Introduction

IN 1988, Timothy May, one of the founding members of the "cypherpunk" movement, warned that "[a] specter [was] haunting the modern world."[1] This specter was not political gridlock, terrorism, racial strife, or an environmental crisis. Rather, it was the growth and expansion of a new form of anarchy, which May defined as "crypto anarchy."[2] As May described in his "Crypto Anarchist Manifesto," the Internet and advances in public-private key cryptography would soon enable individuals and groups to communicate and interact with one another in a more anonymous manner. By relying on untraceable networks and "tamper-proof boxes implement[ing] cryptographic protocols," people would gain the ability to "conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other."[3]

In the end, May predicted that individuals would be liberated from the state, completely altering "the nature of government regulation, the ability to tax and control economic interactions, [and] the ability to keep information secret," along with our very notions of trust and reputation.[4] Cryptographically secured protocols would dismantle the "barbed wire" created by intellectual property, breaking open the flow of information, imbuing individuals with a newfound ability to self-organize, and changing the very nature of corporations and governments.[5] In May's view, the spread was inevitable. The "genie was out of the bottle," as he explained in later writings, and there was nothing to halt the unstoppable wave of technologically induced anarchy.[6]

Blockchains are, in many ways, the "tamper-proof boxes" envisioned by May nearly thirty years ago. They blend together several existing technologies, including peer-to-peer networks, public-private key cryptography, and consensus mechanisms, to create what can be thought of as a highly resilient and tamper-resistant database where people can store data in a transparent and nonrepudiable manner and engage in a variety of economic transactions pseudonymously. Blockchains are enabling the transfer of digital currencies and other valuable assets, managing title to property and sensitive records, and—perhaps most profoundly—facilitating the creation of computer processes known as *smart contracts,* which can execute autonomously.[7]

Blockchains operate differently than earlier databases in that they are not centrally maintained. They are collectively managed by a peer-to-peer network comprised of computers (known as "peers" or "nodes"), often scattered across the globe.[8] These nodes store exact or nearly exact copies of a blockchain and coordinate by using a software protocol that precisely dictates how network participants store information, engage in transactions, and execute software code.

Because blockchains are widely replicated, any data stored in a blockchain is highly resilient and can survive even if a copy of a blockchain is corrupted or if a node on a network fails. So long as a valid copy of a blockchain exists somewhere in the world, a blockchain can be restored and replicated by others to retrieve past records and engage in new transactions.

To ensure the orderly recordation of information and to enhance a blockchain's security, every blockchain incorporates a *consensus mechanism*—a set of strict rules with predefined incentives and cost structures—which makes it difficult and costly for any one party to unilaterally remove or modify data stored on a blockchain. Consensus mechanisms help a blockchain-based network periodically reach agreement as to the current state of the shared database—even if members do not know or trust one another.

By weaving in public-private key cryptography, each blockchain validates the integrity of data recorded to a blockchain and enables people to engage in transactions pseudonymously, without necessarily revealing their true identity.[9] Because blockchains are not centrally maintained, no single party necessarily needs to control access to them. By implication, on publicly accessible blockchains, anyone can create a blockchain-based account—comprised of a public address and a private key, a password—and engage in transactions with others with limited fear of third-party intervention.[10]

More advanced blockchains also integrate decentralized computing systems—in other words, a distributed virtual machine—and Turing-complete programming languages enabling parties to write and deploy smart-contract programs.[11] These programs are stored on a blockchain and executed by multiple members of a blockchain's underlying peer-to-peer network, creating computer processes that are autonomous and potentially difficult to shut down once deployed.

Since the launch of Bitcoin in 2009, blockchains have underpinned an array of online services that seek to use the technology to store information and run computer processes. Some of these applications aim to fulfill May's vision, while others help enhance existing lawful services.

As Bitcoin has demonstrated, blockchain technology supports decentralized, global value transfer systems that are both transnational and pseudonymous. Using a blockchain, anyone can exchange digital currencies, such as bitcoin, or other valuable assets, without the need to rely on a centralized clearinghouse and without affirmatively disclosing their identity. Blockchains are sitting behind novel peer-to-peer remittance systems that decrease the cost of sending funds abroad, and the technology has found an early foothold in the financial services industry, powering new decentralized systems that strike at the heart of global finance, including decentralized securities and derivatives exchanges.

In just a few years, the reach of blockchains has rapidly expanded beyond payments and financial products, helping to support new, autonomous systems that structure social and economic interactions with less of a need for intermediaries. Smart contracts are being used to memorialize all or parts of legal agreements, creating commercial arrangements that are dynamic and potentially harder to terminate.

Governments across the globe are experimenting with blockchains to secure and manage critical public records, including vital information and titles or deeds to property. By leveraging the tamper-resistant, resilient, and nonrepudiable nature of a blockchain, governments are looking to guarantee—with a high degree of probability—the integrity and authenticity of key governmental information. Over time, blockchains could anchor new public infrastructure and potentially even global and transnational systems, available to anyone with an Internet connection.

Blockchains also are beginning to structure collective endeavors, including new forms of digital organizations administered—at least in part—by code.

Because blockchains are widely accessible and can facilitate economic transactions, they are being explored to manage the operations of existing legal entities, serving as a central point of coordination, with smart contracts implementing code-based rules that could decrease the cost and difficulty of managing group activity. Blockchains are even powering new forms of organizations that are more transparent and less hierarchical, helping disparate groups of individuals come to an agreement without having to know one another. Because blockchains enable the execution of autonomous code, over time, they may also provide the infrastructure to create organizations that rely entirely on algorithmic systems and artificial intelligence (AI) to manage group activity. These organizations would not rely on humans for their management but, rather, would lean on code-based rules and other means of algorithmic governance to structure their operations.

Extending beyond the potential to coordinate human activity, blockchains are increasingly being used to control devices and machines, with smart contracts defining the operations of these Internet-connected devices. Eventually, blockchains may mature into a foundational layer that helps machines engage in economic transactions with humans as well as with other machines. If these attempts are successful, blockchains could ultimately be used to manage an increasing range of activities, fostering a new era of machine-to-machine and machine-to-person interactions that could potentially change the very nature of our relationships with physical goods.

However, not all blockchain-based applications and services strictly comply with existing laws and regulations. Blockchain-powered digital currencies operate transnationally and often ignore existing regulations regarding money transmission and money laundering, as well as laws aimed at helping governments, banks, and other private parties track the flow of money across the globe. If not properly regulated, these emerging technologies could be used to commit fraud and engage in money laundering, terrorist financing, or other illicit activities.[12]

Blockchains also are taking a bite out of public markets, enabling parties to sell billions of dollars of cryptographically secured "tokens"—some of which resemble securities—and trade derivatives and other financial products by using autonomous and unregulated code-based exchanges. These blockchain-based systems often ignore legal barriers supporting existing financial markets and undercut carefully constructed regulations aimed at limiting fraud and protecting investors.

Outside of the financial world, blockchains have been used to support applications that skirt restrictions on online gambling and e-commerce transactions, supporting highly automated casinos—untethered from the control of a central party—and decentralized e-commerce marketplaces that facilitate the buying and selling of goods without relying on eBay, Craigslist, or even the Silk Road. These applications help facilitate the sale of drugs and could, with sufficient adoption, break down governmental restrictions on vices and other unpalatable social activity.

Blockchains are further helping to crack open the flow of information, powering new peer-to-peer file-sharing applications, decentralized communication platforms, and social networks, which rely on the tamper-resistant and resilient nature of a blockchain—and other peer-to-peer networks—to disseminate copyright-protected, inflammatory, and indecent material. If widely used, these services could frustrate governmental and corporate attempts to control, filter, and censor information online, without regard for the social and political costs this might entail.

If blockchains improve in terms of speed, performance, functionality, and accessibility, the technology may over a longer time horizon begin to structure organizations that compete with traditional corporations and other legal entities, and perhaps even lead to the emergence of autonomous devices and robots that operate independently of any third party—free from the control of governments and intermediary operators.

As we argue in this book, the ability of blockchains to facilitate and support autonomous systems will increasingly create challenges for states and regulators seeking to control, shape, or influence the development of blockchain technology. Like many other technologies, blockchains can be deployed both to support and undercut existing laws and regulations, but what makes the technology particularly potent is its ability to facilitate the creation of resilient, tamper-resistant, and automated code-based systems that operate globally, providing people with new financial and contractual tools that could replace key societal functions.

With blockchains, people can construct their own systems of rules or smart contracts, enforced by the underlying protocol of a blockchain-based network. These systems create order without law and implement what can be thought of as private regulatory frameworks—which we will refer to throughout the book as *lex cryptographica*.[13] They endow software developers with the power to create tools and services that avoid jurisdictional rules and operate transnationally to coordinate a range of economic and social activities.

Lex cryptographica differs from the existing systems of code-based rules implemented by today's online applications.[14] Currently, most online services generally either act as an intermediary or rely on other intermediaries—such as large cloud-computing providers, search engines, payment processors, domain name registrars, and social networks—to support their services. These intermediaries have the power to impose and enforce laws and their own rules, and to the extent that they are easily identifiable and located in a particular jurisdiction, they also serve as central points of control for regulatory authorities.[15]

Systems deployed on a blockchain—relying primarily or exclusively on *lex cryptographica*—will be harder to control and regulate. Blockchains reduce the need for intermediaries and create systems governed by protocols and other code-based rules, which are automatically enforced by the underlying blockchain-based network. Through the use of a blockchain and associated smart contracts, new online applications can be designed to be highly autonomous and increasingly independent of the whims of centralized intermediaries. These applications are made of nothing more than code and are executed by a blockchain-based protocol in a distributed manner—irrespective of whether they comply with the law—creating tensions with legal regimes focused on regulating centralized intermediaries that currently control or help facilitate social and economic activity online.

Despite showing great promise, blockchain-based networks run the risk of creating discrete risks that could destabilize central banking, financial markets, and the administration of commercial agreements, and support new forms of unlawful activity. These risks are particularly acute because the technology is being deployed to rework fundamental systems and institutions that define modern society, including payment systems, financial markets, commercial agreements, and many of the organizational structures that populate our society.

Today, the focus of societal governance is imposed largely by institutions and bureaucratic systems, which rely on laws and hierarchy to order society.[16] Blockchain-based applications do not depend on these rules to structure their functions; instead they depend on *lex cryptographica* to organize economic and social activity.[17]

As the technology further matures, blockchains could accelerate a structural shift of power from legal rules and regulations administered by government authorities to code-based rules and protocols governed by decentralized blockchain-based networks. Code-based protocols and decisions related to their development would ultimately dictate how these systems work and shape our means of interaction. We could increasingly subject ourselves to the "rule of code"—code that may not be controlled by any one party and that may or may not operate in accordance with the "rule of law."[18]

Our book explores the emerging uses of blockchain technology, describing its perceived benefits and challenges, and the contours of *lex cryptographica.* We refute the idea that blockchains will lead to the crypto anarchy envisioned by its presumed creators, and we outline strategies to regulate the technology.

When the Internet first emerged, it, too, inspired notions of anarchy and lawlessness. As best described by John Perry Barlow in his 1996 manifesto "A Declaration of the Independence of Cyberspace," the Internet was initially perceived as a new world where traditional "legal concepts of property, expression, identity, movement, and context [would] not apply."[19] This world would be populated by "netizens" relying on this decentralized network to organize and govern their own affairs, without interference from centralized authorities.[20]

However, as the Internet matured, Barlow's vision came to be regarded as a mere utopian dream. Although the original design of the Internet sought to decentralize power and encourage freedom of communication—even at the expense of spam, fraud, and crime—over the past decade, it has become increasingly concentrated and regulated. The emergence of mobile phones, app stores, and cloud computing platforms has led to the establishment of a more centralized network, dominated by a handful of corporations that control the flow of information and economic transactions.[21]

Today, the anarchic tendencies of the Internet have largely been tamed. By focusing the locus of regulation on Internet service providers (ISPs) and large intermediaries involved in the creation and deployment of Internet-based services, states have increasingly delegated to these operators the task of policing the Internet.[22] Some countries, particularly in Europe, have even started to balkanize the Internet, implementing data localization requirements to prevent foreign companies from collecting and storing information about their citizens.[23] Countries such as China, Russia, North Korea, and

Iran have gone even further, deploying national firewalls to create an Internet free from Western influence or domestic dissent.[24]

We argue that the growth and development of blockchain technology will follow a similar path. Even though blockchains create increasingly autonomous and potentially lawless systems, there are still means to shape and control their use and deployment. Blockchains may reduce the need for intermediaries, but they are unlikely to eliminate them altogether. Even assuming *arguendo* that blockchains lead to widespread disintermediation, laws, market forces, social norms, and code itself could be leveraged to preserve the rule of law.

Governments will have a number of tools at their disposal to shape or distort the technology as it develops and gains increasing acceptance. They can regulate end users, holding them liable for any illicit activity facilitated by using these systems or even for supporting a blockchain-based application. Alternatively, or in addition to that, they can place increased pressures on software developers maintaining these systems, hardware manufacturers, and intermediaries operating lower on the TCP/IP stack.

For instance, governments can apply regulations on ISPs and information intermediaries—such as search engines—and require that these intermediaries purposefully block or avoid indexing a number of illegitimate blockchain-based applications. They can regulate the parties that support and maintain blockchain-based networks ("miners") and the software developers or hardware manufacturers that provide the tools needed for these networks to operate. Regulation of these parties can be achieved either directly, by imposing certain rules on these actors, or indirectly, by changing their underlying economic incentives and payoff structures.

Blockchains are still immature. Governments thus could shape emerging social norms relating to the technology through education, formal international working groups, or other informal means of discussion and deliberation. They also could rely on blockchain technology itself to achieve specific policy objectives, encoding certain laws and regulations into a blockchain-based network and associated smart contracts.

This book explores the dual nature of blockchain technology, describes the emergence of *lex cryptographica,* and outlines potential avenues for regulation. We assume no knowledge of blockchain technology, so we first provide a detailed history and technical overview, explaining the birth of Bitcoin and Ethereum and other related technologies. We then distill the core characteristics of a blockchain and explain why these characteristics facilitate *lex cryptographica* and push us toward increasing algorithmic control and the rule of code. Next, we map how—through the implementation of *lex cryptographica*—blockchains both support and undermine existing laws, and how the technology is poised to impact current social and political institutions in a variety of contexts, ranging from payments, contract law, and finance to information and communication systems or machine-to-machine interactions.

After describing the legal challenges raised (and faced) by blockchain technology, we outline how blockchain-based systems can be regulated, along with the costs of doing so. We end by peering into the future, examining how blockchain technology could support or complement the law by turning all or parts of laws into code, and we explore some of the dangers of this regulatory path. Our goal is to provide an understanding of how blockchains work, the potential uses for the technology, the distinctive characteristics of *lex cryptographica,* and the potential avenues for regulation.