this task so important to Satoshi?” Was he a libertarian and anarchist or was he politically neutral and simply fed up with banks? An explicit statement from Satoshi on the issue would have been very useful in answering this question. As the situation stands, however, the best anyone can do is to examine surrounding evidence such as his brief online statements and the White Paper, then speculate from the structure of Bitcoin itself.

On October 31, 2008, Satoshi published "Bitcoin: A Peer-to-Peer Electronic Cash System" (the "White Paper") on the Cryptography Mailing List at metzdowd.com. It presents the technology behind Bitcoin and the design of its instrument of implementation—the blockchain. Satoshi's brief explanation is a defining technological document of our century.

It is all the more remarkable, therefore, that no one seems to know Satoshi's identity, if "he" is really a team, or much of anything else about him. Clearly, he coded from a love of technology rather than a desire for fame because he shunned the spotlight; he also did not pursue academic status. Since the code is open source and unpatented, acquiring wealth was not a driving force either, even though the one million bitcoins in his account now constitute an incredible fortune. Unlike May and other predecessors, Satoshi exhibited no swagger or desire to shock; in one post, he apologetically and modestly says, "Sorry to be a wet blanket. Writing a description for this thing [Bitcoin] for general audiences is bloody hard." In short, no one can definitively state Satoshi's motives or his ultimate purpose. By process of elimination, political motivation becomes more probable. His acts and words provide other reasons to reach this conclusion.

Satoshi began writing Bitcoin code in 2007. When the "White Paper" appeared on the Cryptograpy mailing list in 2008, it was also made available on a website created by Satoshi—bitcoin.org. The mailing list consisted of experts in math, statistics, and cryptography, who immediately argued against the viability of Bitcoin. It will not scale, they claimed; it requires too many resources to be practical, they argued. Moreover, "bad" nodes could control the network's CPU power and generate a longer chain than "honest" nodes; bad actors could control the blockchain.

Satoshi's patient responses gradually convinced most of the list that Bitcoin might work. Meanwhile, developments in the rollout happened quickly. Highlights include:

• January 3, 2009, the Genesis Block is mined.
• January 9, 2009, version 0.1 of bitcoin software is released on Sourceforge.
• January 12,2009, the first bitcoin transaction occurs.
• October 5, 2009, an exchange rate of $1 US=1,309.03 BTC is established.
• October 12, 2009, the #bitcoin-dev channel is registered for open source development communities.
• December 16, 2009, version 0.2 is released.
• March 6, 2010, dwdollar establishes a Bitcoin currency exchange.
• May 22, 2010, first real-world transaction occurs when a pizza is purchased for 10,000 bitcoins.
• July 7, 2010, version 0.3 is released.
• October 16, 2010, the first escrow transaction occurs.

In mid-2010, Satoshi transferred bitcoin.org to Gavin Andresen. Andresen explains:

> I started to submit code to Satoshi to improve the core system. Over time he trusted my judgment on the code I wrote. And eventually, he pulled a fast one on me because he asked me if it'd be OK if he put my email address on the bitcoin homepage, and I said yes, not realizing that when he put my email address there, he'd take his away. I was the person everyone would email when they wanted to know about bitcoin. Satoshi started stepping back as leader of [the] project and pushing me forward.

In 2010, Satoshi went silent. Again, it is clear that he did not write for fame.

The systematic and meticulous release of Bitcoin, as well as the elegant structure of the blockchain, reflects a man who thinks situations out in detail and understands their implications. Satoshi grasped the political impact of his revolutionary system, but he made scant comment on the matter.

Evidence of Satoshi's Political Motives

Great debate revolves around Satoshi's politics with many people projecting their own attitudes toward Bitcoin onto him. But all real-world indications point to Satoshi being a libertarian, an anarchist, or both. Evidence of Satoshi's political beliefs dates back to the Genesis block—the first link in the blockchain. It contains the message: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." The message is a headline from the front page of the UK newspaper the London *Times*. January 3, 2009 is the blockchain's birthday—the unveiling of Satoshi's gift to the world. Why did he choose to announce it with these specific words?

Some people think the wording was a random pluck from the January 3 issue of the *Times,* and it was inserted for the sole purpose of proving the date. They claim the message could as easily have been "Ten Sex Workers Arrested in Sting." This contention defies credibility. Satoshi was a methodical programmer who went directly to the heart of matters without frivolity, caprice, or asides. He released what he must have known was a masterpiece of coding, and it is not plausible that he slapped a random message into the Genesis block. The very fact that the first block is named "Genesis"—probably a reference to the first book of the Bible in which God creates the world—shows the significance Satoshi placed on the event.

A much different scenario is highly likely. Satoshi is sitting at his computer, preparing to release the first block to the world like a seed on the wind. He knows its power, and he wants people to know its purpose without having to crack open his shell of anonymity. He has just read the morning paper with its continuing reports of financial turpitude in which political and financial elites have acted solely for their own benefit at the expense of taxpayers. A headline provides the perfect snippet about the two agencies most responsible for the economic rape of taxpayers—government and the banking system. The eight words also capture the collusion between them. Satoshi carefully types, "Chancellor on brink of second bailout for banks," and he embeds this message into the Genesis of a

dynamic he believes can change the world. The intent is anti-Chancellor, anti-bank, and anti-bailout. From the blockchain's first blink, it declares that the power of money is returned to the people.

Evidence From the "White Paper"

Another point of debate on Satoshi's political intentions revolves around the neutral tone of the "White Paper." The paper even states that a system of trusted third party financial institutions "works well enough for most transactions." Only practical objections to the existing system are outlined within it. In short, the "White Paper" does not read like a political manifesto.

Nor should it. A white paper is technical. It is an authoritative explanation of an idea or an experiment and of its results or conclusions, which is presented for review to experts in the same field. Its purpose is to lay out a concept, to solve a problem, or to reveal a finding. Ideology has no place. Moreover, the list on which Satoshi posted the "White Paper" was composed of experts in math, statistics, and cryptography who wanted the bare technical facts, not the politics surrounding them. The members undoubtedly held a variety of political views, and they may well have stumbled over ones with which they disagreed. The List was not the time, it was not the place to state political motives or beliefs.

One political reference is prominently positioned, however. Footnote [1] reads, "W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998." This is Satoshi's nod of appreciation to the 1998 b-money proposal developed by famed cypherpunk Wei Dai, with whom Satoshi had email exchanges. Dai's proposal is widely viewed as a precursor to the "White Paper," with some people believing that Dai is Satoshi. On August 22, 2007, Satoshi emailed Dai to inform him, "I'm getting ready to release a paper that expands on your ideas into a complete working system." The fact that Dai's views are a springboard to the "White Paper" make them worth examining.

Dai's b-money proposal opens:

> I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word 'anarchy', in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations." The proposal concludes, "The protocol proposed in this article allows untraceable pseudonymous entities to cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts. I hope this is a step toward making crypto-anarchy a practical as well as theoretical possibility.

It is also reasonable to examine the features Satoshi chose to embed within Bitcoin as a reflection of his politics. The features include:

• Radical Decentralization. The first line of the abstract of the “White Paper” states, “A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.” No leaders, no bureaucracy, no position of power beyond what the individual wields over himself.
• Privacy. Section 10 of the “White Paper” is entitled “Privacy.” While not perfect, the anonymity sought and offered by Bitcoin is far superior to that of other forms of online payment. Section 10 ends with a warning and, perhaps, an indication of an improvement Satoshi was planning to make to the blockchain. “As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.“
• Pro-capitalism. The “White Paper” stresses Bitcoin’s advantages to commerce and merchants as a free-enterprise payment system. It states, “With the possibility of reversal [which Bitcoin does not accommodate], the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need.” It is difficult to imagine a socialist having this insight or caring about merchants at all.
• Anti-banking. The entire purpose of Bitcoin is “online payments…without going through a financial institution.” On the PGP forum, Satoshi explained, “The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.”
• Anti-government. Although government is not mentioned in the “White Paper,” Bitcoin is a direct attack on an allegedly vital state function—banking. The message in the Genesis block was a slap at the Chancellor as much as at the bank bailout.
• Anti-inflation. Section 6 of the “White Paper,” entitled “Incentive,” claims that “once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.” The predetermined number is 21 million coins that are each divisible down to a tiny fraction of a whole coin.

The preceding features come close to a statement of economic anarchism. A *CoinJournal* article entitled “Op-Ed: Satoshi Nakamoto is Clearly an Anarchist” refers to a 2014 presentation by Daniel Krawisz of the Satoshi Nakamoto Institute. Krawisz states, “Someone who promotes bitcoin who is not an anarchist is a crypto-anarchist because bitcoin is inherently anarchistic.”

Evidence From Posts and Personal Association

Satoshi's less formal posts on forums are further evidence of his politics. Again, the remarks are anti-banking and anti-government while openly acknowledging Bitcoin's appeal to libertarians.

> • Anti-banking. Again, Satoshi writes, "Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with hardly a fraction in reserve."
> • Anti-government: When a poster objects to Bitcoin, saying, "You will not find a solution to political problems in cryptography," Satoshi responds,"Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own."
> • Pro-libertarian. "[Bitcoin is] very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though." Moreover, Satoshi's post on the bitcointalk forum, Bitcoin does NOT violate Mises' Regression Theorem, indicates his familiarity with Mises, and the thread itself discusses Rothbard's signature book *Man, Economy, and State*.

Personal associations are another indicator of personal beliefs. Foremost among Satoshi's associates was the late Hal Finney. A developer for the PGP Corporation, Finney was the first recipient of a bitcoin transaction, which Satoshi sent to him on January 12, 2009. Finney obviously cooperated closely with Satoshi—some believe *he* was Satoshi—which makes Finney's political views relevant. In the early 1990s, Finney contributed regularly to the cypherpunks' listserv. Satoshi also posted a link to his "White Paper" on the P2P Foundation's cypherpunk website, where he was a list member. In a post, Finney states, "Naturally, in today's society, with power allocated so disproportionately, such ideas [cryptography] are a threat to large organizations. Balancing power would mean a net loss of power for them. So no institution is going to pick up and champion Chaum's ideas. It's going to have to be a grass-roots activity, one in which individuals first learn of how much power they can have, and then demand it."

Martti Malmi provides another clue. Malmi was a student at the Helsinki University of Technology, who became a Bitcoin enthusiast. Nathaniel Popper's book *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* describes Malmi's journey. Posting on the anti-state.org forum, which explored free-market anarchism, Malmi writes of Bitcoin, 'I'm really excited about the thought of something practical that could truly bring us closer to freedom in our lifetime'. :-)" In an email to Satoshi, Malmi included a link to this post.

Satoshi replies, "Your understanding of Bitcoin is spot on."

Again, Satoshi fully realized how revolutionary his system would be. When Wikileaks enabled bitcoin donations as a way to sidestep a financial blockade, Bitcoin was propelled to a new level of attention and popularity. An appalled Satoshi posted, "It would have been nice to get this attention in any other

context. WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us." He pleaded with Wikileaks not to spotlight Bitcoin because the project was young enough to be destroyed by government. Indeed, Satoshi's decision to stay anonymous points to his understanding of the danger involved with Bitcoin. After all, earlier creators of digital money had been prominently prosecuted, and Satoshi must have watched closely as the prosecutions unfolded.

The preceding argument is not definitive proof that Satoshi was either a libertarian or an anarchist, but it comes close to it. "Libertarian, anarchist, or both" becomes the most plausible answer *by far* to the question about his political beliefs.

Evidence From Satoshi's Environment

The political-economic atmosphere from which Bitcoin emerged provide one more indication of Satoshi's beliefs.

Bitcoin's coding began in 2007, and the timing is unlikely to be a coincidence. The financial crisis of 2007-2008 has been called the worst one to occur since the Great Depression of the 1930s. It was caused largely by the trusted third parties Satoshi opposed the most: government and banking.

What happened? In simplistic terms the subprime mortgage industry collapsed and sparked the crisis. A subprime mortgage is typically issued to a borrower with poor credit who poses a high risk of default. To compensate the lender for this risk, the borrower pays a high rate of interest. Subprimes became increasingly common in the period before 2007 for several reasons. One was the use of automated underwriting software that sped up the loan process but bypassed the standard review of data and documents. In short, lending institutions failed to authenticate a borrower's eligibility. Housing prices soared on a flood of artificially loose credit. Peaking in 2006, prices started a downward spiral that lasted for years and caused massive foreclosures both in the U.S. and internationally.

The high delinquency rate led to a devaluation of financial instruments, which threatened to collapse the trusted third party system—aka the financial system. The state would not and could not allow this to happen; the financial system was its right arm. On September 7, 2008, the U.S. federal government assumed the liabilities of the extremely shaky Freddie Mac and Fannie Mae. Other bailouts followed. On October 3, the Emergency Economic Stabilization Act of 2008 authorized spending up to $700 billion to purchase distressed assets and to fund financial institutions, including foreign ones. The cost of saving the hierarchy of trusted third parties was passed on to taxpayers, of course.

Satoshi watched the bailouts unfold, as the Genesis block message attests. The looting of tax funds to enrich the elite, while average people lost their homes, must have looked like a trusted third party nightmare come true.

Something else occurred in 2007. The U.S. federal government charged the heads of e-gold, Inc. with money laundering and the transmission of money without a license. E-gold's owners were tried and convicted; the ruined company was forced to close its e-doors. Satoshi must have watched this situation closely as well. And he learned from it. Anonymity was safety.

Satoshi's Legacy

Satoshi produced an elegant, original technology that rivals the Gutenberg printing press in its importance to human progress because it allows easy economic freedom on an individual level.

The parallel deserves expansion. Although his printing press was not the first, Johannes Gutenberg pioneered creative innovations that had an impact similar to Satoshi's creation. He replaced short-lived water-based inks with a durable oil-based one, for example. Most importantly, he used a strong alloy to create close to 300 separate type bits that could be quickly assembled into uniform templates and disassembled. Prior printers used fragile wooden bits or carved the letters of each page into a wooden block that was inked. The innovations transformed the printing press from a tool of elite classes—the court, the clergy—to a tool of the people. Gutenberg opened a world of information and ideas to average people who no longer had to rely on authorities for their version of the truth. The printing press decentralized knowledge into the hands of the common man, and knowledge is power. This made the printing press not merely a technical marvel but also an agent of social change and revolution.

Those in power would have prevented the shift, if they could have, by plugging the flood of opinions and ideas. An illiterate, uninformed public is easier to control. A literate, informed public encourages the rise of populism and reformers who threaten the status quo. Preserving a status quo favorable to power is the main reason state censorship existed then and now, with control of the press being an essential factor. Unfortunately for the powerful, literacy increased and more people were able to judge for themselves which religious and political beliefs resonated within them as real.

An example of social upheaval: without Gutenberg's printing press, the Protestant Reformation would probably not have occurred, or it would have been very limited in scope. Martin Luther launched the Reformation in 1517 by nailing his Ninety-Five Theses to the door of a German church. The document was rapidly translated from Latin into German, then copied and reprinted; in today's jargon, it went viral. As a man, Luther could reach only those people within the range of his voice and pen. As a mass-produced author, Luther spread ideas across Europe within months. Within three years, hundreds of thousands of copies of his Theses had been cranked off hundreds of printing presses. The Catholic Church responded by excommunicating Luther, prompting him to flee and hide. Ideas do not respond to threats of hellfire, however, nor do they flee.

The Gutenberg printing press sparked movements and revolutions. But the printing press itself was not ideological, because any idea could be assembled in templates and printed en masse: Catholicism or Protestantism, individualism or socialism, Karl Marx or Ayn Rand. The machine itself was neutral. The printing press had strong ideological implications, to be sure, because it did empower the individual and the masses. In other words, it was a populist force. But authorities also used the new technology to their own statist ends. As magnificent as the printing press was, it was a tool for good or ill, depending on the purpose of the individual user.

The same could be said of crypto. Its empowerment of the individual is a profoundly political act. But that empowerment makes everyone freer to choose whatever ideology they wish. Crypto itself has no settled ideological slant. That's why individualists, anarchists, socialists and statists alike can use the blockchain as a way to pursue their own goals, whatever those goals may be. Amir Taaki, a developer of the Darkmarket/Openbazaar and Dark Wallet, is an aggressive left-anarchist who spent time in Rojava [Syrian Kurdistan], helping to found a People's Republic through the introduction of Bitcoin. Rojava was "under embargo, so there's no way to move money in or out," he explains. "So we have to actually create our own bitcoin economies. Now we have a technological tool for people to freely organise outside [the] state system. Because it is a currency not controlled by central banks."

Bitcoin can achieve a galloping diversity of goals. This is a great strength. The Gutenberg printing press provided information and perspectives that allowed people to choose religion and politics *for themselves*. Crypto gives people a control of their own economic future that allows them to choose their own lifestyles and commitments. Part of what makes the Satoshi Revolution sparkle is that it is profoundly political in empowering the individual, but it does not mandate an ideological position. That is, it does not tell empowered individuals what they must choose or how they may use their own power. Most people see little difference between the political and the ideological. Often there is not. But sometimes politics and ideology are distinct.

Bitcoin is political in the same sense as the Gutenberg printing press. It decentralizes control down to the individual level—crypto is pure empowerment—but it does not dictate what individuals do with their self-control. This would be a contradiction in terms. Yet this is what the state does when it tries to control crypto; it tries to embed a contradiction in terms within society. The state takes an inherently decentralized and individualistic dynamic and attempts to centralize it into becoming an arm of government. The good news: the state attempts seem doomed to fail. The bad news: the state is going to keep on trying.

CHAPTER 4: The Government Takes Crypto Seriously

The best status to have vis-a-vis the state is none at all—that is, to go unnoticed as you live your life in peace and freedom. Invisibility is a difficult or expensive

status to achieve, however, and the government delivers stiff punishment to those who try unsuccessfully. Crypto has lost the legal invisibility it initially enjoyed from being arcane or dismissed as a flash in the pan. It is being taken seriously and “seen” by authorities. Drawing the state’s attention is probably what Satoshi meant when he lamented the prominence Bitcoin attained through its association with Wikileaks. The technology was young and in early development; the last thing it needed was to be taken seriously by government. As Satoshi commented, “WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us.”

The goal of the swarming state is predictable—control—but the reaction of authorities varies. Some politicians and bureaucrats perceive a threat; others glimpse the fresh plunder that is possible; still others see a means by which to update an inefficient and unpopular central banking system; many want to use it to springboard into a cashless society that they digitally control. Whatever differences in perspective exist, however, the same conclusion is reached: crypto needs to be under their centralized authority.

A State Strategy to Control Crypto

A popular state strategy for dominating crypto is to reclassify it as money and to apply the same stringent laws that cover fiat. A bill currently stalled in the United States Senate embodies common aspects of this tactic, which is far from confined to American shores. Examining the bill is a way to understand how this strategy is likely to play out and how the process would destroy crypto, if successful.

On Tuesday, November 28, 2017, Senate Bill 1241 was heard by the Congressional Committee on the Judiciary. The bill was held in committee where it remains. It is an alarm bell ringing in the night.

Some crypto enthusiasts will applaud this development because they believe regulation means crypto is going mainstream and achieving a respectability that brings more profit. Some of the applauders want to benefit from licenses (government approvals), which could eliminate free-market competitors. Other crypto zealots will just shrug because they think free-market crypto cannot be controlled and the statist efforts will fail. The shruggers may be correct—I hope they are—but lives can be destroyed by the state’s attempt to dominate, and the destruction of good people is a nonshrugging matter. The prudent approach to state intrusion is neither applause nor dismissal but preparation. The government is coming, and it wants more than money. It wants to make hard-hitting examples of crypto users in order to dissuade others from seeking financial freedom.

The “Combating Money Laundering, Terrorist Financing and Counterfeiting Act” (S.1241) is an anti-money laundering bill that regulates cryptocurrency on a federal level. This means there would be a uniformity of crypto’s legal status and treatment across America.

Again, some crypto enthusiasts will applaud this move for providing the situation with clarity. This is a misguided response on several levels. For one thing, control is not clarity; it is the centralization and surrender of choice. And clarity has no intrinsic value apart from the content being clarified; a murderer can be very clear on how he intends to kill you, but this not something to cheer about or seek out. For another thing, if legal inconsistencies in the treatment of crypto cause problems, then the appropriate response is to remove the laws, not to call for more.

Moreover, inconsistencies in the law can be useful because they can work to the advantage of those who seek freedom. This strategy is sometimes called the "parallel institution" approach. Parallel institutions such as Church and State can act as bulwarks against each other's power, allowing individuals to breathe more deeply in the divide. The concept of church sanctuary was traditionally available for criminals and run-away slaves, for example, though it was not offered reliably. On the other hand, people with the "wrong" religious or political beliefs can sometimes escape persecution by fleeing to the sanctuary of a politically friendlier area.

The parallel institution strategy is employed every day across the global. In America, people move from states with high taxes to ones with low or no taxes. The British rich move to tax havens. Marijuana aficionados shift from Texas, with its draconian drug laws, to Colorado, where marijuana is legal. Around the world, people flee for their own reasons.

Freedom does not benefit from the homogenization of government law but from the presence of alternatives. Federalizing law on crypto to eliminate inconsistency also eliminates the ability of users to move to whichever state-level jurisdiction is friendliest to their purpose. Federalizing law also expands government into areas that are not yet addressed on the state level; this includes border and customs control. Consistency may bring clarity, but it does not bring choice. Another word for consistency in the law is centralization.

What is S.1241?

S.1241 was introduced into the Senate Committee covertly. An alert bitcoiner noticed that the Senate Judiciary meeting had been listed on the official webpage at 10 a.m. on the 28th—the same day as the hearing—after being added to the Hearing page at 6 p.m. the previous evening. This maneuver effectively precluded media coverage, public feedback, or protests. Actions to control crypto are likely to follow this pattern—abrupt, unseen, and unexpected. S.1241 can be viewed as a template for how governments intend to proceed. Whither the U.S., much of the world will follow.

S.1241 seeks to amend 31 U.S. Code § 5312, which addresses definitions and their application to money and finance. It sounds dry, but the impact would be dramatic. The purpose of the bill is to include "digital currencies" in the definition of "monetary instruments" and "any digital exchanger or tumbler of digital

currency” in the definition of “financial institution.” $10,000 is the trigger amount. In the U.S., $10,000 triggers a personal declaration at the border; it is the point at which financial institutions complete a state-mandated currency report that can cause accounts to be frozen or confiscated regardless of whether there is evidence of a crime.

S.1241 is a tightening noose.

Section 2: “Transportation or Transhipment of Blank Checks in Bearer Form” declares that any check entering or leaving the U.S. which is “drawn on an account containing more than $10,000” and has no dollar amount specified is “valued in excess of $10,000 for reporting purposes.” Since crypto can be difficult to assess and rarely has a dollar amount specified, the “no dollar amount” allows customs agents to evaluate crypto at the reportable amount.

Section 3: “Increasing Penalties for Bulk Cash Smuggling” addresses the concealment of $10,000 or more in currency or monetary instruments when crossing the border. Maximum punishment is ten years imprisonment with fines increasing by an unspecified amount. When the state punishes a petty offense in a draconian manner, it means authorities have no other solution to a situation except the barrel of a large gun.

Section 4: “Section 1957 Violation Involving Commingled Funds and Aggregated Transactions” deals with “the transfer of criminal proceeds…without the need to demonstrate” criminal intent. Two existing loopholes would close. 1) $10,000 in funds in which allegedly dirty money is commingled with clean money becomes $10,000 of dirty money. 2) A series of transactions under $10,000 that is “closely related in time, the identity of the parties, the nature of the transactions, or the manner in which they are conducted” collectively meet the $10,000 threshold. Legal money that is in the presence of ‘criminal’ money is criminalized through guilt by association, allowing officials to confiscate everything. Undeclared or improperly declared crypto makes all wealth—crypto or not—fair game.

Section 5: “Charging Money Laundering as a Course of Conduct” simplifies the process of charging a person with money laundering and includes “conspiracies to violate…[the] prohibition of unlicensed money transmitting businesses as money laundering conspiracies.” Plans to transmit crypto can be punished as though the act had occurred. It is not clear whether the co-conspirators will also be charged or have their money confiscated.

Section 6: “Illegal Money Services Businesses” makes It a crime for unregistered businesses to send “proceeds abroad.” Ignorance of the need to register is no defense. The term “money transmitting business” is replaced with “money services business” to include “entities…such as check cashiers” that “do not transmit money.” Penalties and fines increase.

Section 7: “Concealment Money Laundering” applies to “couriers or mules.” The Supreme Court ruled in the past that a defendant needs to know the

transportation of funds is clandestine and why the funds are being “so transported” for a courier to be guilty of a crime. Those requirements are diluted or eliminated. Again, ignorance is not a defense.

Section 8: “Freezing Bank Accounts of Persons Arrested for the Movement of Money Across International Borders.” A 30-day hold is instituted on the accounts of those charged and could be extended “for good cause.” This seems to apply to the full amount within an account.

Section 9: “Prohibiting Money Laundering through Hawalas, Other Informal Value Transfer Systems, and Closely Related Transactions” redefines what constitutes a money laundering offense when it involves “a set of parallel or dependent transactions.” All would be considered to be “a single plan or arrangement,” which might well bring the collective transaction up to prosecutable levels.

Section 10: “Restoring Wiretap Authority for Certain Money Laundering and Counterfeiting Offenses” allows the state to monitor those people it suspects of criminal activity.

Section 11: “Applying the International Money Laundering Statute to Tax Evasion” defines the use of foreign accounts to evade taxes as money laundering. Because crypto flows so easily across borders, users tend to frequent “foreign” exchanges —a practice that could be labeled “tax evasion” unless it can be proven otherwise.

Section 12: “Conduct in Aid of Counterfeiting” includes the use of new technology, “materials, tools, or machinery.” This provision takes specific aim at crypto, digital money, and the tools that provide privacy to them.

Section 13: “Prepaid Access Devices, Stored Value Cards, Digital Currencies, and Other Similar Instruments” amends current law to explicitly include “any digital exchange or tumbler of digital currency” as well as any “issuer, redeemer or cashier” of a “digital currency.” Funds stored in a digital format are explicitly subject to money laundering reporting requirements.

Section 14: “Administrative Subpoenas for Money Laundering Cases” expands the availability and ease of administrative subpoenas.

Section 15: “Obtaining Foreign Bank Records from Banks with U.S. Correspondent Accounts” strengthens “this existing investigative tool.” Foreign banks can be subpoenaed for records related to any “civil forfeiture action,” and they can be punished for noncompliance. Remember: S.1241 includes “any digital exchanger or tumbler of digital currency” in the definition of “financial institution,” which leaves foreign exchanges vulnerable to subpoenas.

Section 16: “Danger Pay Allowance” provides special compensation to a wide range of law enforcement agencies. It is unclear what constitutes “danger” but, presumably, agencies will have a vested interest in defining situations in a manner that draws more funding.

Section 17: “Clarification of Secret Service Authority to Investigate Money Laundering” expands police authority.

Section 18: “Prohibition on Concealment of Ownership of Account” makes it a crime for a person “to knowingly conceal, falsify or misrepresent, from or to a financial institution” their identity or “a fact concerning the ownership or control of an account or assets held in an account.” This is particularly relevant to crypto users who routinely employ anonymity or pseudonymity. It becomes a crime to not reveal identities or specific transfers over the blockchain.

Section 19: “Prohibition on Concealment of Source of Assets in Monetary Transaction” allows the government to pursue assets even if the person is not charged with an offense. Instead, their money can be confiscated simply because its source is not stated or unclear.

Lawyer Ballard Spahr explains, “If passed in its present form, S.1241 ironically will take the one kind of offense which Congress has historically *not* allowed to form the predicate for money laundering—i.e., “garden variety” tax fraud not involving illegal proceeds—and turn things on their head. That is, transactions promoting a tax crime, so long as they involve a cross-border transaction, will be the one and only kind of transaction that can constitute a money laundering offense when the proceeds represent otherwise entirely legal funds.”

Those who wish to prepare against the coming crackdown should study S.1241.

Protecting People From Freedom

Money laundering and tax evasion are two justifications that the state proclaims when it reaches out to control crypto. Arguably, these broad and vague justifications are not viewed with general sympathy because it often looks like a blatant money grab.

Other rationales are more successful. The crypto community, government argues, is rife with drug dealers, blackmailers, sex traffickers, child porn producers, gun dealers, and other miscreants. The state points to the “dark web” as proof of perfidy. This is the part of the web that is accessed only by special software, allowing users to remain anonymous or untraceable. Controlling crypto is said to be necessary in order to protect people from dark web crime. In doing so, the state argues it is protecting vulnerable drug users, exploited women and children, gun victims, compliant taxpayers, law-abiding citizens, and a scrolling list of other “victims” of the monetary outlaws.

There are myriad ways to refute this claim, including the fact that it is flatly false. Some crypto users are undoubtedly violent criminals; the same is true of some people who use cash and credit cards. Crypto is a currency and a payment method. Like anything else useful in life, it is a tool that can be employed for good or bad purposes. But the overwhelming majority of people with crypto or with

cash are peaceful human beings who are being criminalized for preferring one payment method over another. The justification for doing so boils down to the claim that their economic choices are dangerous to public welfare.

Clamping down on allegedly exploitative but nonviolent economic practices is a tremendous violation of the rights of vulnerable people; it does not protect them. I know. My life could have been ruined by one measure that was intended to prevent a so-called form of economic exploitation that repulses most people—child labor. When I was 16 years old, I ran away from home and lived on the street for as short a period as I could manage. I refused to go to a shelter or seek government assistance for the same reason as many run-away teens; when teenagers prefer the cement to home, it means adults have betrayed them. The only safety is to take care of yourself.

I was luckier than many. I was barely 16, but this meant I could work legally. I could stand behind the warm counter in a fast food restaurant or, in my case, I could sit in the office of a family-owned furniture store where I did years worth of backed-up paperwork during the day and slept on a couch downstairs during the night. The owner paid me minimum wage and gave me a safe place to sleep. As a result, I worked far longer than the eight hours a day for which I was paid. I saved enough to move into a boarding house and, when I moved on to a filing job in a bank, I had a reference. My future hinged on having those opportunities.

What if I had been one month or one year younger than the legal working age? The store owner would not have risked his business by hiring me. Nor should he have. He was correct to insist upon inspecting and xeroxing my I.D. before offering me the job; he was correct to wait until he knew me a bit better to offer me the basement couch. Why should he put his family's income and future in peril to help a stranger? And that's what he did; he did not exploit me. He *helped* me.

Without the ability to make money legally, my life may have turned out badly rather than well. In the name of humanitarianism, the law would have closed off my one path back into the mainstream of society, and it would have done so self-righteously. How would I have fed myself then? Stealing, begging, sex work, and drug dealing come to mind. But I wanted a way *off* the street, not a way to make it or prison my permanent address.

Closing off nonviolent economic options does not protect vulnerable people. Just as raising the mandatory minimum wage makes it difficult for those starting out to find employment, economic "protections" cut off vulnerable people from being able to climb upward. In my case, not being able to support myself would have created a criminal and a victim, decreasing the public good. If there is violence involved in an economic option, then address the violence. If there isn't, then leave it alone. This principle is the way to help everyone who wants earn their own money and spend it as they see fit. The state does not shield victims or society by taking economic options away from people who have done no demonstrable harm but happen to fall into a category that is either protected or reviled.

Oddly enough, the law's response to both categories is much the same: deny economic rights. As a run-away teen, I was in the "protected" category, and I came within a hair of losing my right to earn a living. Peaceful crypto users are in the "reviled" category, and many may be stripped of the right to retain money they have earned.

To benefit the vulnerable and society, the state needs to do nothing more than get out of the way. The French phrase "laissez faire" is most often associated with "laissez-faire capitalism." It is said to have originated during a 1681 meeting between Jean-Baptiste Colbert, the French Controller-General of Finances, and a group of businessmen. Colbert asked how the state could assist the men in their businesses. The head of the group, M. Le Gendre, reportedly replied, "laissez nous faire" (leave it to us). Leave us alone.

A Second Control Strategy: Government-issued Crypto

Some states plan or attempt to issue their own crypto. Central Bank-Issued Digital Currency (CBDC) refers to a national cryptocurrency that issues from a central bank. It is the crypto counterpart to a physical fiat such as the U.S. dollar or the British pound.

It is also a bitter irony. A monetary wildcat that was designed to undermine the financial system is being redefined to serve the status quo. At least, this is what the status quo hopes will happen. In fairness, some world leaders understand this development is not possible. Putin famously said that a national cryptocurrency is not viable because crypto is an international phenomenon. Other nations are actively exploring the development of CBDCs, however. Japan has launched the digital money J-Coin, for example. It is a digital currency rather than a crypto based on a blockchain, but it serves the purpose of moving Japan closer to a cashless society; it makes tracking digital coin users into a trivial matter; and it allows the state to crack down on real crypto users with greater ease and less backlash. These are three of the main goals of a national e-currency.

CBDCs may seem to parallel free-market crypto, but they are the anti-crypto. Consider just some of the technical differences:

- Bitcoin is decentralized; CBDCs would centralize all aspects of digital currency, often in the hands of one agency or system of agencies that are heavily regulated.
- Bitcoin is peer-to-peer between individuals; CBDCs would be administered by trusted third parties in the worse sense of this term.
- Bitcoin is open-source; CBDCs would be patented, proprietary, and not transparent.
- Bitcoin is mined; CBDCs would be issued by a central authority.
- Bitcoin is limited to 21 million coins; CBDCs' cap would be whatever the authority wished it to be.

- Bitcoin is on a transparent blockchain; CBDCs may not use a blockchain, and probably would not.
- Bitcoin users possess their own private keys; private keys for CBDCs would be owned by a trusted third party that would control the wealth.
- Bitcoin is anonymous; CBDCs would track both the identities of users and how they spent the currency.
- Bitcoin severs the connection between currency and central banks; CBDCs would cement it.

Free-market crypto and CBDCs also have antagonistic goals. Crypto obsoletes the central bank's status as a trusted third party and eliminates the money monopoly. CBDCs are the central-banking system's bid to retain its trusted third party status and the monetary monopoly.

Free-market crypto and CBDCs may have one goal in common, however: the ultimate elimination of physical fiat. But, again, the reasons are antagonistic. Crypto rejects a corrupt currency that steals from honest people. CBDCs want to rescue the status quo for the benefit of financial elites by creating a digital fiat.

Why the Push for a Cashless Society?

Cold cash has always been the enemy of government. In his article "Why Governments Hate Cash," the Economics Professor Joseph Salerno writes:

> Now the reason given by our rulers for suppressing cash is to keep society safe from terrorists, tax evaders, money launderers, drug cartels, and other villains real or imagined. The actual aim of the flood of laws restricting or even prohibiting the use of cash is to force the public to make payments through the financial system. This enables governments to expand their ability to spy on and keep track of their citizens' most private financial dealings, in order to milk their citizens of every last dollar of tax payments that they claim are due.

The problem confronting authorities: When cash leaves the bank and goes into the pockets of individuals, the government loses track of how it is spent. Individuals can buy and sell with an anonymity that blocks the collection of taxes, fees, and other revenue for the state. Government wants to "solve" this. Currency tracking sites can record the serial numbers of fiat, for example, and allow the circulation to be monitored—that is, as long as the serial number is re-entered at every stage. The system requires a high degree of unlikely cooperation.

The drive toward trackable fiat will inevitably fail because of noncooperation. Fortunately for governments and central banks, digital cash is a perfect substitute for physical cash because traceability is built into the design. If governments manage to make digital money work, then the resulting currencies will be a nightmare for freedom. They will combine the efficiency of crypto with the totalitarianism of government. The trusted third party problem that Bitcoin was created to eliminate will be back on steroids.

The state's hostility to cash will cause some nations to move from physical to digital fiat with alacrity. The process is likely to resemble some version of the following:

First: A government explores the possibility of digital cash while it gradually removes physical cash from circulation.
Second: A database for digital currency—probably not based on a blockchain—is written in proprietary code and implemented in a nontransparent manner.
Third: A digital cash is issued and sold as an alternative to both cash and free-market crypto. To encourage its adoption, government regulates free-market crypto which is driven underground or forced to flee to friendlier climes.
Fourth: Automatic taxation is embedded into the new digital currency. The absolute tracking of every unit of currency, which is linked to real identities, gives government an unprecedented control over the flow of wealth.
Fifth: Central banks inflate the supply of digital currency at will, devaluing each unit in circulation. This inflicts a huge, hidden tax on every owner.

The CBDC also gives government greater precision in manipulating the economy. In an article entitled "Why Governments Want a Central Bank-Issued Digital Currency," the Austrian economist Xiong Yue observes:

> [G]iven that these digital currencies are programmable, the government can even control exactly how to spend this new money using scripts. For example, if the government plans to subsidize certain farms, say some corn farms, to support this sector of agriculture, they can directly add a certain amount of money to the wallets of some farms, for instance 100 million dollars and program this money to be sent to certain fertilizer merchants at a certain time, and that each can only spend maximum of 10 million dollars per year.

In short, a CBDC could facilitate a more efficient centralized state. This is hardly a good thing.

Another agenda item of government and central banks is negative interest rates. Negative interest occurs when depositors do not receive interest on money kept in their accounts; instead, they pay interest to the bank for holding their money. This is a money maker for the banks. It also encourages people to spend because the money erodes if it sits unspent, and consumer spending is seen to prop up the economy.

The 2015 bank crisis in Greece provides an example of how negative interest works. To avoid bank runs, Greece imposed a surcharge of one euro per 1,000 euros in cash withdrawals. Salerno observes, "It doesn't seem very big, but the *principle* at work is extremely big because what they're in effect doing is breaking the exchange rate between a unit of bank deposits and a unit of currency." Salerno continues, "To make the calculations easier…let's say that the Greek 'surcharge' is ten dollars for every 100 dollars withdrawn. Now, instead of being

able to convert one euro in your checking account into one euro in cash, on demand, you will only be able to buy one euro in cash by spending 1.10 euros in your bank accounts. That's a negative 10-percent rate in some sense.…So, you would only really get ninety cents for every dollar that you wanted to withdraw and that's very significant because this means it will be more expensive to buy an item with cash than with bank deposits." Predictably, people were driven away from cash. There was an incentive to pay bills out of bank accounts which made all payment trackable.

The main problem with a scheme of negative interest for government and central banks is that people will keep their cash outside of the financial system. Large amounts will stay beyond government's reach. If digital cash is fully adopted, however, then government can insist that people use it instead of physical money for payments such as taxes. This means the wealth will be trapped within the financial system.

The Strategy of Centralized Exchanges

> The root problem with conventional currency is all the trust that's required to make it work…We have to trust them [third parties] with our privacy, trust them not to let identity thieves [including government] drain our accounts—Satoshi Nakamoto

The one thing CBDCs cannot survive is free-market competition. This is why every state that seeks a CBDC will make a concerted effort to eliminate or cripple free-market alternatives. An interesting aspect of this repression is that there is one form of non-state crypto that most governments will tolerate: digital currencies issued by licensed financial institutions. These currencies are no challenge to the central banking system because the issuing institutions are regulated to act as though they were affiliate banks. Licensed exchanges become the outer lobby of the central banking system. The lobby mimics the free market in some ways, but it bears no real relationship to it.

A standard definition of a centralized exchange: "Centralized cryptocurrency exchanges are online platforms used to buy and sell cryptocurrencies. They are the most common means that investors use to buy and sell cryptocurrency holdings." A centralized exchange is a marketplace for trading or converting assets through a single location or service. The definition does not capture the problems that centralized exchanges present to the Satoshi model, however.

But, first, what are problems that centralized exchanges solve? Why did they come into existence? There is a market demand to speculate, to trade in currencies, and to perform other sophisticated financial transactions for which peer-to-peer structures—decentralized exchanges—are not yet adequately equipped. There is also a demand for convenience and access to crypto that does not require technical knowledge or effort. For some, centralized exchanges also have the comforting familiarity of banks. Centralized exchanges fill a niche or else

they would not be popular. They currently dominate much of the crypto world, with a majority of users entrusting exchanges with their wealth and privacy.

The niche occupied by centralized exchanges comes from blending the functions of a stock market and a bank. In many ways, they are similar to the New York Stock Exchange. Currencies can be traded, shorted, and cashed out for fiat, for example; margin trading, stop loss, and lending are also available. In other ways, centralized exchanges resemble traditional banks. After purchasing crypto from an exchange, many customers choose to leave their coins in an account rather than transfer them to private wallets on their own hard drives. Centralized exchanges become trusted third parties; this means they present a terrible danger to the wealth and well-being of account holders. Consider one aspect of the risk. Most centralized exchanges hold the private keys of account holders. But private keys **are** the crypto. The coins have no physical presence, only algorithmic ones. When an exchange controls the keys, it de facto owns the coins. The customer has nothing more than a promise of access to them upon demand in the same way banks promise access to physical money upon an account holder's demand.

Recently, the risks associated with centralized exchanges increased exponentially and for one reason: the exchanges are increasingly complying or partnering with the state to enforce laws and reporting requirements on customers. A February, 2018 *Forbes* article announced the inevitable regarding the world's largest centralized exchange.

> It's finally happening: The much-ballyhooed turnover of documents in the battle between the Internal Revenue Service (IRS) and Coinbase, a company which facilitates transactions of digital currencies like Bitcoin and Ethereum, is moving ahead. Coinbase has announced that it has notified affected customers that it will comply with a court order regarding the release of specific data.

2018 was the year in which American tax agencies got serious about crypto profits and holdings. Governments around the world are watching as Coinbase turns in data on its customers, which will almost certainly lead to audits and/or high-profile prosecutions. Specifically, Coinbase is reporting all customers with transactions of $20,000 or more in a single year between 2013 and 2015. Taxpayer IDs, real names, dates of birth, street addresses, and all transaction records will be delivered. The wealth of data is available because Coinbase, like every other licensed exchange, complies with Know Your Customer and Anti-Money Laundering laws which destroy financial privacy.

Coinbase has become extremely aggressive about gathering information and verifying identities. The exchange uses facial-recognition technology, for example, to compare a real-time face shot from a webcam or smart phone with whatever ID an applicant submits. Expect aggressive intrusion to become the norm for centralized exchanges because they prize their licenses and relationships with government. Expect them to act as data-gathering arms of the state. The danger is not only freezing and confiscation of accounts, but also legal proceedings

against and imprisonment of account holders. The IRS states that “anyone convicted of tax evasion is subject to a prison term of up to five years and a fine of up to $250,000. Anyone convicted of filing a false return is subject to a prison term of up to three years and a fine of up to $250,000.”

Fortunately, the market demand for stock market and banking functions can be satisfied (or soon will be) without sacrificing privacy and safety. A decentralized exchange is a marketplace that does not rely on third party services. Trades are peer-to-peer; they are direct transfers between people who use an automated process to facilitate the exchange. They are trustless. They are transparent with software and transactions being open source. They are Satoshi.

A decentralized exchange allows individuals to hold their own private keys which makes it a less attractive target for hackers. It also requires a minimal amount of personal or financial data to establish an account and to conduct commerce. Often, only an email address is requested, and it can be one that is generated specifically to register, with no connection to a real identity.

Decentralized exchanges employ a wide variety of strategies to facilitate peer-to-peer transfers. Some create proxy tokens; others employ a multi-signature escrow. Peer-to-peer banking uses an auction-type dynamic to facilitate loans of a specific amount and at an agreed-upon rate between members. Smart contracts can assume the traditional functions of banks. *Technology Review* explains:

> Switching back and forth between fiat money and cryptocurrency will require a traditional point of exchange for the foreseeable future. But some technologists say an alternative model for trading crypto that would give people more control over their wealth is possible. Its metaexchanges can be decentralized, they say, using a blockchain. The idea hinges specifically on so-called smart contracts, software code that can be stored in a blockchain and set up to programmatically govern transactions. Imagine, for example, you want to send your friend some cryptocurrency automatically at a specific date and time. You could use a smart contract to do that.

The point here is *not* to advocate a particular decentralizing tactic. It is to offer a sense of the rich and evolving alternatives to centralized exchanges. Many people will still choose a centralized exchange because the platforms are easy to access and use; they are sanctioned by government and this means respectability to some people; and they offer the familiar, advanced functions of a stock market. People have every right to make this choice with their own money, of course. But for those who prize privacy, it is an unacceptable alternative. (More on decentralized exchanges later.)

An analogy illustrates the stark difference in how privacy and rights fare under a centralized and decentralized system: social media.

“’Want To Freak Yourself Out?’ Here Is All The Personal Data That Facebook/Google Collect.” This is a March 2018 headline at *Zero Hedge*. The types of data collected

are too extensive to enumerate. An indication: Android cellphone users who downloaded specific Facebook apps have had data on their personal calls logged by Facebook for years.

A relatively undiscussed cause of social media's privacy hemorrhage and its abridgment of free speech is the centralization of information and discussion that accompany corporate behemoths, like Facebook and Google. Large corporations form alliances of convenience and reciprocal profit with government. An intriguing article in *The Federalist* asks, "Was Social Media A Mistake?" The author, Robert Tracinski, harks back to the 2000s—the golden age of blogs, when everyone and their grandmothers expressed themselves through blogging.

Tracinski writes, "It felt like liberation. The era of blogging offered the promise of a decentralized media. Anybody could publish and comment on the news and find an audience…We were bypassing the old media gatekeepers. And we had control over it! We posted on our own sites. We had good discussions in our own comment fields, which we moderated." It was a whirlwind of free speech, but it was also a bastion of privacy because individuals retained control. Individual control of data and expression is freedom.

Then social media arrived like a juggernaut, and the mom-and-pop blogs migrated their diaries and information to Facebook, Google, Twitter, and other trusted third parties. Like centralized exchanges, the social media giants were relatively easy to access and use; they offered sophisticated software and functions that individual bloggers lacked the technical knowledge or money to implement; social media slid seamlessly onto cell phones via apps that seemed to open up the world. In reality, they closed down personal freedom.

Tracinski notes the result.

> A few of the best and most interesting blogs became full-fledged online publications, but a lot of the small, quirky, one-person amateur bloggers moved onto social media. That turned out to be a big mistake, because the era of social media has *recentralized* the media. Instead of a million blogs—what Glenn Reynolds of Instapundit fame called an 'Army of Davids'—we now have a social media economy mostly controlled by three big companies: Twitter, Facebook, and Google.

The price tag of centralizing personal writing has become apparent. The left-leaning politics of social media giants means that they purge (suspend accounts) or punished (throttled accounts) of those who hold "wrong" views. This is akin to banks and other financial institutions refusing to deal with porn, pot, or gun industries due to political pressure from government. "The old media gatekeepers" have been replaced by the equally intrusive Silicon Valley Puritans. Although both may be preferable to direct government intervention, their quasi-monopolies are bolstered by tax privileges, by favorable regulation, and by direct tax funding. In short, they may not be government, but they are certainly state

cronies and owe their loyalty to it. As a result, individuals have lost control of their own work and data. Perhaps it is more accurate to say they relinquished it.

Nowhere is the price tag of centralizing personal expression more glaring than with personal data. In return for convenience, all social media asked was to know and to market every detail of customers's lives. The role of centralization in this rape of privacy was key to its effectiveness.

Privacy is the front-line defense of individual freedom. Decentralization is the social condition under which privacy thrives. No one can or should tell individuals which strategy to use. But, if you value privacy and safety, stay private and decentralize.

SECTION TWO: THE IMPERATIVE OF PRIVACY

CHAPTER FIVE: When Privacy Is Criminalized, Only Criminals Will Be Private

> I grew up with the understanding that the world I lived in was one where people enjoyed a sort of freedom to communicate with each other in privacy, without it being monitored, without it being measured or analyzed or sort of judged by these shadowy figures or systems, any time they mention anything that travels across public lines.—Edward Snowden

I want my tombstone to read, "I lived. I died. Now mind your own damned business." What do I have to hide? Everything! Which is to say, any information I am required to reveal is data I decline to disclose.

A fundamental question floats over the rhetoric, however. What is privacy?

What is Privacy?

A famous answer comes from an article by the American attorneys Samuel Warren and Louis Brandeis, which appeared in a 1890 issue of the *Harvard Law Review*. It is one of the most influential pieces in the history of Western legal theory. "The Right to Privacy" has been called the first prominent call for privacy as a concept to be cemented into law. The article opens:

> THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.

Elsewhere, privacy is defined as the right to be left alone.

The article argues for privacy as a "foundational" or basic human right upon which all other rights rest. "The right of property in its widest sense including all rights and privileges, and hence embracing the right to an inviolate personality, affords

alone that broad basis upon which the protection which the individual demands can be rested." Privacy is a prerequisite for all other rights: freedom of speech, sexuality, freedom of conscience, and financial security depend upon it because no right can be exercised in the presence of storm troopers smashing through the door. The right to lock the front door behind you is essential.

Interestingly, the Brandeis-Warren article was in response to technological developments that were seen to threaten personal privacy. One of the developments was the portable camera with which journalists photographed prominent people in venues that were formerly private such as restaurants, weddings, and funerals. Today, the focus of protecting privacy has shifted from journalists to the government for which "privacy" is a synonym for "secrecy." Privacy is no longer a right but a probable cause for suspicion. The shift in definition reflects how powerful government has become since the 1890s—and how diminished the individual.

Although privacy has been a theme both in common law and Western societies, its legal status has been vague. Indeed, before "The Right to Privacy," the legal protection of privacy was splintered across specific issues. Laws against trespassing existed, for example, but codification of the broad concept of privacy did not.

After all, what does the "right to be left alone" mean? Much of this chapter explores an answer.

Everyone knows a woman's purse should not be snatched, her window peeped through, or her house burglarized. These are obviously and intuitively cases of privacy violations, but they are not the type of violation that crypto users are likely to confront. Crypto users will deal with their personal information being mined and monitored—often covertly—in order to use against them in some manner. With the government, the goal of mining and monitoring is social control, taxation, confiscation, or imprisonment. With criminals, the goal is theft, blackmail, or extortion.

Peeping through a bedroom window may be an obvious breach of privacy, but what about eavesdroppers who access public information like that embedded in the blockchain? The blockchain's open ledger allows unwanted parties to monitor financial transactions that users voluntarily make public. If an eavesdropper analyzes the pattern of transfers and unmasks a user's identity, then has privacy been violated? The blockchain is a public place where people voluntarily exchange in a manner they know is transparent and recorded. Eavesdropping is akin to listening to people who are speaking audibly in public. Is listening a culpable act, especially when done by state agents or other bad actors? Certainly, how the state or other criminals use the information is wrong, but this issue is distinct from whether the act of listening itself is wrong.

Assessing the question means putting privacy in the context of other human rights.

The Human Rights Context of Privacy

Murray Rothbard claims that all human rights are property rights. That is, all rights come down to the question of who properly controls the use and disposal of a thing, whether the thing is a widget, an idea, or a human body. It is always possible to use force to usurp control of anything, of course, but the question of who is the *proper* owner remains.

Rothbard answers: The owner is the individual who holds valid title to the thing. True ownership is not a matter of control that can be acquired by brute force, but of *rightful* control that comes from peacefully acquiring title. There can be no more obvious or valid title than the one individuals have over their own bodies. Indeed, trying to deny this title reduces either to obscenity or absurdity. There are only three positions possible on who owns a person's body: the person himself (freedom), someone else (slavery), or it is unclaimed baggage. Those who value freedom and human rights argue for self-ownership.

Again, the classic definition of self-ownership: Every human being has a moral and logical jurisdiction over his own body and the peaceful use thereof, including the products of his labor. No right is more fundamental than self-ownership because it is the wellspring of all other rights. Freedom of conscience and speech exist only because individuals have the capacity to think and speak, both of which are aspects of the human body. The right of self-defense exists only because people own their bodies and have a right to protect their property. The flip side of rights is duty. Just as every other human being is morally and logically prohibited from initiating force against you, you have a duty to desist from initiating force against them.

If there is a right to privacy, then it must be rooted in self-ownership. It must be what is called a natural right. And, if privacy is a right, then other people have a duty to desist from violating it.

The issue is non-trivial. Self-ownership and privacy are under concerted attack by the biggest eavesdropper in human history—the state. The state intends to use the data it collects against people with extreme prejudice. In his book *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, the political scientist James C. Scott comments on the role that just one form of data collection has played in the rise of the modern state: the census. "If we imagine a state that has no reliable means of enumerating and locating its population, gauging its wealth, and mapping its land, resources, and settlements, we are imagining a state whose interventions in that society are necessarily crude." The current state is sophisticated and complex.

Information is power, both for the individual and for the government. One reason government succeeds at acquiring data is that privacy is an ill-defined concept that people do not understand in the broader context of rights. Another reason is

that information is ephemeral and seems less prone to ownership than a table or car.

The assessment of whether data privacy is a natural right hinges on two questions. As a prelude to considering them, ponder whether you have a right of ownership over your thoughts and their expression, including the expression of personal information. This broad question is key to the issue of intellectual property, which is the claim that ideas and their expression can be owned. People reach dramatically different conclusions, and intellectual property is frequently claimed as a natural right. The same question confronts privacy, which also addresses the ownership of personal information and its expression.

Question #1: *Who owns what is in your mind?*

Most people would loudly declare, “no one owns what’s in my mind!” Your thoughts are your own for the same reason as your fingers and eyes are; they are part of your body, and your body is who you are. It *is* you. No one else has any business claiming jurisdiction over your body. But what if the thought in your mind is a chemical formula originated by a co-worker and written on a chalkboard during a lecture you attended? The formula is now part of your mind as well as his and, if he can claim a right to use it because it is part of his body, then shouldn’t you be able to make the same claim?

At this point, the co-worker’s argument usually shifts ground. He *originated* the idea, he maintains, which makes the formula a product of his labor, and owning the products of your labor is an extension of self-ownership. It doesn’t matter if the idea is in *your* mind now; it is *his* idea. He found it first.

Putting aside the fact that the co-worker almost certainly utilized the ideas and work of hundreds of people before him—that is, the formula is a product of their labor as well—let’s assume that he added a totally original refinement. What of it? The instant you glimpsed the formula, the concept changed. The formula integrated with every other concept you have about chemistry, technology, and life in general. The formula in your mind is slightly or considerably different than the one on the chalkboard or in the mind of your co-worker. How then can he claim property rights in an idea based on other people’s prior work while denying your property rights in an idea that is based on his prior work?

The bottom line of the scenario: no one has a right to what is in your mind. What is called privacy in this circumstance reduces to self-ownership. You own what is beneath your skin, including ideas. The 19th-century libertarian James Walker states, “My thoughts are my property as the air in my lungs is my property…” When you exhale, however, you lose all claim to ownership of the air expelled. The same is true of ideas or information that are thrown into a public realm; you lose all privacy claim except and unless there is a prior nondisclosure agreement in place. In that circumstance, your claim to privacy or information ownership is not a matter of natural rights but of contractual rights.

The parallel to financial information: Crypto users lose any reasonable expectation of privacy or ownership of information once it goes onto the blockchain or another public form. An eavesdropper who accesses the data does nothing more than view what is public knowledge. The eavesdropper may use the knowledge in a vicious way that harms a user, but the use of information is a different matter than how it was obtained.

Question #2: How was the data obtained?

The answer to this question is to distinguish between legitimate eavesdropping and a criminal act. Legitimate eavesdroppers access publicly or freely disclosed information and in no way violate rights. By contrast, criminal eavesdroppers violate private property rights in order to access data. Tapping a phone or a computer is like breaking into a person’s home to rummage through a file cabinet or desk. A census taker who threatens an unresponsive person with fines or arrest is using criminal means to access information. The litmus test to distinguish between legitimate eavesdropping and a crime is whether the acquisition of data involves a violation of rights.

Rothbard argues, "there is no such thing as a right to privacy except the right to protect one's property from invasion." In other words, there is no natural right to privacy per se. Information is private by virtue of being protected by other rights. A person has a right to conceal information, for instance, because the right to free speech includes the right to remain silent, and breaching a determined silence requires threats or violence. Equally, a person has the right to close his door behind him, and information in the papers on his desk is protected from intruders by his right of property in the house. The privacy of the information is shielded by the wall of rights surrounding it, but this does not make privacy a right in and of itself.

By contrast, if a person shouts personal information in a public square or if he throws his papers out the window into the wind, it is no longer protected by his property rights. He has placed it into the public sphere and abandoned the claim to exclusive control.

The Satoshi approach to privacy has a foot in both worlds—public abandonment of information along with a privacy protected by natural rights. A transparent blockchain functions with anonymous or pseudonymous users who employ both public and private keys. The transactions have been thrown into the wind, but the identities are protected by other rights. In other words, to unmask someone’s identity or his private key requires a violation of the property rights that surround and protect them—the person’s right to his computer, for example. Ownership consists of the exclusive right to control and to use a thing; if government accesses the computer with no regard to the consent of the real owner, then the government usurps ownership of the computer and unabashedly violates the rights of the real owner.

A Dramatic Shift in the Paradigm of Privacy

The Satoshi approach may confuse some people. As long as they cleave to the old paradigm of privacy—that is, privacy equals concealment—then the transparency of the blockchain sounds like a death knell. But the new paradigm of privacy is the transparency of information and the protection of identity. The focus has shifted from information on activities to information on True Names.

The transparency of transactions serves a vital purpose. For the sake of honesty and efficiency, the blockchain publishes every single activity. The protection of True Names also serves a vital purpose. For the sake of personal freedom, participants mask their identities at will and with ease. The blockchain does not require the verification of ID anymore than a grocery store records the names of those who buy milk with cash. Let everyone see, let everyone verify the truth of the transaction. Let no one demand personal information about the who and why of the exchange. Both honesty and privacy are preserved, but the link between a transaction and a True Name is broken. Forcibly reestablishing this link threatens users's wealth and freedom.

In the past, the focus of government and other Eves has been on the forced disclosure or surveillance of information about activities because the state had cornered the "identity industry." From birth onward, people are registered, certified, recorded, and processed according to the numbers and other identifiers issued by the state. David Friedman observes in his essay "The Case for Privacy," "It is hard to pass through the world without leaving tracks. Somewhere there is a record of every car I have registered, every tax form I have filed, two marriages, one divorce, the birth of three children, thousands of posts to online forums on a wide variety of subjects, four published books, medical records and a great deal more."

The identity or True Name of individuals has been far better known than their interactions have, many of which may take place in secret and silence. The Satoshi model turns this situation on its head. It makes all interactions public with all identities remaining private at the discretion of the individuals. Government no longer controls identity and, without such control, access to all other information has little value. The state is well aware of this.

The digital age has changed the cultural, political, and psychological zeitgeist of privacy. "Mind your own damned business!" was once a respected attitude, but government has slowly eroded the idea that innocent people need privacy. The new zeitgeist: Only those who have something to hide refuse to answer questions or to undergo scrutiny. "Only criminals fear government surveillance" is a common response to anyone who defends privacy today. But every peaceful person is now a criminal with something to hide. Why? Because everyone has exceeded the speed limit, taken an illegal drug, smuggled cheap booze or cigarettes across a border, made "unauthorized" additions to a house, fibbed to a government agent, understated their income, or violated one of the tens of thousands of statute laws that criminalize harmless behavior and do so in an

omnipresent manner. Most people are not aware of how many laws they break in the course of conducting a peaceful daily life.

In his book *Three Felonies A Day: How the Feds Target the Innocent*, attorney Harvey Silverglate details how the average American wakes up and goes about his daily route, not knowing that he is likely to commit several federal crimes as he does so. The number of federal crimes has soared exponentially in recent decades and prosecutors can now choose between a cornucopia of vaguely defined crimes with which to charge peaceful individuals of every background, profession, and status. A combination of broad and ill-defined laws, the drug war, and career-building prosecutors who are immune to consequences has turned justice into a conscience-free bureaucracy that seems to care nothing for innocence or guilt. Silverglate notes a standard procedure for the justice bureaucrats:

> Prosecutors are able to structure plea bargains in ways that make it nearly impossible for normal, rational, self-interest calculating people to risk going to trial. The pressure on innocent defendants to plead guilty and "cooperate" by testifying against others in exchange for a reduced sentence is enormous—so enormous that such cooperating witnesses often fail to tell the truth, saying, instead, what prosecutors want to hear.

Silverglate's book is chillingly reminiscent of an infamous Soviet-era quotation from the despised Beria, Stalin's head of the secret police. "Show me the man, and I will find you the crime." When someone asks you, "What do you have to hide?," you should answer, "From Beria and his ilk, everything, especially my identity (the man)."

Or, as Ayn Rand once explained, "The only power any government has is the power to crack down on criminals. Well, when there aren't enough criminals, one makes them. One declares so many things to be a crime that it becomes impossible for men to live without breaking laws."

Crypto users who demand privacy are especially vulnerable to cultural and political assumptions that strongly favor state control rather than individual freedom.

The strong assumptions against privacy include:

- The presumption of innocence belongs to government, not to individuals.
- A double standard of morality is applied to government and to individuals.
- Privacy is equated with concealment.

The Presumption of Innocence. The legal term "presumption of innocence" is sometimes expressed by the Latin phrase "*ei incumbit probatio qui dicit, non qui negat,*" which means the burden of proof is with the accuser and not with the accused. The accused is presumed innocent until proven guilty. The legal doctrine rests on the belief that most people are not criminals, so criminality cannot be

presumed; it must be demonstrated. The doctrine also acknowledges a fundamental principle of logic; because it is impossible to prove a negative, the burden of proof rests upon the person making a positive assertion. Someone may claim you are a thief. And even massive evidence of your honesty will not dispel the accusation because you could be lying about a past misdeed or concealing evidence. That is why the accuser is asked to specify what you have stolen and to provide evidence of the crime.

The presumption of innocence is the cornerstone of due process and a wall of protection against arbitrary prosecution by the state. It is a defining feature of a free society as opposed to a totalitarian one. The renowned British barrister Sir John Clifford Mortimer—best known as the creator of the beloved fictional defense barrister Horace Rumpole—was far from alone in viewing the presumption of innocence as "the golden thread" that weaves justice together.

The golden thread has unraveled.

In the name of security, the public has lost the presumption of innocence even in the absence of accusations. Border and airport agents fingerprint, frisk, interrogate, and bark "Your papers!" to queued hordes; individuals who do not comply are automatically yanked out of line and processed like criminals. Police officers demand ID and arrest those who refuse, whether or not the arrest is legal. After all, government agents are assumed to protect security and to enforce the peace. This means those who resist are against security and the peace. Few people ask where law enforcement obtains the right to demand obedience from people who are doing no harm. The presumption of innocence has transferred from individuals to government agents, which reverses the legal concept's original intent of protecting individuals *from* the state.

The logical principle of being unable to prove a negative has been replaced with the fallacy known as "the argument or appeal from ignorance." Here "ignorance" refers to a lack of contrary evidence—a situation deemed suffice to prove the truth of an assertion. In short, an accusation is true because it is not proven to be false. The criminality of an individual becomes a given because it is not disproven. Why else, the state asks, would he refuse to cooperate with authorities?

It is difficult to overstate the importance of the shift in a presumption of innocence from the individual to state agents. Just as the presumption of innocence is the golden thread of justice, the presumption of guilt for individuals is its death. It obliterates due process and slides society directly into totalitarianism. That's the political meaning and consequence of the question "What do you have to hide?" Government-issued ID is crucial to the process. After your True Name is known, then all other social control becomes possible.

Double Standard of Morality. A double standard of morality is at work in society—one for individuals and one for government. What is *im*moral for an individual to do has become moral for the state. If you take money from a neighbor at gun point, it is an act of theft for which you are justly arrested. If a government agent

does the same thing, it is an act of taxation by which the miscreant pays his “fair share” of earnings and for which the agent receives a salary and a pension. Modern morality is now defined by who is performing the act, not by the act itself. The impenetrable secrecy of the state is prudent while the privacy of individuals is criminal.

No voice rang out more clearly against a double standard of morality than that of the libertarian publisher Raymond Cyrus Hoiles who created the media chain Freedom Communications. Hoiles believed the double standard was more destructive to society than any other concept, and his ferocious attacks upon it blasted frequently through his newspapers.

In an editorial entitled “The Most Harmful Error Most Honest People Make” (December 17, 1956), which appeared in the *Santa Ana Register*, Hoiles explains the error. It “is the belief that a group or a government can do things that would be harmful and wicked if done by an individual and produce results that are not harmful, unjust and wicked. It is the belief that a number of people doing a thing that is wrong for an individual to do can make it right and just.” Hoiles most often critiqued the error with reference to taxation. Again, if it was wrong for a neighbor to steal your goods, then it was equally wrong for a group of neighbors or their appointed representative (government) to perform the same act.

The critique of a double standard did not start with Hoiles, of course. A 1657 pamphlet ascribed to the rebel Colonel Titan argues: “What can be more absurd in nature and contrary to all common sense than to call him Thief and kill him that comes alone… and to call him Lord Protector and obey him that robs me with regiments and troops? As if to rove with two or three ships were to be a pirate, but with fifty an admiral?” Yet this absurdity is what the state enforces when it acts in a manner that would not be tolerated from individuals.

Again, no one asks where government acquires these sweeping so-called rights. Since the only rights that exist are individual ones against which no one can rightfully aggress, if the government wishes to claim legitimate ownership of the private information of others, then it must produce proof of voluntary disclose, a transfer or sharing of title. Otherwise, the so-called rights are nothing more than the assertion of raw violence.

What applies to taxation applies no less to the violation of privacy. If it is wrong for a neighbor to pat down your body and that of your child without consent, then it is wrong for a government agent to do so in an airport. If it is wrong for a neighbor to tap your phone, to record your financial transactions, and to peek through your windows, then it is wrong for the government to do so. Individuals in a group do not relinquish personal responsibility because acts are always committed by an individual, and they are always a matter of personal responsibility. Gang rape is no less rape and the individual rapists are no less personally responsible simply because they were the second or third in line.

Nevertheless, people buy into a double standard that exempts state agents from moral and legal responsibility. If state agents, from the president to post-office workers, were bound by the same standards of decency and legal accountability as individuals are, then the current government would crumble.

Privacy is equated with concealment. Redefining "privacy" as "having a shameful something to hide" is a sleight of hand. In his excellent essay "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," Professor Daniel J. Solove explains the metamorphosis of privacy into concealment. "The argument that no privacy problem exists if a person has nothing to hide is frequently made…When the government engages in surveillance, many people believe that there is no threat to privacy unless the government uncovers unlawful activity, in which case a person has no legitimate justification to claim that it remain private." Oddly enough, people who make the "nothing to hide" argument also hang curtains on their windows and close them when undressing. They do not give their wallets or purses to strangers to rummage through. They close the door before having sex, and they object to their naked photos being posted online. What are they hiding? As Solove comments, privacy is "not about anything to hide, it's about things not being any one else's business."

The assault on individual privacy is toxic to society as a whole.

Consider freedom of speech. I remember being in a restaurant when a relative went on a post-9/11 rant about how the atmosphere in U.S. was beginning to feel like Cuba from which he had escaped. His wife tried to silence him, declaring in an adamant whisper, "You can't say those things in public." She was nervous as she glanced around to see who might have overheard. Surveillance and informants make people reluctant to express opinions that could be used against them in a legal or political manner. Property can be seized, families destroyed, and prison ensue. Why would anyone speak out if his children could lose a parent as a result?

Until recently, many incursions on privacy did not occur for no other reason than that they were difficult to execute. Then technology arrived. Surveillance now is far more efficient with less effort. Even notoriously incompetent bureaucracies are able to surveil as never before. Many people are afraid or complacent regarding surveillance. Some simply no longer believe in the possibility of privacy. The government benefits immensely from the Big Lie that privacy is now impossible due to the omnipotent and omniscient of the state. Balderdash. First of all, technology almost always empowers the individual as much or more than it does the government. Second, there is a world of difference between more difficult and impossible. Privacy may well be more difficult than before or, perhaps, its requirements have merely changed and different protections are needed than before. Perhaps privacy takes more innovation and work.

The Value of Privacy to Society

A healthy society requires privacy. When a government monitors general communication, people do not interact freely. This is especially true of dissenters,

the peacefully aberrant, writers, whistle blowers, drug users, government critics, skeptics, defense attorneys, artists… Anyone who is different in lifestyle or in opinion feels the chill of being watched by authorities who wave guns and jail cells. The bleak gray society of the Soviet Union and other communist states provides a cautionary tale of how fear crushes creativity and discussion. Surveillance strips society of color and vibrancy because it drains individuals of life, and individuals collectively *are* society.

It also prevents people from rising up against injustice. A defense of privacy is a defense of human rights. Financial privacy may not be the issue with which to enter a discussion of this link, however, because money arouses immediate cynicism. But the link must be established.

Consider freedom of religion and due process instead. A 16th century insurrection defined the evolution of both and their connection to privacy. The revolt revolved around a person's right to keep his religious beliefs private so they could not be used against him in a court of law. A current version of this right is called "taking the fifth"—invoking the due process right against self-incrimination. It is called "taking the fifth" because the Fifth Amendment of the U.S. Bill of Rights provides, "No person...shall be compelled in any criminal case to be a witness against himself." Although this mainstay of due process is often portrayed as a recourse for the guilty, the overwhelming beneficiary is the innocent man on the street who is protected against the exercise of arbitrary power, whether he realizes it or not.

The 16th century insurrection: Henry VIII denied papal authority and established the Church of England, which claimed new authority over people's souls. Protestants, called dissenters, were often tried for heresy with torture commonly accompanying trial. In the late 1530s, the Protestant John Lambert was burnt alive for heresy. During his trial Lambert became the first Englishman known to proclaim it was illegal under God and the common law to compel a man to accuse himself. He appealed to the privacy of conscience.

In 1563, the dissenter John Foxe published the immensely influential *Book of Martyrs*, a book of Protestant history and martyrology that has been called a "libertarian primer" on procedural rights. He argues for the right to remain silent in order to keep personal information private. Famously, the Leveller and libertarian John Lilburne employed Foxe's procedures in 1637 when he was brought before the Court of Star Chamber for circulating Puritan books. (The term "Star Chamber" has become a synonym for elitist and abusive courts that meet in secret.) Refusing to take the customary oath, Lilburne declined to answer questions that bore witness against himself. He was fined, whipped, pilloried, and sentenced to prison until he complied. While there, he penned an account of his brutal treatment, which was entitled *The Work of the Beast.* A few years later, the much-hated Star Chamber was abolished and the right to remain silent—the right to privacy—was established.

The right against self-incrimination—the right of privacy in personal information—lies at the core of due process. It is historically anchored in the quest for religious

freedom, but it applies no less to other freedoms, including economic ones. The demand for privacy did not merely protect individuals, however, it also inflamed societies toward freedom.

It is only a slight exaggeration to say that the American Revolution might not have occurred if colonists had not demanded the right of privacy in person and property. Privacy is a revolutionary principle and virtue that prompted American colonists to slam the door in the face of British officials both literally and figuratively. The Third Amendment of the U.S. Constitution, for example, prohibits the then-widespread practice of forcibly quartering soldiers in private homes, even during peace time. The Amendment sounds antiquated to modern ears, but the violation was important enough for revolutionaries to rank it third in the list of liberties declared by the Bill of Rights. The Third Amendment asserts the right of privacy against government's intrusion into that most personal of all realms—the home. As outmoded as the Amendment may seem, no great leap is needed to apply its principle to the current assault against all other forms of privacy.

The Fourth Amendment also asserts privacy. It opens by defending "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In terms of crypto privacy, the important word is "papers" because it can be extrapolated to apply to emails and other computer data, including real identities.

The Fifth Amendment champions privacy by delineating the right of an individual *not to* bear "witness against himself" in criminal cases.

In 18th-century parlance, when the state surveils computers and crypto accounts, it is seizing "papers." Physical-evidence rules do not always cleanly apply to digital evidence, however, and inconsistent rulings by courts on crypto privacy cause confusion. Insight into the growing legal mess over privacy may lie in the Fourth Amendment word—"papers." The Amendment states that both "papers, and effects, [are protected] against unreasonable searches and seizures." But the common law, upon which Western jurisprudence is based, has tended to grant greater protection to "papers" than to "effects," perhaps because papers are seen as a violation of person rather than property.

Law professor Donald A. Dripps opens his pioneering essay "'Dearest Property': Digital Evidence and the History of Private 'Papers' as Special Objects of Search and Seizure" with two questions. "Why does the Fourth Amendment distinctly refer to 'papers' prior to 'effects'? Why should we care?" Dripps asks in order "to ground special Fourth Amendment rules for digital evidence" within statute law to restrict "the volume of innocent and intimate information that must be exposed [or demanded] before the criminal material is discovered." Again, the American Revolution provides insight.

In the 1760s, British warrants for papers began to issue against colonial authors and publishers who were suspected of sedition. *Entick v. Carrington* (1765) is probably the most influential legal case of the time. The bare facts of the case:

John Entick published a paper that opposed the Crown. In 1762, officers broke into Entick's home and stole hundreds of papers in a search for evidence of treason. Entick sued. Entick won. The presiding judge, Lord Camden, offered a famous dictum. "If it is law, it will be found in our books. If it is not to be found there, it is not law." The government's purported right to seize papers was not in the statutes, therefore, it was not law.

Subsequent analysis of the *Entick* case found four aspects of the government's raid to be legally obnoxious; all of them apply to the current surveillance and seizure of financial information. The warrant was *indiscriminate.* The seizure *expropriated* the papers, denying their use to the plaintiff. The warrant was *unregulated* because there was no neutral oversight or avenue of appeal. The seizure was *inquisitorial* because it gave the government information about the private workings of Entick's mind. Counsel for Entick declared: "No power can lawfully break into a man's house and study to search for evidence against him; this would be worse than the Spanish inquisition; for ransacking a man's secret drawers and boxes to come at evidence against him, is like racking his body to come at his secret thoughts." Seizing papers was an attack against person, not property.

Any judge who subsequently considered issuing a warrant for papers had to consider Lord Camden's ruling that an alleged offense needed to be in the statute books if it was to exist in law. Moreover, warrants on papers increasingly ran afoul of state constitutions.

War changes laws, especially laws protecting individual rights. Dripps continues, "America…refused to modify the common law ban by statute until the Civil War." The excise tax was the federal government's major source of funding for the war, but tax evasion was rampant. In response, a unique statute was passed. "[This] act of 1863 was the first act in this country…or in England, so far as we have been able to ascertain, which authorized the search and seizure of a man's private papers, or the compulsory production of them, for the purpose of using them in evidence against him in a criminal case, or in a proceeding to enforce the forfeiture of his property." Seizure of papers was now in the statutes.

The question of papers versus effects legally zigzagged after the Civil War. Arguably, the most important shift came in 1886 when *Boyd v. United States* was decided by the U.S. Supreme Court. "The story of the Boyd case," Dripps writes, "properly begins with a statute authorizing customs officers to seize the books and papers of importers suspected of evading taxes." The Supreme Court ruled in Boyd's favor, saying:

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They…apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private

> property, where that right has never been forfeited by his conviction of some public offense, it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment.

The *Boyd* ruling reinstated greater Constitutional protection to papers than to effects, and it bears directly upon digital papers. The protection was never absolute, however, and it has severely eroded. Dripps explains, "During the last quarter of the twentieth century, the Supreme Court began effectively to equate 'papers' and 'effects'. Another line of modern cases established 'bright-line rules' that gave the same constitutional treatment to all 'effects'." Papers not only lost their special status under common and Constitutional law, they also came closer to becoming legally interchangeable with every other effect. This offered far weaker protection. Nevertheless, the precedent of *Boyd* prevailed for almost a century, and it is still not toothless.

The importance of papers is inextricably connected to the value of privacy to individuals. When the government steals data, it does not violate "property" in the legal sense of the word; it violates person.

Privacy is part of a healthy, creative, and self-reflecting life. Since childhood I've kept a diary into which I pour hopes, confusion, disappointments, and desires. When I read pages from the past, I connect viscerally to who I was at ten years old, and I better understand the person I am today. These diaries are private, not because I am ashamed of them, but because they are *personal*. In his dystopian novel *1984*, George Orwell stresses the importance of diaries:

> The thing that he was about to do was to open a diary. This was not illegal (nothing was illegal, since there were no longer any laws), but if detected it was reasonably certain that it would be punished by death.

1984's protagonist discovers his individualism. In this journey, the diary represents the freedom of speech and conscience that are essential to a sense of self—so essential that the state will kill him for this act of privacy.

Every infringement of privacy erodes the human spirit. A word is not spoken for fear of being overheard; a thought is not formed for fear it will become a word; a feeling is never expressed and, perhaps in time, not even felt. Then, one day, the outer silence becomes an inner one through the now automatic habit of self-censorship. People no longer question. Perhaps they no longer even notice that they no longer question. They have developed the habit of not being an individual, and they have become part of a collective will instead.

Everyone has areas of privacy to protect. Some wear lockets with photos of dead relatives; others harbor a forbidden love; some bolt the door to luxuriate in a hot bath without being disturbed; or they hide a sexual preference that confuses them. Every human being has a right to draw lines that harm no one else, lines that no one else should cross without an invitation. Slam the door in the face of anyone who says differently!

Crypto focus on privacy is more than the desire to retain wealth, as is usually claimed. It is a desire to retain individuality, the human spirit, and freedom.

CHAPTER SIX: True Names and Privacy

> All those who used their knowledge in a bid to enact social change saw cryptography as a tool to enhance individual privacy and to shift power from big, central institutions to the human beings who live in their orbit.—Paul Vigna

The world needs a new paradigm of privacy because the state will always win under the old paradigm as long as it controls the Identity Industry. The industry consists of far more than government ID and forms to fill out. In the last two decades, the Identity Industry has bloated to include airport screening, biometrics, Know Your Customer regulations, clandestine data caches, and surveillance at every turn. Alastair Berg of the RMIT Blockchain Innovation Hub observes, "These are just a handful of segments in an industry which is estimated to grow to USD16 billion by 2022."

The state will not loosen its grip on the industry because identification is an irreplaceable part of social control and the accumulation of wealth. This has been true since the Napoleonic era when an identity card was introduced that foreshadowed the modern ones. The purpose of the ID was to control wages by curbing the mobility of workers who wanted to move to get better jobs at higher wages. The cards were instrumental in converting a relatively free France into a police state.

The state monopoly on identification needs to be broken in the same manner that crypto breaks the monetary monopoly. It should not be confronted; it should be bypassed by providing a better alternative. This not only staves off the state but also provides a free-market alternative for the valid human need for identification. Historically, identification was a free-market function; marriage certificates, for example, were a private contract between families and honored by the church. It can easily be free market again. As long as the Identity Industry is a branch of government, however, this human need will either go unfilled or be satisfied at a staggering cost to freedom.

The new online paradigm for privacy is here. It is exemplified by the blockchain where interactions are transparent and real identities are protected. Privacy resides in shielding True Names—a reference to the 1981 pioneering novella by Vernor Vinge in which a group of hackers (called warlocks) penetrate computers around the world. Their real identities are secret from each other and especially from the Great Adversary—a reference to the American state. Masking real world identities is vital because anyone who knows a warlock's True Name can blackmail him or cause a True Death. Identity is literally a life and death issue.

The Origin of True Names

> I think the Mailman is taking us on one at a time, starting with the weakest, drawing us in far enough to learn our True Names—and then destroying us.— Vernor Vinge, *True Names*

True Names is one of the earliest fictional depictions of a fleshed-out cyberspace. It is widely credited with launching the cyberpunks movement, which later explored many of the themes presented in the novella.

The novella opens:

> In the once-upon-a-time days of the First Age of Magic, the prudent sorcerer regarded his own true name as his most valued possession but also the greatest threat to his continued good health, for—the stories go—once an enemy, even a weak unskilled enemy, learned the sorcerer's true name, then routine and widely known spells could destroy or enslave even the most powerful. As times passed, and we graduated to the Age of Reason and thence to the first and second industrial revolutions, such notions were discredited. Now it seems that the Wheel has turned full circle (even if there never really was a First Age) and we are back to worrying about true names again.

In the story, the protagonist hacker is visited by agents of the Great Enemy who have uncovered his True Name. They strong arm him into tracking down a bigger target known as The Mailman. Thus the story is highly anti-statist with a keen sense of how identity is crucial to freedom.

The novella spiked the admiration of crypto-anarchists who also drew upon its vision of cyberspace. A later reprint of *True Names* includes ten articles and essays by writers who provide commentary upon Vinge's story. One is the essay "True Nyms and Crypto Anarchy" by Timothy May, author of "The Crypto Anarchist Manifesto." (Nyms is short for pseudonyms.) In the *True Names* tribute, May optimistically states:

> Crypto anarchy is the cyber spatial realization of anarcho-capitalism, transcending national boundaries and freeing individuals to consensually make the economic arrangements they wish to make.
>
> It ensures that men with guns cannot be brought in to interfere with mutually agreed-upon transactions, the only kind of economics interaction possible in crypto anarchy. Some people will of course scream “Unfair!” and demand government intervention, which is why strong cryptography will probably be opposed by the masses, unless of course, they are wise and take the long view. This may smack of elitism, but I have very little faith in democracy. De Tocqueville warned in 1840 that, roughly translated, “The American Republic will endure until politicians realize they can bribe the people with their own money.” We reached that point several decades ago.

Strong cryptography and the privacy it offers are essential to the success of crypto-anarchy. Its antithesis is social control that requires identifying people and linking them to activities in order to be effective. Cryptography snaps this link. And not a moment too soon.

Government ID is currently the only way most people can prove their offline identities in order to access the necessities of modern life. In most Western nations, undocumented people cannot board a plane, drive a car, or rent an apartment. They cannot open a bank account, acquire a credit card, access medical care, cash a check, take a visible job, attend a university, or buy a car. They become second-class citizens.

Meanwhile, those with state ID become vulnerable to prosecution and persecution. In a nationalized ID and reporting system, the government knows who everyone is, what everyone owns, and where to find both. As Orwell eloquently argues in novels and essays, the nationalization of privacy is a linchpin of totalitarianism. No wonder the government's appetite for data is so ravenous. No wonder there is a drive to strip anonymity from the Internet under the aegis of concern about bullying.

What is needed now is a new paradigm for offline privacy that can work in tandem with online protections. Or, rather, an old paradigm should be revived. The offline privacy is best achieved by free-market ID that provides the benefits of identification without the liability of becoming a number in a bureaucratic file.

Free-Market ID Systems for Offline

Free-market ID is the antithesis of government ID in that it returns the power of identification back to the individual to use or not according to his own discretion. Free-market ID is a natural ally of cryptography because the goals are the same—to break the state monopoly on the Identity Industry.

When commerce was on the level of barter, people usually knew or knew of the individuals with whom they traded. When commerce expanded to include complex exchanges with total strangers a world away, then direct barter was replaced by indirect exchange that often required trust or a middle-man. A bedrock of trusting someone is the ability to answer the question, "Who am I dealing with?" Thus there is a legitimate need for identification and little danger to it as long as the state is not involved.

Consider a widespread method of identification from centuries ago that is making a comeback—letters of introduction. The basic dynamic: Person A carries letters of identification to Person C to whom A is a stranger. The letters are written by Person B who is a respected and mutual acquaintance. Person B vouches for the identity of the letter bearer and C is able to answer the question, "Who am I dealing with?" Such letters could be prepared by a business that verifies identities for profit.

An e-version of letters of introduction occurs in crypto circles and on networks whenever a respected member vouches for an outsider who wishes to join. Given the size of the community and the fact it is under attack, introductions seem to be an increasingly popular practice.

The letters embody the first and most basic service rendered by free-market ID: *authentication*. There are myriad reasons why someone would want to authenticate a person's identity. The person could be picking up a package, confirming a reservation, joining a club, cashing a check, or applying for a job. The filter of authentication means a stranger cannot commit fraud.

The free-market authentication of real identities can also be performed by companies that issue ID cards. Private ID is common today in a bastardized form that has limited value. Employers issue IDs to employees so they can unlocked offices; financial institutions offer credit cards to customers; universities hand out IDs so students can access services. But the privacy here is illusory. Before an employer or a financial institution issues ID, the recipient is screened in the hiring process or in opening an account . Student cards are prescreened by the extensive paperwork required to enroll in a university. This information is routinely reported to the state in one form or other. These semi-private IDs may be a proof of principle, but they are not free market or private.

The agorist Sunni Maravillosa speculates on what free-market ID might look like in her essay "ID Without Big Brother" in the anthology *National Identification Systems: Essays in Opposition*:

> If an individual wants an ID that attaches a certain label to her, she has several companies to choose from. IDs R Us is a national chain that has minimal requirements for such ID, and offers fast service and low prices. However, because it has minimal requirements, its safety record isn't that great, and many firms do not place much trust in their IDs. The most successful authentication ID issuer is Spooner's Identity Emporium. This company also has minimal requirements for low-level name-only ID, but it takes the additional step of verifying the ID seeker's history under that name, as well as the reputation of those who vouch for the ID-seeker. The company publishes a monthly list on its web site—usually a very short list, given its careful processing—of individuals whose ID has been revoked, along with the reason for revocation…Of course, if an individual doesn't like the requirements of one company, she's free to use another...

Most companies would be careful about accuracy because anyone defrauded by a false document might bring legal action. They would also be careful about client privacy since discretion would be key to the marketability of its ID. If company-issued IDs facilitate fraud or if client information is leaked, then the publicity alone would damage or ruin the company's reputation; free-market ID companies would live or die on their reputations.

The second service free-market ID offers to individuals is *certification*. Letters of recommendation attest to the character, the education, and specific abilities of the bearer. Businesses would be likely to cooperate with each other in providing such letters. Maravillosa offers a hypothetical example:

> Banks issue "credit credentials," which are based on an individual's or company's credit history with the bank, so that another individual or institution is satisfied that the entity in question is unlike to default on a loan or other credit arrangement up to a certain amount.

Again, the crypto version of this service is a personal online recommendation from a trusted figure about a stranger. Alternatively, the outsider could point to certifying documents—perhaps scholarly articles he has written on relevant subjects. His reputation itself can be a certifying ID.

Some forms of current ID perform a similar function. University degrees purportedly certify a level of education and intelligence; a letter of reference from an employer describes the laudable work habits of a former employee; membership in professional or charitable organizations suggests a person's character and social skills.

There is a marked downside to many current certifications, however. One of them: State licenses and diplomas frequently substitute for free-market methods of certification. Everything from neurosurgery to braiding dreadlocks requires licenses, and these tend to replace reputation as a measure of worth. An example: A non-traditional healer is well know for his skill, but he is unable to obtain a license. His reputation is stellar, but local doctors block the licensing process in order to eliminate their competition. The healer is unable to treat people without the risk of going to jail. State-mandated diplomas—even if they have value, which is increasingly in doubt—are barriers to those who are talented but not state sanctioned. In this manner, the state devalues or negates the worth of reputation.

The third purpose of free-market ID is to *authorize* specific actions. Letters can assign limited rights to the bearer. An attorney's firm might assign a limited power to one of its lawyers so he can settle a case on the behalf of a client.

Objections to Free-Market ID

Objections to free-market identification arise. The methods of identification are said to be antiquated, to not provide real anonymity, and to have no uniformity. Besides which, establishing a reputation is a slow process in a fast-moving world.

Antiquated. Some models of identification may be outmoded. But the surest remedy for this is to open up to field and let the marketplace innovate. The most antiquated IDs are the ones produced by the stagnant state.

No Anonymity. The primary purpose of early ID was to verify identity, not to render anonymity. And there is still a free-market demand to verify identity. There

is value in anonymity; there is value in being known. The value depends on whether the individual is able to choose freely between the two.

No uniformity. Another word for “no uniformity” is “diversity,” and it is one of the extreme advantages of free-market ID because it gives choice. Government ID is homogenized because the goal is to enforce conformity to laws and reporting requirements. When ID serves individuals, then its form is dictated by their needs and preferences, not by the state.

Slow to Establish Trust or Reputation. It is a fast-moving world. But the fact that a reputation or a business may take time and hard work to establish is hardly a criticism. Worthwhile achievements take time and hard work.

The State’s Nuclear Option in Weaponizing Data

> Privacy includes the ability to keep things secret from the government.…I might be keeping secret my weakness for alcohol, or heroin, or gambling or pornography and so preventing the government from stepping in to protect me from myself.…If you view government as a benevolent super being watching over you—a wise and kindly uncle with a long white beard—you will and should reject much of what I am saying. But government is not Uncle Sam or a philosopher king. Government is a set of institutions through which human beings act for human purposes. Its special feature—what differentiates political action from the other ways in which we try to get what we want—is that government is permitted to use force to make people do things.—David Friedman

Government is not a wise and kindly uncle. It is self-serving institution occupied by human beings with human passions, especially for power, wealth, status, moralizing, and revenge. These days, crypto users have reason to be particularly private. A recent news story declares, “NSA Has Been Tracking Bitcoin Users Since 2013, New Snowden Documents Reveal.” An abundance of caution both online and off is not paranoia when they actually are out to get you.

A February 6, 2018 headline in *Reason* magazine warns, “Governments Hate Bitcoin and Cash for the Same Reason: They Protect People’s Privacy.” The ensuing article spins off a quote from U.S. Treasury Secretary, Steve Mnuchin, “One of the things we will be working very closely with the G-20 on is making sure that this doesn’t become the Swiss numbered bank accounts.” Mnuchin rejects decentralized crypto as payment, investment, or savings systems because it cannot be easily tracked by government. Mnuchin’s criticism confirms that crypto is a positive good for individuals not only because it empowers them but also because it protects them from statists like him.

Privacy attacks around the globe are going to get more aggressive, and quickly so. Data are being weaponized at a frightening pace, making for a tight race between privacy and totalitarianism. States are developing new ways to use

databases to repress the opportunities and activities of people who make the "wrong" choices or have the "wrong" thoughts.

A headline in *Reuters* read, "China to bar people with bad 'social credit' from planes, trains." Social credit (*xinyong)* is a long-standing moral concept within the Chinese tradition, which indicates the level of a person's honesty and trustworthiness. The Chinese government now extends this moral concept to include loyalty to the state and social or political honesty; it assigns an official rank to each person. Then extreme social control is imposed on those with low scores by denying them "privileges," such as travel and education. Social-credit offenses include using expired tickets to board a train or smoking while on it, buying too much alcohol, watching porn, returning a rented bike in a tardy manner, "not showing up to a restaurant without having canceled the reservation, cheating in online games, leaving false product reviews, and jaywalking."

The trivial offenses may seem puzzling or even funny, but they serve an important purpose for the state and a horrifying one for individuals. The trivial offenses hand the state a blank check on suppressing dissidents, political opponents, or other "undesirables" because virtually everyone commits minor infractions as part of everyday life. As Beria once said, "Show me the man, I will show you the crime." The Chinese government can now pick and choose whom it wishes to convert into a nonperson by barring them from travel and other social interaction. The strategy is similar to that described in the book *Three Felonies a Day* by which everyone who flaunts state authority is vulnerable to criminal charges on one offense or another. Everyone is vulnerable to attack from the state. This danger also provides a huge incentive for people to obey absolutely and not to draw attention to themselves. This is true in China. It is increasingly true in many nations.

The concept of social credit is not uniquely Chinese. In the U.S., passports are denied to those who are sufficiently behind in child support or tax payments, and former felons find it difficult to travel abroad. Foreigners who tell a U.S. border guard that they have smoked marijuana, whether the event occurred in a venue where it was legal or not, will be refused entry. *Global News*, a Canadian outlet, explains, "they're…told to go back to Canada, and told they are inadmissible for life. This is a lifetime ban." Meanwhile, constitutional rights like gun ownership are being denied for an increasing long list of reasons.

Government's voracious appetite for the data required by social control is growing. The Cloud Act became federal law in 2018, for example. The Act allows federal law enforcement to compel U.S.-based technology companies to provide data stored on servers regardless of where the data are stored. It strips away Fourth Amendment rights against unreasonable search and seizure by allowing the U.S. to enter into data sharing agreements with foreign countries and bypass U.S. courts. Targeted users may never know of the warrant.

People need to choose their approach to privacy and prepare.

What Should You Do?

Strategies will vary from person to person because they are based on variables like personality and circumstance. There are many paths to privacy, not just one.

Before answering “What should you do?,” some distinctions are useful. All information is not equal, and encrypting everything may draw unwanted attention. You might consider encrypting only information that is important to your freedom, wealth, and well-being. Everyone has at least three kinds of personal data. First, there are data that should be broadcast widely, such as an employment resume. This information requires marketing, not privacy. Second, there are facts that are harmless to disclose, such as a favorite color or a preference in potato chips. The disclosure may draw unwanted solicitations from business, but these annoyances do not jeopardize rights. Third, there are facts that bad actors can use against you. Financial data are a prime example. This is the point at which privacy becomes a survival mechanism.

The next distinction is the well-trodden ground of privacy versus anonymity versus pseudonymity. I will tread it again briefly.

Privacy is the act of keeping personal data or activities to yourself in its entirety or to whatever is your comfort level. What is your comfort level?

Anonymity is the strategy of making content transparent but hiding True Names. Rick Falkvinge, founder of the first Pirate Party, elaborates,

> The typical example would be if you want to blow the whistle on abuse of power or other forms of crime in your organization without risking career and social standing in that group, which is why we typically have strong laws that protect sources of the free press. You could also post such data anonymously online through a VPN, the TOR anonymizing network, or both. This is the analog equivalent of the anonymous tip-off letter, which has been seen as a staple diet in our checks and balances.

Pseudonymity is the strategy of using a fictional name rather than a True Name. It is anonymity acquired by disguise. Pseudonymity is not a recent phenomenon. The influential *The Federalist Papers* (1787-1788) were written by Publius—a collective pseudonym covering James Madison, Alexander Hamilton, and John Jay. Historians still disagree upon who wrote some of the pieces; this testifies to the effectiveness of pseudonymity.

The most effective tactics to protect online data may well be technological, but this book does not address them, except in passing. Instead, the article points to privacy strategies or habits that have been used for decades, if not for centuries. Some of them will be familiar. The purpose is not to advance new or revolutionary material; it is to make people be conscious of and to think about how to maintain privacy.

They have been updated to focus on crypto. Here is a sampling of some basic, effective techniques:

Obfuscate or "hide in plain sight." Be so inconspicuous or subtle in your outward actions and appearance as to be almost unnoticeable. Blend in and become invisible. Sometimes obfuscation involves participating at venues that are so filled with "noise" that an eavesdropper finds it difficult to distinguish your signal from any other. The core of this strategy is to avoid calling attention to yourself. When you do "noteworthy" things like calling for the overthrow of the central banking system, then do so under a pseudonym. Under your True Name, be restrained.

Avoid Centralized Exchanges and Other Data Sharing Centers. This is an updated-for-crypto-users version of the advice to avoid data collection centers connected with the state, such as the central banks. If you want the state to have all your financial data, then you should just mail it state agencies.

Password Protect Everything and Stay Virus Free. A password is like a lock on a door that makes it more difficult for bad actors to enter. Prevent viruses and malware through which hackers can attack your data and steal your identity. Never open unsolicited files in emails; never download files from unknown or insecure sites. Run a competent an antivirus program and prefer browsers that resist infection, such as Linux ones.

Find Discreet Ways to Cash Out. The crypto veteran Kai Sedgwick writes, "Bitcoin transactions are semi-anonymous: every transaction on the blockchain is broadcast publicly and visible for all eternity, but the owner of each wallet is unknown. Tying addresses to real-world identities is now relatively easy for the powers-that-be, because everyone has to cash out somewhere, and that usually involves linking bitcoin addresses to bank accounts." Don't use trusted third parties to cash out. As much as possible, deal with people one-on-one or through decentralized exchanges that facilitate peer-to-peer buying and selling. Be inventive. Seek venues that exchange crypto for gift cards to stores at which you regularly shop, including grocery stores.

Chose a Search Engine that Respects Privacy. Many search engines record browsing histories and use them to target ads or to generate revenue by selling them. Others, like DuckDuckGo, do not track personal data.

Use a Privacy Currency. Dozens of such currencies exist, and more are coming because privacy is in demand. The founder of Zcash explains the philosophy behind his privacy currency. "We believe that privacy strengthens social ties and social institutions, protects societies against their enemies, and helps societies to be more peaceful and more prosperous.… A robust tradition of privacy is a common feature in rich and peaceful societies, and a lack of privacy is often found in struggling and failing societies."

Never Give Out More Information Than Necessary. Never volunteer information, especially in writing, whenever refusal or silence is an option. If a form is

mandatory, fill out as few blanks as possible in as confusing a manner as possible. Be suspicious of any venture connected to crypto that requires more than minimal information to acquire the service or good being offered. No one in crypto needs to know a social security number, even the last four digits. Always ask those who request info “why” it is needed and the uses to which it will be put. Decide in advance how much data you are willing to disclose and in what form.

Zip It on Public Forums. Public forums, like Facebook or Twitter, are monitored and mined by government and corporations; they are also monitored by criminals and malicious people who bear grudges. Public forums are collection points for personal data, even if a person thinks he is posting anonymously. If social media is necessary for professional reasons, then use it to the bare minimum and only for professional reasons. Never post anything on social media that you wouldn’t put on the front page of the *New York Times.*

Be Careful in Recording Information. Do not write down private keys, for example, without having a secure, undisclosed place to store them. It makes no sense to encrypt online data if the same informative is lying in cursive form on the kitchen table.

Use Only Secure Wi-Fi Connections. It is common for people to hook up to the free Wi-Fi at Starbucks and other venues, but there is no way to tell who may be listening in on your internet traffic. If you must use insecure Wi-Fi, then do not transmit personal data and use a VPN service to encrypt personal data.

Lie When Establishing Password Security Questions. “What is your mother’s maiden name?” With this information, a bad actor can crack his way into your bank accounts and, perhaps, steal your identity. Do not answer this or other standard “identifier” questions truthfully. Have a standard false answer that you do not use on official or important forms that are secure. On those, tell the truth.

The foregoing rudimentary precautions are meant to form the habit of privacy. Many people have a habit of disclosure, of reflexively telling the truth. A habit is nothing more than an automatic response that results from an established pattern of behavior. It may be difficult to break the habit of disclosure and replace it with discretion, but it is necessary to do so. Never lie to a friend, but do not hand a stranger the keys to your identity.

The government is coming for crypto, which means it is coming for users. Its front line attack will be an assault on privacy because privacy is the backbone of crypto as a tool of freedom. Now is the time for heightened vigilance. To paraphrase the comedienne Lily Tomlin, “No matter how paranoid I get, it is never enough to keep up.”

Privacy may be the front-line defense of individual freedom but decentralization is the social condition under which privacy thrives. No one can or should tell individuals which specific strategy to use. But, if you value privacy and safety, stay private and decentralize.

SECTION THREE: DECENTRALIZATION

CHAPTER SEVEN: Decentralization at the Core of Crypto Freedom

> A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system.—Satoshi Nakamoto

Despite the incredible success of crypto, the question of whether the free market can establish a viable monetary system still arises. It is often suggested that crypto is workable only because it exists in parallel with fiat with which it is convertible and upon which it rests. Does the institution of money ultimately require trusted third party oversight and the context of the state? (An institution is an established law, practice, or custom within a society.)

The question can be reduced to a more fundamental one. How does any institution within society arise, and how does it decline? The answer lies within the concepts of decentralization and centralization.

What is Centralization? What is Decentralization?

Centralization concentrates control of an activity or organization under a single authority in order to coordinate results. In terms of the monetary monopoly, the activity is society; the authority is the state that coordinates the flow of finance with the stated goal of producing an efficient and productive economy. Another term for centralized control of society is "social engineering." The state applies theories of social science to the management of human beings in order to control their placement and functioning. The social control is intended to achieve a society that is just or effective according to the vision of those in charge.

Not all centralization dismisses individual choice. Private businesses can centralize under one management team to increase profits, for example. When they do so, they are often called corporations. The crucial difference between this scenario and state centralization is that businesses are voluntary, and the individuals involved are free to walk away to join a competitor. With social control, the individuals have no choice. Walking away constitutes breaking the law, and there is no competitor.

Decentralization is the diffusion of power away from a central authority down to its constituent units. In the political arena, this means passing control from a national level down to a local one. Discussion of decentralization usually starts and stops in the political realm, with the power still vested in a coordinating authority. A local government may be better than a remote one because it is more responsive to the community, but the logical end point of decentralization is the individual who is the building block of all society and its most basic constituent

unit. This arrangement is both a method and a goal. The method is the empowerment of the individual. The goal is a healthy society in which every member makes his own choices according to his own self-interest.

Centralization is so woven into the fabric of the culture that many people believe it is necessary for society to function. Public schools, central banks, the judiciary, public works, government roads, tariffs…most people cannot envision society through any lens other than centralized state control; it is all they have known and all they have been taught.

Throughout most of history, society has been viewed as the result of someone's design. The designer might be God, a tribal chief, a monarch, a committee of socialists or communists, a team of experts, or some other entity that was the state misspelled. Society was seen as an artificial construct created and managed by authorities. Society was deemed to be dependent upon a coordinating authority for its law, morality, and prosperity.

In his three-volume work *Law, Legislation and Liberty*, social theorist Friedrich Hayek refers to this position as "constructivist rationalism." A core constructivist belief is that man can and should consciously invent social institutions such as the law through the application of reason and social science. Hayek argues vigorously against this perspective, claiming that constructivists misunderstand the process by which the institutions of society evolve. Indeed, he believes the constructive approach is antithetical to the real process and hinders social institutions that should evolve rather than follow a blueprint. In a 1974 Nobel Memorial Lecture entitled "The Pretense of Knowledge," Hayek expresses a basic epistemological objection to constructivism—that is, an objection based on a theory of human knowledge. He states that no committee can predict the evolving choices and unintended outcomes of a mass of people who interact over time. Human preference is too variable, and it changes in ways that thwart all planning.

To recycle a quotation from earlier in the book:

> The recognition of the insuperable limits to his knowledge ought indeed to teach the student of society a lesson in humility which should guard him against becoming an accomplice in men's fatal striving to control society—a striving which makes him not only a tyrant over his fellows, but which may well make him the destroyer of a civilization which no brain has designed but which has grown from the free efforts of millions of individuals.

Hayek's contemporary, the Ludwig von Mises comes to the same conclusion from a less epistemological and more economic angle in his masterpiece *Human Action.*

> Human action originates change. As far as there is human action there is no stability, but ceaseless alteration…The prices of the market are historical facts expressive of a state of affairs that prevailed at a definite instant of the irreversible historical process….In the imaginary and, of course,

> unrealizable state of rigidity and stability there are no changes to be measured. In the actual world of permanent change there are no fixed points…

Both Hayek and Mises believe that the knowledge sought by constructivists is unattainable. It is not possible to plan the dynamics of tomorrow based on those of yesterday because people's preferences and other circumstances are unforeseeable, even by the people involved; guesses are possible, but knowledge is not. Even a small thing, like the price of bread yesterday does not give knowledge of the price of bread tomorrow because it might skyrocket due to a flour shortage or a change in people's priorities.

Using a static photo of yesterday's society to engineer the future goes against a basic tenet of human action and human nature: inevitable change. Inevitable change is a fundamentally difference between human beings and the physical objects examined by the hard sciences upon which the constructivists based their social theory. A scientist can learn everything he needs to know to predict the behavior of a rock because the rock is static over time. Water continues to have the same molecular structure, and it continues to be defined by constants such as the law of gravity. But society does not consist of invariable objects. The behavior of human beings is based on altering preferences, emotions, and psychological responses that can be conflicted or hidden even from the people who are acting. Human beings cannot be neatly categorized, stacked, and made to obey the laws of science. Society consists of unpredictable individuals who react to changing circumstances. They are not rocks or water.

There are two ways for social theorists to approach the waywardness of unforeseeable man. They can accept the nature of human beings and work their theories around it, or they can try to change the nature of man to fit their theories.

Constructivists choose the later option, with the new Soviet Man or Soviet Person being one manifestation of their theories. The new Soviet Man was deemed to be the logical evolution of human beings under communist rule. In his book *The Mass Psychology of Fascism* (1933), the German psychoanalyst Wilheim Reich asks, "Will the new socio-economic system reproduce itself in the structure of the people's character? If so, how? Will his traits be inherited by his children? Will he be a free, self-regulating personality? Will the elements of freedom incorporated into the structure of the personality make any authoritarian forms of government unnecessary?"

Human nature, like society, would be reconstructed by those in power. The new Soviet man was an archetype or ideal human being with specific characteristics that would be designed by and evolve out of communism. The new human nature would be shared by all Soviet people irrespective of factors such as differing cultural or ethnic backgrounds. The communist characteristics included selflessness, enthusiasm for communism, physical health, collectivism, and

discipline. There was also to be a new Soviet Woman, the likes of which the world had never seen before—self-sacrificing and devoted to revolutionary ideals.

By contrast, Hayek works dispassionately with human nature as he observes it to be—self-interested and individualistic. He views social engineering as more than merely impossible. It is also tremendously destructive because it is the antithesis of a natural society, and it destroys the liberal institutions that had evolved to serve individuals rather than the state.

Hayek knew first-hand the hideous consequences of central planning. He had witnessed the devastation of classical liberalism by two world wars, but especially by World War I that had shattered the mold of the free market. Wartime government had clamped centralized control over the private sector to ensure the flow of armaments and other "necessary" goods. Money had been drastically inflated and reduced in value to pay for massive military build-ups. War strangled the flow of free trade, which classical liberals thought was a prerequisite to peace between nations, as well as the prosperity of individuals. Hayek watched as the centralizing machine of 20th-century statism destroyed the promise of 19th-century classical liberalism.

In rebuttal to constructivism, Austrian economists describe how institutions in a healthy society arise spontaneously. The descriptions often begin with simplistic models to illustrate a basic principle or point—how a path is forged through a field, for example. One person takes the shortest route across an overgrown field, and his passage leaves a crude trail of trampled grass behind. As a matter of convenience, the next person who crosses the field uses the rough path, which becomes more clearly established as a result. Each person who subsequently crosses contributes to making the path more distinct and easier to walk. No one constructs the path intentionally or as a service to other people; it is simply in each person's self-interest to use the easiest route across the field. Nevertheless, the self-interested reinforcement of the path benefits everyone who walks the field thereafter.

One of Mises's earliest works, *Nation, State and Economy* (1919) analyzes how much more complex social phenomena—such as language—were also the unintended consequences of individual interactions. No committee or central authority decided to invent human speech or to publish a dictionary, let alone to design a specific language like English. Without benefit of law, individuals began communicating in order to get what they wanted from each other. The sounds being uttered gradually became more redefined and varied, even as the meanings of specific sounds became more widely recognized. Language evolved.

Hayek develops a similarly sophisticated system of social theory to explain how all of society's institutions naturally evolve from the bottom up—from the voluntary and unplanned interactions of individuals—rather than from the top down—from experts or the powerful who imposed their will. Natural institutions, Hayek maintains, are the collective but unintended results of human interaction: "the result of human action but not of human design." Even complex social

phenomena—such as writing, religion, or money—are the unintended consequences of human interaction. The alleged efficiency of government programs paled by comparison, to say the least.

Constructivists counter-argue that an unplanned society is chaotic and wasteful. With sufficient knowledge and a scientific approach, they believed a perfectly efficient society could be engineered. No surpluses, no scarcities, no waste, no unemployment. Stock markets would not crash, and currencies would not fluctuate, except when they were supposed to do so. Society could be constructed so that its members walked in unison toward the same allegedly desirable social goals, just as they had marched in unison as soldiers toward victory in war.

Mises's answer to constructivists would recast the concept of individualism.

The New Austrian Individualism

A new conception of individualism arose in response to a theory that accompanied constructivism. Social holism became popular in the early twentieth century. Social holism claims that systems must be viewed as wholes rather than as collections of their parts, and a whole's dynamic differs from the sum of its parts. In short, the collective is greater than and different from the units that comprise it. A holistic analysis of society usually begins with a study of the collective, not the individual, and it assumes that the behavior of the individual is determined by the collective. Individual behavior is defined by the category or properties of the class that is its context. Society is more than the sum total of the individuals who constitute it.

Austrian economists claim the opposite. Society results from and it is explained by the behavior of the individuals who collectively *are* society. Society has no independent existence apart from its individual members, all of whom act on their self-interest. Self-interest is not equivalent to selfishness, however, as traditionally selfless acts—giving to charity, helping a neighbor, sacrificing for family—are frequently viewed by individuals as behavior that enriches life. In what seems like a paradox to some, traditionally selfless acts are often undertaken as a matter of self-interest.

Marxists accuse those who reduce society to individuals of being atomistic; that is, they are said to splinter society into unconnected and isolated units so that society does not truly exist. In response, some Marxists go so far as to assert that it is the individual, and not society, who is the true abstraction. That is, individuals do not exist without a surrounding society that defines them and constructs them. Mises observed of this position, "The notion of an individual, say the critics, is an empty abstraction. Real man is necessarily always a member of a social whole."

Karl Marx argues a point similar to this by using a Robinson Crusoe scenario, which is a popular way to construct an argument about human nature from its absolute basics—man in isolation. An individual who is born and abandoned on a desert island, Marx contends, will be more of a potential human being than an

actual one. (Some socialists, like Hegel, argue that man himself was an abstraction.) Marx makes a distinction between "human nature in general" and "human nature as modified" by historical periods of epochs. Two types of human drives exist: ones that are fixed like hunger, and ones that "owe their origin to certain social structures and certain conditions of production and communication." Marx's point is that, beyond inherent characteristics like instinct, human nature is a social construct defined by social context; society creates the humanity of its individual members. This meant society could construct what Marx considers to be the right type of humanity—like the new Soviet man—if the institutions of society are thoroughly oriented toward achieving this goal.

Classical liberals argue the opposite. A person raised in isolation will still be a realized human being with human characteristics far beyond a drive for the basic needs of survival. For example, Crusoe will have a scale of preferences that economists call marginal utility, and he will act to achieve the highest one first; he will get water to drink before water to bathe in. He will have curiosity and an ability to feel sorrow. Without social interaction, huge parts of his potential will never develop, of course, but this does not make him less human or make him lack an individual will and personality. Collectives offer incentives for specific behaviors, but they do not define humanity. Human beings and their innate nature define collectives. Under Mises's analysis, this simple argument evolves into a sweeping new approach to individualism.

As a general social theory, individualism means the advocacy of individual freedom as opposed to the power of a collective, especially the state. As a personal matter, it means people make their own peaceful choices and take responsibility for them. Although an individualist is sometimes characterized as a loner, the opposite is usually true because human beings are social animals who crave interaction almost as much as they do food and shelter. Cooperation and trade are the realization of individualism because they allows the individual to express preferences and satisfy needs. "Once it has been perceived that the division of labour is the essence of society," Mises observes, "nothing remains of the antithesis between individual and society. The contradiction between individual principle and social principle disappears."

A core concept of Mises's philosophy of individualism is "praxeology"—a word meaning "deed or action," which derives from ancient Greek. Its modern meaning is "the study of human action, based on the belief that human behavior is purposeful as opposed to unintentional or reflexive like blinking." Except for reflexive behavior, people act because it is in their self-interest to do so, if only to remove what Mises calls "felt uneasiness." It is true both of shifting in a chair to relieve an aching muscle and of investing in the stock market to provide for retirement. All human action is individual, purposeful, and self-interested.

Mises then delineates the theory most associated with him. His masterpiece *Human Action* describes methodological individualism:

> First we must realize that all actions are performed by individuals… If we scrutinize the meaning of the various actions performed by individuals we must necessarily learn everything about the actions of the collective whole. A social collective has no existence or reality outside of the individual members' actions. For example, the individuals who comprised a family interacted with each other within a specific context and sum of those individual interactions was what constituted the abstraction 'family'.

Mises uses the nonideological or neutral concept of methodological individualism to describe the basic nature of human action, as well as to deconstruct the abstraction of the state. If only individuals act, then everything the state does or is can be reduced to actions taken by the individuals who collectively constitute the state. In a famous example, Mises explains, "The hangman, not the state, executes a criminal. It is the meaning of those concerned that discerns in the hangman's action an action of the state." Individuals who look at the hangman see the state only because they have accepted the abstraction called "the state" to provide a framework in which to understand his behavior. Without the context of the state, the hangman would be viewed as a murderer rather than as an instrument of justice.

Mises readily admits that the hangman acts in relationship to other individuals such as judges who also constitute the state; the hangman is part of the penal system. He may also act under duress because a refusal to execute a criminal could cause dismissal and hardship for his family. But praxeology is concerned only with an individual's behavior, which is the starting point for and the only observable proof of individual preference. Praxeology does not address the social or psychological influences upon human action; that is for another field of study to do. Mises simply states that all actions are initiated by and carried out through individuals who act to advance their own self-interest. Otherwise explained: It is not the state but the individual executioner who raises the deadly axe. It is *his* arm, and he cannot escape responsibility for the actions he chooses to take. (Of course, this does not exonerate other individuals involved, again such as judges.)

If only individuals act, then collective behavior is nothing more than the sum total of the actions and interactions of the individual members. It is common to speak of collectives or abstractions as though they were separate entities that are more important than their members. It is common to speak of them as though they acted and thought as a group. When a man is arrested, for example, the news reports that he was picked up by the police department. In reality, the man was picked up by an individual policeman after an individual judge had signed a warrant. When a battle occurs, the newspaper reports a military advance when individual soldiers were the ones who actually advanced. Groups do not act or think. Individuals do, and sometimes they choose to obey a central authority, which gives the impression of collective thought.

Methodological individualism sounds antisocial to some. The impression could be bolstered by Mises's use of a Robinson Crusoe framework as well—man in isolation—to explain praxeology. This use does not suggest that human beings are

antisocial, however. Quite the opposite. The Crusoe thought experiment is meant only to remove the complicating factor of interpersonal relations while pursuing the question “what is human action qua human action?” It is similar to a scientist returning to fundamental principles in order to understand a dynamic. The Crusoe conclusions are then applied to the real world of society.

Human Action explains:

> If praxeology speaks of the solitary individual, acting on his own behalf only and independent of fellow men, it does so for the sake of a better comprehension of the problems of social cooperation. We do not assert that such isolated autarkic human beings have ever lived and that the social stage of man’s nonhuman ancestors and the emergence of the primitive social bonds were effected in the same process. Man appeared on the scene of earthly events as a social being. The isolated asocial man is a fictitious construction. (Note: Autarky is the characteristic of self-sufficiency.)

Society increases individualism because it moves human beings further from the animal level, allowing each person to reach his potential and to achieve goals that are impossible in isolation. Interaction is also a survival mechanism. Jointly-produced wealth can be far more abundant than privately-produced wealth, for example, which leaves everyone involved richer and more likely to thrive. It is precisely this sort of cooperation that led mankind to dominate the planet. Human beings are profoundly social and the rewards of society are immense.

Mises argues that collectives—such as family or society—are invaluable abstractions that allow people to understand and to describe their interactions with other individuals. Collectives provide the specific context in which to make sense of individual action and shifting group dynamics. He explains, “Methodological individualism, far from contesting the significance of such collective wholes, considers it as one of its main tasks to describe and to analyze their becoming and their disappearing, their changing structures, and their operation. And it chooses the only method fitted to solve this problem satisfactorily.” Individualism is the key to understanding collectives. It is decentralization applied to real and everyday life.

And, yet, if only individuals act, how can collective institutions arise? The answer returns to the concept of spontaneous order advanced by Hayek, among others.

Spontaneous Order in Economic Production

The analysis so far has focused on how institutions and society can arise—arguably, how a healthy system *must* arise—as a function of the free market and free association. The dynamic is easy enough to describe with reference to an isolated tribe. But can the framework of individualism be expanded from a local level to a global one to provide for mechanisms like international trade where individuals most often do not know each other nor interact directly?

On the local level, cooperation is usually intentional. Farmers sell produce to local markets; a team of programmers design the latest, greatest app; a hospital coordinates staff schedules, with doctors consulting with patients; truck drivers deliver goods to a given address; a start-up business contracts with a marketing expert. These are intentional and direct contacts within the limited context of one society.

How can individuals in foreign countries who do not know each and do not even speak the same language hope to cooperate in the creation of anything? Isn't an overriding authority necessary for the coordination of strangers in global trade? If so, then the overriding authority—that is, government—is also required domestically because all modern nations live or die on global trade. A requirement for centralization reintroduces the state as a powerful policeman of the economy.

Global trade does not require oversight. It may seem paradoxical to say that strangers will unknowingly cooperate to mutual benefit because it is in their own self-interest to do so. But that's what happens. The cooperation is not aimed at creating society or institutions. Each participant aims at enriching himself.

"I, Pencil" is a brief essay by Leonard Read, founder of the Foundation for Economic Education. It is a tale told from the perspective of a pencil that chronicles its own creation. The saga begins with the harvesting, mining, and forming of raw materials in far away lands, including cedar, glue, wax, graphite, lacquer, and pumice. Foreign workers meet quotas for the variety of businesses for which they labor in order to make money to feed their families. They may not know the final destination or purpose of the raw materials; they may not care.

The crews of foreign ships transport the materials to a destination where dock workers unload the containers, and truckers convey them to a pencil-making factory. Individuals in a crew and on the dock are probably indifferent to or ignorant of the cargo contents because they are paid the same wages whatever the shipment. Up to this point, everyone involved in the prepencil manufacturing cares nothing about pencils themselves; they do not even know the part they play in the manufacturing process. Their purpose is to earn a living, pure and simple.

The raw material arrives at a pencil factory, where self-conscious cooperation toward creating the pencil may begin. Although pencil factories today are probably automated, this does not mitigate the human cooperation necessary to produce a pencil. Even automated factories require management oversight, equipment providers, repairmen, janitors, investors, and an array of other individuals to produce one pencil. This does not mean these people know each other, however, nor do they necessarily care about pencils. They want to profit through wages or returns.

The end product of a multitude of strangers who act solely in their isolated self-interest is a pencil.

In his introduction to “I, Pencil,” the Nobel-winning economist Milton Friedman writes:

> None of the thousands of persons involved in producing the pencil performed his task because he wanted a pencil. Some among them never saw a pencil and would not know what it is for. Each saw his work as a way to get the goods and services he wanted—goods and services we produced in order to get the pencil we wanted. Every time we go to the store and buy a pencil, we are exchanging a little bit of our services for the infinitesimal amount of services that each of the thousands contributed toward producing the pencil.
>
> It is even more astounding that the pencil was ever produced. No one sitting in a central office gave orders to these thousands of people. No military police enforced the orders that were not given. These people live in many lands, speak different languages, practice different religions, may even hate one another—yet none of these differences prevented them from cooperating to produce a pencil. How did it happen? Adam Smith gave us the answer two hundred years ago.

Smith’s answer was the “invisible hand.” The term is introduced in the book Smith considered to be his masterpiece, The Theory of Moral Sentiments, and it reappears in his subsequent work, Wealth of Nations . The invisible hand refers to the unintended but immense benefits to society that flow from people who act in their own self-interests, especially economic self-interest, in the manner described by “I, Pencil.” Almost invisibly, order arises out of the self-serving actions of individuals who cooperate with others, whether intentionally or not, whether knowingly or not. The natural order declines when voluntary interaction is hindered by government interference. In short, liberty brings civilization and prosperity; power produces conflict and poverty.

“I, Pencil” and the “invisible hand” clarify another confusion that can come from discussions of spontaneous order; namely, the definition of spontaneous order as the “result of human action but not of human design” is a bit ambiguous. Clearly, there is designed order within the chain of activities necessary to make a pencil. The workers who gather the raw materials work for a designed company with a specific goal, as do the ship and dock workers. The factory is a highly-designed machine.

The phrase “the result of human action but not of human design” does not deny that production requires design. “Not of human design” means that no central planner organizes or coordinates the various stages of production. All organization and structure are provided by those individuals who, at various points, independently own, manage, or work for the endeavors that result in a pencil. Without an overseeing authority, they coordinate with each other and function well. Indeed, an overseeing authority would be an obstacle to their efficiency. The phrase “the result of human action but not of human design” seeks to explain how

complex networks can arise out of the apparently unintentional cooperation—a cooperation upon which modern life depends.

“Not of human design” refers to the army of strangers whose self-serving and ostensibly uncoordinated actions deliver a stunning array of goods, with no conscious intention of doing so. They act in their own self-interest. As a result, the average person enjoys a higher living standard today than nobles did in the past, including fruit out of season and a magnificent array of wine to accompany it. The cooperation also binds people together in peace because they have a vested interest in continuing to profit from each other through trade. Multiply this cooperation by the many millions of interactions that create millions of products and services, and the collective dynamic becomes a glue that holds societies together and allows global trade to emerge—trade that is the engine of peace.

So far, spontaneous order has been applied to economics—the bedrock of society. Within spontaneous order, economics is often called catallaxy.

CHAPTER EIGHT: Crypto as an Austrian Economic Phenomenon

> Bitcoin…is better understood using the conceptual lens of the Catallaxy: participants in Bitcoin spontaneously form a decentralized monetary and financial ecosystem, collectively choosing Bitcoin as a medium of exchange and store of value. Bitcoin is…an irrefutable demonstration of spontaneous order in action.—Francis Pouliot

The Catallaxy of Crypto

Catallaxy examines how *economic* order emerges in a system through the uncoordinated and diverse actions of individuals who pursue their own self-interests; it is economic spontaneous order. Sometimes called “catallactics,” the economic concept is one of the intellectual breakthroughs that allowed free-market advocates explain how society evolved without a central authority. Hayek defines it as “the order brought about by the mutual adjustment of many individual economies in a market.”

The obscure term captures the dynamic that creates civilization: spontaneous economic cooperation between individuals and groups of individuals. If human beings are to rise above the level of Robinson Crusoe, then they must interact to mutual advantage. Cooperation is so valuable to individual freedom that Satoshi provided the blockchain’s blueprint for free as a way to better the world because this bettered him. It was in his self-interest.

The Satoshi revolution exemplifies how methodological individualism and catallaxy work together. Economic control is vested in individuals. People store their wealth in private wallets with which they conduct international trade, without going through a banking system that would be the equivalent of going through the state. The decentralization is reinforced, not contradicted, by the cooperation

of a network of people who are strangers acting in their own self-interest. Yet the strangers all benefit each other, even though they might not like each other in person should they ever meet. Crypto is true economic society.

Throughout the work of Hayek, Mises and other free-market economists, two fundamental concepts emerge repeatedly: methodological individualism and spontaneous order. The two concepts are the backbone that forms the ideological structure of cryptocurrency. They also explain why the explosion of crypto freedom was so unexpected. It sprang from individuals and freedom of action, both of which encourage unpredictable bursts of creativity. With crypto, the explosion occurred in the area most in need of it.

The most difficult area in which to implement methodological individualism is finance because it has been controlled for so long by one of the most powerful collectives in existence: central banks that function as arms of the state. This means that the institutions surrounding central banking have been formed by its presence and requirements. Public attitudes have been similarly formed.

Society needs to be reminded: Government does not produce wealth. Yet the state needs vast amounts of money to finance bureaucracy, the military, and other centralized trappings of power. This means government needs to steal vast amounts of wealth from the private sector. But to do so directly might cause resistance in the form of tax revolts or worse—worse for the state, that is. So government issues bonds, compulsory fiat, encourages inflation, and it forces all commerce to go through crony institutions that are under its control. Many people accept this status quo as the way of the world. What else have they known? Others, especially those with an understanding of history, know that the situation is not politically or morally inevitable. For a long time, however, dissenters saw no viable path around the centralization of finance.

Enter crypto. It is a pure expression of methodological individualism and spontaneous order. It what ways? The ways include:

- It is decentralization writ large. The central engineering of money and its flow is embodied by legal tender laws, inflating fiat, central banking, financial licensing laws, reporting requirements, and the other economic monopolies that are artificially created by the state. As long as individuals must play by the state’s rules, especially the use of fiat and banks, there is no financial freedom. In what seemed like an instant, but which really took years, Satoshi (and his crypto antecedents) decentralized both money and its means of transmission. The abstractions of state and central banking have been replaced by the reality of individuals acting in their own self-interest.

- It is conscious decentralization. The purpose of bitcoin and the blockchain is to bypass the need for a trusted third party, specifically central banking and the state. The first line of “Bitcoin: A Peer-to-Peer Electronic Cash System” reads, “A purely peer-to-peer version of electronic cash would allow online

payments to be sent directly from one party to another without going through a financial institution." In doing so, crypto bypasses the institutions used by the ruling elite to steal wealth.

- Money is given value by individuals. The constructivists believe money is a social construct that is given meaning and worth by government in much the same manner as human beings are said to be given humanity through socialization. Satoshi flips the script. Government money is a fraud. The individuals who construct and use crypto infuse it with value whenever they prefer it as a means of exchange and for the other uses of money. Individuals not only create wealth but also define its worth.

- Crypto is profoundly individualistic. This is true not merely of how it functions but also of its structure. It functions through the unintentional cooperation of self-interested individuals, such as miners. The blockchain's structure cannot be centralized or nationalized; it is decentralization exemplified. Vladimir Putin famously said "neither Russia, nor any other country can have their own crypto, 'by definition'. If we talk about cryptocurrency—this is something that goes beyond national borders." Crypto on a blockchain comes as close as possible to a currency that the state cannot control or centralize. Some argue that crypto is already collectivist because it depends on a cooperative network of miners, nodes, developers, and administrators; some claim the network itself constitutes a trusted third party. It does not. The network is a model of how a trustless system operates. The accusation mistakes cooperation for collectivism, and consensus for central planning.

- Crypto expresses the same sort of worldwide spontaneous order as "I, Pencil." Around the globe, strangers unintentionally cooperate with each to mutual benefit. Their subjective and self-interested evaluations strengthen some types of crypto and devalue others to create an exchange rate for each one. Crypto has thrived precisely because an immense number of strangers control nodes, do transfers, innovate, write code, and cooperate. Each act is done for selfish reasons, but it results in profit for others.

- Crypto can look like chaos, but it expresses a natural order. The order of centralization resembles a military parade or the obedient single-file lines at airport screening. Spontaneous order resembles a busy freeway where cars change lanes constantly, getting on and off at will. What appears to be chaos is a sophisticated form of organization in which strangers voluntarily participate. The chaotic-looking freeway takes people to their desired destination day after day.

- Crypto brings order to the monetary realm through a diversity that offers almost infinite choice. Central banks and state-licensed financial institutions enforce uniformity because they need customers to conform to government regulations and reporting requirements. The imposed uniformity and centralized order do not reflect the preferences of individuals; they reflect

the preferences of the state. The crypto community eschews uniformity because crypto serves individuals whose preferences are incredible diverse. Only when "uniformity" is used as a synonym for "order" does crypto become *dis*orderly. Otherwise, crypto mirrors the same sort of order as the trading floor at a stock exchange.

- Government is irrelevant and a hindrance to crypto. Centralization requires the state or its equivalent because uniformity is unnatural and must be enforced. Decentralization does not requires a state because there is no forced conformity of action or preference. All choices are made by the individuals involved.

- Crypto is the "invisible hand" of currency. The term describes the unintended social and economic benefits of actions taken by self-interested individuals. By pursuing their own financial interests, crypto users do far more to create sound currency and financial practices than monetary reformers who agitate for change within the status quo without questioning its fundamentals.

Crypto is a pure expression of Austrian economics.

The Unacknowledged Revolutionary Aspects of Crypto

Crypto resembles the "lone gunman theory." Although the term is usually associated with the assassination of President John Kennedy and the subsequent Warren Commission, its application can be expanded. History stumbles along a fairly steady path, albeit not always a salutary one, which is largely planned by government. Then a lone gunman jumps out of the bushes and shoots Archduke Franz Ferdinand of Austria, President McKinley, or JFK. Society reels. In the case of Ferdinand, the assassination sparked WWI. History changes forever, and the change cannot be undone.

The state control of the financial world chugged along splendidly throughout the 20th century—or wretchedly, depending on your perspective. A net of global control was thrown over the finances of individuals through measures like the Foreign Account Tax Compliance Act (FATCA) which tried to ensure that freedom-seeking individuals had nowhere to go with their money. Then crypto jumps out of the bushes and assassinates the banking system. Economic history changes forever, and the change cannot be undone.

The effect of crypto on statist financial institutions is well known. But the effects on social policy are less discussed. Predictably, the blast of freedom that shook up the central banking system also impacted other institutions and policies of the state. To touch upon a few, in passing:

Foreign Policy. Food is frequently used as a weapon of foreign policy. An article in the *Free Thought Project* describes how the blockchain neutralizes the weaponization of food: "Revolutionary Blockchain Tech is Helping Disaster Victims

& Feeding the Hungry Without Government." "As governments and bankers claim cryptocurrencies and the blockchain are tools of criminals, millions of dollars in aid —generated by these technologies—are helping the less fortunate all over the world." The gist of the article is that crypto allows needy nations and individuals to skirt economic sanctions imposed upon them by more powerful nations. It has become more difficult to starve people for political advantage.

Domestic Policy. When Venezuela's government devalued the Bolivar by removing three zeros from the currency, citizens flocked to the free-market alternative of bitcoin, with which they were already familiar. "In advanced economies, crypto assets like bitcoin have so far had little purpose apart from speculation and gambling. In countries where the monetary system and financial structures are crumbing, bitcoin may provide an alternative store of value relative to the local currency." Crypto rescues businesses; it saves lives.

The Social Control of 'Vice'. "Operation Chokepoint" was an Obama-era banking policy that attacked allegedly undesirable but legal businesses such as the selling of medical marijuana, sex, and guns. The banking system closed accounts, canceled credit cards, and refused all services to "miscreant" customers. The practice is being revived today. Again, banks are targeting marijuana outlets, sex workers, and gun businesses whether or not these customers are conducting a legal business. Increasingly, sellers of frowned-upon goods and services have turned to crypto to sustain their livelihoods.

Protection of Free Speech. After circulating documents that embarrassed governments, Wikileaks faced a banking blockade that killed off the donations that were its life-blood. Wikileaks opened donations via bitcoin, and wealth poured in once more. Censorship was sidestepped. The same is true of the porn industry, which is a target of Operation Chokepoint.

The Free Flow of Information. Intellectual property prosecutions are usually based on following the money and uncovering the individuals at the other end. Since crypto can be close to anonymous, that strategy is gutted. A bitcoin.com article entitled "EU Intellectual Property [IP] Office: Bitcoin Hinders Anti-Piracy Efforts" explains, "Bitcoin's inherent threat, according to the report, is that transactions can't be easily tied to an individual in the real world. This problem is a bad one for the EUIPO since copyright enforcement is usually based on the strategy of following the money." This benefits the global flow of information.

Immigration Policy. Immigration and temporary migration are often motivated by a desire to send money back home. But migrants are also often "unbanked" by financial institutions that require documentation. Or they have to pay huge fees to send money through a private business, with their families waiting days for the transfers. President Trump has threatened to cut off this incentive for migration by closing down more channels of transmission. Fast, cheap transfers of crypto are incredibly difficult to control.

The Strangle-Hold of Lawyers and Courts. Smart contracts are legally binding agreements that use software to self-execute the terms of the agreement. Peer-to-peer smart contracts may someday become ubiquitous, from real estate deals to insurance claims which will dramatically reduce the need for lawyers.

The Autonomy of the Family. Inheritance taxes are heinous because they are double taxation; a person whose wealth has already been taxed is relooted by government when he dies and passes an estate on to his family. Crypto can invisibly divide assets among loved ones.

The foregoing is a small sampling of the revolutionary impact of crypto use. The institutions that serve a free-market function are being slowly returned to the control and service of individuals. The institutions that serve the state are fast being ignored.

Crypto is the money of society, not of the state. Its evolution offers a rare glimpse into how essential institutions can arise in a free market with no assistance from government. Free-market crypto is methodological individualism and spontaneous order writ large in an essential area of life.

Decentralization as Disobedience

Decentralization as a freedom strategy means individuals seek empowerment by seceding from the state and reclaiming their autonomy as individuals. One way to secede is to disobey the law. Most people disobey the law in trivial and peaceful ways every day of their lives. They ignore speed limits, build an unauthorized addition to their house, cross against red lights, fib on government forms, get paid under the table, burn rubbish in their backyard, jaywalk, decline census questions, walk an unleashed or unlicensed dog, and text while driving. These minor offenses carry little risk beyond a fine, but they show that people think nothing of disobeying laws that make no sense or which unreasonably inconvenience them.

Then there are those who disobey the law in a more serious manner. They evade taxes, establish unlicensed businesses, use illegal drugs, lie to the police, trade sex for money, or smuggle. These offenses carry a possible jail sentence, but people's willingness to disobey shows that a significant portion of the population hold victimless-crime laws in such contempt that they will not comply, even at considerable risk to their well-being.

In the '80s, a popular strategy by which individuals completely decentralized their lives became known as "Browning-out" because practitioners used Harry Browne's best-selling book *How I Found Freedom in an Unfree World: A Handbook for Personal Freedom* as a blueprint. Browne defines freedom as living life as you wish to live it while allowing others to do the same. Instead of protesting the state or seeking distant reform through organizations like the Republicans or Democrats, Browne claims people can enjoy a high degree of freedom here and now. Chapter 7 of his book, entitled "The Government Traps," states, "But who is 'society' if not the same people who are already expressing their needs and

preferences in the marketplace? If they aren't willing to pay for the service in the free market…who can say they're willing to pay for it through government?…All government actions depend upon one-sided transactions, in which an individual is forced to choose between paying for what he doesn't want and going to jail." Those who Browned-out from the Government Trap decentralized the power in their lives down to the personal level where they were the only authority over their own choices.

Dropping out of society comes at a steep cost, however. It is not merely that the state tries to make examples of dissidents. It is also that society is an amazing benefit to mankind. It facilitates "goods" such as knowledge, prosperity, culture, progress, and emotional self-fulfillment in a manner impossible to human beings in isolation. Retreating becomes preferable only when a society is so totalitarian that it constitutes a danger or torment to life itself. That's the point at which American slaves risked their lives to flee North, with hounds and armed men on their heels. That's the point at which desperate people climbed a barbed-wired wall in East Berlin, despite guns trained on their backs. Desperate people try to escape a savagery that passes itself off as social order, and they risked their lives to do so.

The lesson: Society is of value to individuals only to the extent that they have the ability to say "no." Nothing is an unconditional "good"; even the food with which life is sustained is not an unconditional good. Ask people who wish to commit suicide or a protesting prisoner who must be force fed. What is good or bad depends on circumstances that must be evaluated by the individual himself. The value of society depends upon the decentralization of power down to the individuals who comprise it so that they can always say "no."

Crypto provides a new freedom strategy that avoids many of the disadvantages of open disobedience or literally dropping out; it offers a peaceful revolution based on self-interest which bypasses the state rather than confront it. People can say "no" to intolerable aspects of society, such as the monetary monopoly, while physically remaining connected with the rest.

To many, a peaceful revolution sounds like a contradiction in terms. Confusion surrounds the issue of revolution because it has been so badly portrayed in political science and badly acted out in reality. Barricaded streets, people rampaging, cars on fire, clashes with the military, tear gas, smashed windows of looted stores…that is not revolution. True change comes from the hearts and minds of people when they embrace a new idea, a new vision. True revolution is not rage and despair; it is hope and realization.

John Adams wrote to Thomas Jefferson about the American Revolution. "What do We mean by the Revolution? The War? That was no part of the Revolution. It was only an Effect and Consequence of it. The Revolution was in the Minds of the People, and this was effected, from 1760 to 1775, in the course of fifteen Years before a drop of blood was drawn at Lexington." Adams explained where the American Revolution could be found. "The Records of thirteen [Colonial]

Legislatures, the Pamphlets, Newspapers in all the Colonies ought be consulted, during that Period…" For fifteen years prior to the uprising, speakers and writers had been incessantly educating the public about their natural rights and the common law. That was the true American Revolution.

A social revolution is nothing more than a fundamental change across a society that shifts power from one group or class to another. True revolution occurs only after the intellectual groundwork has been laid to change the hearts and minds of a sufficiently significant portion of the population; some estimate that the portion needs to be no more than 10%. If the intellectual groundwork has not been laid, then the violent eruptions inevitably become coups, with a new group of elites replacing the old group. As long as it is politically led, revolution will devolve to "new boss, same as the old boss." Individuals will not empowered.

A revolution of and for average people means the shift in power is decentralized from the elites down to the individual level. Violence only interferes with this process. It is tempting to speculate what would have happened if the intellectual revolution in the American colonies had not been interrupted by violence. The true revolution referenced by Adams was slowly winning the loyalty of average people, and it might have produced a non-violent overthrow of the British yoke. What would America now look like if it had not been born in blood? Fortunately, its true birth was in newsprint, which may account for why it ended better than the French Revolution.

The quiet explosion caused by Satoshi in 2008 was "a revolution" because it overturned the reality of statist financial control and decentralized power downward from the government to the average person. Those who call Bitcoin revolutionary, however, are dismissed as being hyperbolic because the crypto eruption does not conform to the images of barricaded streets and people screaming "Pig of a Government!" The pioneers of crypto do not resemble gun-toting jungle-slogging revolutionaries in the mold of Che Guevara. Satoshi himself remains anonymous, and this is unheard of for a revolutionary leader. But Bitcoin breaks with convention in many ways. It was an unassuming, unpretentious revolution in which no blood was shed. The area of life it threw into turmoil was finance—also known as "filthy lucre"—and **that** is rarely considered to be a noble cause that deserves a revolution. Shouldn't a self-respecting banner read "FREEDOM, JUSTICE" instead of "PRIVATE MONEY"

It does because financial independence *is* freedom and justice. The ability of people to make and keep the wealth they earn is how they feed their children and pursue dreams; it is how they rise from starvation to well-being; wealth allows people to own the land they walk on; filthy lucre turns an assembly of strangers into a civil society that trades with each other rather than makes war. Money is the engine of civilization itself because freedom of speech, art, literature, and the other amazing human accomplishments only follow in the wake of people being able to feed themselves.

The Satoshi revolution is one of rising expectations, which became possible through the decentralization of economic control that crypto forged. It is a revolution of average people who now have a viable alternative to oppressive fiat and central banks.

“The revolution of rising expectations” refers to a situation in which even a slight increase in prosperity and freedom leads average people to believe they can improve their lives through their own efforts. This belief makes them demand political and economic changes that bring more freedom and more prosperity. The average person is not a freedom fighter, and their demand for change doesn’t hinge on ideology. It hinges on self-interest. They want a better life for themselves and for their children. For *that*, they are willing to fight, especially in a nonviolent manner.

The phrase “revolution of rising expectations” emerged after World War II had destabilized the power structure of the world. Former colonies from the Far East to Latin America and Africa threw off imperialism and despotism because average people glimpsed the possibility of finally achieving more freedom and prosperity.

The advent of crypto has destabilized the financial power structure of the world, and it is causing another second revolution of rising expectations. It does not occur on the national level—crypto recognizes no borders—but within the lives of individuals, who can finally control their own finances in privacy and without permission. This has deep political implications, of course, because independent people are far less likely to obey.

Every successful revolution must answer, “What is the end point?” If there is no good answer, then a bad system will be replaced by another bad system that rushes into the void. The French Revolution overturned a corrupt monarchy only to see it replaced by a “Committee of Public Safety” that instituted what is called the “Reign of Terror.” The Satoshi revolution must answer, “What is the end point?” Gandhi said, “the means are the ends in progress.” Decentralization is the means. Decentralization is the end in progress: the total empowerment of individuals.

Anarchism, the End Point of Decentralization

> Man is born free, but everywhere he is in chains.—Jean Jacques Rousseau

So much confusion and slander surrounds the term “anarchism” that it is useful to introduce the concept through an explanation of what it is not.

- Anarchism is not violence. Most traditions are explicitly peaceful. The nonviolent anarchism of Henry David Thoreau and Mahatma Gandhi are examples.
- Anarchism is not chaos. It means “without the state,” not without order.
- Anarchism is not pacifism. A few forms, like the Christian-anarchism promoted by Leo Tolstoy, hold pacifism as a central tenet, but most traditions fully recognize the right to use force in self-defense.

- Anarchism is not inherently left wing. Left-wing anarchism has received the bulk of historical attention, but the first American anarchist was the libertarian Josiah Warren (1798–1874).
- Anarchism is not an impractical ideal. It is a realistic approach to living within society without sacrificing individuality.

If that's what anarchism is not, then what *is* it? Simply stated, anarchism means "without the state."

What is the state? It is the institution that claims jurisdiction over a given territory and a monopoly on the use of force. The state is institutionalized force that requires obedience from the people living within this territory. Anarchism looks at the state and does not see services for which people pay in taxes. What passes for services are monopoles sustained by theft and force.

One of the easiest ways to grasp how anarchism functions is to realize that it is how most people conduct their daily lives. They live without the state without realizing it. Anarchism is how they function with family, friends, business associates, and even strangers. When a person wakes up in the morning, no law forces him to feed his children breakfast rather than starve them or to kiss his partner "hello" rather than beat her. When he carpools with associates to work, there is no policeman present to prevent him from picking their pockets or punching them in the nose. As he moves through the day, no bureaucrat hovers nearby to make sure he pays for a cup of coffee or contributes in his fair share of the lunch tab. As the man walks down the street, he doesn't attack random strangers or pull a woman into the alley to molest. When a stranger begins to step off the curb into oncoming traffic, he reaches out a quick hand to restrain the person.

It is not government that makes people act with habitual decency. It is civil society, family, and the bonds of humanity that does so. Civil society is naturally peaceful because it consists of voluntary exchanges rather than coerced ones. It is from civil society that men acquire the habits and rewards of cooperation. Otherwise stated, most individuals already deal with each other in their daily lives as though they all live under anarchy.

It is the state and other criminals that introduce force into daily life. The state arrives in the form of monopoly law enforced at the point of a gun. The state tells a person, "you cannot open a business because it would compete with us or with a state-favored corporation". It says "your property is not yours to use but ours to administer, tax, and confiscate if you refuse to obey." The state steals a person's earnings to support its own ventures, even ones that repulse him, such as war; it declares, "your money is ours to spend as **we** choose, and your conscience does not matter." The state requires obedience to a myriad of nanny laws that trivialize an individual's alleged right to choose, down to what type of straw he can use to drink a soda. The state claims, "you are mine to command."

By contrast, anarchists tell peaceful people: "open any business you wish"; "your

property is yours”; “your money and soul are your own”; and “the state has no authority over you.”

If the foregoing does not sound like the anarchism that is usually discussed, it is because there are different traditions of anarchism, and the loudest, most violent ones receive the most attention. The various forms of anarchism include individualist-anarchism, communist-anarchism, socialist-anarchism, mutualist-anarchism, Christian-anarchism, anarcho-syndicalism, and anarcho-capitalism. What unites them all? What separates them?

Traditions within anarchism agree that the state is an institution of organized force and undesirable; that's what unites the hyphenated anarchisms—a rejection of the state as institutionalized violence. Where they disagree, however is on what constitutes violence and how a society without it would function.

Contrast the approaches of communist- and individualist-anarchisms.

Communism views laissez-faire capitalism as a form of theft which is a form of violence. One reason is “surplus value.” Popularized by Karl Marx, this concept refers to the value allegedly created by workers that is in excess of the costs of their labor and of production. Simplistically stated: A factory worker earns $1 an hour and uses raw material that costs $1 to produce a good that sells for $10. According to Marx, a surplus value of $8 has been created by the worker who is the rightful owner of this amount. The surplus value is pocketed by the capitalist factory owner in an act of theft. The capitalist is able to steal the $8 because he owns the means of production which is protected by the muscle of the state. Thus capitalism is irrevocably entangled with the exploitation of workers and the violation of their rights. To leftists, anarchism is necessarily both anti-statist and anti-capitalist because both are forms of violence.

Individualist-anarchism challenges this interpretation. It looks at the same factory worker and owner, and it sees a consensual relationship by which the worker is paid a wage to which both have agreed and from which both benefit. The so-called surplus value or profit that the capitalist receives is in exchange for the risks of doing business, overhead, a continuing investment of capital, marketing, and his own time. No force or fraud is present. As long as the state does not promote the capitalist's profit by doing anything other than enforcing property rights—for example, it does not grant him a monopoly—then no force or fraud is present due to the state either. The factory expresses only the free market and voluntary exchange.

If the state does intervene by passing laws that favor or harm the business, then the arrangement ceases to be free market or laissez-faire capitalism and becomes crony capitalism; this is an arrangement in which the state and some businesses align to their mutual advantage and to the disadvantage of everyone else. The ones who suffer most are workers, competing businesses- and consumers. To individualist-anarchists, anarchism is anti-state and anti-state cronies. It is pro-free market and capitalistic.

The profound disagreement over the free market has implications for key concepts used by both forms of anarchism. For example, communist- and individualist-anarchism define “class” and class affiliation in dramatically different ways. Communist-anarchism defines a person's class affiliation by reference to his relationship to the means of production. He is either a worker or a capitalist; he is either exploited or an exploiter. The two classes are locked in irresolvable class warfare.

By contrast, individualist-anarchism defines class affiliation with reference to a person's relationship to state power; he either cooperates with others on a voluntary basis (society) or he uses force (the state). He is a productive member of society or he is a criminal. Individualist-anarchists view the two classes—society and the state – to be locked in irresolvable class warfare.

In summary: Although all forms of anarchism reject the state as organized violence, some forms of anarchism profoundly disagree on what constitutes violence.

What is Individualist or Libertarian-Anarchism?

> This brings us to Anarchism, which may be described as the doctrine that all the affairs of men should be managed by individuals or voluntary associations, and that the State should be abolished. When Warren and Proudhon, in prosecuting their search for justice to labor, came face to face with the obstacle of class monopolies, they saw that these monopolies rested upon Authority, and concluded that the thing to be done was, not to strengthen this Authority and thus make monopoly universal, but to utterly uproot Authority and give full sway to the opposite principle, Liberty, by making competition, the antithesis of monopoly, universal.— Benjamin R. Tucker

Those who call themselves individualist- or libertarian-anarchists do not agree on all aspects of theory. After all, they are anarchists. The foregoing is the dominant view, however.

Individualist-anarchism is usually based on Natural Law from which natural or individual rights arise. The word “Law” is not used in a legal or legislative sense. It refers to a principle or a governing rule, such as the laws of physics. “Natural” means the law is based upon the facts of reality and upon man's nature. In its simplest form, the version of Natural Law used by individualist-anarchism is an attempt to ground human values in the facts of reality and of human nature.

Otherwise stated: Given what we know about reality and about human nature, is it possible to reason out rules of behavior that maximize the well-being of human beings? Individualist-anarchism answers “yes!,” and it turns to the concept of natural or individual rights. It asks, “who owns the individual?” As previously discussed, there are only three possible answers: the individual does (personal

freedom), someone or something else does (slavery), or he is unclaimed property. Individualist-anarchism argues strongly in favor of the first position.

A person's claim to his own body is described with different terms, including “sovereignty of the individual,” “self-ownership,” “autonomy,” “self-proprietorship,” and “individual rights.” But to claim his birthright of freedom, every man must respect the equal freedom of others. If he initiates force, then his actions constitute a statement that he does not consider freedom to be his birthright or any right at all. Rights are either universal—they exist to the same degree within each human being—or they are not based on human nature at all. It is this duty to respect the rights of others that an individual carries with him into society.

Rights and duties are the tools by which society resolves conflict and avoids violence. The 19th-century individualist Benjamin R. Tucker uses this approach while speculating about the nature of property. Tucker believes ideas arose only because they serve a need or answer a question. To illustrate his point, Tucker asks readers to imagine a universe that is parallel to our own but which runs along different rules. The inhabitants could satisfy their needs simply by wishing for goods. Food magically appears in their hands, clothes miraculously drapes their limbs, and a bed pops into existence under their tired bodies. It is unlikely that this parallel society will come up with the concept of private property. Why?

Tucker asks, “What is it about the reality of our own world and the nature of man that gives rise to the concept of property in the first place?” He concludes that the idea of property arises as a way to resolve conflicts caused by scarcity. In the real universe almost all goods are scarce, and this leads to competition for their use. Since the same chair cannot be used in the same manner at the same time by two individuals, it is necessary to determine who should use the chair. The concept of property resolves that social problem. The owner of the chair should determine its use. “If it were possible,” writes Tucker, “and if it had always been possible, for an unlimited number of individuals to use to an unlimited extent and in an unlimited number of places the same concrete thing at the same time, there would never have been any such thing as the institution of property.”

However rights, duties, and property are derived—from natural law or utilitarianism—they are the context that individuals bring with them when they enter society.

A Nod to Henry David Thoreau

Few philosophers have worn self-empowerment as gracefully as the 19th-century American Henry David Thoreau. He had good reason to ask himself, “How does an individual deal with morally intrusive government?” His solution is simple; throw government out of your life and never look back. That’s what Thoreau did in real life.

Thoreau's most famous political tract is *Civil Disobedience.* It was his response to a 1846 overnight imprisonment for refusing to pay a tax that violated his conscience. A famous and perhaps anecdotal exchange occurred while he was imprisoned. Ralph Waldo Emerson visited and urged him to pay a fine so he would be released.

Emerson asks, "Henry, what are you doing in there?"
Thoreau replies, "Waldo, the question is what are you doing out there?"

Thoreau was not embittered by his brief imprisonment. Near the end of his life, he was asked, "Have you made your peace with God?" He answered, "I have never quarreled with him." For Thoreau that would have been the real cost of paying the tax; it would have meant quarreling with his own conscience, which was akin to quarreling with God.

Civil Disobedience ends on a happy note. After Thoreau's release from jail, the children of his hometown pleaded with him to join a hunt for huckleberries. Huckleberrying was one of Thoreau's valued pastimes, and his skill at locating fruit-laden bushes made him a favorite with children. He ends his chronicle of imprisonment with the words, "I joined a huckleberry party, who were impatient to put themselves under my conduct; and in half an hour…was in the midst of a huckleberry field, on one of our highest hills, two miles off, and then the State was nowhere to be seen."

The State was nowhere to be seen. This is the legacy of Thoreau and Satoshi for those who wish to grasp it: for those who are willing to cast it off and not look back, the State will be nowhere to be seen. Thoreau, in his joy of running with all the other children, knew his imprisonment was not his reality. Huckleberry hunting was his reality.

What is left when there is no state? Individuals and society.

SECTION FOUR: STATE AND SOCIETY

CHAPTER NINE: Relevance of State, Society, and Obedience to Crypto

> The wall separating state and society is crumbling. Or, rather, the state is taking a jackhammer to it in an aggressive attempt to control every aspect of productive and cooperative life…The people you deal with on a daily basis are ceasing to be good neighbors, honest merchants, and disinterested strangers. They are becoming state informants who monitor your expression, your money, your behavior and attitude in order to report you to the authorities. They are ceasing to be "society" and becoming instead "the state."—Murray Rothbard, "Society without a State"

Classical liberalism draws a sharp distinction between the state and society, which cryptocurrency adopts. Crypto was not designed to mimic state-issued currency or

state-controlled monetary systems. Its structure and function was created to empower the individual through providing a state-free means of achieving financial independence. Its ends and its means are as uniquely compatible with society as they are antagonistic to the state.

The concepts and realities of state, society, and obedience are the context in which Bitcoin was born and in which crypto now operates. To understand crypto's past, present, and future, it is necessary to understand these concepts.

The Structure of State, Society, and Crypto

> The problem of the Means is, as I see it, a twofold problem: first, the problem of End and Means; second, the problem of the People and the State, that is, the means by which the people can supervise or control the State.…Means must be proportioned and appropriate to the end, since they are ways to the end, so to speak, the end itself in its very process of coming to existence. So that applying intrinsically evil means to attain an intrinsically good end is simple nonsense and a failure.—Jacques Maritain, *Man and the State*

A simple method by which to understand the difference between the state and society is to analyze their means and ends.

The end of a state is to regulate society in order to maintain its existence and enforce its privileges. Its primary privilege is a monopoly on the exercise of violence over the people and property within a defined territory. The state uses force in the form of law or the threat of law to impose its policies. Behind every law is a gun with the possibility of violence erupting if the law is not obeyed. The state prefers to elicit compliance, however, rather than to punish anyone because punishment is a clumsy process that could inspire resistance. The state prioritizes the acquisition of wealth because it produces nothing and has no revenue except what is derived from others through threats or violence. Otherwise phrased, those in power use a monopoly of force as the means to create and sustain the goal of privilege.

Society is the voluntary interaction of individuals along with the institutions that evolve from the associations. An institution is a custom, behavioral pattern, or relationship within the dynamic of a society; marriage, a church, or the family are illustrations. Money is a vital institutions to both the state and society.

The goal of society—if a highly decentralized network can be said to have a conscious purpose—is to be a venue in which individuals can exchange for mutual benefit, whether this benefit is defined in economic, spiritual, or other terms. Society is voluntary, with legal obligations arising only from consent and contract. This is the social means: free association. The end or goal of society is expressed by each member who acts in his own self-interest. Because individuals are diverse and unpredictable, the form of society is fluid and unpredictable, except for being nonviolent.

“Form follows function” means the basic shape of anything is determined by its purpose. The form of a chair is dictated by its function as a structure upon which people sit, which is why a successful chair has a stable surface. For the architect Frank Lloyd Wright, the form and function of a thing had to be inseparable if its synthesis was to be successful. “Form follows function—that has been misunderstood,” Wright observes. “Form and function should be one, joined in a spiritual union.” If the two are in conflict, then the form either fails or the function is revealed to be different than what has been stated. If keeping the peace involves killing innocent people, for example, then it means peace keeping is not the end being expressed. During the Vietnam War, a U.S. army official justified bombing civilian areas in the Bến Tre province of the Mekong Delta with the statement, “It became necessary to destroy the town to save it.” This explanation morphed into the infamous saying, “We had to destroy the village in order to save it.” A jarringly discordant form and function often reveals a hidden, true function.

Mahatma Gandhi famously expressed the connection between form and function in social dynamics. “If one takes care of the means,” he writes, “the end will take care of itself.” This reflected the reality of the means being the ends in progress. Gandhi does not devalue the importance of the end in sight, but he recognizes that every stage of the means must express the end in a logical progression if the end is ever to materialize.

Most people concentrate on goals, like prosperity, and then figure out how to achieve them. Strategies are viewed as pragmatic and almost interchangeable: whatever works or provides a shortcut. But cruelty cannot lead to loving relationships; only benevolence can. Theft does not create respect for property rights; only honesty does. If the goal of crypto is to financially free individuals, then the means of accomplishing it is inseparable from this end. The means are a respect for individual rights, free markets, peace, and society. The opposite strategies are collectivism, monopolies, and violence, with the state being a predictable result.

“There oughta be a law” is a common knee-jerk solution to achieving almost any social goal these days; people clamor to use the institutionalized violence of the state to enact laws that punish or incentivize others into accepting a desired end that they would not accept willingly. The goal can be comparatively modest like imposing a dress code by which men and not women go topless. Or it can be a sweeping one like the imposition of a particular religious doctrine. The reflexive reaction of “there oughta be a law” bypasses the question of whether the means and ends are in conflict. Few people ask if it is even possible for the law to impose ideas and attitudes, thoughts and feelings; it is not. The most that is possible is for the law to intimidate people into outwardly expressing “correct” thoughts and feelings despite what they think and feel inside.

Because such laws intrude upon an individual’s freedom of conscience and speech, a free society does not impose them; as a means, such laws contradict society’s ends. Because they give the state immense power over its population,

however, such laws are standard practice for those in power; as a means, they achieve the desired ends. The vaguer the statement of a goal is—"income equality" or "social justice"—the more power it confers on the state because the definition is elastic. With free-market crypto, the end is well defined: a decentralized and private transfer of funds or other information on a peer-to-peer network. With fiat and banking, the end is subjective and open to redefinition: monetary stability.

Everyone knows that some goals demand specific means. Staying healthy requires eating well, exercising and adopting good habits. The proper means become less obvious when the end is complex, amorphous, or not candidly expressed. Somehow the logical connection between the two gets lost. "The ends justify the means" has become an excuse to abandon both practical and moral considerations about how to achieve specific goals. Once an end is established, a menu of means is scrutinized for ones that are supposed to achieve the goal as quickly and cost-efficiently as possible. More fundamental questions about the relationship between means and ends are rarely asked. Can war actually bring peace? Can censorship create an open society? Does banning crypto protect financial safety?

When the ends and means conflict, then the end becomes a practical impossibility. A person who declares "the ends justify the means" is either badly misguided about how goals are achieved, or he has an entirely different goal in mind than what is stated. The use of a means that is hostile to achieving an end introduces an Orwellian element. The double-think intrinsic in the World War I slogan "A War to End All Wars" is obvious. The means obviously failed to achieve the stated goal because the elimination of conflict was never the real goal; territory, power, and profit were the purpose of World War I. The false goal was accepted, however, and it is still trumpeted even though it makes no sense. No one speaks of "A Truth to End All Truths," "A Point of Logic to End all Logic," or "A Virtue to End all Virtues" because these are self-contradictory absurdities. The way to end war is not to wage it but to refuse engagement. The means—fighting a war—is diametrically opposed to the stated end—preventing more war. When this occurs, it is time to look under the surface for the actual intent.

This reveals a profound ideological difference between advocates of the state and advocates of society or the free market. Statists are ends-oriented; advocates of civil society are means-oriented. This does not suggest that civil society—that is, the individuals within it—do not have or state specific goals. It says that society realizes the proper means to achieve any end must be employed. By contrast, statists focus entirely on the end and use any and all means necessary or expedient.

Statists provide a detailed blueprint for what constitutes a just society, for example. An declared end of this society might be a socio-economic equality that requires the state to monopolize all monetary matters, including commerce, to ensure the proper distribution of wealth and opportunity. The end dictates the means. The same is true of a moral society, whatever definition of "morality" is

employed. The end requires the state to monitor the behavior, words, and attitudes expressed by every individual. Whenever a specific end is identified as an overriding and independent goal, then the use of force becomes necessary to impose it upon people who peacefully disagree because someone always will.

By contrast, the free-market approach is means-oriented. A just society does not aim at an outcome such as a specific social-economic arrangement. Whatever arrangements result from individuals making free and peaceful choices is considered to be just. Whatever is voluntary is just—or, at least, as close to it as imperfect human beings in an imperfect world can come. For instance, a private college that discriminates against blacks and one that enforces a black-only policy would exist side by side in the marketplace. As long as both are privately funded and no one is forced to participate, both arrangements are just, and the law can not properly interfere. If people consider the school policies to be immoral, then they are free to use a wide variety of peaceful means to agitate for change. These strategies include education, protest, picketing, boycott, and moral suasion. What they cannot do is use force to dictate the way in which the colleges use their own money to establish their own policies. Freedom of association requires the right to discriminate.

Statists are not similarly restricted. Their first choice in seeking to “reform” a peaceful but immoral practice is to apply the institutional force of law.

The 20th-century French philosopher Jacques Maritain considered the “Means Versus End Dilemma” to be *the* problem of political philosophy. The French Revolution provided him with the model of how an end failed miserably because the means used to achieve it were “intrinsically evil.” In a stereotypical revolution, individuals rise up en masse to wrest power from elite and oppressive rulers. The revolutions are called “popular” because they start with a groundswell of popular resistance against the status quo. And it is true; this how many revolutions begin. Then they go horribly wrong. France transformed from an absolute monarchy that ravaged the rights of common people into “a superior person called the Nation State” that ravaged the rights of common people. The promised “Liberté, Égalité, Fraternité” (Liberty, Equality, Brotherhood) never materialized. Instead, blood-thirsty autocrats like Robespierre and Saint-Just, along with a nouveau class of petty bureaucrats, conducted mass arrests and executions that most often targeted average people who violated economic laws—smuggling, for example.

The Bolshevik Revolution is another cautionary tale. The catastrophic death toll and starvation caused by Russia’s involvement in World War I, more than a commitment to Marxism, drove Russians to revolt. The trusted third party called “leaders” had pushed society too far, and they lost all trust. Their collapse left a power void. Under the slogan ”Peace, Land, Bread,” revolutionary officials rushed in to fill this void with a totalitarian and dogmatic regime, rather than the workers’ paradise they had promised. It is the well-worn path of revolutions; meet the new boss, same as the old boss.

They do not achieve the “final aim and most essential task of the body politic or political society,” Maritain explains. The task was to “better the conditions of human life itself” and “to procure the common good of the multitude, in such a manner that each concrete person, not only in a privileged class…may truly reach that measure of independence which is proper to civilized life.” In colloquial terms, Maritain is saying, “you can’t get there from here.”

Why? Because the revolutionary leaders became a new set of trusted third parties. The revolutionaries formed a new upper class who adopted the same basic power structure as before: absolute government that rules through claims of legitimacy, intimidation, and raw force. The faces, ideologies, and declared ends changed but not the means of centralized power that was imposed through institutionalized force. The revolutionaries used the same means as their predecessors and arrived at much the same results: the oppression of average people. Only if by changing the means—only by decentralizing power back to the individual—can a revolution avoid turning into just another state. Only when revolutionary leaders cease to evolve into a trusted third party will a Robespierre, Lenin, Pinochet, Mao, or Castro cease to be inevitable.

The revolution of cryptocurrency resolves the Means Versus Ends Dilemma within political philosophy because crypto is both the means and the end at the same moment. Gandhi also states, “There is no wall of separation between means and end. Means and end are convertible terms in my philosophy of life.” The strategy of crypto: decentralize financial exchanges through a blockchain in order to bypass trusted third parties and return monetary control to the individual. The political end: decentralize financial exchanges in order to bypass trusted third parties and return monetary control to the individual. The means and end are one in the same. The pseudonymous, decentralized, peer-to-peer process is transformative. When the flexing of individual power becomes sufficiently widespread, then it becomes a leaderless revolution—a trustless revolution—which depends on individuals pursuing their own self-interest. The means are “anything that is peaceful.” The end is whatever results from the means.

The State Versus Society

In his classic work, *The State* (1914), the German sociologist Franz Oppenheimer spearheads an analysis of the two most important terms in political discussion: “the state” and “society.” The antithetical terms each express a mode of human organization and each reflect the importance of wealth or productivity to human existence. The natural condition of man is poverty. A baby is born with nothing but its own helplessness, and it will die without the tenacious intervention of a caretaker. Once a person is able to use his labor to transform resources or to create them, then he is able to care for himself through continuous effort. The production of wealth is literally what allows people to sustain their lives. The ability to produce and control wealth is a matter of life or death.

Oppenheimer identifies two antagonistic means by which wealth is controlled: the state and society. He defines the state as “that summation of privileges and

dominating positions which are brought into being by extra-economic power." The words "extra-economic power" mean force or threat of force. The institutions of the state include the military, law enforcement, legislatures, and bureaucracies. Their common denominator is the administration and maintenance of state power through the use of institutionalized violence. "I define the state," Rothbard writes, "as that institution which possesses one or both (almost always both) of the following properties: (1) it acquires its income by the physical coercion known as 'taxation'; and (2) it asserts and usually obtains a coerced monopoly of the provision of defense service (police and courts) over a given territorial area. An institution not possessing either of these properties is not and cannot be, in accordance with my definition, a state."

Oppenheimer defines society as "the totality of concepts of all purely natural relations and institutions between man and man." The words "purely natural" mean "voluntary," with society being the sum total of the peaceful interactions of the individuals within it. The institutions of society include the free market, places of worship, schools, charities, and the arts. Rothbard describes society as a place "where there is no legal possibility for coercive aggression against the person or property of an individual. Anarchists oppose the state because it has its very being in such aggression, namely, the expropriation of private property through taxation, the coercive exclusion of other providers of defense service from its territory, and all of the other depredations and coercions that are built upon these twin foci of invasions of individual rights." The state is called the public sphere; society is the private sphere.

(Note: The state and society are abstractions, and care must be taken not to make something overly concrete of them. The analytic approach of classical liberalism is methodological individualism, which contends that only individuals exist and act. All institutions—including those of both the state and society—can be reduced to the actions of the institution's individual members.)

Wealth can be controlled by either the state or society—that is, by the individual members of either—but it can only be produced by society. The state employs what Oppenheimer refers to as "the political means"—that is, force or threat of force—to acquire the wealth it neither produces nor acquires through voluntary exchange. The wealth is taken from people who do produce and exchange, which Oppenheimer calls "the economic means" of acquiring goods.

The state does not usually take wealth by brute force, however. Instead, the state uses more subtle, less risky methods of theft. For example, it channels the productivity of society into a form of money that it monopolizes by issuing it and imposing legal tender laws. Then the monetary monopoly is cemented by regulating the financial institutions through which the money is forced to flow. This allows the state to conduct subtle theft, like inflation. The direct violence is the monetary monopoly that prohibits and punishes free-market competitors.

Otherwise expressed: The end of the state is to maintain its existence and power. To fulfill this goal, the state needs the wealth and cooperation of society because

it does not produce wealth. The state must steal from society because its only source of “income” is what it grabs through means that include taxation, confiscation, fines, fees, tariffs, inflation, and bribes. Force and threats of force are the necessary means—the political means—of the state.

By contrast, society has no ends. Although it is an engine of creation and exchange, society has no consensus as to what the results of such productivity should be. Each individual member acts to pursue his own perceived self-interest with every person having a unique definition of what comprises this goal. The goal of one person might be to earn a million dollars, while that of another might be to acquire an education. The means by which each individual achieves his end is through creation and trade—the economic means—that produce his own version of wealth. Again, what constitutes riches differs from person to person, and it includes money, culture, knowledge, family, spirituality, and every other possible human value. Society’s means are the opposite of coercion because an exchange occurs only when all parties to a transaction agree to its terms and all parties benefit.

Rothbard highlights the key difference between interacting with society and with the state.

> If I cease or refrain from purchasing Wheaties on the market, the Wheaties producers do not come after me with a gun or the threat of imprisonment to force me to purchase; if I fail to join the American Philosophical Association, the association may not force me to join or prevent me from giving up my membership. Only the state can do so; only the state can confiscate my property or put me in jail if I do not pay its tax tribute.

The key difference is consent.

The American individualist Albert Jay Nock was the main conduit of Oppenheimer’s thought into the United States. He captured his mentor’s core sentiment in the book *Our Enemy, The State* in which Nock observes, “Taking the state wherever found, striking into its history at any point, one sees no way to differentiate the activities of its founders, administrators, and beneficiaries from those of a professional criminal class.”

The prospect of “striking into the the state’s history” has appealed to many political theorists because it bears directly on the nature of the state and whether it is legitimate. In turn, this addresses the question of why people obey the state. Many people appear to consent to the state’s presence, all the while grumbling about how corrupt the system is and double standards in the law. Even those who consider most laws to be unjust seem to comply without being explicitly forced to do so. Why?

Examining the roots of the state is the starting point of an answer. In general, there are four basic and sometimes overlapping theories of how a state

originates. Each theory carries different implications for the state's relationship to society and the legitimacy it claims.

The first theory is supernatural. It contends that the state exists through the will of God or some equivalent. This is the divine right of kings or rulers, and the theory often results in a theocracy. Lesser members of society—who presumably are also placed in their positions by God—owe allegiance to the anointed leaders as part of their duty to God. An established church sometimes acts as an arm of the state with religious leaders bolstering the ruler's divine legitimacy.

The second theory of how a state originates draws on a more naturalistic explanation. The state is a spontaneous institution that arises from the act of community, it is argued. The person and property of individuals require protection, and their contracts require an enforcement mechanism. This makes an overriding authority evolve to provide the necessary services by acting as a policeman and an arbiter of disputes. Society pays the state in much the same manner as it pays a contractor for rendering a valued service. According to the consent theory, no hard line distinguishes the state from society because both are engaged in a cooperative venture.

The third and fourth theories entail conflict. The third theory claims the state emerges due to internal warfare within a society. Karl Marx popularized this view by analyzing the state as part of the class warfare through which capitalists control and exploit workers; that is, capitalists use the state—or join with the state—to oppress the workers. For Marx, the state expresses and protects one class of society at the expense of another, and the latter owes no allegiance whatsoever to its oppressors. Indeed, the duty of workers is to resist and rebel.

The fourth theory of the state's origins points to external conflicts in which one tribe conquers another. The victorious tribe forms the upper class within the resulting society, and the conquered tribe pays tribute through obedience and wealth.

Within classical liberalism, the two theories that have struggled for dominance are the consent theory by which the state evolves naturally from the needs of society and the conquest theory by which the state is in constant warfare against the nonprivileged class(es) of society. These are not merely historical suppositions. They are also analytical approaches to whether or not the state can claim legitimacy.

The Consent and Conquest Theories of the State

If the state rules through the consent of society and provides a necessary service, then the argument against revolution—in the form of crypto or in the name of anything else—is weakened considerably. The monetary system is likely to be seen as being in need of considerable reform rather than in need of elimination.

In the consent theory of the state, the 17th-century English philosopher John Locke looms large through his *Two Treatises of Government*. The contemporary American philosopher Karen Vaughn observes of his *Second Treatise*, “Locke argues the case of individual natural rights, limited government depending on the consent of the governed, separation of powers within government, and most radically, the right of people within society to depose rulers who fail to uphold their end of the social contract.” Locke’s work, upon which both the French and American revolutions drew, remains a touchstone of consent theory for limited government within classical liberalism.

Locke believes God had given the world to all men in common, and he justifies private property—the appropriation of a common good for personal use—by arguing that each man has an ownership claim to his own person. Based on self-ownership, Locke argues, “The labour of his body, and the work of his hands, we may say, are properly his. Whatsoever then he removes out of the state that nature hath provided, and left it in, he hath mixed his labour with, and joyned to it something that is his own, and thereby makes it his property.” So far, this does not seem to suggest that the state, as opposed to individuals, produces wealth or value.

Locke then postulates that the need to protect “life, liberty, and estate” prompts men to form a government. One of main reasons the state arises is as a shield against confusion as to property titles and other conflicts that occur when individuals accumulate and compete for wealth in a world of scarcity. Through an explicit social contract, men give the state the right to adjudicate disputes. For its part, the state pledges to secure men’s claim to property—through inheritance laws, for example. Locke rejects the contention that the consent rendered to the state by initial members of society can bind future generations, however. Instead, he develops a doctrine of tacit consent by which people who did not consent explicitly are still bound to accept the state’s authority. Each person who lives in society and enjoyed its benefits is said to agree to the rules by which a limited state governs.

A withdrawal of tacit consent is possible. A man can relinquish his estate and leave the community. As long as he remains, however, he implicitly accepts the state’s authority. After all, as Locke argues, the “good title” of his property came from the state that facilitated its just transfer. A similar argument can be made about wealth accumulated by virtue of a contract: the contract has validity because of the legal context provided by the state. Only when state ceases to fulfill its part of the social contract is rebellion against its authority justified. Otherwise, the state and society are partners.

The conquest theory of the state stands in sharp contrast to the Lockean model, and it is the theory favored by individualist-anarchists. It attempts to ground the primitive state in historical fact rather than political conjecture. A common expression of the conquest theory runs as follows: Agricultural tribes settle down and become dependent upon specific areas of land. Roving nomads wage war on the more sedentary tribes for the economic benefits that come from pillaging and

looting. The nomads begin by killing and razing, but they discover it is in their long-term economic interest to enslave and exact tribute instead. Why steal for one season when it is possible to steal in perpetuity? This is the simplistic conquest model to explain how the state arose and its relationship to society.

In *Our Enemy*, *The State*, Nock defends the conquest theory of the state on a historical basis. In *For A New Liberty,* Rothbard advances a modified version of the theory. He contends that conquest was the typical genesis of the state, but he concedes that some states may have evolved in a different manner. But even a state that emerged from an explicit social contract, he argues, could not bind new generations through tacit consent because an assignment of natural rights requires an explicit contract. Since no generational renewal of the contract exists, any current state has no legitimacy.

In arguing for the conquest theory, both Nock and Rothbard rely heavily upon Oppenheimer who maintains that the state consists of people who wish to satisfy their "economic impulse" through the political means—through the use of force. Oppenheimer posits six stages through which a conquering group typically passes in order to become a state.

- First, a warlike group raids and plunders a vulnerable community to steal wealth rather than produce it themselves. The Viking raids on the British coast are an example.
- Second, the victimized community ceases to resist actively; sometimes an explicit agreement between the aggressors and the victims is struck. The raiders begin to loot only the surplus, leaving their victims alive and with enough food to ensure the production of future wealth to be plundered repeatedly. Eventually, the two groups acknowledge mutual interests, such as protecting the crops from third-party outsiders.
- Third, the victims offer tribute to the raiders, eliminating the need for any violence at all.
- Fourth, the two groups merge territorially and live together in the same area.
- Fifth, the warlike group assumes the authority to arbitrate disputes, which involves a monopoly over the use of force.

Oppenheimer describes the last stage in which both groups develop the "habit of rule." In his chapter "The Genesis of the State," he explains, "The two groups, separated, to begin with, and then united on one territory, are at first merely laid alongside one another, then are scattered through one another. They intermingle, unite, amalgamate to unity, in customs and habits, in speech and worship. Soon the bonds of relationship unite the upper and the lower strata." The upper strata was called the "master class."

The state, which originated from external conquest, evolves into an agency of internal conquest by which the upper strata of the state uses the political means to benefit economically at the expense of the lower strata of producers. In this view, the state arises and maintains itself as a parasite and an enemy of society.

Whatever path leads to the emergence of a state, however, a question remains. Why do people accept its authority over their lives, their property, and the future of their families?

Voluntary Servitude

Force is usually a last resort that the state introduces when other methods of persuasion, like an appeal to patriotism, do not work. After all, the presence of open force could bring the legitimacy of the state into question. To prevent disobedience or rebellion, the state tries to justify itself in the eyes of society so that it can secure the advantages of violence without incurring its dangers. No analysis of the relationship between the state and society is complete without examining the issue of legitimacy.

A 16th-century essay entitled "Discourse of Voluntary Servitude" by the French jurist Étienne de La Boétie is an early discussion of a haunting question. Why do people obey unjust laws? La Boétie asks, "If a tyrant is one man and his subjects are many, why do they consent to their own enslavement?" Correctly or not, La Boétie does not believe the state rules primarily through force. After all, there are many more people in society than there are agents of the state. If even a small percentage of the populace refuse to obey a law, then the law becomes unenforceable; tyranny is automatically defeated if people withdraw their consent. Yet most people obey without being forced to do so. La Boétie evolves an explanation; he calls it "voluntary servitude."

Discourse first circulated privately in France (circa 1553) against a backdrop of foreign war and domestic conflict. European nation states were on the rise, and monarchs clashed not only with each other but also with their own citizens from whom they demanded vast money and obedience. The 16th century gave birth to the tyranny that led to the French Revolution centuries later.

Born into an affluent and politically connected family, La Boétie escaped the illiteracy, misery, and disease that befell most of his countrymen. Famine was so common in France that men carved crosses on newly baked bread to symbolize the sacredness of food. Plagues erupted repeatedly. As the peasant struggled to survive, state taxes consumed one-third or more of his income, with church tithes absorbing another one-tenth. Roving bands of soldiers stole at will and kidnapped young sons to fill their ranks. France was an absolute monarchy, which meant national power was not distributed but rested with the king and was administered through appointments. To raise money for war and luxury, the king sold titles to the "nouveau riche" that formed a fresh aristocracy with a notorious contempt for the lower classes. Meanwhile, the ranks of lawyers swelled as they administered bureaucracies to feed the appetite of a growing state.

Why did the common man obey a system that treated him so wretchedly and was clearly rigged against him? The monarch was anointed by God and blessed by the dominant Catholic Church, to be sure, but the rise of Protestantism in France—the

Huguenots—meant that a growing segment of society did not recognize the king's divinity. There were also provincial loyalties that competed with national ones. Most Frenchmen gave primary fealty to the province of their birth rather than to the nation or king, and the provinces varied widely in customs, religious practices, and language. These differences divided the nation. As well and with reason, the king feared that foreign powers would align against him with rebellious provinces. A perfect storm between the state and society seemed to be brewing.

Discourse was most likely written while La Boétie was a law student at the University of Orléans, renowned for Huguenot activity. Indeed, one of his professors would be later burned at the stake for heresy. The essay itself was in response to a specific event—the Revolt de Gabelle in Bordeaux. The Gabelle was a much-hated tax on salt, which was not only a human necessity but also a state monopoly. Protesters killed the Gabelle's director general along with two of his officers. In retaliation, 140 commoners were killed, many others were whipped, and exorbitant fines were imposed.

La Boétie was an acute observer of society. When the people finally rebelled, he watched and puzzled over why the state had been able to do almost anything it wanted for so long, no matter how tyrannical. He watched closely as well after the Revolt de Gabelle was quashed. Why did the people not rise up again, he wondered, this time en masse? Why did society tolerate the state? *Discourse* was La Boétie's answer.

In it, La Boétie concludes that the collective obedience of society comes from "a vice for which no term can be found vile enough, which nature herself disavows and our tongues refuse to name." He names it "voluntary servitude." It is a vice because it contradicts human nature; indeed, even brute animals struggle to be free when caught in a trap. Each man is given his own ability to reason, La Boétie argues, and virtue lies in every person's cultivation of his own innate independence. But man's ability to do so required the death of tyranny, which is the antithesis of individual independence. Advocating tyrannicide was not new to European theory but La Boétie takes a different slant. The way to "kill" a tyrant is to destroy his power through nonviolent resistance. In that manner, the people kill not a man but the tyranny itself. Liberty requires only that enough people withdraw their consent and cooperation.

> He who thus domineers over you has only two eyes, only two hands, only one body…; he has indeed nothing more than the power that you confer upon him to destroy you. Where has he acquired enough eyes to spy upon you, if you do not provide them yourselves? How can he have so many arms to beat you with, if he does not borrow them from you? The feet that trample down your cities, where does he get them if they are not your own?

La Boétie addresses the French peasant directly. "You yield your bodies unto hard labor in order that he [the tyrant or the state] may indulge in his delights and wallow in his filthy pleasures; you weaken yourselves in order to make him the stronger and the mightier to hold you in check." Why obey?

La Boétie explores the main ways in which the state engineers consent from society.

The generations that had been born “under the yoke and then nourished and reared in slavery” accept their condition as natural. It is the way of the world. Thus, La Boétie considers *custom* to be the first explanation of voluntary servitude. People believe life has always been this way; life will always be this way; and it takes great effort to introduce a new vision to them.

The French author and theorist Michel de Montaigne, who was La Boétie’s best friend, dramatized the incredible power of tradition in his essay “Of Custom.” It opens with the words:

> He seems to have had a right and true apprehension of the power of custom, who first invented the story of a country-woman who, having accustomed herself to play with and carry a young calf in her arms, and daily continuing to do so as it grew up, obtained this by custom, that, when grown to be a great ox, she was still able to bear it.

But, La Boétie argues, a few people will always try to shake off “the yoke,” perhaps because they “remember their ancestors and their former ways.” Aware of history, they compare the past to the present and dare to long for a better future. “These are the ones who, having good minds of their own, have further trained them by study and learning. Even if liberty had entirely perished from the earth, such men would invent it.”

After the majority become accustomed to automatic obedience, the tyrant’s main challenge is to reduce dissent by silencing the few who try to shake off the yoke. Two basic means of doing so are to control the press and to monopolize education so that people do not compare the past with the present and realize how much more is possible in the future. With strong control of information, the state can inculcate the belief that it acts for the public welfare to uphold the peace, patriotism, and tradition. It can convince people that it embodies the public good. *Brainwashing* is another reason people obey.

The state then reinforces its larger-than-life image through a process of *mystification*: that is, it tries to appear greater than the mere assembly of human beings in its ranks. The rulers align with religion, are crowned by Church officials, conduct pompous ceremonies, swear to protect the nation, appeal to the authority of a founding document, and so forth. State agents are clothed in uniforms; monuments to state power and past leaders are constructed; the rituals of office are conspicuously displayed; and manifestations of state authority, such as courts, are housed in awe-inspiring buildings.

This is yet another reason why people render automatic obedience: *mystification*. After a regulated press and school system convinced them that the ruler’s

authority is legitimate, the mystification of state power leads them one step further. They become awed, intimidated, and even fearful.

Some people will still be difficult to convince, however. Those who will not obey through custom, brainwashing, or awe might well be bought off. And, so, the ruler also engages in largesse. La Boétie points to the state-sponsored distractions that serve as “opiates.” Fascinated by pleasure, the people do not notice their own enslavement. At other times, rulers literally feed the people by distributing stocks of food. “And then everybody shamelessly cries, ‘Long live the King!’” La Boétie remarks scornfully. “The fools did not realize that they were merely recovering a portion of their own property, and that their ruler could not have given them what they were receiving without having first taken it from them.” By providing bread and circuses—state welfare and popular distractions—the people are *bribed* into surrendering their liberty.

The direct bribery pales in significance, however, beside an indirect form that La Boétie calls “the mainspring and the secret of domination, the support and foundation of tyranny.” This is institutionalized bribery by which millions of people are employed at state jobs and receive tax funds with which they pay their bills. These state employees “cling to the tyrant” and offer up their loyalty. Some state employees, such as police officers, become the hands of the state, reaching throughout society to implement laws and policies. Tax-supported intellectuals, such as university professors, become the voices of the state, defending its policies. Still others, working as clerks or minor bureaucrats, make the daily machinery of the state grind on.

Over generations, a vast new class of people emerge from state employees: people who serve the rulers in exchange for a tax-funded salary and other benefits. These state employees willingly destroy their own liberty and that of their neighbors. And they do so without reflection because the force of custom leads them to believe that things have always been this way and always will be.

La Boétie’s solution to voluntary servitude is for people to withdraw their consent and cooperation from the state. La Boétie advises the average man,
“I do not ask that you place hands upon the tyrant to topple him over, but simply that you support him no longer; then you will behold him, like a great Colossus whose pedestal has been pulled away, fall of his own weight and break into pieces.” La Boétie is widely recognized as one of the earliest voices for civil disobedience and nonviolent resistance against authority.

If he is correct, if freedom is a natural human urge, then nature itself argues the logic of not cooperating with tyranny. Something within human beings and even beasts resists the tension of a leash. Rather than break the tension by attacking those who hold the reigns, La Boétie told people to let the tension go slack; let their end of the leash drop. People should refuse either to defend themselves violently or to submit.

They should simply say “No.”

State, Society, Obedience, and Crypto

To repeat: The concepts and realities of state, society, and obedience are the context in which Bitcoin was born and in which crypto now operates. They will also define its future.

The state must take wealth from society to exist. Crypto is not only a new rich source of wealth to plunder, it is also a stiff competitor to the state's most lucrative, current source—the monetary monopoly. The goal of the state is to access the bonanza of crypto *and* to preserve the monetary monopoly. Being entirely ends-oriented, the state will use any and all means at its disposal to achieve this goal. The strategies already on display include:

Propaganda: Crypto is linked to crimes such as terrorism, ransoms, and human trafficking in a manner that makes these crimes seem to be the prevalent uses. The linkage serves at least two purposes. It creates a justification for the state to take action against crypto, and it reduces any backlash the action might occasion from the general public. Instead, the public will cry, "There oughta be a law."

The Use of Force: Since the state itself is institutionalized force, this is its ultimate strategy in situations in which obedience cannot be elicited in other ways. And crypto is irredeemably disobedient. The violence or conquest strategy employed by the state generally accelerates through stages:

- It plunders. The privacy of blockchain transfers and the anti-statist bias of the crypto community make this option problematic. Vulnerable individuals and exchanges are attacked, and their funds are confiscated, but much of crypto remains beyond easy reach.
- It comes to an agreement with compliant crypto users. Centralized exchanges that agree to abide by banking regulations and reporting requirements are licensed and become crony exchanges.
- It protects the crony exchanges from competitors. Individuals who function outside the regulated crypto zones—and especially decentralized exchanges—become targets. Attacking these "external enemies" benefits both the state and the obedient exchanges.
- It attempts to usurp crypto as a new type of fiat. Through financial institutions, the state may mimic the dynamic of crypto in such a manner as to reproduce the monetary monopoly it enjoys with fiat. Digital currency that does not use a blockchain may be offered, for example; this will allow for lucrative inflation and for the state to track every transaction back to a user.

While moving through the stages of using force, the state will engage in active double think that is akin to the slogan "A War To End All Wars." Centralized exchanges will be presented as way to ensure the safety of users's wealth, for example, even though the greatest danger to their wealth is the central banking system that the exchanges mirror.

The propaganda against unregulated crypto will continue because, in the presence of alternatives, the state needs the public to continue accepting the monetary monopoly. Many people will do so through custom. Some will do so because of brainwashing by complicit media that focuses on any wrongdoing by crypto users. Meanwhile, the state will mystify its own activities, assisted by the fact that few people understand the technology of crypto or digital currency. The former—if unregulated—will be diminished as unsafe, criminal, and fake. The latter—under state control—will be elevated as safe, legitimate, and sound.

Crypto that refuses to be regulated will remain the money of society—that is, the money of individuals who interact freely and in their own self-interest to mutual benefit. It will continue to produce wealth. Because crypto is means-oriented, like society, it will evolve toward diverse ends with only the means being predictable: nonviolence and consent. The conflict between private money and fiat will persist because the two of them have fundamentally antagonistic dynamics that threaten each other. One of the main battlefields will be public opinion.

On this battlefield, the greatest challenge crypto faces is to convince enough people to simply say “No.”

CHAPTER TEN: Crypto Class Theory and Free-Market Law

Class theory underlies the free market and crypto: the state versus society. Bitcoin was designed to bypass a central banking system that serves the political class at the expense of the economic one. As an enemy of the state, crypto is an ally of society.

Class Warfare and Crypto

Many people assume that anything to do with banks and finance expresses the class interests of capitalists versus the common man. The opposite is true, but the confusion is understandable. The word “capitalism” is commonly applied to crony capitalism these days—that is, an economic arrangement by which some businesses enjoy a close, mutually beneficial relationship with state officials and receive privileged treatment. A traditional “capitalist” is someone who owns and uses capital goods while remaining in society with no connection to the state; this economic arrangement is sometimes called “laissez-faire capitalism.” It is an expression of the free market and a benefit to the common man because laissez-faire capitalism acts as an engine of prosperity.

Central banking and most financial institutions express crony capitalism. Laissez-faire capitalism expresses the free market. Thus a more specific statement of the class conflict is state and crony capitalism versus society and laissez-faire capitalism. In this conflict, crypto falls cleanly on the side of society. The class allegiance of crypto is evident from the remarkable parallels between its form and function and those of society. The parallels include:

- The individual is the locus of power.
- Both are decentralized down to the level of the individual.
- Voluntaryism is the mode of operation.
- Their purpose is to facilitate exchanges, especially economic ones.
- Exchanges occur only if all involved consent.
- Trusted third parties are unnecessary.
- Privacy is preserved, if the participants wish to do so.
- There is no artificial barrier to entry.
- Neither has a single point of failure at which the entire system is vulnerable.
- Wealth is being constantly created.
- Wealth and status are based on merit, such as hard work.
- Exchanges are not based on ideology or politics.
- Reputations matter.
- The state is the class enemy.

By contrast, the form and function of the state is antithetical to crypto and the free market.

- The state is the locus of power.
- All power is centralized into bureaucracies.
- Coercion is its mode of operation.
- The state's purpose is to maintain its own existence.
- Forced transfers of wealth and power to benefit of the state.
- It is the ultimate third party.
- Privacy is frowned upon and undercut at every turn.
- Barriers to entry are erected, sometimes amounting to prohibitions.
- Those in power are the system's point of failure.
- No wealth is created.
- Wealth and power are based on politics.
- Wealth is accumulated through theft and privilege.
- Reputation is not necessary and less important than status.
- Society is the class enemy.

Another litmus test of whether crypto serves the state or society is rooted in the answers to two questions about money. #1. Who issues it? Fiat is issued either by the state or by an authority controlled by the state, with competition prohibited by law. Crypto is issued by entrepreneurs who compete vigorously with each other for popular acceptance. #2. Can people choose to use the currency or not? The state requires people to accept its fiat as legal tender. Crypto leaves the decision up to individual.

Perhaps the greatest threat to unregulated crypto is the state's drive to change the form and function of crypto so that it no longer expresses and enriches society but expresses and enriches the state. The state wanted to sculpt crypto into its own image through state-issuance, regulation, and other measures so that it

becomes a type of fiat crypto. This cannot be done; the blockchain cannot be centralized under a single authority. No blending of inherently antagonistic forces is possible. It is not even clear that state and free-market cryptos can co-exist.

The state will keep attempting to forge a bastardized crypto, however, until it is convinced that efforts are futile. At this point, crypto will cease to be viewed as an opportunity and be seen as a danger. The very existence of free-market crypto encroaches on an irreplaceable source of state power—the issuance of money. Crypto has the ability to weaken this source of power and, perhaps, to destroy it.

The features of crypto that weaken the state include:

- Peer-to-peer transfers deny wealth by sidestepping central banks through which the financial flow is controlled.
- The privacy of crypto hinders the state's campaign of social control. The data from financial institutions that report on their customers are vital to the state's ability to impose social and economic control.
- Privacy also sidesteps the centralization of the state. The state can almost be defined as the centralization of power to benefit the elite.
- Crypto's existence raises the question of whether the state is necessary. If the free market can so easily assume one essential state function—the issuance and circulation of currency—then why can't it assume others, or them all?

Crypto is the money of society; it cannot and does not serve the state.

Law Enforcement as a Tool of Class Warfare

> The government's coercive taxing power necessarily creates two classes: those who create and those who consume the wealth expropriated and transferred by that power. Those who create the wealth naturally want to keep it and devote it to their own purposes. Those who wish to expropriate it look for ever more-clever ways to acquire it without inciting resistance. One of those ways is the spreading of an elaborate ideology of statism, which teaches that the people are the state and that therefore they are only paying themselves when they pay taxes. The state's officers and the court intellectuals at universities and the news media go to great lengths to have people believe this fantastic story, including the setting up of schools. Alas, most people come to believe it.—Sheldon Richman

One of the most powerful weapons the state possesses in the class warfare it wages against society is law enforcement, including legislation and the court system through which the state asserts its class privileges. Law is integral to the state's monopoly on force and its ability to coerce the transfer of wealth from society into its own hands. Without a monopoly on law enforcement, it is difficult to imagine how the state could win the class conflict because society enjoys the enormous advantages of being productivity, innovation, and energetic.

The state invests immense time and money in convincing society that law enforcement is a protection, not a threat. As a state drifts closer to totalitarianism, however, it becomes more difficult to maintain this deception because its guns—that is, the industries of law enforcement—become more visible.

One of the final tools the state wields to retain legitimacy before it has to start using guns is the T.I.N.A. argument: there is no alternative. The state incites fear of a terrible enemy—terrorists, perhaps—and then assures society that armed guards at airports, surveillance cameras, and a militarized police force are necessary. Besides which, there is no alternative. Or, rather, the only alternative is terrorism. Many will believe this false choice and accept the lesser of two evils.

Happily, there is an alternative: free market law.

Free-Market Law

> There's an important distinction between legislation and law. Legislation is the law that comes from political action...Law is more general in that legislation is a form of law, but law can also be the kind of law that evolves through human interaction. In England and the United States we are often referred to as 'common law' countries and that's because a great deal, and in fact, the majority of our law came about through an evolutionary process that didn't involve the action of political representatives.—John Hasnas

There oughta be a law. The meaning of this statement depends on the definition of "law." The state treats the word as a synonym for legislation or statutory law, which is law that results from a political process. Any person or group who holds sufficient power can pass legislation and use law enforcement to impose it on society. This is a trickle-down, centralized model by which an upper class determines how the lower class should behave. The effect of upper class decisions flows down vertically into the lives of lower-class people. Just one danger to a top-down system is that human beings act in their own self-interest, and legislated law is likely to reflect the interests of politicians rather than those of the people upon whom it is imposed. The system is a formula for corruption and a gateway for the state to expand ever deeper into society.

Can there be viable law without the state? Anarchists and advocates of limited government have debated this question for centuries, with many free-market voices concluding that law must emanate from the state in much the same manner as they believe money must. Law is a human need without which civil society is unlikely to last long. If the free market cannot provide this essential good, then anarchism fails and limited government is the most practical alternative. Society will become a junior partner to the state. The eternal struggle between Liberty and Power of which Rothbard wrote will be over, with Power declaring victory.

It is useful approach to begin by defining the term "law." Law is a more general term than "legislation," which is merely one form of law; the general term refers

to any code or set of rules that govern human interaction. “Govern” does not imply a state.

The answer: “yes, it can.” For one thing, society precedes the state, which must arise out of human beings gathering to interact. Society precedes both the state and law.

Another reason free-market law can exist is because it already has.

A popular form of free-market law is called common or customary law. This is a set of rules based on precedents that evolve through time to resolve disputes in a specific community. It is not preemptive but reactive. When a dispute erupts, the parties go to an impartial third party or to a community assembly to have their cases heard. In a rural community, for example, if one man accuses another of stealing a farm animal, then the arbitrator assesses the case and applies a community standard that has emerged from similar cases in the past. Since the adjudicators themselves could be involved in a future community dispute, they have a vested interest in infusing the proceedings with common sense.

This is grassroots law. It is decentralized law that does not have the broad application of federal statutes because it is tailored to local circumstances and standards. A fishing village would almost certainly evolve different rules of behavior than a mining town, for example. Rules governing the crypto community would differ from rules within the construction industry. As long as the purpose is to preserve peaceful interaction and to rectify breaches, there is no right or wrong to the specific content of the law.

Legal scholar John Hasnas explains:

> Customary law is the type of law that evolves when disputes arise…Over the decades and centuries, as things evolved, the decision maker became more and more specialized and by the time you get to the Norman era in England, decisions are made by juries. Juries are still drawn from the ordinary people in the country...In our system, you don’t have the courts organized into a hierarchal fashion until the late 19th century, so it’s 1873 and 1875.

Can a complex modern society function without a homogenized set of rules that are mandated? Can grassroots decentralized law work within a far larger framework than a fishing village or a rural community?

The prospect has been discussed for centuries.

The First Discussion of Free-Market Law and Defense Systems

> All around us are the almost unimaginable benefits of markets, cooperation, and technology, yet somehow we’re naïve if we don’t want to funnel human activity through government cattle chutes. The vast material and digital abundance we enjoy every day is provided without any state apparatus, in

> fact *in spite of* that apparatus. Is this private world not part of reality? Government is the artifice, and statists are the utopian dreamers who imagine that individuals acting under the magical banner of government can plan, coerce, and coordinate millions of lives.—Jeff Deist

The 19th-century classical liberal Gustave de Molinari respected the free market so deeply that colleagues referred to him as "the law of supply and demand made into man." Highly praised in his day, Molinari has fallen into obscurity. His legacy should be retrieved, however, because he raised a pivotal issue. Why is security a service monopolized by the state rather than performed by a free market that provides all other services more efficiently and inexpensively?

Molinari is the first explicit precursor to free-market anarchism. Rothbard alludes to his 1849 essay, "The Production of Security," as "the first presentation anywhere in human history of what is now called 'anarcho-capitalism' or 'free market anarchism'." Core to Molinari's anarchism is his theory of how society arises.

> There are two ways of considering society. According to some, the development of human associations is not subject to providential, unchangeable laws. Rather, these associations, having originally been organized in a purely artificial manner by primeval legislators, can later be modified or remade by other legislators, in step with the progress of *social science*. In this system the government plays a preeminent role, because it is upon it, the custodian of the principle of authority, that the daily task of modifying and remaking society devolves.
>
> According to others, on the contrary, society is a purely natural fact. Like the earth on which it stands, society moves in accordance with general, preexisting laws. In this system, there is no such thing, strictly speaking, as social science; there is only economic science, which studies the natural organism of society and shows how this organism functions.

Molinari believes men form society out of self-interest to satisfy the same "instinct of sociability" displayed by other high-order animals; sociability was built into man's nature in much way as hunger. Society is spontaneously organized for the purpose of making broadly defined exchanges; these are the proper sphere of economic study, not of social science.

Molinari presents three methods by which any good or service can be produced.

- The first method is to grant a monopoly to a privileged entity. This is what happens when the state is given a monopoly on the use of force and law within a jurisdiction. Dissenting individuals are forced to obey, or they are silenced.
- The second is through a collective that produces a service that is said to benefit society in general. Authority vested in a democracy is an example.

This less centralized form of control is no less dangerous for a dissenting individual.

- The third is free-market competition. The authority resides with individuals who are businessmen and customers. Individuals freely choose to do business or not.

All services and goods should be purely economic matters, including security and defense. Like every other service that fills a human need, security is best provided by a free market in which individuals wield the ultimate power of “yes” or “no.” Molinari is the first theorist to present a cohesive argument on how free-market mechanisms can replace the so-called essential functions of the State, especially protection against aggression. He claims the marketplace also establishes a more just society than government.

> This option the consumer retains of being able to buy security wherever he pleases brings about a constant emulation among all the producers, each producer striving to maintain or augment his clientele with the attraction of cheapness or of faster, more complete and better justice.
>
> If, on the contrary, the consumer is not free to buy security wherever he pleases, you forthwith see open up a large profession dedicated to arbitrariness and bad management. Justice becomes slow and costly, the police vexatious, individual liberty is no longer respected, the price of security is abusively inflated and inequitably apportioned, according to the power and influence of this or that class of consumers. The protectors engage in bitter struggles to wrest customers from one another. In a word, all the abuses inherent in monopoly or in communism crop up.

In short, there ought **not** to be law; there ought to be an economic service.

Molinari briefly sketches a blueprint of what the economic service of security might look like. To begin with, it would focus entirely on the protection of person and property rather than the protection of the state or a moral code. This eliminates the vast majority of laws. It also reduces the wars constantly waged over territory by nations that disregard the preferences of populations.

Security would be a business—or many businesses—including private police forces and arbitration services. Prospective customers would probably ask a series of questions of a provider, including one Molinari suggests; Will “any other producer of security, offering equal guarantees…offer… this commodity on better terms?” In short, Molinari envisions a system of security providers that functions in much the same way as insurance companies do today. He concludes, “Under a regime of liberty, the natural organization of the security industry would not be different from that of other industries.”

One counter-response inevitably arises; law requires consensus.

Locke on the Consensus Argument for Law

The perceived need-for-consensus problem has haunted the issue of the state versus private law and justice. Its most persuasive advocate was John Locke.

> The key to…an anarcho-capitalist court system is found in the concept of a "personal judiciary". [Acting as your own judge.]…The courts' purpose is to enable men to settle disputes so as to avoid violent resolution as well as aggression-overcompensation cycles. Regarding the courts' decisions as legitimate is the only way for the litigants to avoid **personal judiciary** actions.—Karl T. Fielding, "The Role of Personal Justice in Anarcho-Capitalism" [Emphasis added]

"Personal judiciary" is an idea Locke presents in *Second Treatise of Government*. The term refers to a person's natural right to assess his own experiences and to act upon his conclusions; this includes judging his own case. Additionally, since everyone has a right to reclaim his property from a thief, everyone can act as his own agent of restitution. If someone snatches your wallet, you have a right to grab the thief to retrieve it. The grab is an act of defensive force, not of aggression.

Locke acknowledges this right, but he thinks it is unwise to exercise it. He writes:

> That in the state of nature every one has the executive power of the law of nature, I doubt not, but it will be objected, that it is unreasonable for men to be judges in their own cases, that self-love will make men partial to themselves and their friends: and on the other side, that ill-nature, passion and revenge will carry them too far in punishing others; and hence nothing but confusion and disorder will follow.

It is unwise for men to judge their own cases because the act will produce conflict in society. Even a fair man views matters from his own perspective and self-interest; this is human nature. Moreover, he can be mistaken about the facts, including fundamental ones like the thief's identity. In other words, even a good man lacks objectivity. People who are less honest or more emotional may be even less fair, and they may exact inappropriately harsh remedies.

Locke argues that a society in which people judge their own cases will fall into "confusion and disorder." Why? Because an unjust verdict or inappropriate remedy aggrieves the recipient who then judges *his* own case and rectifies the wrong done to him. The process can become an endless loop because the justice administered is not accepted as legitimate by both parties.

Locke believes that breaking the cycle requires an unbiased judge whose assessment is widely accepted as legitimate. In crypto terms: Locke wants the decentralized justice of each man judging his own case to be centralized and placed under the authority of a trusted third party. The need for legitimacy in justice is one of the major reasons Locke advocates a limited state. And, for

centuries, Locke's approach has been used to argue against the possibility of private law and justice in civil society.

But if a trusted third party is irrelevant to exercising rights like freedom of religion, shouldn't the same be true of exercising a property right claim over goods? If crypto is stolen, shouldn't the victim be able to reclaim his property directly by hacking back the coins?

Yes, Locke would say, but there are good reasons for *not* exercising it. One-on-one remedies present danger to the victim. First, if he is mistaken about the thief's identity, the mistake converts an act of self-defense into one of aggression for which he is liable. Second, the victim may seek more remedy than is appropriate, prompting the original aggressor to retaliate. Achieving restitution may also be dangerous or beyond the victim's ability to achieve. And so on and so on.

Judging your own case also introduces the good Samaritan problem. Bystanders will base their judgments on appearance. If they witness an attack on the street from the beginning, they know who the aggressor is, of course. Or do they? What if you witness a man grab a woman and yank her roughly to him? She screams for help. You rush to the rescue, striking the man across the face with a heavy book you are carrying. As he covers his broken nose, the released woman sprints off. Later you learn the woman is a pickpocket; the man was recovering a stolen wallet.

You have facilitated a crime and injured an innocent man. And, yet, all you intended to do was to exercise a corollary principle of self-defense: the right to defend innocent people against aggression. Without this corollary, spouses could not legitimately defend each other, and parents could not protect children. You behaved in a reasonable manner, but your assessment was incorrect. The man had a right to pursue recovery from her and, now, from you.

The confusion can be greater with the theft of crypto. Consider a scenario. Your account at an exchange or on your hard drive is cleaned out of coins. Through detective work, you identify the thief and seek restitution by hacking into his wallet. His exchange detects the activity and views *you* as the criminal simply because that is how it appears. The exchange calls the police and prosecutes you. Eventually, you clear your name at the cost of money, inconvenience, and embarrassment. Moreover, you do not retrieve the coins.

It is often impossible for a bystander to distinguish between a victim and an aggressor through observation. This is especially true with crypto crimes. The man who reclaims his wallet can prove it is *his* wallet by showing the ID inside. It is not similarly easy to prove that coins or fiat belong to one person—a coin is a coin, a dollar is a dollar, and they do not come with certificates of ownership.

Fortunately, there is one sure way to identify who is the victim.

The litmus test: who owns the property in question? Ownership means having a valid title to the property. Possession is not 9/10ths of the law; title is 100%. But, again, proof of title requires a determination based on examining the evidence.

> If no man may invade another person's "just" property, what is our criterion of justice to be? There is no space here to elaborate on a theory of justice in property titles. Suffice it to say that the basic axiom of libertarian political theory holds that every man is a self-owner, having absolute jurisdiction over his own body...It follows then that each person justly owns whatever previously unowned resources he appropriates or "mixes his labor with." From these twin axioms—self-ownership and "homesteading"—stem the justification for the entire system of property rights titles in a free-market society. This system establishes the right of every man to his own person, the right of donation, of bequest (and, concomitantly, the right to receive the bequest or inheritance), and the right of contractual exchange of property titles.—Murray Rothbard

As concepts, theft and restitution depend on the idea of property titles. In most cases, restitution is best done by a trusted third party agent or agency. As long as the third party is free-market, this presents little problem. Unlike law enforcement, a free-market agency can be hired and fired at will. This the difference between the state and society.

Before proceeding to a more concrete discussion of free-market security and its relevance to crypto, another aspect of free-market security is best addressed: the prevention of crime.

Preemptive Security

> Perhaps the main problem in this area is to see the importance of protection —to get people to concentrate more on locking the criminal out, and less on locking him up after he has committed a crime. Successful efforts to reduce the incidence of crime must be based upon better methods of protection. That is, we must concern ourselves with trying to prevent trespasses instead of worrying about what we will do after we have been trespassed...Men who see the necessity for protection realize that the government is not in a position to provide it, and they turn elsewhere. The best source of protection is the marketplace.—Robert LeFevre, The Fundamentals of Liberty

A drawback of entrusting your security to the state is the tendency to become dependent upon it and neglect to protect yourself. If there were no police, then people would be more aggressive about preemptively securing their own safety. The situation resembles how people approach their bank accounts. Because the Federal Deposit Insurance Corporation insures deposits in the U.S. against bank failures, customers rarely give a second thought to the security of their accounts. This attitude or habit makes people vulnerable to losing crypto in exchanges or imprudent investments. State dependency makes them lose or never develop the

habit of self-protection. Yet self-protection is as much an individual's responsibility as his health.

LeFevre highlights another drawback. Those who use the services of law enforcement are reinforcing the myth of the state's legitimacy.

Then how is justice to be obtained? LeFevre answers: preemptive defenses that avoid crime before it happens. This contrasts sharply with how most libertarian theorists approach private justice; they focus almost entirely on issues such as restitution versus retribution. These issues come into play, however, only after a rights violation occurs. Like Satoshi, LeFevre wants a system that prevents the crimes from happening in the first place.

There are striking parallels between LeFevre and Satoshi. Both men want to avoid and replace a trusted third party state agency with a private alternative. LeFevre focuses on replacing traditional law enforcement, while Satoshi targets the central banking system. Their motivations are similar. LeFevre sees law enforcement as a massive failure, or far worse. Under the guise of providing justice, it oppresses individuals by regulating almost every activity short of breathing. Equally, Satoshi knows that central banks and fiat are massive failures, or far worse. Under the guise of providing financial stability and protection, they loot the wealth of individuals through mechanisms like inflation.

Both men did not confront the state but avoided a need for it. LeFevre writes, "Is government the only device we know of self-protection? No, it is not. Voluntary insurance is another device. So are private policemen, private organizations such as the American Legion, night watchmen, merchant police, the Triple A and perhaps a score of others…"

Practical advantages adhere to LeFevre's and Satoshi's commitment to prevention. For one thing, after a crime has occurred, it can be almost impossible to make a victim whole, even in non-criminal cases of contract or straightforward torts.

The state does not want people to self-protect because this breaks its trusted third party monopolies over law enforcement and banking. Or, at least, it ignores them. The state wants people to believe the police "serve and protect," because then they accept a loss freedom as the price of security. Society's main weapon of self-defense is to demonstrate that the state's protection and services are unnecessary. People do not need to pay with their freedom to be safe.

A Haunting Question

The stress on prevention captures a schism within the crypto community. Prevention and avoidance are natural companions. Confrontation is not. Which approach is more effective in dealing with the state? Or can a blanket statement be made? Satoshi seemed to think so.

The two attitudes are embodied in an incident between Julian Assange and Satoshi. Both of them fully understand the freedom value of crypto, but they seem to disagree on the best way to attain it.

Assange tweeted in October 2017: “My deepest thanks to the U.S. government, Senator McCain, and Senator Lieberman for pushing Visa, MasterCad [sic], Paypal, AmEx, Moneybookers, et al, into erecting an illegal banking blockade against @WikiLeaks starting in 2010. It caused us to invest in Bitcoin—with > 50,000% returns.”

Satoshi’s attitude is epitomized by his response to an earlier tweet from Assange who crows, “Bring it [bitcoin] on.” Satoshi objects. “No, don’t ‘bring it on.’ The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy.” Less than a week later, on 12 December 2010, Satoshi vanished after posting the message: “WikiLeaks has kicked the hornet’s nest, and the swarm is headed towards us.” The swarm is government and, perhaps, those users who care nothing about Bitcoin as a vehicle of freedom and can dilute its potential.

It is tantalizing to speculate on the software with which Satoshi wanted to strengthen Bitcoin. Protections against bad actors? A decentralized exchange for complex trading and cashing out? It is disturbing to realize that Bitcoin may have been hindered badly by becoming popularized too soon.

But the main question posed here is whether Satoshi’s attitude of prevention and avoidance is the most effective approach to battling the state. If so, then those who confront the state with taunts and challenges may be weakening a primary strength of crypto: freedom through prevention, not confrontation. They may be handing an advantage back to the state and away from society. The theories and strategies nonviolent resistance offer a blueprint on how to handle the state.

SECTION FIVE: CRYPTO, LAW, AND JUSTICE

CHAPTER ELEVEN: Dealing With Crime Without the State

The final challenge for crypto is the same one that confronts anarchism itself: what of law and order? How can crime be prevented and redressed?

Human beings need justice as surely as they need food and shelter. It is an economic good that the free market can and will fill in order to make a profit. The dynamics of how crypto can prevent and redress crime will be largely technological. They will evolve constantly to address circumstances and preferences, most of which are unpredictable. The purpose here is to sketch the principles and context within which free-market justice must function and to argue for its superiority over the state system.

Compared to What?

Perfection does not exist. When assessing and comparing systems that allegedly address the same problem, at least two questions must be answered. What is the goal of each system? And how effectively do they achieve it?

Despite the word “justice” appearing in both terms, the goals of free-market and state justice are incompatible. One empowers the individual; the other centralizes power in the hands of authority. Free-market justice is the full realization of an individual’s right to self-defense; state justice destroys the right of self-defense by centralizing it in the hands of authority. The situation is similar to that in the financial realm. Crypto and the blockchain allow individuals to become self-bankers and to control their own finances; fiat and central banking allow the state to monopolize finance and take control from individuals.

The methodology and goals of the two systems are diametrically opposed and, to understand both, it is useful to compare them, especially regarding crimes committed by individuals against each other.

A fundamental advantage of free market justice must be stated first, however. Free-market justice addresses only the problem of crime—that is, the violation of rights—and it acts only to make the victims whole. The state creates pseudo-crime—that is, it criminalizes peaceful but objectionable behavior—and it acts only to protect its own power. It is difficult to overstate the impact of this difference.

> Government is a law factory. It passes laws in the same manner that another type of factory extrudes metal molding…But, whereas a factory which extrudes metal molding is providing a product which is useful to the citizens generally, and which certain citizens will purchase voluntarily; the government factory extrudes compulsion which is useful principally to the government, itself, but is purchased [through taxes and other ‘fees’] in advance by the people, who are never in a position to refuse to buy.—Robert LeFevre, The Nature of Man and His Government

The state’s system of justice routinely manufactures two types of real criminals—people who intentionally violate the rights of others. The largest group consists of sanctified criminals who plunder wealth and impose social control in the name of the state. They are politicians, bureaucrats, law enforcement, and other state agents or their cronies. They rule with a velvet glove when people accept their claim of legitimacy and obey. When people refuse, however, the system’s true nature is seen, and obedience is commanded through raw coercion.

The second group consists of unsanctified criminals. These are individuals who choose violence or the threat of it as a quick path to profit, but they do so without the claim of legitimacy. Common criminals would exist in any system, but state justice multiplies their number by processing people in a manner that strips away their humanity and makes them abandon all belief in law—any law. The prisons

act as training grounds for crime, not only in the how-to sense but also psychologically.

The system produces pseudo-criminals as well—that is, people whose behavior is peaceful but unacceptable to the state. Drug dealers and drug users are examples.

The state benefits from the manufacture of criminals in at least four ways.

- The human need for safety and justice gives the state a justification to claim a monopoly over the use of violence. The state then centralizes and industrializes the “services” it provides: the legislative industry, regulatory bureaucracies, the police industry, the court system, the prison industry, the surveillance state, and a myriad of associated industries. State power is cemented into every niche of daily life.
- If people believe the state is the only source of safety, they more willingly accept violence committed by the state. They render obedience for protection in the belief that there is no alternative.
- The state justifies taxes, fines, and other fees in the name of funding law and order. Safety and its enforcement are cash cows.
- Less direct dynamics, such as prison labor, are extremely lucrative to the state and to the crony corporations that use prisons as manufacturing centers with extraordinary cheap labor.

An entirely different approach is required to fill the human need for safety and justice. Nothing addresses human needs as efficiently and impartially as the free market. A return to basics is required.

The stakes are high. Consider what currently passes for justice.

The State Destroys What It Cannot Control

Comparing free-market and state justice requires a grasp of the goals and methodology of each. Free-market justice seeks to protect the person and property of individuals and to rectify any violation with as little force as possible. State justice seeks to maintain the state’s control over society and to punish any violation of its rules with as much force as necessary to discourage further violations. The state’s goal makes it a law factory; its methodology makes it a criminal factory.

> Most people fail to appreciate the fundamental obstacles placed in the path of crime prevention by the perverse logic of *public* property, *public* law enforcement, and *public* imprisonment. Step one: start with public streets, sidewalks, and parks where every citizen must be permitted unless proved guilty of a crime. Step two: rely on an inherently inefficient public bureaucracy to catch, prosecute, and try those criminals against whom enough evidence of guilt exists. Step three: should they be convicted, subject criminals to the dangerous, unproductive, and sometimes

> uncontrollable setting of public prisons to prevent them from engaging in further misconduct. Step four: periodically release most prisoners back into the community and then return to step one and repeat the cycle. Each step follows from the preceding step, and each step unavoidably leaves considerable room for criminal conduct to thrive.—Randy Barnett, *The Structure of Liberty: Justice and the Rule of Law*

In short, the state creates criminals not only through legislation but also through methodology. It claims authority over the very cement people walk on and then criminalizes them for any misstep. This does not help real victims. Once within the justice system, criminals have little to no chance to remedy their mistakes through restitution. For state justice, the victim is usually the state itself. This is especially true of victimless crimes—so-called "crimes" in which all involved participate voluntarily. Victimless crimes account for the majority of imprisonments.

The state's monopoly on force is essential to maintain all other monopolies, including over the flow of finance. Anyone or anything that threatens those monopolies is criminalized, including crypto. The state accurately identifies crypto as a violation of its monetary monopoly and privileges. Bypassing the state and central banks is criminalized, therefore, by being associated with black market activity and other peaceful conduct that deprive the state of revenue. These pseudo-crimes justify a crackdown.

Of course, people who use cash do the same, but there is a remarkable difference in how the state approaches offenses committed with fiat.

1) Targeted users are demonized—sex workers, for example—but the cash itself is not accused of being criminal, perhaps because is issued by an agent of the state. That is to say, the vast majority of people who use cash are not viewed as miscreants. By contrast, both users *and* crypto are demonized. Crypto is the true bull's-eye, with categories of users that are viewed as unsavory being prominently attacked as a way to undercut crypto's legitimacy.

2) The entire category of crypto users is criminalized—or, rather, the entire category of those who use *unregulated* crypto. This is a characteristic of state justice. Categories of people become criminals—drug dealers and sex workers, for example—irrespective of whether any of them have aggressed against another individual. Again, cash is exempt from this treatment, with the vast majority of those who use cash not being accused of crime.

The state's fundamental problem with crypto, as opposed to cash, is that crypto makes trusted third parties extraneous. This makes the state itself extraneous because it is the ultimate trusted third party. If individuals do not require the state's trusted third party services, then there is no legitimate reason for the state to exist. That's why the state is so desperate to convince people that they need it for money, safety, retirement, medical care, education, and every other free-market good and every other service it can commandeer. The current justice

system is about the preservation of the state, not the protection of society or individuals.

Unfortunately, a second justification backs the state's campaign against unregulated crypto: the claim that crypto violates individual rights. Specifically, crypto is said to be involved in violence against individuals, such as human trafficking. The "unfortunate" aspect of this justification is that some accusations are true. This is the state's most dangerous attack on crypto because it resonates with decent people who are and should be appalled by crimes like human trafficking.

A March 2018 bitcoin.com article addresses another real crime: fraud. "$9 Million a Day Is Lost in Cryptocurrency Scams," opens:

> In the time it takes you to read this sentence, $850 will have been lost to cryptocurrency scams. In the time it takes to complete this article, that figure will have risen to $17,000. Phishing; fraud; theft; hacking; it's all rife. In the first two months of 2018, there were 22 separate scams involving thefts of $400,000 or more. Put it all together and that equates to an average of $9.1 million a day. Oh, and that doesn't include 2018's outliers—Coincheck, Bitconnect, and Bitgrail. Otherwise, the total would actually stand at $23 million a day.

The state uses real crimes as cover to achieve its actual goal regarding crypto: to eliminate competition that threatens one of its vital monopolies. Part of the state's campaign is to exaggerate the real crimes and portray its own services as the only remedy possible.

Crypto is accused of shielding almost every conceivable act of violence. The article "10 of the Biggest Lies Told About Bitcoin" deals with the charge that crypto is the terrorism's money of choice.

> If you want to blame a currency, try the U.S. dollar which has been used to fund more wars, proxy wars, bombings, hijackings, and insurgencies than any other. Europol found no evidence that terrorists were using cryptocurrencies to fund their activities. That's not to say it hasn't happened and won't happen. It's telling however that the only people linking bitcoin with terrorism are governments seeking to crackdown on digital currencies.

Crypto is also accused of facilitating hate groups.

> We could launch into a lengthy explanation as to why it's ridiculous to blame a currency for the actions of a tiny subset of its users, but sometimes the simplest responses are best: "You've probably heard about cars—but what you haven't heard is how much they are helping bank robbers."

It is often difficult to see through the smoke and discern the hard, cold crimes in which crypto is involved. These crimes must be addressed, however, not only

because they invite state involvement but also because victims deserve redress. But agreeing with the state on this point is the beginning of a deeper dispute that comes down to more fundamental issues.

What is Justice?

> Libertarianism is about individual rights, property rights, the free market, capitalism, justice, or the nonaggression principle. Not just any of these will do, however. Capitalism and the free market describe the catallactic conditions that arise or are permitted in a libertarian society, but do not encompass other aspects of libertarianism. And individual rights, justice, and aggression collapse into property rights. As Murray Rothbard explained, individual rights are property rights. And justice is just giving someone his due, which depends on what his rights are.—Stephan Kinsella, "What Libertarianism Is."

What is justice? The answer is the rudimentary framework for any system of law. The American political-philosopher Michael Sandel answers, "The simplest way of understanding justice is giving people what they deserve. This idea goes back to Aristotle. The real difficulty begins with figuring out ***who*** deserves ***what*** and ***why****."* [Emphasis added] This is private justice. It needs further definition.

Private justice is distinct from divine justice, the two of which are sometimes conflated. Divine justice envisions a deity or some other ultimate power that weighs each person's worth on a scale and allocates good fortune on the basis of the reading. "Why me, Oh Lord, why me?" is the cry of someone who believes he has been betrayed by divine justice. The theory underlying this cry is that there is something beyond the non-initiation of force that a good person is entitled to demand of the world: good health, for example. When bad things happen instead, the situation is called "unjust." The word is either being used colloquially or being misused. Perhaps a better word would be "unlucky."

Private justice is not based on a deity or some other overarching power. It is, as Aristotle maintains, justice that consists of people receiving what they deserve from each other. And, as Kinsella explains in the opening quote, "Justice is…giving someone his due, which depends on what his rights are." It is based on human nature and every individual's self-ownership.

The content of private justice rests on two principles. The first is the non-initiation of force, which is a restatement of a person's duty to respect the self-ownership of others; justice resides in living together in peace. The second principle is contract law by which a person voluntarily exchanges with another. The justice here resides in each person receiving whatever has been agreed upon. When justice does not occur, a remedy is required. Neither a breach of contract nor its remedy have to involve violence, however. A breach does not even have to be a person's fault; it could be occasioned by an unexpected change of circumstance. But the person who is disadvantaged by the breach still has a right to be made whole.

That is where the right to justice begins and ends, however. There is a common confusion about justice. Namely, it is often called “unjust” when one party treats another with disrespect or hostility. This assumes that one person can have an enforceable claim to another person’s attitude. No such claim exists; there is only the right to live without being molested and to the fulfillment of a contract. A seller who is rude to a buyer is unlikely to have repeat business, and this is a strong incentive for him to be civil. But the seller’s only duty under justice is to be nonviolent and honest in the exchange, not to manifest the correct attitude while doing so. As Rothbard writes, “It is not the business of the law to make anyone good or reverent or moral or clean or upright.”

Returning to Sandel’s early statement, the ***who*** of justice is twofold: 1) whomever is deprived of what is rightfully his—bodily autonomy, property, or a contracted benefit—and 2) the person responsible who owns the victim a remedy. The ***how*** is addressed in this chapter. The ***why*** is because every person is a self-owner.

Few things are as just as the free market in which two people directly exchange for agreed-upon values and then walk away, each satisfied. A woman who buys a tomato and goes home with her purchase to make a salad is enjoying justice. The tomato vendor who pockets the woman’s money and moves on to the next customer is also experiencing justice. The free market provides people with what they deserve by right. In other words, the free market is Aristotelian justice in practice.

Another way of saying this is that private justice is proprietary. In his essay “The Proprietary Theory of Justice in the Libertarian Tradition,” the co-founder of the modern Voluntaryist movement, Carl Watner, provides a fair summary of private justice. “The proprietary theory of justice is concerned with just one thing: the crucial determination of just versus unjust property titles of individuals in their own bodies and in the material objects around them.”

The most persuasive theorist on proprietary justice may well be the libertarian legal scholar Randy Barnett. In his book *The Structure of Liberty*, Barnett argues that law should be privately administered, with any inefficiencies addressed by the free market. Part of the efficiency of proprietary justice derives from its sheer simplicity and the minimal number of laws. Barnett writes of the current system, “Every dollar spent to punish a drug user or seller is a dollar that cannot be spent collecting restitution from a robber. Every hour spent investigating a drug user or seller is an hour that could have been used to find a missing child. Every trial held to prosecute a drug user or seller is court time that could be used to prosecute a rapist.” Barnett argues that private law is **the** solution to the inevitable corruption of vested interests and monopolies.

The Requirements of Private Contract Law

Contract law requires two things to function: the presence of agreement and an instrument of enforcement. The contract is the presence of agreement; it expresses the consent and the terms agreement. Contracts can be implied,

verbal, or written, but the more explicit the agreement is, the easier the administration of justice becomes.

The obstacle over which law often stumbles is the instrument of enforcement. How do you enforce the law on another person and exact restitution? Ethical and practical issues arise. A common ethical issue: what about the individual rights of those forced to provide restitution? A common response: anyone who violates the rights of another relinquishes his own to the proportional degree of the harm inflicted and until this harm is rectified. A common practical issue: restitution invites the participation of a trusted third party. In state law, the third party consists of state agents who often use violence. In proprietary or free-market law, the third party consists of free-market agents who are restrained by dynamics like the use of proportional force and the need to preserve a good reputation. But any model that depends upon a trusted third party is vulnerable to corruption, incompetence, and other risks.

Satoshi removed the trusted third party problem from economic exchanges, but the blockchain can also remove it from many areas of the law. A peer-to-peer transfer on the blockchain fulfills all the requirements of a good contract. It embodies a voluntary agreement; it memorializes the terms of the exchange; its validity is proven through transparency. The blockchain can also fulfill a requirement of law—namely, it is an instrument of enforcement in and of itself. When it does so, it is called a smart contract—a self-executing contract. A recent U.S. Senate report states, “The concept [of smart contracts] is rooted in basic contract law. Usually, the judicial system adjudicates contractual disputes and enforces terms…With smart contracts, a program enforces the contract built into the code.” Smart contracts offer the same opportunity to avoid the trusted third parties of lawyers and state courts as crypto avoids central banks. Moreover, In acting as both the agreement and the instrument of enforcement, crypto can eliminate much of the expense of justice.

Today’s smart contracts are undoubtedly primitive compared to the ones that will evolve, but they are a proof of principle.

The impact on society of such mechanisms as self-executing contracts could be enormous. In a society organized around exchange, contracts would be the basis of *all* law. Even the use of violence that violates individual rights can be viewed as a breach of the duty—the implied contract—that everyone must respect the rights of others if they wish to claim these rights for themselves. Again, those who commit crime lose their own rights to the same extent as they have denied them to another and for as long as the wrong is not remedied. Then the contract is reinstated. All law can be reduced to contract.

An article in *Futurism*, “An AI Law Firm Wants to Automate the Entire Legal World,” indicates how easily the transition from physical contracts and lawyers to smart contracts and algorithms could be. “On LawGeex [an automated service], users upload a contract and, within a short period of time (an hour on average), they receive a report that states which clauses don’t meet common legal standards.

The report also details any vital clauses that could be missing, and where existing clauses might require revision. All of this is calculated by algorithms." For a modest fee, LawGeex can detect clauses that enable fraud or provide inadequate protection.

Such services highlight a rarely discussed aspect of justice; it is an economic good. Basically, there are two sides to justice as an economic good. Owners should pay for the cost of protecting their property, if they choose to do so. Criminals should pay for the cost of restitution, which includes the restitution itself, the expense of attaining a remedy, and the inconvenience or suffering of the victim.

> The economic analysis of crime starts with one simple assumption: Criminals are rational. A mugger is a mugger…because that profession makes him better off, by his own standards, than any other alternative available to him.… If muggers are rational, we do not have to make mugging impossible in order to prevent it, merely unprofitable.…If little old ladies start carrying pistols in their purses, so that one mugging in ten puts the mugger in the hospital or the morgue, the number of muggers will decrease drastically–not because they have all been shot but because most will have switched to safer ways of making a living. If mugging becomes sufficiently unprofitable, nobody will do it.—David Friedman, "Rational Criminals and Profit-Maximizing Police"

Anyone who values their property should make crimes against it unprofitable and difficult. This approach by itself could vastly reduce crime. People generally handle their personal safety in one of four ways, however.

- People self-protect. They directly assume responsibility for their own safety by protecting access to their property and by learning self-defense. This involves costs such as locks and an investment of time.
- People ignore their own safety, relying on luck or the good will of others. The cost is the potential damage to their property and person.
- People trust to state protection. The cost is their freedom and the chance of real safety.
- People view safety as a private service to which they subscribe—hiring a night watchman, for example. The cost is the cost.

If safety is a good, like food or shelter, then the consumer of the good should bear the price of procuring it. The cost is not always monetary. It can be the time and energy it takes to set up protections. (See discussion of protection in the preceding chapter.)

A glimpse of how free-market protection might work for communities is offered by networks that do not enjoy the protection of police and need to take care of themselves. Consider sex workers. The property here is the sex worker's body.

In her article "A Hundred Years of Crypto Anarchy," block chain engineer Elaine Ou comments, "Public Key cryptography isn't just for encrypting private messages. It also provides proof that the sender is who they say they are. When buyers and sellers conduct transactions, they sign messages with their private keys. The signatures become digital identifiers." If this seems peripheral to preventing violence, talk to sex workers whose front line defense is to verify the identities and reputations of clients, which they then share with each other through networking. An overlooked role of a pimp—many of whom are not abusive—is to ensure the safety of sex workers by screening customers, handling money, providing transportation or safe places, and waiting. Pimps are trusted third parties and, like every third party, they can be more trouble than they are worth. Crypto shifts this dynamic so that some tasks of a pimp are replaced by a peer-to-peer filter with transparency. The sex worker is in control, which translates to less risk of violence and more money, both of which promote safety.

The second economic aspect of proprietary justice is making the criminal pay the cost of remedying a crime. What would this look like?

A commonly proposed mechanism of restitution has been the private defense agency (PDA). The PDA is a free-market business whose profits and reputation depend on the accuracy and fairness of its practices in remedying crime. A victim of crime freely chooses the trusted third party, whose trust is tested by the constant presence of competitors. The business relationship lasts only as long as the customer values the service.

The PDA's purpose is to recover stolen or damaged property or the value of it from the criminal; again, the property damaged may be the victim's body. But the PDA also acts as a protection for the victim and for the aggressor himself during the recovery process. The victim is insulated from any harm or danger that might be involved; the aggressor deals with a professional who wishes only to secure restitution, not to vent anger. Indeed, the PDA has a strong business incentive to avoid the expense and complications of injuring anyone.

Friedman offers one vision of a PDA in his book *Machinery of Freedom*. Friedman begins by considering "the easiest case" of a conflict, which is "the resolution of disputes involving contracts between well-established firms...Currently, arbitrated decisions are usually enforceable in the government courts," Friedman admits, "but that is a recent development; historically, enforcement came from a firm's desire to maintain its reputation."

What of disputes involving violence, including theft? "Protection from coercion is an economic good," Friedman explains. "It is presently sold in a variety of forms—Brinks guards, locks, burglar alarms. As the effectiveness of government police declines, these market substitutes for the police, like market substitutes for the courts, become more popular. Suppose, then, that at some future time there are no government police, but instead private protection agencies. These agencies sell the service of protecting their clients against crime. Perhaps they also guarantee performance by insuring their clients against losses resulting from

criminal acts.” Insurance that has been purchased from a PDA becomes the immediate remedy offered to the victim, perhaps in the same manner as car insurance pays for damages after an accident; the PDA can then pursue remedy from the criminal with the added incentive of recouping its money. Or a victim can hire the PDA after a crime has been committed; then the PDA would investigate and retrieve both the property and the cost of its services from the aggressor.

Friedman concludes, “What I have described is a very makeshift arrangement. In practice, once anarcho-capitalist institutions were well established, protection agencies would anticipate such difficulties and arrange contracts in advance, before specific conflicts occurred…” But, again, it is not possible to predict future mechanisms of restitution.

In fact, the most accurate response to a question posed earlier—what would proprietary just look like?—is one many people will find unsatisfying. No one knows, anymore than anyone knew how Bitcoin would morph and manifest itself.

One Reason the Future Face of Proprietary Justice is Unpredictable

In *Human Action*, Ludwig von Mises argues for the concept of “consumer sovereignty,” which expresses how consumers and producers relate in a market economy. Producers are the engine of prosperity, Mises claims, but they are not the ones who determine the direction an economy takes. Consumers are. Specifically, consumer preference is. These diverse preferences lead to an explosion of economic choices—a dynamic that would be true of the economic goods of safety and justice.

Consumer sovereignty flies in the face of the mainstream belief that capitalists and businessmen determine the course of an economy along with the lives of average people within it. Traditional wisdom: economic control is vested in the ownership of the means of production while average people are forced to accept the crumbs.

To Mises, the relationship is symbiotic, with the consumer being an equal or greater partner. He describes the sovereignty of consumers.

> The direction of all economic affairs is in the market society a task of the entrepreneurs. Theirs is the control of production. They are at the helm and steer the ship. A superficial observer would believe that they are supreme. But they are not. They are bound to obey unconditionally the captain's orders. The captain is the consumer...Neither the entrepreneurs nor the farmers nor the capitalists determine what has to be produced. The consumers do that. If a businessman does not strictly obey the orders of the public as they are conveyed to him by the structure of market prices, he suffers losses, he goes bankrupt, and is thus removed from his eminent position at the helm. Other men who did better in satisfying the demand of the consumers replace him.

A consequence of consumer sovereignty is that no one can foresee the preferences expressed in the marketplace, including the consumers themselves. No one can predict the institutions, agencies, or dynamics that will arise to profit from those preferences. Undoubtedly, technology and other innovation will evolve to offer new alternatives; the change will be dizzying. Mises observes:

> They [the consumers] are no easy bosses. They are full of whims and fancies, changeable and unpredictable. They do not care a whit for past merit. As soon as something is offered to them that they like better or is cheaper, they desert their old purveyors.

The free market shifts constantly in response to how consumers vote with their dollars. It is fluid, in flux, and beyond anyone's ability to predict. Consumer sovereignty is one of the main reasons why it is not possible to offer a fixed blueprint of how proprietary justice will perform in the future. It is only possible to describe the concepts surrounding justice, not the specific applications.

Toward A New Vision of Justice

Cryptocurrency changed the world's view of money—of what it was and what it could be. Proprietary justice similarly revolutionizes the concept and enforcement of law. In both cases, the principles and definitions remain unchanged. Money is a means of exchange, a form of wealth, and a unit of accounting. Justice is every person receiving what they deserve; law is the means and rules of enforcement. But the form that proprietary justice takes, like crypto, is something new under the sun.

Traditionally, the state has justified its monopoly over money and justice by pointing to an alleged need for "consensus." The state justifies its money monopoly by a so-called need for a currency to be "trustworthy" and broadly accepted within a given territory. Lockeans justify the state itself by civil society's alleged need for one final arbiter of justice whose judgment is "trustworthy" and generally accepted within a given territory. (Consensus that is compelled by force, of course, is not consensus at all; it indicates the opposite.)

Consensus is last-century reasoning. It is invalid for currency; it is invalid for justice. Crypto proved that individual consent along with an instrument of enforcement—the blockchain—creates a valid currency. It does not matter if the individual users constitute a small portion of the population. As in colonial America, a multitude of currencies can circulate to fill a variety of niches and preferences.

The same is true of justice. People who contract together may have a different view of what is just than the one held by their neighbors or the general public. The primacy of contracts and the use of the blockchain mean that, as long as violence is eschewed, there is no one standard justice. Whatever is agreed upon is just. Those who believe charging interest is usury, for example, will make loans

that include none. For capitalists, the opposite will be true. Both arrangements are just, with the content of justice being defined by participants.

The most important point: contracting individuals will define their own standard of justice, which can and will vary from contract to contract within the same jurisdiction. This divorces justice from geography—from the dictates of an authority that claims jurisdiction over a given territory—and locates the content of justice within individuals themselves. Justice is decentralized down to the level of the individual.

The state resorts to the consensus argument because its jurisdiction is inextricably linked to geography. A nation is defined geographically and a state is the institution that claims jurisdiction over a specific nation, which it maintains through a monopoly on force. In reality, the consensus being lauded is the verdict of its own authority, which everyone within the jurisdiction is compelled to honor. The populace must accept legal tender, obey the law, and obey the verdict of judges. No one is allowed to dissent.

What happens when geography becomes irrelevant to the law and justice as the transfer of money now is? Can the state still exercise authority?

Crypto answers this question. Crypto crosses the globe like wind and assumes no nationality. Currency no longer flows through physical choke points called banks over imaginary lines called borders. Crypto bypasses geography just as it bypasses the trusted third party problem. The state loses its monopoly on money and the financial system, which is its lifeblood. When geography becomes irrelevant so does the state because, by definition, the state is a territorial claim.

This is Justice without geographical boundaries. It is justice that does not go through the choke point of state law that imposes conformity in the form of the state's preferences. This decentralized justice that expresses only the preferences of the individuals involved. It the same prospect of freeing individuals from state justice as crypto freed them from the monetary monopoly.

Unfortunately, the perceived need for consensus makes people believe that free-market justice is "anarchy" in the worst sense of this word. They do not understand the principles, purpose, and content of proprietary justice. Its core principle is the right of every individual to exist in peace. Its purpose is to facilitate voluntary exchanges between individuals so that each receives what they deserve; when they do not, then the purpose becomes restitution. Except for the prohibition on violence, the content of justice would be as varied as crypto itself because individuals would decide what is just in much the same manner as as they decide the proper price for a good—through agreement.

Otherwise stated: The blockchain acts as the contract, law, and enforcement mechanism in one package. It embodies the terms to which parties have agreed; it enforces those terms without third party involvement; and the enforcement occurs with no regard for jurisdictions or geography. Just as crypto sidesteps the

monetary monopoly, blockchain justice can sidestep the law enforcement and justice monopolies of the state.

People's confusion over free-market law and justice is understandable because the concepts run against everything people have been taught. What they have been taught is incorrect, not only the theory of it but also the history.

In his article, "Why the Elites Prefer a Centralized Legal System," historian Chris Calton explains how the conventional view of centralized justice became embedded. "The motivation to centralize legal authority was entirely political." A vital function of civil society was usurped and homogenized in the name of consistency and consensus. It was not always this way. Calton continues,

> But in the early nineteenth century, consistency was valued less than flexibility in the legal system. When the courts were local, the people of a given community had a vested interest in seeing justice carried out according to the particularities of each individual case.…And for those who were not fortunate enough to find themselves at the top of the legal hierarchy—the uneducated, the poor, women, children, and blacks—this flexibility upheld even modern notions of justice—if imperfectly—more effectively than did the centralized and legally consistent courts that followed.

Law was decentralized down to the local level in order to serve the requirements of local people.

Justice was once decentralized at the local level. And if centralized law did not always exist, then it is neither inevitable nor necessary. The final step, of course, is to decentralize justice down to the individual.

In fact, instances of decentralized law function around us right now and offer practical models for building new systems. One is called Creative Commons Law (CCL). CCL is an open-source venture to build a practical system of law for stateless societies. It stresses concrete application and in no way blocks other competing systems. Most people have encountered a manifestation of CCL: the Creative Commons licenses for publishing material that has been traditionally viewed as the purview of intellectual property—copyright and patents. Many authors and inventors dismiss the legitimacy of IP, and they offer their work without the normal copyright restrictions on republication; other Creative Commons licenses specify terms such as crediting the original source within the reprint. The author or inventor chooses the license he prefers; his choice in no way infringes upon people who choose different terms of publication and wish to contract with others to preserve a quasi-monopoly on their work. Open source ideas and development have been a cornerstone of the crypto community. CCL is a proof of principle for free-market law.

In summary, blockchain law is proprietary justice that is free of the geographical jurisdictions known as nations. It is bound instead by algorithms and individual

choice. It does not require consensus or the trusted third party called the state. The code is the law, and the code's content is whatever those involved agree upon. The individuals define and execute their own law without a legislature or a political process. And, if justice consists of each person receiving what he deserves—that is, receiving the agreed-upon exchange—then each individual also defines justice for himself. The only restriction is that agreements must be voluntary; that is, they must remain agreements.

> Anarchism, liberty, does not tell you a thing about how free people will behave or what arrangements they will make. It simply says the people have the capacity to make the arrangements. Anarchism is not normative. It does not say how to be free. It says only that freedom, liberty, can exist.—Karl Hess, "Anarchism without Hyphens"

Without a need for consensus, multiple versions of law and justice can and will co-exist peacefully within one territory. They can function directly next door to each other or within the same house, and they can vary from contract to contract for the same person, depending on his purpose and circumstances. If someone prefers Western common law while a Jewish neighbor embraces Hasidic law, then so be it; neither is bound by the other's values because one person's execution of terms in no way hinders the ability of the other to execute a different set of terms. Communists can reject a politically objectionable provision like paying rent while capitalists can require contracts to include it.

The code is the law. Execution of the code is justice. And individuals are in control.

Consider the Dynamics of a Specific Crime: Fraud

Crime would still exist under blockchain justice, as it will always exist in every society, but it would be reduced to a minimum.

One of the private crimes against which crypto users require the most protection is fraud, which is a form of theft. It is certainly not the only crime but examining fraud can provide insight into how the others might be handled.

Theft is the usurpation of property without the owner's consent; that is to say, no transfer of title accompanies the actual transfer of a good. Wherever the property ends up, the title remains with the owner. If the property is taken through direct violence, such as a burglary, then a straightforward theft has occurred. If it is taken through deception, then the theft is called fraud. The fraud may consist of a false exchange of value; a person is sold a Rolex that turns out to be a cheap knockoff, for example. Or the exchange may occur on false terms; the genuine Rolex turns out to be stolen property to which the seller has no title and no rightful ownership. The seller lies; the buyer believes; the contract of sale—explicit or implicit—is invalid because the agreed-upon exchange did not occur.

Before discussing crypto fraud, however, it is important to realize that the crime may not be as common as many assume.

The Australian Competition & Consumer Commission released a report on the level and types of scams that happened in 2017. Crypto-related fraud constituted 0.6% of the total. Or, as a headline at Panda Security recently stated, "Cryptocurrency fraud is the exception, not the rule." For every scam, there are many millions of times crypto and the blockchain are used to create opportunities, grow wealth, and facilitate cooperation. Each instance of fraud seems to draw high-profile attention, however, partly because the accusations are used to call for regulation.

Paying attention to fraud is warranted, of course, but the problem requires more than attention. It requires a due diligence on the part of users that cannot be legislated. Consider the 2017 "mybtgwallet.com" scam. Mybtgwallet.com offered users free online Bitcoin Gold wallets through which they could check their balances and conduct free transactions for a limited time. The wallet was a fraud but it was lent credibility by briefly appearing on the official Bitcoin Gold site—an act of extreme carelessness at best on this site's part. To take mybtgwallet.com up on its offer, users had to submit their private keys or recovery seeds. A scam link was a hidden aspect of the process. After unwary users accepted mybtgwallet's offer, the crypto in their wallets was forwarded to other addresses. According to *Coindesk*, "more than $3.3 million has been stolen as part of an elaborate scam that took advantage of bitcoin users seeking to claim their share of the newly created cryptocurrency bitcoin gold. At least $30,000 in ethereum, $72,000 in litecoin, $107,000 in bitcoin gold and more than $3 million in bitcoin were confiscated."

No one should have fallen for this scam because no one should have surrendered their private keys, but even crypto veterans did. The fact they did so does not mean "they had it coming"; this is not the message here. A person with cash bulging out of his pockets may decide to sleep off a binge in a back alley behind the bar. His choice is foolish and dangerous, but it does not make him legally responsible if the cash is stolen. He would be the victim of a crime. Unfortunately, those who hand private keys over to strangers do the equivalent of sleeping in a back alley with bulging pockets. Such people would be well advised to develop caveat emptor habits. Part of ownership in a predatory world is to decentralize self-defense, including the defense of property.

What are some of the lessons to draw from the mybtgwallet.com debacle in order to prevent fraud? The specifics include:

- Always assume a strange site may be trying to steal crypto, your identity, your data, or all of the preceding. Extend real trust only after conducting due diligence.
- Do not deal with sites that require anything beyond the most basic personal information. Prefer those who encourage pseudonymity.
- Due diligence or not, never trust anyone with private keys or recovery seeds. This is equivalent to disclosing the combination of a safe or handing over a wad of cash for someone to hold while you run an errand. Keys and

recovery seeds are the proof and control of ownership. They constitute title to crypto.
- Never store your keys or seeds anywhere that is vulnerable to being copied or by another person.
- Always keep a paper version of both in a secure place as backup.
- In essence, maintain privacy. Thieves require access in order to loot. Leave no open doors.

Those are the specifics. The more general and fundamental point: always exercise due diligence and protect your property. These are the responsibilities of ownership. Remember: when crypto leaves a wallet, it is gone forever. At least, that should be the assumption. The transaction cannot be reversed, and few exchanges or other crypto business provide insurance against theft. Even determined victims with documented cases rarely receive back more than a few cents on the dollar, as the Mt. Gox victims did after years and years of strenuous effort.

Happily, the situation is changing due to a market need for protection. A June 2019 article on Zero Hedge commented, “Crypto prices took a hit overnight after Hong Kong-based Binance, the world's biggest crypto exchange, revealed that hackers had absconded with 7,000 bitcoins—worth roughly $41 million at current prices - stolen from the exchange's hot wallet. However, prices swiftly pared some of their losses after the exchange announced that customers wouldn't be responsible for the losses: Instead, depositors would be made whole with assets from Binance's 'Secure Asset Fund for Users'.” SAFU was established on July 3, 2018 as a market response to users’s desire for safety. Binance allocates 10% of trading fees received into a fund that is stored in a separate cold wallet in order to protect customers in “extreme cases.”

Market mechanisms, including education, minimize the damage of fraud so that unlucky or careless people can be protected. It is difficult to shield those who rush into crypto out of FOMO (fear of missing out), however, just as it is difficult to shield people who hand their lifesavings to a stranger from theft. Again, crime will always occur; the goal is to drive it down to a minimum.

For one thing when fraud does occur, people cry out for government regulation. There is a subtle and bitter irony to this dynamic. One reason people can be prone to fraud is because they approach wealth and investing with a statist mindset. That is, they are accustomed to guarantees of safety from the state. Those guarantees are illusions, but this does not matter; what matters to people’s behavior is that they believe in the guarantees. In the U.S., for example, the Federal Deposit Insurance Corporation insures the money that a person deposits into a bank for up to $250,000. Law enforcement operates fraud divisions that records reports of the crime. In short, the state makes people feel safer than they should, and this makes them neglect due diligence. The state induces people to relinquish their sense of responsibility.

The world's most fraudulent trusted third party—the state—is not a remedy. Its false guarantees come at the cost of sacrificing privacy and freedom, which are the greatest protections of all for wealth. And, in the end, the wealth still gets looted.

A Practical and Decentralized Revolution

The Satoshi Revolution is here and now. It is a practical revolution that is decentralized down the individual.

First, the practical part: Perfection is not possible for anything administered by imperfect beings. The crypto-anarchists who created Bitcoin were not only idealists but also realists who knew that the world and crypto would never be perfectly safe from violence. The state would intrude, if nothing else, and wallets would be hacked. The crypto-anarchists also knew that working toward an ideal is the one way to come as close as possible to it. The situation is similar to taking daily vitamins even though perfect health may not be attainable; vitamins and exercise will take someone as close as possible. And approaching ideals like justice is a worthwhile journey even if the destination is never quite reached.

Practical idealism has at least two utilitarian benefits. The network of principles for an ideal society are an intellectual map by which to assess whether a specific act moves closer or farther away from freedom. If free speech is one of the principles, for example, then suppressing an offensive book moves away from freedom and should not occur. An ideal is like true North on a compass. It says, "Yes, this is the correct direction." The one thing more powerful than an idea whose time has come is an *ideal* whose time has come.

The decentralization: The Satoshi Revolution is one of rising expectations; it is driven by a demand for freedom, financial privacy, and hope for the future. The revolution is occurring on an individual-by-individual basis because it is no longer necessary for people to rise up en masse, to agree on revolutionary strategies, or to coordinate events through trusted third party committees. Each user rebels without drama or ideology as he pursues self-interest, which is the strongest human motivation of all. Self-interest in *all* its forms must be the foundation of a revolution that succeeds. Anyone who stays true to Satoshi's vision of cryptocurrency becomes a freedom fighter, whether they mean to or not, because the radical decentralization of power is almost the definition of revolution.

The state remains the largest criminal of all; its power should not be underestimated but neither should it be feared. The best attitude and approach toward the state I have ever seen was that of the late Samuel E. Konkin III (SEK3), the father of agorism and an old drinking buddy of mine. SEK3 routinely answered his phone with the salutation "Smash the State"; his attitude toward the state was unfailingly rebellious. And, yet, his attitude was not the practical approach he adopted toward the state. His lifestyle did not stress direct confrontations with authority; defiance was his attitude, not his lifestyle. Whenever possible, SEK3 avoided contact and replaced whatever valuable services the state had usurped

from the free market—such as banking—with private ones. His actions were a walking-talking blueprint on how to defeat the state by eliminating it from your life because he knew that the most effective way to smash the state was to render it irrelevant and to establish private alternatives.

SEK3's lasting legacy to anarchist theory was the economic system or philosophy called agorism, which achieves peaceful revolution through counter-economics. SEK3 defined the latter as "the study or practice of all peaceful human action which is forbidden by the State." Counter-economics is a black market version of Mises's praxeology—the study of human action. It is the study of human action necessary to negate the presence of the state in personal life and society. Smash the state in attitude but replace it in daily life. Don't smash the state; bypass it.

SEK3 would have reveled in the audacity of cryptocurrency that was created with the attitude of "Smash the State" but which takes the approach of avoiding direct confrontation. He would have immediately recognized that establishing a better and free-market currency is the surest way to disempower fiat. He would have declared crypto to be "counter-economic currency"—the currency of agorism. But more than this. In a flash, SEK3 would have recognized crypto's implications for justice—precisely because it avoids and replaces state laws with the free market, privacy, and contracts. In my mind, I see SEK3 take a swig of the awful black beer he relished, followed by a drag on his constantly present pipe, before announcing "Anarchy has arrived!"

AFTERWORD

I meant to end this book by discussing the blockchain's impact on physical violence, on crimes of violence. I can't. I don't think there is an impact. I don't know how the blockchain can prevent back-alley rapes, for example. I could talk about putting sex work on an open ledger, but that would be weak tea, and it would feel like an evasion. This is a book of original theory, which explores what has never been said before about cryptocurrency. I don't always know where the ideas are taking me. But the impact on physical violence isn't one of those destinations.

And, so, I am writing the afterword to my book, instead.

My journey through cryptocurrency began in a kitchen in Chile. I was the featured speaker at a conference that also presented a panel of three experts on Bitcoin. My husband and I decided to rent a house through airbnb because we wanted to extend the couple of days into two weeks of bouncing around the country, which was magical. The house we ended up in, however, was outfitted for weddings. Translation: There were no fewer than thirty beds crammed into about twenty rooms that were linked by floors that consisted of cracked plywood below which there was a two-story drop. It wasn't a house; it was an adventure, with one working bathroom. I prefer to consider it quaint.

The conference housed the speakers and attendants on a remote compound, which quickly filled up. The organizers asked us to put up the Bitcoin experts. We gladly agreed. They were pleasant, presentable fellows—albeit men who spoke of matters that made no sense to me. Fortunately, my husband develops hardware and software for embedded systems, so I am used to not always understanding things.

And, then, there was the morning after they arrived. One fellow slept in. One insisted on cooking breakfast; I do not mean to cast aspersions upon him, because he was very pleasant and trying to be a good guest. But people do not cook around me. I cook; you eat; we get along fine. He cooked.

So I was in a cranky mood when I stared across the breakfast table into the coal-black eyes of Michael Goldstein, whom I later learned **is** the Satoshi Institute. A remarkable young man. Michael is nicknamed Bitstein by those who have affection for him…and, really, all you have to do is meet him for that to happen. When I looked into his eyes, I had an oh-so-familiar feeling because I do have mirrors in my own bathroom. “This is a fanatic,” I concluded. I happen to like fanatics, depending on the topic under discussion, of course. And I had nothing against the topic of Bitcoin, which had started to interest me because so many people I admired took it so darned seriously.

With an unwavering stare, Bitstein told me the blockchain was an open ledger that delivered anarchy. Okay. I immediately understood the power of crypto to bypass the central banking system…*if* it was widely adopted; *if* it was not outlawed, *if*… But anarchy?

All my reservations were political and entirely different than those of my husband, who joined us after about fifteen minutes. Brad waited until Michael took a breath, and then he said one word: “scalability.” It was the first time Michael stumbled. He said, “we’re working on that.” I saw Brad lose some interest.

I didn’t. I didn’t know what scalability meant in this context, except in the definitional sense. But I didn’t care because the word “anarchy” had been uttered, and *that* I knew about. Michael seemed more than happy to leave behind scalability for politics, and I pursued why he thought the dawn of freedom had arrived like the cavalry on an algorithm.

Michael answered, and he did not convince me, but he did prompt me to read. As did my old friend Jeff Tucker. As did the incredible Stephan Kinsella. Other people tried to raise my awareness, as well. Mihai Alisie, of Bitcoin Magazine, asked me to write for him on anarchism, for example. I don’t think I adequately thanked the man for having such confidence in me. And, at that point, his confidence was probably ill-founded. I submitted one article to *Bitcoin Magazine*, which was far from my best work. It drew a better response than I deserved: they were willing to “work with me.” I thanked the editor, and backed away with the absolutely genuine excuse that I did not know if I had anything original to contribute to the discussion. I had nothing new to say. I had not yet grasped the hard, cold edges of

crypto theory, and I did not understand its power. Which meant I had not yet staked out the one area where I could and can contribute something original: the integration of crypto-anarchism with the rich history of anarchist-libertarian theory that has spanned centuries.

As I read further, I became ashamed of myself. Crypto-anarchism: the most important political development in my lifetime had occurred without my noticing it happening, which is inexcusable. I had spent my time on “official” libertarianism—donation-driven and donation-defined institutes, tax-funded universities, academic journals. When did freedom ever come packaged in tax dollars, awards, and honors delivered at rubber-chicken dinners? Freedom is a street fight. Crypto-anarchism took over the streets without my noticing. I notice now.

Enter Roger Ver. Our first contact was an email that he sent out of the blue. Roger’s email “had” me at hello, because he used the word “voluntaryism.” In 1982, I was one of three people who created the modern Voluntaryist movement during a bull-session in a two-bedroom rent-controlled apartment in Hollywood, California. I remember my fingertips literally buzzing from the excitement of the ideas and plans we were forging back then: Carl Watner, George H. Smith, and me. But, mostly, Carl. It was and is almost unbelievable to me that, decades and decades later, a voluntaryist visionary named Roger would be knocking on my door (so to speak). He asked me to write for his site.

Roger had good timing. In science-fiction language, I had finally *grokked* bitcoin; I tip my hat to Robert A Heinlein for that word, BTW. I also tip my hat to Roger and the entire bitcoin.com crew for never—and I mean not once, in any manner whatsoever—trying to influence the ideas as I spun them out in my sometimes clumsy attempt to integrate crypto-anarchism into the broader traditions of classical liberalism, Austrian economics, and individualist anarchism.

Assembling the book turned into a massive rewrite followed by a period of fierce editing. The book before you now is based on the columns I serialized at bitcoin.com, but at least half of the material is new—the section on justice especially.

Before closing, I must address another aspect of crypto-anarchism. I did not expect this side benefit, but there you have it; life is often unexpected. Crypto has made me young again.

I had the immense good fortune to befriend and to spend many years with people who helped to found the modern libertarian movement. Murray Rothbard used to joke at conferences in the 1980s that libertarianism could be eliminated by one well-placed bomb. He was correct. Now it is immense.

There is a downside to my great good fortune, however. The people with whom I grew into intellectual adulthood now make me feel old, mostly because so many of them are dead; I was usually the youngest one in the room. Feeling old is feeling tired, with nothing in sight that makes your eyes sparkle.

I remember Murray, and his passion—I remember it so vividly. But, over years, something went wrong with his passion. It came from anger, I think, and it was expressed by attacking other people. I remember an after-conference dinner at which a fellow diner had the misfortune to say something positive about Keynes. And, then—God help us all!—he elaborated. Murray finally exploded into a rant in his Brooklyneque-squawk of a voice, and the fellow started to back down. I think he would have backed his chair out of the restaurant, if that had been a possibility. He conceded that Keynes may have been wrong on “this” issue, and on “that” one, and Keynes was probably weak on historical context. Murray slammed his open hand down on the table and declared, “And Hitler was ‘weak’ on the Jews!” Everyone laughed, but it was an attack, nevertheless, and a harbinger.

Crypto sparkles like a spinning thing in the sun, and the sparkle is clean, because it does not come from anger or from demeaning someone or something else. The passion is positive. A door has been flung open, and I don’t know where the path outside of it will lead me because I could never have predicted the path up to this point. Let it evolve.

One thing I know. I am in good company; the bitcoin.com crew has been nothing but decent and grinning toward this woman who plopped down into their midst. This means the world to me. I don’t know where I will end up next, but I do know that technology—not merely crypto—is going to give us all a wild ride for the rest of our lives. I will have my hands on the keyboard, trying to put the dizzy changes into historical perspective, even as they happen.

I have a chance of doing so…because I am young again. I am hopeful. And nothing, nothing is impossible. That’s what this book has meant to me. I pause in this journey to thank you for being part of it.