**PREFÁCIO**  
  
por Jeffrey A. Tucker  
  
O mundo tem precisado desse livro para que ele dê a figuração da revolução ocorrendo, e Wendy McElroy é exatamente a pessoal para escrever isso. Seu trabalho tem sido imerso na história da liberdade e da luta contra o controle autoritário. Ela traçou essa luta desde o século XIX até o presente, tendo escrito artigos pioneiros e livros a total alcance da experiência humana. Em *A Revolução Satoshi*, ela voltou a atenção dela ao que eu estou convencido de ser uma das inovações mais momentosas da história: criptomoedas e ativos e serviços relacionados. Ela explica como, em nosso próprio tempo, essa tecnologia pressagia mudanças fundamentais, grandes mudanças, na relação entre o indivíduo e o estado. Nos últimos dez anos - historiadores futuros notarão isso - observamos a criação de uma nova arquitetura monetária e financeira que poderia servir como uma substituição para tudo que tem sido conhecido e usado no tempo de vida de toda pessoa viva   
  
Experienciamos um dinheiro seguro e útil que trabalha ao redor do mundo todo, não é conectado ao estado, e não precisa do atual sistema bancário. O mesmo sistema pode servir como substituição a todo sistema atual de pagamentos que usam moedas nacionais. Esse dinheiro é puramente uma criação do mercado que adiciona às funções de contabilidade e de reserva de valoir uma característica adicional: ele é também um meio de pagamento global peer-to-peer.  
  
Uma década atrás, até mesmo teóricos de alto escalão disseram que isso não poderia acontecer. E então isso aconteceu   
  
Vimos a criação de um sistema de conrtatos inteligentes que pode gerenciar um vasto número de acordos. comprometimentos e interações humanas. Até mesmo pessoas que aceitaram que o Bitcoin era real duvidaram que a Ethereum poderia alcançar isso. Mas isso aconteceu de qualquer forma   
  
 Nós até observamos como esse sistema se tornou um instrumento para levantar capital e substituir as funções de empréstimo tradicionais. Três anos atrás, isso era meramente uma   
  
ideia especulativa. Então isso se tornou uma realidade de cem trilhões de dólares, e novas formas de cpaital sendo levnatadas através de tokenização.  
  
Aparentemente do nada, temos agora todo um conjunto de tecnologia que poderia concebivelmente deslocar e até mesmo substituir a moeda nacional, opções de pagamento tradicionais, e até mesmo mercados de capitais regulados, e trazer algo novo.  
  
Você está lendo isso e pensando: aqui vamos nós de novo com o cripto-utopismo. Mas aqui está a coisa. Não é mais apenas uma teoria. Essas tecnologias existem em tempo real, mesmo se somente em seus estágios iniciais. É por issoque há tantos bitcoiners por aí que falam tão exuberantemente sobre o futuro. Eles já experienciaram isso. Há motoristas de Maseratis nas estradas cheios de Modelos T e eles sabem disso. Uma melhoria do status quo que é tão impressionante não será suprimida.  
  
Você pode não ter usado qualquer uma dessas novas tecnologias. E está tudo bem com isso. Com todas as falhas do atual sistema, as antigas estruturas terminam seu trabalho. Na medida em que há uma grande crise no sistema, as pessoas confiam nele. Não há razão forte para mudar, mesmo qse o novo sistema for mais seguro, mais rápido, mais democrático, inclusive e menos arriscado e menos comprometedor da privacidade individual. Ainda assim, o antigo sistema goza do impulso que vem a partir do efeito de rede. Todos os outros usam isso, então você continua usando isso   
  
**Regulação é a Chave**  
  
Há outro fator que está atrasando a mudança do antigo pro novo. As regulações estão tentando forçar a nova tecnologia para se comportar como tecnologia antiga. Nos Estados Unidos, para comprar Bitcoin ou qualquer criptomoeda, você precisa cumprir com regulações know-your-customer, cedendo cada detalhe sobre a sua pessoa. Qualquer dinheiro que você faça de movimentos de preço em ascensão em seu noo acesso precisa ser registrado e você precisa pagar impostos sobre ele. Companhias que desejam assistir no onboarding e no offboarding de cripto para moeda fiduciária têm de se registrar ao governo como casas de câmbio. E, com as funções de alavancamento de capital da tecnologia blockchain, os reguladores estão ameaçando acabar com todas e fazê-las se comportar com títulos tradicionais.  
  
Eu vi essas regulações sendo gradualmente impostos e sendo arbitrariamente impostas, tem introduzido um elemento de medo em uma tecnologia sem medo, distorcendo o setor e fazendo dele menos inovativo e competitivo. Toda vez que um novo uso de redes distribuidas é revelado e começa a engajar, alguns manda-chuvas surgem do chão para advertir sobre a conformidade com leis de décadas atrás designadas para diferentes tecnologias.  
  
Os consumidores ficam co memdo e e a experiência de usuário final não é aprimorada o tanto quanto ela poderia ter sido na ausência de tantos custos de conformidade. Eu vi o quanto que a incerteza legal fez com que os mercadores e os consumidores percam acesso a uma variedade de serviços. Eu vi empreendedores porem seus planos em suspenso esperando algum édito administrativo vindo de Washington, DC.  
  
O quão mais avançados estaríamos no caso da ausência dessas regulações? É impossível ver as inovações que não experienciamos. Sabemos apenas que as coisas seriam diferentes. Mas uma vez que você considera o quão diferente, a realidade se torna algo além do incrível. E ainda não é para ser.  
  
**Quanto Tempo a Demora?**  
  
Considere oque acontece quando o poder é usado para parar o progresso de uma nova tecnologia. Isso realmente funcionaria no longo prazo? Para responder a questão, temos de engajar em contrafatos.  
  
Imagine se os governos na Europa tivessem se empenhado para parar a prensa. E se as cidades ao redor do mundo tivessem banido os automóveis? Qual teria sido o destino das ferrovias, da iluminação doméstica e do encanamento fechado se interesses especiais tivessem-los suprimidos em favor das tecnologias prevalecentes?  
  
Podemos apenas chutar, porque nada disso realmente aconteceu É verdade que nem todo mundo recebeu bem a prensa. Escribas em monastérios se preocuparam com o futuro de seus talentos. Algumas pessoas perguntaram se a velha fé poderia sobreviver às pessoas tendo acesso aos textos antigos. Mas, na maior parte, o advento da prensa foi visto como uma inovação bem-vinda. Assim também com a combustão interna, eletricidade e encanamento. Algumas pessoas foram devagares em adotar eles, para ter certeza, mas os governos em sua maioria deixaram a inovação acontecer.  
  
E se eles não tivessem? Alguém realmente acredita que essas inovações poderiam ser paradas e não meramente atrasadas? Eu penso que não. Há casos na história em que garantias de monopólios por parte do governo retardam os competidores de adetrarem no mercado com melhorias. Isso aconteceu com os navios a vapor na Inglaterra, com os aviões nos EUA, e com algumas aplicações de software nas últimas décadas. Mas esses retardamentos são temporários; patentes expiram e a história vai para frente.  
  
Regulações são diferente. Os empreendedores têm de inovar ao redor delas. Os mercados cinza e negro emergem. Tomadores de risco lidam com o conflito com as autoridades. Mas, eventualmente, alguém cede. Considere, por exemplo, os resultados se todo lorde e barão na Europa do século XII tivesse banido a ferradura. Você acha que isso teria parado a implementação dessa tecnologia por séculos? Altamente duvidoso, e a razão é fundamental: ideias são mais fortes que governos. Eventualmente, os custos de imposição excedem vastamente os benefícios da classe governante existente.  
  
**Um Mundo Criptonizado**  
  
À luz do que temos visto durante por dez anos, aqui está um experimente mental com o qual eu vim brincando. Ele ocorreu a mim enquando eu estava devaneiando enquanto meu advogado tributário estava me explicando há muito sobre eventos tributáveis nos acordos cotidianos com cripto. Eu estava considerando o quão incompatíveis eram essas imposições com uma tecnologia que emergiu de e opera dentro de uma estrutura de perfeita libertação.  
  
Algumas legislações vieram entender isso. O Wyoming, por exemplo, isentou a cripto de toda tributação, definiu certos tokens de um modoq ue faz deles isentos de leis de títulos, e fazem provisões especiais para formas corporativas que são distribuidas, entre outras mudanças. A legislação fez o seu melhor para fazer o estado atrativo para essa nova indústria.  
  
Agora, deixe-nos entrar no campo da fantasia. Digamos que o congresso dos EUA passou uma legislação que isentou toda criptomoeda, todo criptotrading e criptoativos de toda tributação e regulação. A legislação estabelece laissez-faire completo nesse setor, enquanto todo o resto no mundo normal (o dolar, o Fed, a SEC, o Tesouro, e todo o resto que conhecemos) permaneceria o mesmo.  
  
O que você acha que aconteceria? Dez anos atrás, tivesse o Congresso feito a mesma cosia, não muito teria mudado, obviamente. A tecnologia não existia, e nós realmente não sabiamos que ela poderia existir.  
  
O que aconteceria hoje se todas intervenções ao redor dessa tecnologia fossem repelidas? Você não é mais punido por comprar e vender em cripto, emitir novos tokens, desenvolver novos aplicativos em plataformas de contrato inteligente, inovar novos sistemas de pagamentos e assim em diante. Companhias poderiam tokenizar em vez de flutuar estoque. Os negócios poderiam pagar em cripto e fazer sua contabilidade em cripto e enfrentar nenhuma penalidade. Considere com cuidado: você poderia manter um terço a mais dos seus ganhos justos simplesmente mudando para uma melhor tecnologia.  
  
Quanto tempo levaria para a criptoeconomia substituir todo o resto? Se essa mudança legislativa realmente acontecesse - e não, obviamente não vai - poderíamos observar o deslocamento do atacado dos sistemas econômicos e financeiros do velho mundo com os sistemas do século XXI, e talvez isso aconteceria muito mais cedo do que qualquer poderia esperar, talvez de 12 a 48 meses, dado que a infraestrutura da cripto poderia escalar a tempo de satisfazer a nova demanda.  
  
**Forçando o Passado no Presente**  
  
Agora, se esse experimento mental está correto, há algumas implicações poderosas. Isso sugere que o mundo financeiro e monetário, tal como existe hoje, está sendo mantido junto pela força que está nos prendendo às velhas formas. Essa força está impondo limitações e ineficiências; ela está literalmente mantendo uma vasta infraestrutura no lugar que de outro modo poderia cessar de dominar ou até de existir, e impedindo o início de um novo modo de viver. E esse novo modo não é somente sobre comprar e vender. Tão central para nossas vidas públicas são a moeda nacionalizada e os mercados de capital regulados que o advento de um mundo criptonizado mudaria fundamentalmente a relação do indivíduo com o estado.  
  
Estaria eu errado em estar maravilhado com essa percepção?  
  
Manter um sistema vasto vivo apenas pela força não me parece tão sustentável no longo prazo. Se você possui um conjunto massivo de tecnologia que está esperando para assumir o controle  
  
 e está apenas sendo atrasado por meios puramente artificiais, isso não soa bem para a probabilidade de que o passado poder sempre ser preservado. O futuro não pode para sempre ser adiado mesmo pelos governos mais poderosos do mundo. Eventualmente as ideias vencem.  
  
Wendy McElroy, a partir de seus estudos passados de história e de seu mergulhoi profundo na cripto-tecnologia, entende o poder das ideias. O bitcoin e todo que é relacionado a ele estão entre as ideias mais revolucionárias na história. Ela demonstra como eles vão transformar para melhor a estrutura da economia, da política, e das relações humanas num geral. Ir daqui para lá requer o entendimento mais amplo possível do que está acontecendo. McElroy é a guia expert e erudita pela qual estávamos esperando.  
  
JEFFREY A. TUCKER é Diretor Editorial pelo American Institute For Economic Reserarch e antigo Diretor de COnteúdo pela Foundation for Economic Education. Ele é parceiro de gestão da Vellum Capital: Blockchain Financial Managetment, o fundador da Liberty.me, Membro Honorário Distinto do Mises Brasil, conselheiro econômico para a FreeSociety.com, companheiro de pesquisa no Acton Institute, conselheiro político do Heartland Institute, fundaor da CryptoCurrency Conference, membro da bancada editorial da Molinari Review, um conselheiro para o desenvolvedor de aplicativos blockchain Factom. Ele é o autor de milhares de artigos na imprensa acadêmica e popular e é autor de oito livros em oito línguas, o mais recente sendo [The Market Loves You](https://www.amazon.com/dp/1630691682/ref=sr_1_fkmrnull_1). Ele fala amplamento sobre economia, tecnologia, filosofia social, e cultura   
  
**INTRODUÇÃO**  
  
Você nunca muda as coisas lutando contra a realidade existente. 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](https://news.bitcoin.com/rutgers-bitcoin-study-ideal-system-misunderstood-public/) 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](https://blog.blockchain.com/2014/12/29/drawing-the-distinction-between-the-uppercase-b-and-lowercase-b-in-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](https://mises.org/library/conceived-liberty-4)), 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](https://news.bitcoin.com/bitcoin-built-incite-peaceful-anarchy/) 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](https://www.fff.org/explore-freedom/article/revolution-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 [solve](https://news.bitcoin.com/the-slow-criminalization-of-peer-to-peer-transfers/)s 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](https://www.bitcoin.com/bitcoin.pdf) , “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](https://news.bitcoin.com/decentralize-life-tour-interview-derrick-broze/), 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](http://www.wendymcelroy.com/soceng.htm) 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](http://files.libertyfund.org/pll/quotes/328.html). 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](https://news.bitcoin.com/bitcoin-bill-rights/) 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.