DECENTRALIZED BLOCKCHAIN TECHNOLOGY AND THE RISE OF *LEX CRYPTOGRAPHIA*

Aaron Wright[*] *& Primavera De Filippi*[**]

Just as decentralization communication systems lead to the creation of the Internet, today a new technology—the blockchain—has the potential to decentralize the way we store data and manage information, potentially leading to a reduced role for one of the most important regulatory actors in our society: the middleman.

Blockchain technology enables the creation of decentralized currencies, self-executing digital contracts (smart contracts) and intelligent assets that can be controlled over the Internet (smart property). The blockchain also enables the development of new governance systems with more democratic or participatory decision-making, and decentralized (autonomous) organizations that can operate over a network of computers without any human intervention. These applications have lead many to compare the blockchain to the Internet, with accompanying predictions that this technology will shift the balance of power away from centralized authorities in the field of communications, business, and even politics or law.

In this Article, we explore the benefits and drawbacks of this emerging decentralized technology and argue that its widespread deployment will lead to expansion of a new subset of law, which we term Lex Cryptographia*: rules administered through self-executing smart contracts and decentralized (autonomous) organizations. As blockchain technology becomes widely adopted, centralized authorities, such as governmental agencies and large multinational corporations, could lose the ability to control and shape the activities of disparate people through existing means. As a result, there will be an increasing need to focus on how to regulate blockchain technology and how to shape the creation and deployment of these emerging decentralized organizations in ways that have yet to be explored under current legal theory.*

---

[*] Assistant Clinical Professor of Law and Director of the Cardozo Tech Startup Clinic, Benjamin N. Cardozo School of Law, Yeshiva University; Founder/Director of the Cryptocurrency Research Group.

[**] Research fellow at the Berkman Center for Internet and Society at Harvard Law School and associate researcher at the CERSA / CNRS / Université Paris II.

INTRODUCTION

We stand at the edge of a new digital revolution. The Internet is beginning a new phase of decentralization.[1] After over twenty years of scientific research, there have been dramatic advances in the fields of cryptography and decentralized computer networks, resulting in the emergence of a profound new technology—known as the blockchain—which has the potential to fundamentally shift the way in which society operates.[2] The blockchain is a distributed, shared, encrypted database that serves as an irreversible and incorruptible public repository of information. It enables, for the first time, unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority.[3]

Blockchain technology has the potential to reduce the role of one of the most important economic and regulatory actors in our society—the middleman. By allowing people to transfer a unique piece of digital property or data to others, in a safe, secure, and immutable way, the technology can create: digital currencies that are not backed by any governmental body; self-enforcing digital contracts (called *smart contracts*), whose execution does not require any human intervention; decentralized marketplaces that aim to operate free from the reach of regulation;[4] decentralized communications platforms that will be increasingly hard to wiretap; and Internet-enabled assets that can be controlled just like digital property (called *smart property*).[5]

Many compare the emergence of the blockchain to another revolutionary technology, the Internet,[6] and predict that this technology will

---

[1] As defined by Yochai Benkler, "'[d]ecentralization' describes conditions under which the actions of many agents cohere and are effective despite the fact that they do not rely on reducing the number of people whose will counts to direct effective action." *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS 62 (2006) (hereinafter "Wealth of Networks"). This differs from "centralization," which "is a particular response to the problem of how to make the behavior of many individual agents cohere into an effective pattern or achieve an effective result." *Id.*

[2] *See* Part I, *infra.*

[3] *See id.*

[4] *See* Part III, *infra.*

[5] *See id.*

[6] Prominent venture capitalists such as Marc Andreessen of Andreessen Horowitz and Albert Wenger of Union Square Ventures have analogized the anticipated impact of the blockchain to that of the personal computer in the 1970s and the Internet in the mid-1990s. *See* Marc Andreessen, *Why Bitcoin Matters*, N.Y. TIMES DEALBOOK (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/; Albert Wegner, *Bitcoin as a*

shift the balance of power away from centralized authorities in the field of communications,[7] business,[8] and even politics or law.[9] The blockchain has the potential to usher in a new era characterized by global payment systems, digital assets, decentralized governance, and even decentralized legal systems.[10] It enables collective organizations and social institutions to become more fluid and promote greater participation, potentially transforming how corporate governance and democratic institutions operate. The technology could impact capital markets, by enabling everyday citizens to issue financial securities using only a few lines of code.

Beyond these opportunities, the blockchain has the possibility to fundamentally change the way people organize their affairs. The technology can be used to create new software-based organizations referred to as *decentralized organizations (DOs)* and *decentralized autonomous organizations (DAOs)*.[11] These organizations can re-implement certain aspects of traditional corporate governance using software, enabling parties to obtain the benefits of formal corporate structures, while at the same time maintaining the flexibility and scale of informal online groups. These organizations also can be operated autonomously, without any human involvement. They can own, exchange, or trade resources and interact with other humans or machines, raising novel questions around traditional notions of legal personality, individual agency, and responsibility.[12]

In this Article, we outline the potential benefits of blockchain technology, while also exploring the concrete challenges that this technology presents to law enforcement, how we contract, and how we envision property rights in a world that will be increasingly connected to the Internet. We also question whether this technology will enable the creation of advanced forms of digital rights management and, even worse,

---

Protocol, UNION SQUARE VENTURES BLOG (Oct. 31, 2013), https://www.usv.com/posts/bitcoin-as-protocol. This sentiment has been confirmed by large US companies, such as IBM, which have indicated that the blockchain could be as large as the Internet itself. *See* Finextra, *Inverview of Richard Brown, IBM, Executive Architect for Banking and Financial Markets Industry Innovation*, YOUTUBE (Nov. 6, 2013), https://www.youtube.com/watch?v=VDO7TDMlxsY.

[7] *See*, MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY 19 (2015).

[8] *See* Andreessen, *supra* note 6.

[9] *See*, Chris Dixon et al., *Beyond Bitcoin: The Blockchain*, A16Z ACADEMIC ROUNDTABLE 2014 (Oct. 24, 2014), http://a16z.com/2014/10/24/the-bitcoin-network-effect/.

[10] *See* Parts II, *infra.*

[11] *See id*.

[12] *See id.*

algorithmic governance systems that may eliminate many of our fundamental freedoms.

We further maintain that blockchain technology raises a series of novel legal questions that refer to a new body of law—which we term *Lex Cryptographia*—or rules administered through self-executing smart contracts and decentralized (autonomous) organizations. Legal theory has predominantly focused on the struggle between the individual, the state, and the market, seeking to harmonize competing power dynamics and trying to find the appropriate balance between the interests of the public sphere, eager to preserve public order and national security, and the interests of the private sphere, characterized by the need to support economic growth, while promoting individual autonomy and fundamental rights.[13]

Traditional conceptions of Internet regulation need to be re-examined in a world inhabited by decentralized applications, encrypted communication channels, and autonomous agents. If blockchain technology becomes more widely adopted, centralized authorities, such as governmental agencies and large multinational corporations, may lose the ability to control and shape the activities of disparate people through existing means. As a result, there will be an increasing need to focus on how to regulate this new technology and how to shape the creation and deployment of decentralized (autonomous) organizations.

This Article unfolds in four parts. Part I provides a technical overview of blockchain technology. Parts II outlines the emerging uses of this technology. Part III articulates the future impact it might have on society and the many risks the blockchain might pose to current legal regimes and government action. Finally, Part IV outlines some preliminary principles on how to regulate decentralized blockchain technologies, in ways that protect fundamental rights, while at the same time ensuring the promotion of economic growth, democratic institutions, and the continued protection of individual liberties.

I. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Blockchain technology represents the next step in the peer-to-peer economy.[14] By combining peer-to-peer networks, cryptographic algorithms,

---

[13] *Id.*

[14] The peer-to-peer economy refers to "decentralized individual action—specifically, new and important cooperative and coordinate action carried out through radically distributed,

distributed data storage, and a decentralized consensus mechanisms,[15] it provides a way for people to agree on a particular state of affairs and record that agreement in a secure and verifiable manner.

Prior to the invention of the blockchain, it simply was not possible to coordinate individual activities over the Internet without a centralized body ensuring that no one has tampered with the data. A group of unrelated individuals could not confirm that an event had occurred without relying on a central authority to verify that this particular transaction was not fraudulent or invalid. In fact, many computer scientists did not believe that distributed group of people could reach consensus without a common clearinghouse. This notion is encapsulated in a well-known computer science problem from the early 1980s, commonly referred to as the "Byzantine Generals Problem."[16] This problem questioned how distributed computer systems could reach consensus without relying on a central authority, in such a way that the network of computers could resist an attack from ill-intentioned actors.[17] It posits that three divisions of the Byzantine army are camped outside an enemy city in hopes of conquering it. An independent general commands each division and, in order to plan an

---

nonmarket mechanisms that do not depend on proprietary strategies" *See* Wealth of Networks, *supra* note 1, at 3.

[15] In a sense, blockchain technology is not a huge technological advance. It is an incremental improvement. Public-private key encryption was developed in the late 1970s. *See* Whitefield Diffie & Martin E. Hellman, *New Directions in Cryptography*, 22 IEEE TRANSACTIONS ON INFORMATION THEORY 644 (1976) (introducing the concept of public key cryptography); R.L. Rivest et al., A *Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, http://people.csail.mit.edu/rivest/Rsapaper.pdf. Peer-to-peer networks have also been used since late 1970s, and gained mainstream acceptance in the early 2000s. *See* ANDREW ORAM, PEER-TO-PEER: HARNESSING THE BENEFITS OF A DISRUPTIVE TECHNOLOGY 4-5 (2001) (providing a history of peer-to-peer applications online and noting that Usenet, introduced in 1979, was the "grandfather of today's peer-to-peer networks."). Consensus mechanisms, such as Proof of Work, described in Part I *infra* have been around since the late 1990s. *See* Adam Back, *A Partial Hash Collision Based Postage Scheme*, http://www.hashcash.org/papers/announce.txt (describing a proof of work system to eliminate email spam). Decentralized, distributed data storage, like that offered by the popular source code management system Git, has been used for nearly a decade. *See A Short History of Git*, GIT, http://git-scm.com/book/en/v2/Getting-Started-A-Short-History-of-Git.

[16] Leslie Lampert et al., *The Byzantine Generals Problem*, 4 ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS at 382 (July 1982).

[17] *Id.* at. 384 ("The Byzantine Generals Problem seems deceptively simple. Its difficulty is indicated by the surprising fact that if the generals can send only oral messages, then no solution will work unless more than two-thirds of the generals are loyal. In particular, with only three generals, no solution can work in the presence of a single traitor.").

attack, they need to decide upon a common course of action.[18] Yet, the generals can only communicate with one another through a messenger, and there is a traitor in the group who is actively trying to prevent the generals from reaching an agreement by either tricking them into attacking prematurely or concealing some relevant information so that the generals cannot plan a coordinated attack.[19]

A blockchain solves this problem through a probabilistic approach.[20] It forces information traveling over a network of computers to become more transparent and verifiable using mathematical problems that require significant computational power to solve. This makes it harder for potential attackers to corrupt a shared database with false information, unless the attacker owns a majority of the computational power of the entire network.[21] Blockchain protocols thus ensure that transactions on a blockchain are valid and never recorded to the shared repository more than once, enabling people to coordinate individual transactions in a decentralized manner without the need to rely on a trusted authority to verify and clear all transactions.[22]

A blockchain is simply a chronological database of transactions recorded by a network of computers.[23] Each blockchain is encrypted and organized into smaller datasets referred to as "blocks."[24] Every block contains information about a certain number of transactions, a reference to

---

[18] *Id.*

[19] *Id.*

[20] Satoshi Nakomoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG 3 (2009), https://bitcoin.org/bitcoin.pdf. ("The blockchain represents majority consensus through the longest block chain. To succeed in a malicious attack, a fraudulent node would have to redo all the work of the target block plus all the work of the following blocks and surpass the work of the honest nodes. Nakamoto showed that "the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.").

[21] *Id.* at 6.

[22] *See* Joseph Bonneau et al., *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, IEEE SECURITY AND PRIVACY (forthcoming May 2015), http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf. ("Bitcoin is filling an important niche by providing a virtual currency system without any trusted parties and without pre-assumed identities among the participants.").

[23] *Blockchain*, BITCOIN FOUNDATION WIKI, https://en.bitcoin.it/wiki/Block_chain (last accessed Mar. 1, 2015) (noting that "[a] block chain is a transaction database shared by all nodes" on a network).

[24] *See id.* (noting that a blockchain is "implemented as a series of blocks of transactions, each containing the hash of the previous block, committing this block as its sole antecedent"); *Blocks*, BITCOIN FOUNDATION WIKI, https://en.bitcoin.it/wiki/Blocks (last accessed Mar. 1, 2015) (same).

the preceding block in the blockchain, as well as an answer to a complex mathematical puzzle, which is used to validate the data associated with that block.[25] A copy of the blockchain is stored on every computer in the network and these computers[26] periodically synchronize to make sure that all of them have the same shared database.[27]

To ensure that only legitimate transactions are recorded into a blockchain, the network confirms that new transactions are valid and do not invalidate former transactions. A new block of data will be appended to the end of the blockchain only after the computers on the network reach consensus as to the validity of the transaction.[28] Consensus within the network is achieved through different voting mechanisms, the most common of which is *Proof of Work,*[29] which depends on the amount of processing power donated to the network.[30]

---

[25] All operations in the blockchain are validated through a digital fingerprint created through a particular hash function (SHA256 in the case of Bitcoin), which is used to map all transactions incorporated in a block into a fixed-length string of data. Any differences in input data will produce differences in output data and thus a different digital fingerprint. *See* Bonneau, *supra* note 22, at 4.

[26] These computers are referred to as "nodes."

[27] Nakamoto, *supra* note 20, at 3 (explaining that every node in the Bitcoin blockchain network has a copy of the longest blockchain and nodes only accept new blocks when "all transactions in it are valid and not already spent."). This provides for an exceptional degree of resiliency: given that the same copy of the blockchain is stored by multiple computers connected to the network, even if a number of computers fail at any given time, the shared database can be recreated in its entirety.

[28] *See* PEDRO FRANCO, UNDERSTANDING BITCOIN: CRYPTOGRAPHY, ENGINEERING, AND ECONOMICS 15 (2014).

[29] The Proof of Work consensus mechanism requires that certain computers on the network (colloquially referred to as a "miners") solve computationally-intensive mathematical puzzles, while others verify that the solution to that puzzle does not correspond to a previous transaction. *See* Bonneau, *supra* note 22, at 2. To incentivize miners to invest computational power, the first miner to solve the mathematical problem is rewarded either through the issuance of currency or through transaction fees. *Id.* at 4.

[30] There are other types of consensus mechanisms currently being explored, such as Proof of Stake. The Proof of Stake consensus mechanism is less computationally-intensive that proof of work. *See Proof of Stake*, BITCOIN FOUNDATION WIKI, https://en.bitcoin.it/wiki/Proof_of_Stake (last accessed Mar. 1, 2015). Proof of Stake mechanisms do not require any processing power. Rather, voting rights depend on the amount of resources (e.g., a virtual currency) held by every computer connected to the network.

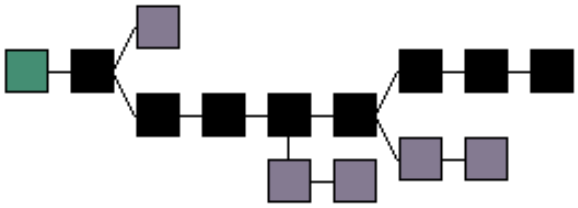

Fig. 1. A graphical representation of the blockchain

After a block has been added to the blockchain, it can no longer be deleted and the transactions it contains can be accessed and verified by everyone on the network. It becomes a permanent record that all of the computers on the network can use to coordinate an action or verify an event.

II. EMERGING USES OF BLOCKCHAIN TECHNOLOGY

Software developers have quickly realized the potential for blockchain technology and have started to use it to create digital currencies,[31] self-executing *smart contracts*, as well as cryptographic tokens that can represent property or ownership interest in emerging services. It is also being used to create: censorship-resistant communications and file sharing systems; decentralized domain name management systems (DNS); and fraud-resistant digital voting platforms.[32] Because the blockchain is a powerful decentralized database, the technology is increasingly recognized as a way to support machine-to-machine communications that will soon emerge from Internet enabled devices that constitute the Internet of Things.[33] By combining digital currencies, smart contracts, and distributed data storage, the blockchain further is ushering in entirely new decentralized organizations (including decentralized autonomous organizations) that use source code to define an organization's governance structure.

---

[31] Bitcoin is not the only digital currency that uses blockchain technology. There are no a number of virtual currencies that employ blockchain technology. *See* LITECOIN, https://litecoin.org/ (last accessed Mar. 1, 2015); DARKCOIN, https://www.darkcoin.io/ (last accessed Mar. 1, 2015).

[32] *See* Scott Rosenberg, *How Bitcoin's Blockchain Could Power an Alternate Internet*, MEDIUM (Jan. 13, 2015), https://medium.com/backchannel/how-bitcoins-blockchain-could-power-an-alternate-internet-bb501855af67 (summarizing emerging use cases for blockchain technology including distributed finance, distributed data, distributed identity, and others).

[33] *See* Part III, *infra.*

A. Digital Currencies and Global Payment Systems

One of the earliest applications for blockchain technology has been digital currencies such as Bitcoin. Released in 2009 by Satoshi Nakamoto (a pseudonymous individual or group),[34] Bitcoin relies on a decentralized blockchain to establish a digital currency that, unlike the US dollar, does not depend on any bank or government.[35] As explained by Nakamoto, the system is "completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust."[36]

Since its launch, Bitcoin has captured the world's attention.[37] Yet, Bitcoin is being used for more than just speculation. It is powering an entirely new payments system that allows for the seamless transfer of funds around the globe. Unlike existing payments systems, which generally take days to transfer funds, Bitcoin can be sent across the world in a little over seven minutes[38] at fees that are drastically lower than those imposed by existing money transmitters, such as Western Union.[39] All that is needed is an Internet connection and a computer or a simple mobile device.[40]

---

[34] Nakamoto *supra* note 20.

[35] *Id.* at 1.

[36] Satoshi Nakomoto, *Bitcoin Open Source Implementation of P2P Currency,* P2P FOUNDATION (Feb. 11, 2009), http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

[37] Indeed, Bitcoin has evolved from being worth less than $1 in 2009 to over $1,000 in 2014. *See Market Capitalization*, BLOCKCHAIN.INFO, https://blockchain.info/charts/market-cap?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address= (last accessed Mar. 1, 2015) (providing a chart that demonstrates the price of Bitcoin started at less than $1 in 2009 and hit $1,000 in January 2014).

[38] *See Average Transaction Confirmation Time*, BLOCKCHAIN.INFO, https://blockchain.info/charts/avg-confirmation-time?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address= (last accessed Mar. 1, 2015) (showing that the average confirmation time for a Bitcoin transaction has hovered around 7.5 minutes in 2014).

[39] *Compare Transaction Fees*, BITCOIN FOUNDATION WIKI, https://en.bitcoin.it/wiki/Transaction_fees (last accessed Mar. 1, 2015) (explaining that the default transaction fee for sending a bitcoin is 0.0001 BTC/kB, or $0.02/kB), *with* Christopher C. Williams, *Western Union: Calling to Investors*, BARON'S ONLINE (May 11 2013), http://online.barrons.com/articles/SB50001424052748704253204578468923751573136 (noting that in 2013 the average Western Union transaction was $341 with a fee of up to 5%).

[40] Bitcoin can even be transferred via radio broadcast. *CBC KW Sends Bitcoin Over The Airwaves*, CBC NEWS (Jan. 20, 2014), http://www.cbc.ca/news/canada/kitchener-waterloo/cbc-kw-sends-bitcoin-over-the-airwaves-1.2503580.

Adoption of Bitcoin has spread rapidly,[41] and the currency—as well as its many imitators[42]—have the potential to be the first breakthrough application that relies on blockchain technology.[43] As noted by Stanford economist, Susan Athey, these digital currencies "can potentially expand international commerce, support financial inclusion, and transform how we shop, save and do business in ways we probably cannot even yet fully understand."[44] It can lead to faster, cheaper bank transfers, unleash banking and e-commerce functions to third world countries, expand global remittances, and drastically reduce merchant fraud.[45]

B. Smart Contracts and Automated Transactions

Blockchains are not just powering digital currencies. They are also enabling the creation smart contracts, one of the first truly disruptive technological advancements to the practice of law since the invention of the printing press. Using a distributed database, like the blockchain, parties can confirm that an event or condition has in fact occurred without the need for a third party.[46] As a result, the technology has breathed life into a theoretical concept first formulated in 1997: digital, computable contracts where the

---

[41] As of the end of 2014, nearly 8 million Bitcoin accounts (wallets) have been created—a number that has been growing at a 200% yearly rate. *See State of Bitcoin 2015*, COINDESK at Slide 6, http://www.slideshare.net/CoinDesk/state-of-bitcoin-2015 (last accessed Mar. 1, 2015). Moreover, over 82,000 merchants accept Bitcoin as a form of payment, including Microsoft, Dell, Time Magazine, Overstock, and Braintree, a division of Paypal. *Id.* at Slide 44.

[42] *See* Tom Simonite, *Bitcoin Isn't the Only Cryptocurrency in Town*, MIT TECH. REVIEW (April 15, 2013), http://www.technologyreview.com/news/513661/bitcoin-isnt-the-only-cryptocurrency-in-town/; Ariel Schwartz, *Bitcoin 2.0: Can Ripple Make Digital Currency Mainstream?*, FAST CO. EXIST, (May 14, 2013), http://www.fastcoexist.com/1682032/bitcoin-20-can-ripple-make-digital-currency-mainstream.

[43] *See* Bonneau et al., *supra* note 22.

[44] Susan Athey, *5 Ways Digital Currency Will Change the World*, WORLD ECONOMIC FORUM AGENDA (Jan. 22, 2015), https://agenda.weforum.org/2015/01/5-ways-digital-currencies-will-change-the-world/.

[45] *Id.*

[46] Smart contracts were initially conceived of as digital contracts. *See* Nick Szabo, *The Idea of Smart Contracts* (1997), http://szabo.best.vwh.net/smart_contracts_idea.html (describing the concept of digital "smart" contracts) (hereinafter "Idea of Smart Contracts"). However, smart contracts have been conceived of as having applications that are broader than just contractual language. They are generally defined as "cryptographic 'boxes' that contain value and only unlock it if certain conditions are met." Vitalik Buterin, *A Next Generation Smart Contract & Decentralized Application Platform*, GITHUB (last edited Jan. 5, 2015), https://github.com/ethereum/wiki/wiki/White-Paper (hereinafter "Ethereum White Paper"). As described below, software developers believe that smart contracts can be used to facilitate machine-to-machine communications and the creation of decentralized organizations. *See* Parts III, *infra.*

performance and enforcement of contractual conditions occur automatically, without the need for human intervention.[47]

In some cases, smart contracts represent the implementation of a contractual agreement, whose legal provisions have been formalized into source code. Contracting parties can thus structure their relationships more efficiently, in a self-executing manner and without the ambiguity of words.[48] Reliance on source code enables willing parties to model contractual performance and simulate the agreement's performance before execution.[49] In other cases, smart contracts introduce new codified relationships that are both defined and automatically enforced by code, but which are not linked to any underlying contractual rights or obligations. To the extent that a blockchain allows for the implementation of self-executing transactions, parties can freely transact with one another, without the technical need to enter into a standard contractual arrangement.[50]

To date, smart contracts have mostly been created to automatically execute derivatives, futures, swaps, and options.[51] Yet, they are also being used to facilitate the sale of goods between unrelated people on the Internet without the need for a centralized organization.[52]

---

[47] *See* Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, FIRST MONDAY (1997), http:// firstmonday.org/ojs/index.php/fm/article/view/548/469 (outlining the concept for smart contracts); *see also* Harry Surden, *Computable Contracts*, 46 U.C. DAVIS L. REV. 629 (2012) (continuing to explore how the representation of contractual obligations as data allows for new contracting properties, including "computable" contract terms).

[48] *See* Part III *infra* (describing the benefits and societal implication of smart contracts);

[49] *See* MINTCHALK, http://www.mintchalk.com (last accessed Mar. 1, 2015). For example, a smart contract has been created which simulates the mechanics of a crowd funding campaign in 56 lines of code. *See id.* at http://www.mintchalk.com/c/68f3e (last accessed Mar. 1, 2015).

[50] Irrespective of the technical need, there may be a legal need to memorialize a smart contract in writing in order to make such arrangements enforceable in a traditional court or other judicial tribunal.

[51] For example, the startup Hedgy helps creates digital currency based derivatives. *See* HEDGY, http://hedgy.co/ (last accessed Mar. 1, 2015). Hedgy offers helps create "BitForward" smart contracts, which are "executed between counterparties with zero default risk and less settlement risk. It allows speculators to gain consistent exposure to the price movement of bitcoin, enabling them to realize profit potential without buying or selling the underlying asset." *Id.* The Counterparty platform also allows people to create option contracts and contracts for difference. *See Why Use Counterparty*, COUNTERPARTY, http://counterparty.io/why-counterparty/ (last accessed Mar. 1, 2015).

[52] One notable example is OpenBazaar, an open-sourced service that resembles Ebay. It aims to establish global decentralized marketplace through the use of smart contracts and a decentralized judicial system. Using OpenBazaar, people can directly buy and sell

The development of smart contracts is expanding rapidly. Over the past several months, a number of open source projects—such as Ethereum,[53] Counterparty,[54] and Mastercoin[55]—have been developed to create programming languages that enable the creation of increasingly sophisticated smart contracts. Using these programming languages, smart contracts could be used to enable employees to be paid on an hourly or daily basis with taxes remitted to a governmental body in real time.[56] The technology could be employed to create smart contracts that automatically check state death registries and allocate assets from a testator's estate, send applicable taxes to governmental agencies without the need of administering the will through probate.[57] Music royalties could be administered instantaneously, with distributions provided to both composers and performers in real time.[58] Complicated securitizations could, similarly, be transformed into a smart contract, eliminating the technical need for trustees and servicers.

C. Distributed and Secure Data Stores

Because it is an encrypted and decentralized database, blockchains are also beginning to impact how we communicate and share data online. Not only are they changing the way the Internet is managed, they are also increasingly seen as a way to facilitate machine-to-machine communications of Internet-enabled devices. Thanks to the blockchain, it is

---

products, with little to no fees, and no centralized control. *See* OPENBAZAAR, https://github.com/OpenBazaar/OpenBazaar (last accessed Mar. 1, 2015) (describing OpenBazaar as an open source, decentralized marketplace that has, inter alia, an "[o]rder management system; [r]icardian-style contracts; [m]ultisignature escrow-based transactions; [a]rbiter management and marketplace; [p]rivate messaging; and an "[i]dentity/[r]eputation system").

[53] *See* ETHEREUM, http://www.ethereum.org (last accessed Mar. 1, 2015); *see also* Buterin, *supra* note 46.

[54] *See* COUNTERPARTY, http://counterparty.io/ (last accessed Mar. 1, 2015).

[55] *See* MASTERCOIN, http://www.mastercoin.org/ (last accessed Mar. 1, 2015).

[56] *See* Giulio Prisco, *Bitcoin Governance 2.0: Let's Block-Chain Them*, CRYPTOCOIN NEWS (Oct. 13, 2014), https://www.cryptocoinsnews.com/bitcoin-governance-2-0-lets-block-chain/ (proposing a blockchain-based taxation system); *see also* BITWAGE, www.bitwage.co (last accessed Mar. 1, 2015) (a Bitcoin-based payment system allowing employees to be paid in micro amounts over a pay period).

[57] *See Contracts*, BITCOIN FOUNDATION WIKI, https://en.bitcoin.it/wiki/Contracts (last accessed Mar. 1, 2015).

[58] D.A. Wallach, *Bitcoin for Rockstars: How Cryptocurrency Can Revolutionize the Music Industry*, MEDIUM (Dec. 10, 2014), https://medium.com/backchannel/bitcoin-for-rockstars-ca8366802f9.

no longer necessary to route communications or files through a centralized system or online platform (like Gmail for e-mails or Dropbox for the exchange of digital files). Using decentralized, encrypted communication protocols[59] and a blockchain, parties can store and retrieve messages without the risk of government intervention.[60]

This same technology also allows for the exchange of data in a way that is both decentralized and secure. Information can be published (in encrypted format, if necessary) and distributed across hundreds of thousands of computers, making it virtually impossible for any single entity to censor. Early examples include anonymous decentralized cloud storage systems that use blockchain technology and other peer-to-peer technology to encourage people to use excess capacity on their hard drives.[61] From the user's perspective, these powerful platforms look similar to popular centralized cloud computing platforms. However, on a technological level, they operate completely differently. In these systems, users are awarded a digital currency for storing other people's data, which users in turn can use to pay for storage of their own data on other users computers.[62] Because of this incentive system, people who use these services are encouraged to rent out their own hard-drives, so they can gain access to the collective hard-drive of the network.[63] By design, the decentralized, encrypted nature of these platforms makes them seemingly censor proof—no centralized organization is technically able to view the content of any file on the network or stop its transmission.

Beyond managing data, software developers are exploring the blockchain's potential to enable unrelated people to securely vote over the Internet or on a mobile device. A blockchain can serve as a distributed, irreversible, and encrypted public paper trail that can be easily audited.[64] Voters could verify that their own votes *were* counted, and—due to

---

[59] One notable example of an encrypted communication protocol is Telehash. Telehash uses strong cryptography and mesh networking to create a decentralized communication layer. *See* TELEHASH, http://www.telehash.org (last accessed Mar. 1, 2015).

[60] *See, e.g.*, BITCRYPT, https://github.com/barisser/bitcrypt (last accessed Mar. 1, 2015) (explaining that the BitCrypt software package allows users to "[w]rite encrypted messages in the language of Bitcoin" and "[s]end encrypted messages to Bitcoin addresses").

[61] *See, e.g.*, STORJ, http://www.storj.io (last accessed Mar. 1, 2015).

[62] *Id.*

[63] *Id.*

[64] *See* HELIOS, https://vote.heliosvoting.org/ (last accessed Mar. 4, 2015); ETHELO, http://ethelodecisions.com/how-it-works/ (last accessed Mar. 4, 2015); *see also* Chris Malmo, *Bitcoin Could Revolutionize Voting*, VICE (Mar. 31, 2014), http://www.vice.com/en_ca/read/bitcoin-could-revolutionize-voting.

encryption—any blockchain-based voting system would be resistant to hacking.[65] Elections and proxy fights would no longer need to rely on the fallibility of paper and hanging chads. They could be safely waged on mobile devices.

Decentralizing data stores, like the blockchain, are further seen as a technical replacement for the domain name registry system that underpins the entire Internet. Currently, domain names—such as *Google.com* and *Facebook.com*—are managed through the Internet Corporation for Assigned Names and Numbers (ICANN),[66] an international organization charged with maintaining how people access Internet sites. New blockchain based applications seeks to upend this order, by creating a distributed domain name registry system that would store lists of domain names on a distributed blockchain database, without having to go through governments and large corporations to route traffic.[67] With just a single digital currency transaction, worth several pennies, a blockchain can extend our existing DNS system in a way that is censor-resistant and more secure.[68]

A blockchain's ability to manage data from a variety of untrusted source may further make it a foundational tool for the mainstream deployment of the Internet of Things. The Internet of Things will consist of billions of networked Internet-enabled devices, not all of which can be trusted and some of which may even be malicious. These devices need a central reference point that can help facilitate private, secure, and trustless machine-to-machine coordination.

---

[65] Any digital voting system would still be potentially suspect to hacking on the user level. For example, a bad actor could infect users computers or mobile devices to place fraudulent votes. However, given the transparent nature of the blockchain, this type of fraudulent behavior should be discernable. *See* Emil Kirkegaard, *Some Thoughts on Online Voting* (Mar. 14, 2014), http://emilkirkegaard.dk/en/?p=4166.

[66] *See* Susan P. Crawford, *The ICANN Experiment*, 12 CARDOZO J. INT'L & COMP. L. 409, 409 (2004) ("The Internet Corporation for Assigned Names and Numbers ('ICANN') is a private California not-for-profit corporation that has taken responsibility for allocating domain names and IP addresses.").

[67] *See* NAMECOIN, http://bit.namecoin.info/ (last accessed Mar. 4, 2015) (allowing people to register a ".bit" domain name on their decentralized network). Alternative systems, such as BlockName, allow anyone to register a domain/host name on the blockchain and use the blockchain as a fallback cache if traditional domain name hosting fails. *See* BLOCKNAME, https://github.com/telehash/blockname (last accessed Mar. 4, 2015).

[68] *See* NAMECOIN, http://bit.namecoin.info/ (last accessed Mar. 4, 2015).

For this problem, the blockchain offers an elegant solution.[69] Devices and other tangible property can be registered onto a blockchain and turned into *smart property*, using smart contracts described above,[70] allowing tangible property to be controlled over the Internet and even controlled by other machines. A blockchain can store the relationship between Internet-enabled machines at any given moment, and smart contracts can allocate corresponding rights and obligations of connected devices.[71] What's more, different relationships and credential could be encoded into the blockchain with regard to certain *cryptographically activated assets* (such as key locks or smartphones) so as to ensure that only certain people have access to the property's features at any given time.

D. Decentralized (Autonomous) Organization

A blockchain's coordinative power is not solely limited to facilitating the action of machines. It also allows for the execution and interconnection of a variety of smart contracts that interact with one another in a decentralized and distributed manner. Multiple smart contracts can be bound together to form *decentralized organizations* that operate according to specific rules and procedures defined by smart contracts and code — thereby transforming Michael Jensen's and William Meckling's theory that entities are nothing more than a collection of contracts and relationships into reality.[72]

---

[69] Paul Brody & Veena Pureswaran, *Device Democracy: Saving the Future of the Internet of Things,* IBM (Sept. 2014), http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03620USEN&attachment=GBE03620USEN.PDF#loaded

[70] Mike Hearn, *Turning Festival 2013*, YOUTUBE (Sept. 28, 2013), https://www.youtube.com/watch?v=Pu4PAMFPo5Y (outlining the development of smart property using smart contracts).

[71] IBM and Samsung recently debuted this technology, building a demo that had an internet enabled washing machine that automatically ordered a product by executing smart contracts when the machine ran out of detergent. *Adept Demo By IBM/Samsung*, PROTOCOL.TV (Jan. 13, 2015), https://www.theprotocol.tv/adept-demo-ibm-samsung/; *see also* Arvind Narayanan, *Nine Awesome Bitcoin Projects At Princeton*, FREEDOM TO TINKER (Jan. 30, 2015), https://freedom-to-tinker.com/blog/randomwalker/nine-awesome-bitcoin-projects-at-princeton/ (outlining various blockchain-based projects at Princeton University, including an implementation of smart property).

[72] Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 305, 310-11 (1976) (arguing that corporation—or, more generally, a firm—is a collection of consensual relationships among shareholders, creditors, managers and perhaps others); *see also generally* Frank H. Easterbrook & Daniel R. Fischel, THE ECONOMIC STRUCTURE OF CORPORATE LAW (1991).

Using a blockchain-based decentralized organization, people and machines (or a combination of both) can coordinate through a set of codified smart contracts, without the need to incorporate into traditional business entities. Governance can be achieved by recording transactions directly to a blockchain, reducing operational costs, while providing a more transparent and auditable trails of every decision. Corporate governance models can be replicated by distributing decision-making power to multiple parties using *multiple signature (multi-sig) technology*,[73] which prevents the execution of an action until multiple parties agree to a transaction.

As opposed to traditional organizations, where decision-making is concentrated at the top (*i.e.*, at the executive level), the decision-making process of a decentralized organization can be encoded directly into source code. Shareholders can participate in decision-making through decentralized voting, distributing authority throughout the organization without the need for any trusted centralized party.

By facilitating coordination and trust, a blockchain enables new forms of collective action that have the potential to bypass existing governance failures. It can thus potentially resolve many of the common problems related to the opacity and corruption inherent in the decision-making of many organizations.[74] Large hierarchical organizations are both imperfect and inefficient. Their imperfections are, for the most part, due to excessive centralization, delegated decision-making, regulatory capture, and sometimes even corruption. With the blockchain, most of these imperfections could evaporate. Interactions and organizations can be predefined by smart contract, and people or machines can interact without having to trust the other party. Trust does not rest with the organization, but rather within the security and auditability of the underlying code, whose operations can be scrutinized by millions of eyes. In that sense, decentralized organizations can be thought of as *open-sourced organizations*.

---

[73] *See* Vitalik Buterin, *Multisig: The Future of Bitcoin*, BITCOIN MAGAZINE (Mar. 12, 2014), https://bitcoinmagazine.com/11108/multisig-future-bitcoin/ ("[Multi-sig verification services] will play an even larger role in the cryptocurrency world, and may even fuse together with private arbitration companies; whether it's a consumer-merchant dispute, an employment contract or protecting a user from the theft of his own keys . . . ").

[74] Primavera De Filippi & Rafaelle Mauro, *Ethereum: The Decentralized Platform that Might Displace Today's Institutions*, INTERNET POLICY REVIEW (Aug. 25, 2014), http://policyreview.info/articles/news/ethereum-decentralised-platform-might-displace-todays-institutions/318.

Over time, as Internet-enabled devices become more autonomous, these machines can use decentralized organizations and the blockchain to coordinate their interactions with the outside world. We could thus witness the emergence of *decentralized autonomous organizations* that enter into contractual relationships with individuals or other machines in order to create a complex ecosystem of autonomous agents interacting with one another according to a set of pre-determined, hard-wired, and self-enforcing rules.[75]

Decentralized autonomous organizations are a specific kind of decentralized organization that are both autonomous (in the sense that, after they have been deployed on the blockchain, they no longer need nor heed their creators) and self-sufficient (in the sense that they can accumulate capital, such as digital currencies or physical assets). Decentralized autonomous organizations can charge users for the services they provide, in order to pay others for the resources they need. As long as they receive sufficient funds to operate on their own, they can thus subsist independently of any third party. If a decentralized organization is truly autonomous, no one (including its original creator) can control it after it has been deployed on the blockchain.[76] An ill-intentioned decentralized autonomous organization thus could be akin to a biological virus or an uncontrollable force of nature.

III. SOCIETAL IMPLICATIONS OF BLOCKCHAIN TECHNOLOGY

As blockchain technology develops and is increasingly deployed, traditional business organizations, financing, and government could be impacted, fundamentally rewiring how core aspects of our society function. It also raises a number of legal and ethical challenges that must be carefully considered, introducing new regulatory issues that draw into question some fundamental tenets of law.

---

[75] Vitalik Buterin, *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*, ETHEREUM BLOG (May 6, 2014), https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.

[76] As opposed to traditional software, a decentralized autonomous organization may not be a static piece of code, it can be designed to evolve over time in order to adapt to the context in which it operates. Depending on the governance rules used to build the autonomous organization, its conceivable that it could be programmed so that it can be updated by third parties. This could occur, for example, through the vote of its members. It could also occur, in the case of a purely independent decentralized autonomous organization, through the use of evolutionary algorithms that would change the organization's behavior as it collected information during the course of its operation.

A. The Transition Towards Decentralization and Encryption

Prior to the invention of the blockchain, a centralized authority was needed to organize businesses or states. For centuries, banks acted as central referees, who kept ledgers managing the inflow and outflows of wealth, enabling commerce and business to thrive.[77] Central governments periodically tallied votes of the populations, collected taxes, and maintained property registries, enabling the creation of flexible democratic or republican institutions that redistributed wealth and maintained order.[78] Centralized legislative and judiciary systems were empanelled by the state to elaborate laws and resolve potential disputes.[79] And, of course, centralized businesses were in charge of producing, aggregating, and distributing resources and services, often generating substantial producer surpluses.[80] In order to obtain efficiency gains, these centralized organizations vertically and horizontally integrated, consolidating markets and generating enormous concentrations of power, often at the expense of the individual.

The Internet offered a promise to upend this social order through the distribution of communication tools. A more interconnected world—early Internet pioneers posited—would lead to smaller, more flexible online organizations governed by their own set of rules.[81] However, these early

---

[77] *See generally* SIDNEY DEAN, HISTORY OF BANKING AND BANKS: FROM THE BANK OF VENICE TO THE YEAR 1883 40 (1884) (detailing the development of banks created for the purpose of aiding governments in their financial operations by providing a uniform currency and for the purpose of protecting commercial interests by facilitating exchanges and providing a safe deposit for the money of customers).

[78] *See generally* AREND LIJPHART, PATTERNS OF DEMOCRACY: GOVERNMENT FORMS AND PERFORMANCE IN THIRTY-SIX COUNTRIES 264 (2012) (noting that central democracies exhibit a high degree of regulatory quality and a strong rule of law, as measured by the quality of property rights and the strength of the police, judiciary, and tax powers).

[79] *See generally id.* at 176 (outlining the primary characteristics of centralized federal governments).

[80] *See generally* ALFRED DUPONT CHANDLER, STRATEGY AND STRUCTURE: CHAPTERS IN THE HISTORY OF THE INDUSTRIAL ENTERPRISE 52-78 (1969) (analyzing the history, expansion, and structure of industrial businesses as exhibited by American companies such as du Pont, General Motors, Standard Oil, and Sears).

[81] One notable expression of this sentiment is John Barlow's *A Declaration of the Independence of Cyberspace*, penned in February 1996. *See* John Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUNDATION (Feb. 8, 1996), https://projects.eff.org/~barlow/Declaration-Final.html. In this Declaration, Barlow declared that the Internet was difference "consist[ing] of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live" and claiming

visions have yet to materialize. While the Internet has liberated information, and contributed to the democratization of markets, it has done little to transform many of the centralized organizations that existed before the dawn of the digital age.[82] Governments and large corporations have in fact grown, as they leveraged the raw distributive power of the Internet.[83]

With the blockchain, the need for these centralized authorities could be lessened. Internet users can act as a collective middleman, administering their own affairs through a shared decentralized database and automated software. Any piece of content, data, or even property can be registered or represented digitally on the blockchain in an encrypted form, enabling people to transact directly, instantaneously, and pseudonymously. As such, blockchain technologies offer the promise that many early Internet visionaries hoped for: a more flexible and fairer space of interaction with a lower number of centralized organizations whose functions are unbundled into more decentralized entities.

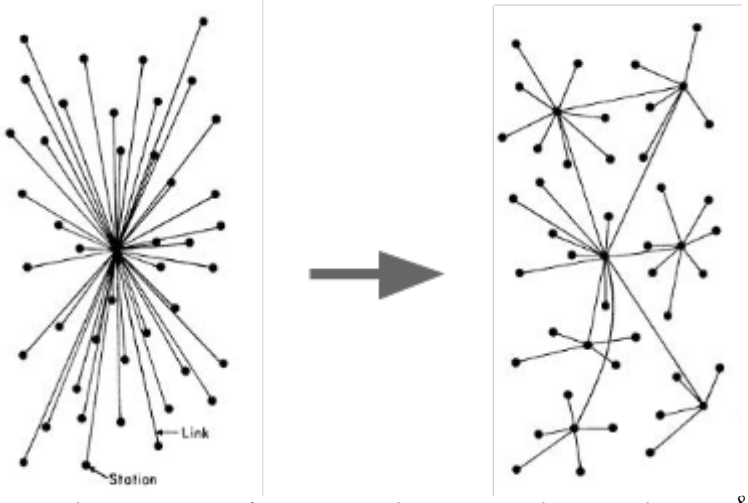

Fig. 2 The transition from centralization to decentralization[84]

However, there are downsides to decentralization. There will be fewer chokepoints to guide and assist the flow of data. Decentralized

---

that "legal concepts of property, expression, identity, movement, and context do not apply" because "[t]hey are all based on matter, and there is no matter here."

[82] *See generally* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD 142-161 (2006) (arguing that the Internet has not produced a global borderless network but rather "a collection of nation-state networks—networks still linked by the Internet protocol, but for many purposes separate.").

[83] *See Wealth of Networks*, *supra* note 1, at 3.

[84] This graphic is based on the network model of Paul Baran. *See* PAUL BARAN, ON DISTRIBUTED COMMUNICATION NETWORKS 2 (1964).

applications and decentralized blockchain-based organizations could be more difficult for governments to control and regulate. Take for example, the case of digital currencies. If digital currencies gain widespread adoption, given the lack of a central (regulatory) authority, such currencies would be nearly impossible to shut down.[85] As a result, governments may have a harder time implementing monetary policies using existing methodologies, which many believe have effectively smoothed the cyclical nature of western societies.[86] The disintermediation of multiple central banking systems could lead to a more volatile worldwide economy.[87] Without these centralized organizations and centrally issued currencies, the financial system in many countries, including Europe and the US, could potentially devolve, possibly leading to continual waves of severe recessions and depressions.[88]

The same issues may also face consumer marketplaces. The government has attempted to limit the flow of illicit drugs, child pornography, and other illegal products by targeting middlemen that control access to these products. While government officials were able to prosecute early versions of decentralized, unregulated marketplaces, like the notorious

---

[85] It is possible to shut down decentralized software. However, the steps needed to do so are fairly extreme. As noted by Michael Froomkin, if "digital cash is banned by a government, many corporations active in that jurisdiction will be reluctant to use it because they are subject to audit and disclosure requirements, and have assets to lose if subjected to civil or criminal penalties. At a minimum, a ban would raise the cost of using anonymous digital cash, perhaps to the point where few people were willing to trade in it. Even a refusal to enforce contracts or debts based on the exchange of anonymous currency would have a significant deterrent effect." A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 476 (1996).

[86] *See generally* Richard Clarida et al., *Monetary Policy Rules and Macroeconomic Stability: Evidence and Some Theory,* NAT'L BUREAU OF ECON. RESEARCH Working Paper No. 6442 (1998) (analyzing the quantitative relationship between monetary policies and the U.S. economy); *see also* Jeremy Rubin, *Regulating Bitcoin by Mining: The Regulator Mining Attack*, Medium (Jan. 22, 2015) (outlining, *inter alia*, how a regulatory body could regulate Bitcoin by hoarding coins or by only selling coins to parties who have complied with regulations).

[87] Richard Brearly et al., FINANCIAL STABILITY AND CENTRAL BANKS: A GLOBAL PERSPECTIVE xiii (noting that "[o]ne thing all central banks have in common is an interest in financial security as a public policy objective").

[88] *See*, Marvin Goodfriend, *Central Banking In The Credit Turmoil: An Assessment Of Federal Reserve Practice*, NAT. BUREAU OF ECON. RESEARCH (2010), http://www.carnegie-rochester.rochester.edu/april10-pdfs/goodfriend.pdf (analyzing the stabilizing effect of the United States Federal Reserve during the 2007 Recession).

drug-marketplace Silk Road,[89] evolved permutations of these dark markets are already emerging.[90]

For now, humans are running these organizations. However, that may soon change, as human-run functionalities are replaced by software operating over a blockchain. A decentralized autonomous organization could be programmed and released such that it facilitated the trade of illicit goods or banned products. The software could resemble a normal website and have a simple user interface where people can post illegal goods at a specified price for purchase. The site could be accessed using traditional domain name services (e.g., darkmarket.com), but could be rendered censor-resistant through the use of decentralized DNS-like protocols. While people who purchased goods using the marketplace may not be anonymous, governments or other regulatory bodies will have a hard time shutting down the service, because it is both stored and executed in a distributed manner across an entire network of computers.

Further, the pseudo-anonymous nature of blockchain technology presents significant regulatory challenges. Its widespread use could potentially undermine the ability of law enforcement to uncover and clamp down on illegal activity. Digital currencies can be used as tax havens.[91] A party seeking to avoid taxes could set-up multiple digital currency accounts and transfer funds between these accounts with ease.[92] To further obscure digital transaction histories, the tax-avoider also could employ anonymization techniques—such mixing[93]—making it harder for

---

[89] *See* James Ball, *Silk Road: The Online Drug Marketplace That Officials Seem Powerless to Stop*, THE GUARDIAN (Mar. 22, 2013), http://www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace.

[90] *See* Andy Greenberg, *Inside the 'Dark Market' Prototype, a Silk Road the FBI Can Never Seize*, WIRED (Apr. 24, 2014), http://www.wired.com/2014/04/darkmarket/ (detailing a prototype for a launched version of the illicit Silk Road site that plugs some security holes that may make it more elusive to shut down).

[91] *See* Omri Marian, *Are Cryptocurrencies Super Tax Havens?*, 112 U. MICH. LAW REV. FIRST IMPRESSIONS 38, 39 (2013) (arguing that "[c]ryptocurrencies possess the traditional characteristics of tax havens" and that as "cryptocurrencies continue to gain momentum, we could reasonably expect tax-evaders . . . to opt out of traditional tax havens in favor of cryptocurrencies.").

[92] *Id.* at 41-43.

[93] *See* Simon Barber et al., *Bitter to Better—How to Make Bitcoin a Better Currency*, FINANCIAL CRYPTOGRAPHY 12-14 (2012), http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf (outlining various mixing techniques to increase anonymity on the Bitcoin network); Greg Maxwell, *CoinJoin: Bitcoin privacy for the real world*, BITCOIN FORUM (Aug. 22, 2013), https://bitcointalk.org/index.php?topic=279249.0 (outlining a procedure for obscuring bitcoin transactions by joining them together and shuffling them).

government authorities to track down the owner of these accounts.[94] Without know your customer (KYC)[95] or anti-money laundering (AML) measures by payment intermediaries, it is possible to use digital currencies to transfer money in a way that could frustrate law enforcement or governmental control.[96]

Similarly, the deployment and adoption of anonymous decentralized communication channels could prevent the government from intercepting communications without permission. Blockchain technology makes encrypted communication easier. Data can be encrypted as it travels between two points (referred to as end-to-end encryption), [97] and the content of the message can also be stored in an encrypted format on a blockchain, requiring that the message be unlocked with a secret key only known to the parties.

If widely adopted, these networks could effectively counteract mass-surveillance by governmental or corporate entities; but, as a collateral effect, they would also eliminate the possibility for legitimate forms of surveillance used for prosecution and law enforcement.[98] By allowing

---

[94] *See* Froomkin, *supra* note 85, at 477 (noting that "[i]f . . . digital cash that does not have to be cleared through a bank . . . becomes widespread, the ability of authorities to control money laundering will depend greatly on the extent to which the scheme allows authorities to trace the funds."); Sarah N. Welling & Andy G. Rickman, *Cyberlaundering: The Risks, the Responses*, 50 FLA. L. REV. 295, 327 (1998) (noting that "[m]oney laundering with electronic cash could become a major crime if the government does not move carefully" and implement laws to require that electronic cash have "audit trails").

[95] Know Your Customer rules "refers to the requirement for banks and other financial institutions to monitor, audit, collect, and analyze relevant information about their customers (or potential customers) before engaging in financial business with them." Genci Bilali, *Know Your Customer-or Not*, 43 U. TOL. L. REV. 319, 319 (2012); *see generally id.* (providing an overview of know your customer laws).

[96] Anti-money laundering rules are rules enacted by the U.S. government after the September 11, 2001 terrorist attacks. These rules placed heightened requirements on banks, broker-dealers, and other depository institutions to identify and verify account holders for anyone opening an account at any U.S. financial institution. *See generally* Jonathan M. Winer & Debra D. Bernstein, *New Anti-terrorist Law has Significant Search and Seizure and Money Laundering Implications For U.S. Companies*, 4 PRIVACY & INFO. L. Rep. 10 (2002).

[97] *See* Telehash, *supra* note 59.

[98] Online anonymity presents a range of benefits. As noted by Bryan Choi, "[a]nonymizing technologies allow dissenting voices to challenge existing norms and hierarchies. Likewise, generative technologies allow new innovations to break settled patterns of behavior. The freedom to transcend such constraints can foment positive change and progress. But it can also lead to harmful disruption and disorder. When anonymity allows perpetrators to escape detection, harms go unredressed and the aggregate incidence of harmful behavior increases." Bryan H. Choi, *The Anonymous Internet*, 72 MD. L. REV. 501, 538-39 (2013).

online communications to transact under shield of secrecy, blockchain-based technology would significantly lower the barrier to coordinate criminal activity, supporting the operations of online gambling websites and black market operations, such as those described above.

While many of these issues are not new, with the advent of blockchain technology, the impact may be harder to control. The telecommunications industry faced a similar challenge nearly 20 years ago when the telecommunications industry began to use digital telephone exchange switches that made wire-tapping phones harder and in some cases impossible.[99] The reaction from the United States government was swift and resulted in the enactment of the Communications Assistance for Law Enforcement Act (CALEA),[100] which required that telecommunications companies modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities, allowing federal agencies to wiretap any telephone, internet, and VoIP traffic.[101]

Unlike the decentralization of the telecommunication networks, however, blockchain-based communication systems can be deployed without a middleman, preventing governments from enacting similar regulations, except for an unenforceable ban of the use of the technology. These anonymous communication channels—combined with decentralized (autonomous) organizations—could increase the ability of bad actors to effectuate harm. With communication networks that are harder to crack and the possibility of coordinating through the use of decentralized

---

[99] *See* FED. BUREAU OF INVESTIGATION, JOINT PETITION FOR RULEMAKING TO RESOLVE VARIOUS OUTSTANDING ISSUES CONCERNING THE IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT 22 (2004), available at http://askcalea.fbi.gov/pet/docs/20040310.calea.jper.pdf. ("[T]he movement toward packet-based networks . . . has already progressed far enough to have a serious impact on law enforcement's ability to perform authorized electronic surveillance. The Commission should avoid these dangerous results by acting decisively today to bring CALEA into the broadband age. Preserving law enforcement's ability to conduct lawfully-authorized electronic surveillance in the face of the increasing migration to new technologies—namely, broadband access services and broadband telephony services.").

[100] Hildegarde A. Senseney, *Interpreting the Communications Assistance for Law Enforcement Act of 1994: The Justice Department Versus the Telecommunications Industry & Privacy Rights Advocates*, 20 HASTINGS COMM. & ENT L.J. 665, 684 (1998) (outlining the expansion of the telecommunications industry, noting how these technological advances put severe constraints on law enforcement's ability to effectively wiretap, and explaining how this expansion and decentralization lead to the enactment of CALEA).

[101] *See* 18 U.S.C. § 2703; *see also* Senseney, *supra* note 100, at 671-82 (detailing the statutory requirements of CALEA).

organizations, crime may be easier to plan and execute and an entirely new chapter of cyberwarfare and cybercrime may emerge.[102]

B. *Automated Contractual Negotiation, Execution, and Enforcement*

Beyond notions of decentralization and anonymization, smart contracts—in and of themselves—are likely to have a significant impact on our everyday life. This technology decreases the marginal cost of contracting, much like the Internet did to the transmission of data and information. Smart contracts thus have the potential to drastically reduce friction in both commerce and society by providing greater clarity and speed to transactions.

Because smart contracts are drafted using source code, they can be standardized and executed at nearly no cost like other programming languages.[103] The practice of law could thus follow the path of software. As with web-based programming languages, smart contract scripting languages could become easier to manipulate overtime, democratizing the process of who can create contracts. In the near future, it is conceivable that people will rely on powerful smart contract programming languages to organize their own affairs without the technical need for a lawyer. This is likely to have a significant impact on the legal profession. Lawyers will no longer focus on the drafting of boilerplate legal provisions; they could leave the details to a machine, and concentrate on higher order legal work to identify the core provisions of a contractual agreement that should be implemented into code.[104]

Smart contracts further improve one of the most frustrating aspects of contractual drafting: the inherent ambiguity of natural language. Words often have multiple meanings and interpretations.[105] And, in many

---

[102] *See Exploring Tomorrow's Organised Crime*, EUROPOL (2015), https://www.europol.europa.eu/sites/default/files/Europol_OrgCrimeReport_web-final.pdf.

[103] In order to execute smart contracts, many existing platforms require that you expend small amounts of digital currency for each condition executed. *See, e.g.*, Ethereum White Paper, *supra* note 46, at 14 (noting that "gas" is required to execute each contractual step).

[104] Smart contracts will not be the only technical trend that makes contract drafting easier. As recognized by John McGinnis and Russell Pearce advances in machine learning—in and of itself—will enable computers to generate useable transactions documents and gain wider adoption in the legal community. *See* John O. McGinnis & Russell G. Pearce, *The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services*, 82 FORDHAM L. REV. 3041, 3050 (2014). Smart contracts will accelerate that process.

[105] *See generally* E. Allan Farnsworth, "*Dmeaning" in the Law of Contracts* 76 YALE L.J. 939 (1967) (outlining some of the difficulties in contractual interpretation).

instances, ambiguous language can make it easier for parties to enter into a contractual arrangement, creating flexibility in terms of contractual performance.[106] However, ambiguity and poor drafting can also be used by parties to wrestle free from contractual conditions that parties no longer want to honor.[107] Smart contracts provide a solution to this problem by incorporating legal provisions ("wet code") into code ("dry code").[108] If parties want certainty, they can use a smart contract to ensure that a contractual condition is executed, forcing the parties to remain bound to their respective obligations.

The power of smart contracts, however, does not solely rest with their ability to reduce contractual ambiguity and increase the ease of contracting. It also derives from the fact that smart contracts dramatically increase the speed with which contractual relationship can be executed. Because they are not reliant on paper, and can execute in real-time, our collective use of costly paper-based contracts may seem—in hindsight—anachronistic. Just as we marvel today at how people used to conduct business or communicate through letters and fax machines, in just a few years, we may marvel at how it presently take days to send a payment abroad, at how we still pay monthly bills for basic utilities instead of remitting them on a daily basis, or at how we still pay taxes on a yearly basis, rather than having them automatically remitted upon payment or sale using smart contracts.

Yet, while smart contracts may facilitate the execution of complex agreements with greater clarity, they also present a series of new challenges. They implement, by default, a zero-tolerance policy where parties have no

---

[106] *See* Mark P. Gergen, *The Use of Open Terms in Contract*, 92 COLUM. L. REV. 997, 1006 (1992) ("[O]pen terms are used because of the difficulty of writing and enforcing contracts that precisely specify performance subject to finely drawn conditions to deal with many known risks."); Gillian K. Hadfield, *Judicial Competence and the Interpretation of Incomplete Contracts*, 23 J. LEGAL STUD. 159, 159 (1984) ("In recent years writers in both economics and law have recognized the prevalence and importance of incomplete contracting in the design of markets and organizations.").

[107] *See* Scott J. Burnham et al., *Transactional Skills Training: Contract Drafting-Beyond the Basics*, 2009 TRANSACTIONS: TENN. J. BUS. L. 253 (2009) (noting that "[a]mbiguity is really an aspect of interpretation, and interpretation is actually the number one litigated issue in contracts. So by preventing ambiguity, what you are doing is preventing litigation from arising over the meaning of contract terms.").

[108] *See* John W.L. Ogilvie, *Defining Computer Program Parts Under Learned Hand's Abstractions Test in Software Copyright Infringement Cases*, 91 MICH. L. REV. 526, 531 (1992) (explaining that "[t]he literal text comprising a program's instructions, known as *source code,* is written in one or more *programming languages*. These languages resemble human languages such as English, but have much less room for ambiguity.").

choice but to execute the contract.[109] In the current legal framework, the law establishes a series of rules that people must abide to. Nevertheless, everyone is free to infringe these rules (at the risk of being held liable for damages) because legal enforcement takes place *ex post*, after the act. As opposed to traditional contracts, where parties can decide whether or not to fulfill their obligations, smart contract cannot be breached. Once the contracting parties have agreed to be bound by a particular clause, the smart contract's code immutably binds them to that clause without leaving them the possibility of a breach.[110]

In a system regulated by self-enforcing smart contracts and other technical arrangements, there is less of a need for judicial enforcement, because the way in which the rules have been defined—*the code*—is the same mechanism by which they are enforced. Overtime, law and code may merge, so that the only way for people to infringe the law is to effectively break the code.

This raises the question over what is legally versus technically binding. While contract law implements a series of safeguards to protect consumers that might either invalidate the contract or make it non-enforceable (*e.g.*, information asymmetries, undue influence, unconscionability, and incapacitation), smart contracts operate within their own closed technological framework. Although implementing basic contractual safeguards and consumer protection provisions into smart contracts is theoretically possible, in practice, it may prove difficult given the formalized and deterministic character of code.

C. *Reducing Friction in Capital Markets and Financing*

With smart contracts and digital currencies, the entire world of commerce and finance may soon be re-conceptualized. These technologies provide a technical framework to create digital assets and decentralized exchanges. Prior to the invention of blockchains, it was nearly impossible to raise money and allocate equity in a company without enlisting the help of an attorney. Today, using services like Swarm[111] or Koinify[112] a site can issue a *cryptotoken* to raise funds to power software development and

---

[109] As noted above, it is possible to prevent the execution of a contract by requiring multiple signatures to be signed before certain conditions are met. *See* Buterin, *supra* note 73.

[110] Of course, the parties could terminate the smart contract if they decided that they did not want to remain bound to it.

[111] *See* SWARM, http://www.swarm.fund (last accessed Mar. 1, 2015).

[112] *See* KOINIFY, http://www.koinify.com (last accessed Mar. 1, 2015).

reward early adopters. With a few lines of source code, a company can create its own cryptotoken to represent an ownership interest in a company or voting rights.

The result could be profound. Just as the Internet and personal computer placed a digital copy machine in everyone's home, blockchain technology could provide millions of people with the power to easily issue quasi-financial or financial instruments. Overtime, centralized Wall Street exchanges could no longer be technically necessary to facilitate public markets. They can be replaced by one or more blockchain-based, decentralized exchanges.[113] Because settlement and payment can happen instantaneously, these exchanges can facilitate the trading of cryptotokens, as well as existing securities that are digitally represented on the blockchain. The need for a licensed market decreases, because instantaneous settlement effectively eliminates counterparty risk.

As with other industries, at first, these decentralized exchanges could be run by traditional corporations. However, it is entirely conceivable that, in the near future, they will be replaced by distributed (and potentially autonomous) organizations. Financial assets could be recorded directly into the blockchain, where they could be easily aggregated and disclosed. In order to limit the decentralized market to legitimate companies, smart contracts could be used to define a series of characteristics that must be fulfilled before a party can list a cryptotoken on an exchange.

One possible approach would be to structure the decentralized exchange so that it only listed securities if the issuing organizations met certain earnings or asset thresholds as detailed on a publicly available blockchain. If listed, the security could be traded over the Internet in real-time. Once purchased, payment and title in the cryptotoken could transfer instantaneously by creating a new record on a blockchain. After being listed, if the price of an equity dropped or if revenues dipped below a particular threshold, the cryptotoken could be removed from the exchange without any human intervention. The technical need for clearing and settlement services like the Depository Trust and Clearing Corporation

[113] Indeed, the founder and CEO of Overstock.com, Patrick Byrne, has recently announced his intention to build such an exchange. *See* Michael Casey, *BitBeat: The Promise and Limits of Overstocks Crypto Stock Exchange*, WALL ST. J. (Oct. 24, 2014), http://blogs.wsj.com/moneybeat/2014/10/24/bitbeat-the-promise-and-limits-of-overstocks-crypto-stock-exchange/.

(DTCC), as well as the technical need for multiple stock exchanges, could consequently evaporate.[114]

Securities are not the only property that can be managed by a blockchain. Paper-era registries—like those of the US Patent and Trademark Office and the US Copyright Office—could be digitized and overtime globalized, eliminating the needless redundancy of multiple filings for the same product or service.[115] Disparate title registries could be recorded to a public blockchain, drastically lowering the need for title insurance.[116] Security interests could also be recorded to a blockchain, providing greater certainty in the lending markets. As a result, real property, intellectual property, and debt could become more liquid and could transfer around the world without the need to pass through layers of intermediaries. With digitized property registries, digital currencies, and smart contracts, real property could be effectively virtualized, making it easier to transfer property from one party to another.

However, the digitization of assets and securities could raise new challenges, most notably in the realm of securities laws. If more and more people bootstrap their businesses through decentralized mechanisms, without abiding by the mandatory disclosures required by law, there is a risk that they will be clamped down by regulatory agencies. This could lead to battles reminiscent to those that emerged after the advent of file sharing.[117]

---

[114] The DTCC is a multi-billion business found that helps banks settle and clear stock trades. *See About*, DTCC, http://www.dtcc.com/annuals/museum/index.html (last accessed Mar. 1, 2015).

[115] Given the patchwork nature of property registries for real and intellectual property both in the United States and in foreign countries, digital property registries will likely be difficult to create. Indeed, discussion of digitizing title registries has been raised since the late 1990s. *See* Dale A. Whitman, *Digital Recording of Real Estate Conveyances*, 32 J. MARSHALL L. REV. 227, 233 (1999) (outlining the benefits to a digital title registries). However, because blockchain technologies do not just enable the creation of local-US based digital property registries, but the development of a global digital property registry, this technology may finally enable the creation of these registries. Governments do not need to trust another government—or a third-party—to manage its property registries. Rather, trust can be placed in the mathematical certain provided by blockchain technology.

[116] *See* Joshua Fairfield, *BitProperty*, 88 S. CAL. L. REV. (forthcoming 2015), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2504710 (outlining how blockchain technology could be used to create a digital property registry).

[117] *See generally* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 726-45 (2003) (detailing the evolution of sharing music online from client side services to the emergence of various peer-to-peer services).

Just as regulators did not succeed in controlling the dissemination of information and knowledge, governments could fail to contain technological advancement in the world of digital finance. Although sensible in the current economical framework, security laws might need to be reformed to better account for the opportunities offered by blockchain-based technologies, so as to support (rather than constrain) the creation of promising new businesses that could have never existed before the creation of blockchain technology. Indeed, it may turn out to be increasingly unpractical—and ultimately lead to slow economic growth—to force every member of the public to create extensive and onerous disclosures about the risks and potential rewards of a particular project before seeking to raise funds.

D. The Rise of the Metered Internet and the Growth of the Peer-to-Peer Economy

Finance is only the beginning of the story. Smart contracts and digital currencies may also rewire how we interact with the online world. Programmers are working hard to fuse blockchain technology into every Internet browser, in order to make it easy for websites to utilize these distributed data stores.[118] This may finally enable the mainstream implementation of a *metered Internet*, where actions are tied to small micropayments and accompanying smart contracts.[119] Since digital currencies and smart contracts can dramatically reduce the cost of transacting, artists, musicians, and authors may soon use this technology to

---

[118] *See DEV Plan,* ETHEREUM 8 (2014), https://www.ethereum.org/pdfs/Ethereum-Dev-Plan-preview.pdf. ("EtherBrowser [will be] the primary client used by individuals for accessing Dapps built on Ethereum. The client . . . will be a fully functioning web-like browser . . . with the intent that it be usable for both browsing the traditional centralized web and the decentralized, more ethereal, web, all within one program.").

[119] Micropayments have long been discussed as a potential business model for the Internet. Despite a number of attempts, they have yet to gain mainstream acceptance. *See, e.g.*, Tom Steinert-Threlkeld, *The Buck Starts Here*, WIRED (Aug. 1996), http://archive.wired.com/wired/archive/4.08/nanobucks.html (extolling some of the benefits of "nanobucks"); Tania Hershman, *Towards a Click-and-Pay Standard*, WIRED, (Nov. 3, 1999), http://archive.wired.com/science/discoveries/news/1999/11/32092?currentPage=all (outlining IBM's attempt to build a micropayment system for the Internet in 1999); Mitche Thierry, *Common Markup for Micropayment Per-fee-Links*, WORLD WIDE WEB CONSORTIUM (Aug. 25, 1999), http://www.w3.org/TR/WD-Micropayment-Markup (a document by the World Wide Web Consortium where they explored establishing a micropayment scheme for the Internet. It would have allowed people to embed in their website's html a way to initialize a micropayment with information such as price, title, buy-id, duration, expiration, and type. The W3C eventually abandoned this project).

automatically collect royalties on their works each time they are viewed or consumed.[120] If the content is a derivative work, smart contracts could be used to remit a "remix fee" in real-time to all applicable rightsholders. Similarly, a "micro-referral fee" could be paid to parties that list or drive traffic to the content.

Combined, this could lessen the need for content creators to rely on advertising-based revenue models. If micropayments are implemented and adopted, creators will have an incentive to disseminate their works widely and encourage people to remix them, because the more these works are used or reused by third parties, the larger rewards they will reap. Micropayments and smart contracts could, therefore, be used to realign the incentive structure of the Internet, redistributing wealth more efficiently.[121]

Micropayments can also fix a number of the Internet's woes. Spammers clog email servers and online communities' forums simply because the cost of a post is virtually zero. Online communities have few ways of compensating dedicated users who spend countless hours on their site in order to help build value, resulting in digital sharecropping.[122]

Blockchains offer a potential solution to these problems by facilitating the transmission of micropayments that most people would consider trivial. If it costs a fraction of a penny to post or send a message, email spamming would become cost prohibitive, because spammers send

---

[120] Wallach, *supra* note 58; Walter Isaacson, *Big Idea 2015: The Coming Micropayment Disruption*, LINKEDIN PULSE (Dec. 15, 2014) https://www.linkedin.com/pulse/big-idea-2015-coming-disruption-walter (noting that "[a]n easy micropayment system for digital content could help save journalism. . . . people could click and pay a few pennies for an article. . . . It would encourage news sites to produce content that is truly valued by users rather than churn out clickbait that aggregates eyeballs for advertisers"); Frank Fischer, *Saving Journalism, A Farthing at a Time*, GUARDIAN (May, 19, 2009) http://www.guardian.co.uk/commentisfree/2009/may/18/news-online-payment-journalism (arguing that micropayment are the financial scheme that can save journalism by making online publishing profitable).

[121] Isaacson, *supra* note 120.

[122] *See* Nicholas Carr, *Sharecropping The Long Tail*, ROUGHTYPE (Dec. 19, 2006), http://www.roughtype.com/archives/2006/12/sharecropping_t.php. ("One of the fundamental economic characteristics of Web 2.0 is the distribution of production into the hands of the many and the concentration of the economic rewards into the hands of the few. It's a sharecropping system, but the sharecroppers are generally happy because their interest lies in self-expression or socializing, not in making money, and, besides, the economic value of each of their individual contributions is trivial. It's only by aggregating those contributions on a massive scale–on a web scale–that the business becomes lucrative.").

out millions of messages in hopes of finding a handful of victims.[123] Online communities can use economic incentives to coordinate actions, by associating micropayments with basic Internet actions like "liking" a website, "retweeting," or "upvoting" a page on popular Internet waterholes like Reddit. Wikipedians could be paid small sums for writing, removing spam, or fact-checking a page.

Decentralized organizations could also empower unrelated content creators with the ability to set up their own communities that would more efficiently share advertising revenues and payments without the need for a middleman. For instance, a group of popular YouTube personalities could decide to establish their own decentralized organization, without ever meeting one another. They could use smart contracts to codify governance rules and implement a fluid, less formalized organization that, in some ways, could resemble a traditional corporation, but in other ways could significantly differ from it.

Like a corporation, the decentralized organization could define the management of the organization and the decision-making processes. It could, for example, determine each party's voting rights based on the number of views that each member's videos receive. The organization could generate advertising revenue with little to no human oversight, by means of increasingly sophisticated turnkey online advertising solutions. And, profits could be distributed to members in real-time based on voting rights, using smart contracts.

Unlike existing corporations, that decentralized organization could have features that are trivial to implement using blockchain technology, but difficult to incorporate into existing limited liability entities. Membership or ownership of the decentralized organization could be designed to be fluid and automatic, depending on factors such as the votes of other members, or a specific threshold of popularity in terms of video views, subscribers to a

---

[123] *See* Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 427-28 (1999) (discussing use of small ecash payment to prevent spam); Andreessen, *supra* note 6 (noting that "[a]nother potential use of Bitcoin micropayments is to fight spam. Future email systems and social networks could refuse to accept incoming messages unless they were accompanied with tiny amounts of Bitcoin – tiny enough to not matter to the sender, but large enough to deter spammers, who today can send uncounted billions of spam messages for free with impunity."); CoinSummit, *Bitcoin Fireside Chat with Mark Andreessen and Balaji Srinvasan*, YOUTUBE (Mar. 24, 2014), https://www.youtube.com/watch?v=iir5J6Z3Z1Q (discussing economics of microtransactions and spammers with both email and other social networks).

video channel, or social media followers. If members of this newly formed organization did not carry their creative weight—as measured by these factors—rights could be revoked automatically or membership terminated without any human interaction through predefined smart contracts.

This type of decentralized organization thus acts as a new type of organization that sits between an informal online group and a more formalized corporate entity. By aggregating and managing access to content through automatic software, content creators could maintain most of the advertising revenue that their content generates, without having to share profits with centralized Internet operators. And, if it becomes a popular destination on the Internet, an invitation to join the organization could even be regarded as a signal of prestige and accomplishment.

Overtime, these new types of organizations could enable people to monetize their creative and cognitive surpluses in more efficient ways, making it easier to engage in the types of peer-to-peer production outlined in detail by Yochai Benkler.[124] The result could be a more dynamic online world where people receive payments for making the Internet a more enjoyable place. Anyone may be able to join these decentralized organizations and creating software, videos, animated gifs, articles could be automatically rewarded.

At the same time, these systems could fundamentally challenge the free nature of our online world. Smart contracts could, in effect, be an evolution of digital rights management (DRM) that could jeopardize the open nature of the Internet. These evolved digital contracts have the power to conceivably control access to and consumption of digital content. Content companies could wrap their content and use smart contracts to ensure payment, limit transferability, and protect content that is in the public domain.[125] Taken to its logical extreme, if content creators develop the ability to identify all of their content online, copyright law—including

---

[124] Wealth of Networks, *supra* note 1, at 63-90, 216-25 & 337-44 (identifying social production in peer-to-peer file swapping networks, open source programming, the World Wide Web, massive multi-user online games like Second Life, the blogosphere, Internet search engine algorithms, experimental crop breeding, and WiFi Internet access); Eric von Hippel, *Innovation by User Communities: Learning from Open-Source Software*, 42 SLOAN MGMT. REV. 82 (2001), http:// sloanreview.mit.edu/smr/issue/2001/summer/8.

[125] *See* Chris Walters, *B&N Wraps Public Domain Books In DRM To Protect Authors' Copyrights. What?*, CONSUMERIST (July 29, 2009), http://consumerist.com/2009/07/29/bn-wraps-public-domain-books-in-drm-to-protect-authors-copyrights-what/.

the regime of limitations or fair use[126]—could be rendered less relevant, as self-executing contracts could tabulate and track every reproduction, distribution, derivative work, and display, narrowing the possibility for online copyright infringement.

While this benefits content creators,[127] if the cost of information is set too high, it may effectively serve as a tax on creativity and consequently chill the development of the arts. Vast swaths of information currently freely available on the Internet could be converted back into a market-based commodity.[128] The mass deployment of micropayments could lead to a situation where "tiny bundles" of small-scale innovation are protected by strong intellectual property and contractual rights. As well recognized by J.H. Reichman, this could produce "a tangled web of property and quasi-property rights that in itself constitute a barrier to entry."[129]

E. Smart Property and Machine-to-Machine Communications

Thanks to the blockchain, Internet-connected machines also will be able to communicate and transact in real-time.[130] Physical property can be manipulated and controlled through source code, turning formerly static, everyday items into "smart property."[131] Smart property could be imbued with digital capabilities and designed to transact and communicate with

---

[126] *See* Randal C. Picker, *From Edison to the Broadcast Flag: Mechanisms of Consent and Refusal and the Propertization of Copyright*, 70 U. CHI. L. REV. 281, 295 (2003) ("as the internet creates a ubiquitous structure for micro-transactions—microconsents with micropayments—fair use might cease to play a meaningful role"); Tom W. Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine,* 76 N.C. L. REV. 557, 596-605 (1998) (suggesting that fair use doctrine is unnecessary where consumers are charged micropayments for small uses of copyrighted works).

[127] Justin Hughes, *Size Matters (or Should) in Copyright Law*, 74 FORDHAM L. REV. 575, 616 (2005) (noting that "[i]ndependent protection of microworks and a micropayment structure would transfer wealth to existing owners of informational or financial capital.").

[128] *See id.* (noting that micropayments and microworks "weaken the egalitarian, empowering aspect of intellectual property," because "it allows individuals with little or no preexisting property to develop valuable property out of public domain materials, completely unencumbered by obligations to prior property owners.").

[129] J. H. Reichman, *Of Green Tulips and Legal Kudzu: Repackaging Rights in Subpatentable Innovation*, 53 VAND. L. REV. 1743, 1776 (2000) (illustrating how the use of techno-legal mechanisms for creating artificial scarcity on information could create a "weed-like thicket of exclusive rights" that "throttle[s] more innovation that [it] could ever possibly stimulate.").

[130] Brody & Pureswaran, *supra* note 69, at 8.

[131] *See* Nick Szabo, *The Idea of Smart Property* (1997), http://szabo.best.vwh.net/smart_contracts_idea.html (first proposing smart property in 1997).

humans and other machines. They will be managed with precision either through direct human control, algorithms, or artificial intelligence.[132]

In an increasingly connected world, people will be able to instantly search, use, and pay for available resources. For example, autonomous cars could be ordered from our mobile phones. Each order could be recorded onto a blockchain which, when scanned, would inform the autonomous car of the transaction.[133] We would then be able to pay for a ride, like a normal taxi, with our fare deposited into the car's own bank account (presumably a digital currency account).[134]

The rise of coordinated Internet-enabled machines could also create liquid, transparent marketplaces by enabling real time matching of supply and demand with increased transparency and automation. Conference rooms, hotel rooms, warehouse bays, and factory lines could be made intelligent, reporting capacity, utilization, and availability in real-time.[135] Networks of Internet-enabled sensors could optimize farms by measuring heat, humidity, nutrition levels, light, and weight in order to automatically adjust irrigation and fertilization levels.[136] If every farm used sensors to optimize crop growth, and recorded pseudo-anonymized versions of this information to a searchable blockchain, a public dashboard could be created to measure national or regional crop yields or even areas of over-fertilization, resulting in more efficient farms and commodities markets. Likewise, a mobile phone could securely communicate with a door lock and automatically open if the owner's smartphone had the necessarily credentials to open the lock (such as verified biometric data).[137] Using this

---

[132] *See* Brody & Pureswaran, *supra* note 69, at 8.

[133] Hearn, *supra* note 70 (discussing the use of blockchain technology to coordinate autonomous cars and drones)

[134] *Id.*

[135] *See* Brody & Pureswaran, *supra* note 69, at 9.

[136] *Id.* at 11 ("Instrumenting and digitizing every step in the agriculture process could yield substantial returns from close collaboration among farmers, biotechnology companies, farm equipment manufacturers and capital providers. The array of IoT [Internet of Thing] technologies that can and will be deployed to make agriculture more productive includes drones to monitor large areas cheaply, instrumentation for optimized planting and harvesting based on soil and weather conditions, and field sensors for detailed monitoring."); *see also* Warwick Ashford, *IOT Could Be Key to Farming Says Beechman Farming*, COMPUTER WEEKLY (Feb. 4, 2015) (reporting that the Internet of Things could improve crop yields by 70% by using internet enabled devices to prepare the soil, plant, and harvest at precisely the best time).

[137] An early prototype of this type of technology is AirLock. Airlock allows a user to create an Internet enabled lock and then grant access to the lock to any person. "Access can be

technology, real world spaces, such as homes or hotels, could be managed and secured with no human interaction. As these locks become smaller and cheaper, they could eventually be embedded into an increased array of physical objects.

Nevertheless, the creation and mass deployment of smart property also raises novel challenges that cannot be easily addressed within the current legal framework. A party that owns property is generally assumed to have received a bundle of rights.[138] Those rights can voluntarily transferred or taken away by the law through mechanisms such as seizure, divestiture, or judicial action. In the case of smart property, however, ownership could be both defined and managed by source code. A person who qualifies as the technological owner (as opposed to the legal owner) of smart property enjoys absolute sovereignty over that resource, which cannot be seized by anyone unless specifically provided for by the underlying code.

But code can also be used to implement a series of technological arrangements that might ultimately limit the exercise of property rights over a particular object. For instance, access to property can be programmatically limited to specific users or device, or even be limited to a person who is identified in a record on a blockchain.[139] When brought to the extreme, every piece of property could be tied to a potential kill switch,[140] whereby property could be disabled or divested remotely through the simple click of a button or a computer algorithm. In such a world, property ownership could vanish, replaced by a web of temporary leasehold interests governed by contracts.

With the rise of the Internet of Things, it also will be increasingly easy to instantiate laws using blockchain technology. For example, smart contracts could conceivably manage constitutional rights. In the US, they

---

open-ended, limited by date and time, or one-time only, as determined by the" owner of the lock. AIRLOCK, http://airlock.me/ (last accessed Mar. 4, 2015).

[138] For discussions of the bundle of rights theory of property law, *see*, e.g., LAWRENCE C. BECKER, PROPERTY RIGHTS: PHILOSOPHIC FOUNDATIONS 11-21 (1977); JOHN CHRISTMAN, THE MYTH OF PROPERTY: TOWARD AN EGALITARIAN THEORY OF OWNERSHIP 3-27 (1994)

[139] *Smart Property*, BITCOIN FOUNDATION WIKI, https://en.bitcoin.it/wiki/Smart_Property (last accessed Mar. 1, 2015) (outlining how an automobile could be connected and controlled by a blockchain).

[140] *See* Cathy Reisenwitz, *Smart Contract's Promise for the Poor*, BITCOIN MAGAZINE (Jan. 27, 2014) (noting that "Smart Property makes it possible for locks to change automatically the moment a renter violates their lease agreement. And makes it possible for a car to refuse to start the moment a payment is late. Most importantly, it does so on a trustless basis.").

could be used to automatically check a decentralized online identity platform and digitized criminal records to assess whether the person satisfied certain preconditions that define who can and who cannot own or use guns. A person that satisfied these preconditions would be allowed to purchase a gun, whereas failure to meet these requirements would bar the person from completing the purchase. More drastically, smart contracts could be tied to an Internet-connected gun, which could only be operated if these pre-conditions were met.

F. Distributed Real-time Governance

The transition towards more decentralization may not only impact the implementation or application of laws, but also how we govern business organizations and society at large. Blockchain-based applications present a genuine promise for new kinds of scalable innovations in governance and institutional design, where the ideals for a corruption free and effective social democracy may come true.

Corporations have long relied on a set of passive shareholders with a limited role in the management of the corporation's core business.[141] Through the deployment of new and innovative blockchain-based applications, shareholders may take a greater role in the management of their organizations, with innovations such as real time accounting, nearly instantaneous voting mechanisms, and more efficient markets. In a world of decentralized autonomous consensus, collective decision-making could take on more prominence, resulting in the rapid reformulation of corporate structures and the more efficient allocation of corporate resources.

Consider for example, the simple task of electing a board of directors. Today that task is accomplished using paper mailings or insecure e-proxy services.[142] Shareholders must jump through multiple hoops to submit simple corporate proposals or calls for reform.[143]

---

[141] *See* Mark J. Roe, *A Political Theory of American Corporate Finance,* 91 COLUM. L. REV. 10, 12 (1991) (noting that "corporate wealth is held by shareholders as a 'passive' investment while managers control the corporation.").

[142] An example of an e-proxy service is Proxy Vote. PROXY VOTE, https://east-online.proxyvote.com/pv/web.do (last accessed Mar. 1, 2015).

[143] For example, the United States Securities and Exchange Commission gives shareholders some rights to offer proposal for vote at the annual shareholder meeting. However, there are various limitations on this rule, For example, a shareholder can only offer one proposal per year and, unless set altered by the corporation, the proposal must be submitted at least 120 days before the date of the company's proxy statement is released to shareholders in connection with the previous year's annual meeting. *See* Rule 14a-8, 17 C.F.R. 240.14a-8.

This entire system could be made less cumbersome and more responsive. Votes could be instantaneously recorded on a blockchain, making elections of directors a trivial task. Annual in-person meetings could be eliminated, replaced by virtual meetings live-streamed over the Internet. Requisite votes could be entered remotely, using a blockchain, as a secure data store, and subsequently tallied in real-time in a trusted way.

The ease of shareholder voting could make corporations more dynamic. Restrictions on shareholder proposals could be lessened, as shareholders could submit any proposal they want and only proposals that have garnered a sufficient number of votes from other shareholder (on a percentage basis) would be presented to a board of directors. By lessening the noise, shareholders' voices could be actually heard and legitimate shareholder concerns addressed.

Beyond corporate governance, the blockchain can help implement new decentralized models of commons-based management. Commons-based communities are generally institutionalized around centralized or federated structures,[144] which bring a series of trade-offs in terms of democratic governance, flexibility, and ability to evolve. These institutions were built, for the most part, to facilitate the coordination of disparate groups that would otherwise have had a hard time coordinating.

("A shareholder proponent can offer only one proposal per year, and must submit the proposal to the company about five months before the next annual meeting. A proposal must also meet substantive requirements, the most important of which are that it must: involve a proper subject for shareholder action; not relate to ordinary business operations or the election of directors; and not conflict with a manager proposal.").

[144] Jonathan M. Barnett, *The Host's Dilemma: Strategic Forfeiture in Platform Markets for Informational Goods*, 124 HARV. L. REV. 1861, 1907 (2011) ("Like other successful open source projects, Linux code development is governed by a strict hierarchy, in which a limited core of qualified developers . . . develop code and approve changes to the code. These core developers are in turn assisted by reports of 'bugs' and 'fixes' contributed by a larger mass of participants."); Greg R. Vetter, *"Infectious" Open Source Software: Spreading Incentives or Promoting Resistance?*, 36 RUTGERS L.J. 53, 80 (2004) ("Most large open source software projects, including Apache and GNU/Linux, operate using this collaborative development model. A core development group generates a substantial portion of the software. Other non-core developers and users operate and debug the software. The leaders of the project make design decisions and filter software submittals for inclusion in the product.").

Today, traditional issues related to shared common-pool resources—such as the free rider problem or the tragedy of the commons[145]—could be addressed with the implementation of blockchain-based governance. Adopting transparent decision-making procedures and introducing decentralized incentives systems for collaboration and cooperation could make it easier for small and large communities to reach consensus and implement innovative forms of self-governance. The possibility to record every interaction on a incorruptible public ledger and the ability to encode a particular set rules linking these interactions to a specific transactions (*e.g.* the assignment of cryptographic tokens or the allotment of micro-payments) enables the design of new sophisticated incentive systems that could improve the efficiency of commons-based communities.

Blockchain technologies thus could bring trust and coordination to shared resource pools, enabling new models of non-hierarchical governance, where intelligence is spread on the edges of the network instead of being concentrated at the center. Flexible decentralized organizations, such as the one described in Part III above, could more effectively compete with the hierarchical format of current centralized formations. Instead of relying on traditional top-down decision making procedures, blockchain technology allows for such procedures to be increasingly crowd sourced, delegating to the community the collective responsibility to monitor and evaluate its own achievements. While online communities will probably be the first one to experiment with these new apparatus, as the ease of creating these organization decreases through standardization, online communities could be easily brought offline to create and build new organizations that operates in the physical world.

Indeed, thus far, it has been difficult for direct democracies to scale, due to the inherent coordination problems they entail. As encryption techniques improve,[146] digital public voting could become viable, leading to the implementation of systems where towns, cities, and even entire nations

---

[145] J. Bradford DeLong & A. Michael Froomkin, *Speculative Microeconomics for Tomorrow's Economy*, FIRST MONDAY (Feb. 2000), http://firstmonday.org/ojs/index.php/fm/article/view/726/635 (outlining that traditional economic theory dictates that open source software is susceptible to "tragedy of the commons issues" and detailing how open source communities attempt to address this problem through due to reputation).

[146] Public electronic voting will likely not be fully implemented until it can be assured that citizen's votes cannot be discerned from a public blockchain. For an overview of this problem, see Jonathan Keane, *The Perils And Promises Of Online Voting: Can The Ballot Box Ever Truly (and Safely) Go Digital In Europe?*, TECH.EU (July 9, 2014), http://tech.eu/features/2071/online-voting-europe-perils-promises/.

can be managed more directly by their population using blockchain technology.

Imagine a small suburban town in the not so distant future. The town's mayor could propose a budget and release it for public vote via blockchain-based software. Inhabitants of the town could be prompted to vote for the proposed budget on their mobile device. People could input their position and those who voted against a proposal could provide feedback directly to the mayor's office. If a sufficient number of votes were cast in favor of the proposed budget, the allocated funds could be immediately released to relevant departments in the town using smart contracts. If the budget did not receive enough votes, the mayor's office could either review the comments and propose a new budget or decide to call a public vote. Elections and public participation in politics could become as mundane as replying to an email.

Friction in government could be further reduced by implementing new governance models where politicians could become unelected during their term if they failed to maintain minimum public approval levels. Voters could lodge their vote for a specified politician. Once elected, if the electorate disapproved of the politician's actions, it could shift votes to another candidate at any point during the politician's term. If a politician's approval fell below a specified threshold, the politician would have to make the case for why he or she should remain in office. Poor approval ratings would not just be a passing news story. With the cost of voting drastically reduced, politicians hampered by scandal, corruption, or incompetence could easily be removed from their offices, making governance more efficient and decreasing the impact of politicians who have lost the confidence of their constituency.

As blockchain technologies develop, governments themselves may be replaced by decentralized (autonomous) organizations. People could band together and set rules for their own governance, collect taxes, and distribute wealth in ways the group believes is fair. Communities could form into nations, unbounded by geographical boundaries, and governed through a set of algorithmic rules that can be both established and enforced through voting mechanisms and smart contracts. This could lead to the emergence of a constellation of *techno-democratic systems*, allowing for a diaspora to be governed and organized into a self-governing state.[147]

---

[147] As an alternative, it could make it easier to form "reverse diasporas" where people organize online and then find a physical location to settle. *See* Balaji S. Srinivasan, *Software is Reorganizing the World*, WIRED (Nov. 22, 2013),

Alternatively, smart contracts could be used to set up decentralized prediction markets that could underpin a *Futarchy*[148]—an alternative form of government proposed by economist Robin Hanson, using prediction markets as a means to identify the policies expected to yield the most positive outcomes. Under this model, elected representatives would formally define and coordinate an after-the-fact measurement of national welfare, while people speculate on the success or failure of specific policies by placing bets to select the policies they expect will ultimately raise national welfare.[149] By turning *prediction markets* into *decision markets*, Futarchy presents itself as a solution to the current apathy and demagoguery of democracy. It provides financial incentives for citizens to participate in the governance process, although only the most skilled individuals (*i.e.* those who can effectively predict the specific policies' outcomes) will be rewarded, at the expenses of others. Of course, the potential drawback of such systems are most likely to outweigh their benefits.[150]

G. Algorithmic Governance

The widespread deployment and adoption of smart-contracts also could make it easier for citizens to create custom legal systems, where people are free to choose and to implement their own rules within their own techno-legal frameworks. As such, the blockchain could support and facilitate the deployment of a decentralized alternative to the current legal

---

http://www.wired.com/2013/11/software-is-reorganizing-the-world-and-cloud-formations-could-lead-to-physical-nations/.

[148] *See* Robin Hanson, *Futarchy: Vote Values, But Bet Beliefs* (Aug. 2000), http://hanson.gmu.edu/futarchy.html (outlining a "futarchy"— a new form of government where "[e]lected representatives would formally define and manage an after-the-fact measurement of national welfare, while market speculators would say which policies they expect to raise national welfare").

[149] *Id.*

[150] In spite of these benefits, a more direct democracy and futarchy may introduce a series of important drawbacks. Direct democracies have populist risks. Populist governance disregard minority rights and has never been able to achieve long term sustainability. Futarchy presents the risk of market manipulation. Players with strong market power might collude to manipulate prices within the prediction market so as to favor one decision over the other. *See* Monica Anderson, *Robin Hanson and Mencius Moldbug: "Futarchy Debate" at Foresight 2010 Conference*, VIMEO (Feb. 6, 2010), https://vimeo.com/9262193. This, combined with the inherent volatility and self-referentiality of market mechanisms, might lead to the emergence of speculative bubbles that reinforce rather than counteract price distortion, ultimately bringing the system to decide upon a particular set of policies that will not necessarily yield the best outcomes.

system—a new *digital common law*[151]—consisting of an interconnected system of rules interacting with one another in a reliable and predictable way, without the need of any third party institution to enforce these rules. As opposed to current legal systems, whose provisions are universal and applicable to everyone, regardless of whether they have actually been consented to, under this new paradigm, people would be free to choose among a particular set of provisions that better reflect their underlying preferences or needs. In fact, people could chose to participate into two or more regulatory frameworks, arbitrarily switching between one or the other depending on the contextual circumstances and contingencies.

With the growing amount of data that is being created or collected and the deployment of sophisticated data mining techniques, it is now possible to extract valuable information and elaborate detailed users profiles stemming from big data analysis and inference techniques. As more of this data is used to inform the operation of smart contracts and decentralized (autonomous) organizations, algorithms and source code will soon start playing a significant role in our everyday life. Once widespread, we could witness the emergence of so-called *algorithmic governance*: a new normative system capable of regulating society more efficiently, reducing the costs of law enforcement and allowing for a more customized system of rules that is personalized to every citizen, and that is constantly revised based on their corresponding preferences and profiles.

Algorithmic governance could help achieve highly optimized systems. It could measure the cost of a product in terms of both consumer surplus and environmental impact, revealing to consumers the true value of a product. Self-driving cars could be coordinated through sophisticated algorithms that could drastically reduce the number of accidents on the road. In the case of an imminent crash, a quick assessment of the contextual setting could be made by an *ethical algorithm* deciding, based on the number and reputation of people or things that might be affected by the crash, how to minimize the impact of the accident according to the specific value or values that the system is designed to optimize.[152].

---

[151] John Henry Clippinger & David Bollier, *The Rise of Digital Common Law An Argument for Trust Frameworks: Digital Common Law and Digital Forms of Governance*, ID3 (2012), https://idcubed.org/digital-law/the-rise-of-digital-common-law/ (outlining "[d]igital common law . . . a bottom-up, voluntary, user-driven system that establishes context-specific norms for governing a given online community/market.").

[152] Of course, this would require encoding a set of moral values and ethical principles into the algorithms of these machines—a task that might be doomed to failure absent human intervention.

Algorithmic governance could also be employed voluntarily by people to ensure that they achieve their pre-selected goals. By setting personalized rules, algorithms could help us face the constant tensions or temptations of our modernized world. This is especially apparent in the context of many quantified self[153] communities, as more and more people rely on specific sensors and devices to collect data about themselves and their environment, in order to subsequently analyze this data so as to better understand themselves and the fellow members of their community. These practices are becoming especially popular in the field of personal health and chronic illness management, where big data analysis can help identify potential solutions to specific disease.[154] But the trend is growing steadily,[155] and the tendency to quantify oneself may soon reach mainstream adoption: from monitoring one's sleep to analyzing one's eating habits; from counting one's steps to calculating the daily amount of calories intake—if we want to improve our quality of life, there are more and more reasons to rely on algorithms to govern our everyday behavior.

But when algorithms are matched with self-enforcing smart-contracts things might go wrong. By way of illustration, people willing to lose weight could be automatically informed of their progress; algorithms might sometimes suggest that they walk to work or do more exercise, or they could also propose a daily menu that would best their diet. Yet, using smart contracts, an algorithmic governance system could actually prevent people from purchasing highly caloric products from stores until their weight returned to a pre-programmed number. Similarly, while algorithmic governance could help us achieve a more balanced lifestyle, reminding us to

---

[153] The quantified self movement seeks to collect data about every aspect of a person's daily life using technological devices, including food consumed, quality of surrounding air, mood, arousal, blood oxygen levels, and performance. For an overview of this movement, see *The Quantified Self: Counting Every Moment*, THE ECONOMIST (Mar. 3, 2012), http://www.economist.com/node/21548493.

[154] For example, in a clinical trial for Parkinson's disease conducted in 2014, Intel used smart watches, connected to Wi-Fi connection, over 300 data points per second from each patient, including tremors, gait, and sleep patterns. Analytics and machine learning tools developed by intel analyzed the data for insights into how medications and other treatments were working and enabled Intel to measure the progression of the disease. *See* Clint Boulton, *Intel Fighting Parkinson's Disease With Smartwatches, Big Data*, The WALL STREET J. (Aug. 13, 2014), http://blogs.wsj.com/cio/2014/08/13/intel-fighting-parkinsons-disease-with-smartwatches-big-data/.

[155] Steve Allen, *The Promise of the Quantified Self*, SILICON VALLEY BANK (Apr. 3, 2014), http://www.svb.com/uploadedFiles/Blogs/Steve_Allan/svb-quantified-self-report-0614.pdf (a detail report that outlines how the confluence of advances in technology, changing consumer preferences, mobile devices, and social media "has driven the acceleration of this young, but rapidly growing [Quantified Self] sector").

take a break from work or to spend more time with our friends or families, problems might arise when smart contracts automatically shut off access to the Internet, mobile phones, and other distractions in order to ensure that we comply with our predefined goals and criteria.

Indeed, despite the potential benefits of software-based governance, increased automation could result in decreased freedom and autonomy. The drawbacks of algorithmic governance are already visible today, as content curation and evaluation, sorting and ranking mechanisms are often shielded from the public by large Internet silos, proprietary companies—such as Google and Facebook—which, through their algorithms, are continually framing and reframing our experience of the digital world.[156] In spite of the advantages that users might derive from greater personalization, the opaqueness of these algorithmic rules is such they are generally left with little to no insight into how these companies truly decide how to sort and display information.

As algorithmic governance expands, its risks become higher. It could be used to determine the job that one should choose; it could suggest a range of partners that one should marry or raise a family with; or it could suggest the optimal places in which one should live, given his work and that of his family. Faced with a range of "optimal" choices, people would live under the illusion of free will, although their realm of choices would ultimately be determined by a network of algorithms optimizing our lives according to a specific set of predefined metrics.

When pushed to its logical extreme, algorithmic governance, might eventually result in a system that is highly prescriptive and deterministic; a system where people are, indeed, free to decide the particular set of rules to which they want to abide, but—after the choice has been made—can no longer deviate from these rules, to the extent that smart contracts are automatically enforced by the underlying code of the technology, regardless of the will of the parties. This could potentially lead to the emergence of the modernized version of a totalitarian regime—a society based upon a restrictive technical framework that is almost exclusively controlled by self-

---

[156] *See generally* Eli Parser, THE FILTER BUBBLE (2011) (outlining how increased personalization and computer created algorithms, such as Google's search engine algorithms, impact how we consume information and our online world view); Robinson Meyer, *Everything We Know About Facebook's Secret Mood Manipulation Experiment*, ATLANTIC (Jun. 28, 2014), http://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/ (outlining Facebook's sorting algorithm that shows users more positive news to increase mood).

enforcing contracts, *walled gardens* or *trusted systems,* owned and managed by a sophisticated network of decentralized organizations that dictate what people can or cannot do, without any kind of constitutional safeguards or constraints.

IV. THE EMERGENCE OF LEX CRYTPOGRAPHIA

Given the aforementioned characteristics of blockchain technology, the deployment and mainstream adoption of this technology may require a shift in the way we perceive the role of law. We might need to rethink the mechanisms we use to regulate individuals, and society more generally, in order to grapple with the emergence of this new set of technological rules.

A. The Establishment of Lex Mercatoria

During medieval times, domestic trade was regulated by customary laws, a system of common rules and customs that were specific to a kingdom.[157] Advances in transportation infrastructures led to an expansion of trade, which extended beyond the scope of the kingdom to reach a variety of towns, often close by. As trade was no longer restricted to one kingdom, internal (domestic) rules could no longer apply. A new set of rules and principles therefore were established to regulate trade within and amongst kingdoms.[158] This was achieved by means of private ordering, as merchants themselves established the rules that would regulate different types of transactions.[159] Over time, some of these customs and best practices became recognized as a customary body of law for international (or interregional) commerce. This marked the advent of the so-called *Lex Mercatoria* (Latin for "Merchant Law").[160]

---

[157] *See* Bruce L. Benson, *The Spontaneous Evolution of Commercial Law*, 55 SOUTHERN ECON. J. 644, 646-47 (1989) (before the development of Lex Mercatoria, merchants faced "localized, often contradictory laws and businesses practices" producing "hostility towards foreign commercial customs and lead to mercantile confrontations.").

[158] *See* Leon E. Trakman, *From the Medieval Law Merchant to E-Merchant Law*, 53 U. TORONTO L.J. 265, 270-76 (2003) (chronicling the development of merchant law); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 553 (1998).

[159] *See* David R. Johnson & David Post, *Law and Borders-the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1389 (1996) ("Merchants could not resolve their disputes by taking them to the local noble, whose established feudal law mainly concerned land claims. Nor could the local lord easily establish meaningful rules for a sphere of activity that he barely understood and that was executed in locations beyond his control. The result of this jurisdictional confusion was the development of a new legal system—Lex Mercatoria").

[160] *See* Johnson & Post, *supra* note 159, at 1389; Benson, *supra* note 157, at 646-47.

Lex Mercatoria was not dictated nor recognized by any particular kingdom, it emerged organically from the interactions of merchants seeking to extend the reach and reduce the uncertainty of trade.[161] The emerging Merchant Law was not enforced by any sovereign authority, as royal courts generally avoided cases involving international trade or simply refused to acknowledge the validity of foreign contractual deals.[162] Hence, merchants developed their own courts to enforce their own legal framework stemming from voluntary contractual deals.[163] Merchant courts progressively emerged along the main trading routes, recognizing *Lex Mercatoria* as a universal set of rules that is applicable to everyone regardless of the geographical location.[164]

B. The Rise of Lex Informatica

A similar trend emerged in the 1990s, with the widespread adoption of the Internet and the rise of private ordering as the dominant tool for regulating online interactions. The transnational character of the Internet posed serious challenges to the traditional conception of law based on national boundaries and jurisdictions.[165] Today, in order to compensate for the regulatory gap that subsists within the framework of both national and international law, Internet service providers and online operators increasingly rely on contractual agreements, *i.e*. End-User Licensing Agreements (EULA) or Terms of Use (ToU), to manage their relationship with users.[166] Most of these policies ignore the underlying provisions of

---

[161] Lawrence M. Friedman, *Erewhon: The Coming Global Legal Order*, 37 STAN. J. INT'L L. 347, 356 (2001) ("The original lex mercatoria was a body of mercantile custom in the middle ages. It was closely associated with the Lombard merchants, who formed a kind of transnational business class. Quite a number of institutions of modern commercial law, relating to banking, negotiable instruments, and the like, grew out of customs and practices that were aspects of the lex mercatoria"); Trakman, *supra* note 158, at 270-72.

[162] *See* Johnson & Post, *supra* note 159, at 1389.

[163] *See* Trakman, *supra* note 158, at 274; *see also* Robert D. Cooter, *Decentralized Law for A Complex Economy: The Structural Approach to Adjudicating the New Law Merchant*, 144 U. PA. L. REV. 1643, 1647 (1996) ("The merchants in the medieval trade fairs of England developed their own courts and practices to regulate trade.").

[164] *See* Fabrizio Marrella & Christopher S. Yoo*, Is Open Source Software the New Lex Mercatoria?,* 47 VA. J. INT'L L. 807, 811-12 (2007) ("[D]isputes between traders that arose under the law merchant would be resolved in special merchant courts run by the merchants themselves . . . As a result, lex mercatoria reflected the collective wisdom of the entire trading community distilled from the bottom up . . . rather than being the conscious creation of any person or sovereign.").

[165] Johnson & Post, *supra* note 159, at 1390; GOLDSMITH & WU, *supra* note 82, at 13.

[166] *See* Marrella & Yoo, *supra* note 164, at 816 ("Today, choice of law clauses permit harmonization of international commercial law by specifying that the substantive legal rules used to resolve the dispute may encompass, via the lex mercatoria, general principles

national laws, supplanted by a privately negotiated contractual framework. Similarly, in the context of intellectual property rights, while copyright law operates on a strictly territorial basis, a number of online communities developed specific contractual tools, such as the Free/Libre Open Source Software (FLOSS) or Creative Commons licenses, introducing their own system of rules to define the production, distribution, and exploitation of information.[167] In both cases, these contractual agreements can be regarded, to a large extent, as a form of *Lex Mercatoria* specific to the digital realm, *i.e.*, a system of universal (customary) rules that apply equally to everyone, independently of the jurisdiction.[168]

The real innovation brought about by digital technologies is that, in the digital world, technology itself can be regarded as a parallel form of regulation. Such regulation derives from the technical features of various online platforms, which ultimately determine what can or cannot be done.[169] Inspired from the notion of *Lex Mercatoria*, this particular form of regulation has been described as *Lex Informatica* (Informatics Law)[170]—a particular set of rules spontaneously and independently elaborated by an international community of Internet users, which constitutes today an alternative normative system consisting of a particular set of rules and customary norms arising directly from the limitations imposed by the design of the infrastructures subtending the network.

Lex Informatica is viewed as a natural extension of *Lex Mercatoria*, a complementary toolkit for the regulation of online transactions through the establishment of technical norms, in addition to contractual rules. Just like *Lex Mercatoria*, *Lex Informatica* ultimately relies on self-regulation: it is a system of customary rules (or standards) and technical norms elaborated by online users for internal use by community members.[171] The system

---

of law and the customs and practices of international trade rather than the substantive contract law of any particular state.").

[167] *Id.* at 819 (analyzing whether open source software principles can serve as the new Lex Mercatoria of the Internet).

[168] Johnson & Post, *supra* note 159, at 1389 ("[T]he most apt analogy to the rise of a separate law of Cyberspace is the origin of the Law Merchant" or *Lex Mercatoria*).

[169] Joel R. Reidenberg, Lex Informatica: *The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 570 (1998) ("For example, the protocol for sending electronic mail, SMTP, sets a substantive policy default rule for the circulation of identifying information which is an immutable rule of communications transmission.").

[170] *Id.* at 555 ("[T]he set of rules for information flows imposed by technology and communication networks form a "*Lex Informatica*" that policymakers must understand, consciously recognize, and encourage.").

[171] *Id.* at 772 ("*Lex Informatic*a . . . allows for automated and self-executing rule enforcement.").

operates transnationally, across borders, independent of national boundaries and domestic laws.[172] Indeed, by enabling or restricting the type of actions that can be performed on a digital platform, *Lex Informatica* establishes a particular system of (technical) norms which are a direct expression not of the legislator's will, but rather that of the person in charge of developing of such platform.

This particular form of *regulation by code* is currently used to regulate a large variety of relationships on the Internet.[173]-Instead of relying on traditional law enforcement mechanisms, such as court orders or proceedings, which often result in unsatisfactory results because of the difficulty of localizing the tort (since both the infractions and wrongdoers are distributed in several jurisdictions), online operators increasingly rely on technological means as some kind of customary transnational rules applicable at the global level, in a consistent and predictable manner.

In the early 1990s, as the Internet gained popularity, the question emerged as to whether there was a need for a new body of law—*cyberlaw*—that would better understand the relation between the law and the Internet. The question arose as to whether the specificities of cyberspace were enough to justify the creation of a different body of law, with its own logics and rules.

Some claimed that the cyberspace did not qualify as something that is sufficiently unique to constitute a separate section of law. By comparing the *Law of Cyberspace* with the *Law of the Horse,*[174] Professor Frank Easterbrook argued that there was no such thing as *cyberlaw*, since it did not qualify as a substantive legal subject (unlike media law or intellectual property law) which could be regarded as an independent field of legal scholarship. Conventional bodies of law (such as telecommunications law, copyright law, or data protection law) could simply be applied—by extension or analogy—to the digital world.

---

[172] *See* Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 914 (1996) ("Political and economic communities based predominantly on geographic proximity and physical contact have less relevance in cyberspace because network communities can replace physically proximate communities.").

[173] For example, TCP/IP, the basic communication protocols for all Internet activity, allow for transfers of information "without the networks knowing the content of the data, or without any true idea of who in real life the sender of a given bit of data is." Lawrence Lessig, *Code Is Law, On Liberty in Cyberspace*, HARVARD MAGAZINE (Feb. 2000), http://harvardmagazine.com/2000/01/code-is-law-html.

[174] *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996).

This view was challenged by others, most notably by Lawrence Lessig,[175] who considered cyberspace different from the physical space insofar as it is governed by different logics, mainly as a result of the strong malleability of "code" which can itself be turned into law.[176] According to Lessig, when compared to traditional legal doctrines, this requires a significant shift in legal perceptions which might justify the establishment of a separate body of law,[177] one that would better account for the distinctive characteristics of the digital world.

In spite of the initial divergences on the matter, it is now widely acknowledged that *cyberlaw* does, indeed, constitute a separate legal doctrine which comes along with its own theory and underlying principles.

C. The Rise of Lex Cryptographia

Today, we might be facing a similar inflection point in the history of the Internet. Just as the growth of decentralized communications layers, such as TCP/IP and HTTP, lead to the recognition of *Lex Informatica*, the progressive deployment of blockchain technology may give rise to yet another body of law—*Lex Cryptographia*—characterized by a set of rules administered through self-executing smart contracts and decentralized (and potentially autonomous) organizations.

The rise of *Lex Cryptographia* may reopen earlier debates about how to regulate the Internet and will raise new challenges concerning the regulation of decentralized (autonomous) organizations. Existing legal theory assumes that an individual's use of decentralized technology can be controlled by a nation or other regulatory body through the threat of law enforcement (coercive force), the manipulation of markets (financial incentives and disincentives), the development of new social norms (social pressure), or by exerting pressure on centralized intermediaries, such as Internet service providers and other gateways to the Internet like search

---

[175] *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

[176] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE VERSION 2.0 3 (2nd ed. 2006).

[177] *Id.* at 3. ("Cyberspace demands a new understanding of how regulation works. It compels us to look beyond the traditional lawyer's scope—beyond laws, or even norms. It requires a broader account of "regulation," and most importantly, the recognition of a newly salient regulator.").

engines or social networks.[178] With the proper mix of these different levers of power, legal theorists have persuasively argued that our use of the Internet could be tamed and controlled.[179]

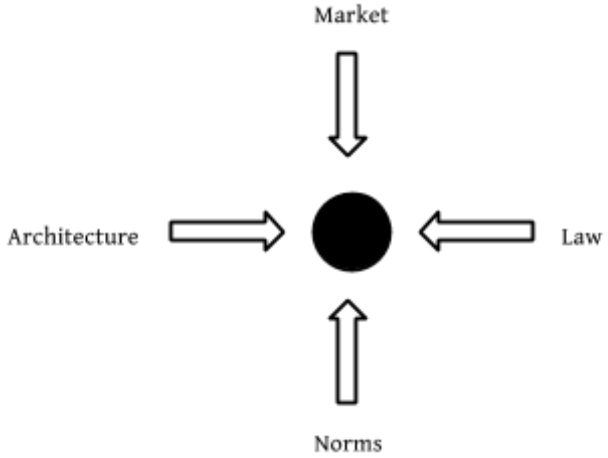

Figure 3 - Lessig's Four Modes of Regulations[180]

This theory has been borne out in practice. Countries routinely pass laws to ban online services, and employ coercive power to seize and shut down illegal services, such as online gambling. Governments and private interests increasingly manipulate markets by pressuring search engines, advertising networks, and other financial intermediaries to protect existing business models, most notably in the case of content and media companies. Regulators, in countries such as China, try to preserve cultural and societal norms, while attempting to further influence individuals by controlling the flow of information that they can be exposed to.[181]

---

[178] GOLDSMITH & WU, *supra* note 82, at 70. ("The rise of networking did not eliminate intermediaries, but rather changed who they are. It created a whole host of intermediaries, most important of which (for our purposes) are ISPs (Internet Service Providers), search engines, browsers, the physical network, and financial intermediaries. In short, the Internet had made the network itself the intermediary for much conduct that we might have thought had no intermediary at all prior to the Internet").

[179] *Id.* at 72-80.

[180] LESSIG, *supra* note 176, at 123.

[181] The most notable example of this conclusion is China. In stark contrast to the decentralized Internet predicted in the 1990s, Chinese Internet users experience a radically different online experience than United States Internet users. Using basic routing technology, and carefully crafted access lists maintained by the Chinese government, China effectively filters access to online services that it does not want its population to use. *See* GOLDSMITH & WU, *supra* note 82, at 87-104.

The advent of *Lex Cryptographia* may force us to reevaluate the interaction between these regulatory levers. One of the key consequences of the blockchain could be a rapid expansion of what Lawrence Lessig referred to as "architecture"—the code, hardware, and structures that constrain how we behave[182]—or at a minimum a redefinition of how laws and regulations are designed, implemented, and enforced

Laws fulfill a variety of different roles: they establish the rights that individuals can invoke against each other or their own governments; they embody threats of punishment and coercion in order to maintain social order, punishing bad actors and incentivizing good behavior; they represent societal values and outline the structures of governments, organizations, and markets.[183]

As set forth above, through the deployment of increasingly complex systems of smart contracts and decentralized organizations, the technology can be used to establish rules and structures for organizations, formal entities, and potentially even governmental bodies. If designed to capture human input, the technology can be used to reflect community values and social norms, automatically enforced through self-executing code. Smart contracts may even re-write or bypass some of the most basic tenets of property law, effectively turning property or even constitutional rights into a subset of contract law.

Judicial enforcement of law could also be displaced by blockchain technology. Smart contracts can be made to rely on a certain degree of human judgment at any point during the contract's execution. For instance, in order to determine whether or not certain contractual conditions have been met, contractual conditions could be made dependent on the judgment of one or more external parties (so-called "Oracles").[184] Of course, one of these parties could be the judiciary, but it could also be a panel of independent arbitrators, or a jury summoned from around the Internet, selected and paid based on their track record of deciding earlier disputes.

---

[182] LESSIG, *supra* note 176, at 24 ("Important rules are imposed, not through social sanctions, and not by the state, but by the very architecture of the particular space. A rule is defined, not through a statute, but through the code that governs the space.").

[183] *Id.* at 340.

[184] *See Contracts*, THE BITCOIN FOUNDATION WIKI, https://en.bitcoin.it/wiki/Contracts (last accessed Mar. 1, 2015) (outlining the technical specifications for oracles); Vitalik Buterin, *Ethereum and Oracles,* ETHEREUM BLOG (July 2014), https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/ (outlining how smart contracts can rely on inputs from third-party data sources).

These decentralized judiciaries can expand dispute resolution procedures, narrowing the role of centralized judicial bodies.

D. The Regulation of Decentralized Architectures

While it might seem that smart contracts and decentralized organizations could take away many of the functions of law and governments, the mainstream deployment of blockchain-based application is unlikely to eliminate the role of these centralized institutions. Rather, it may shift the balance between law and architecture, requiring alternative regulatory mechanisms to successfully manage society.

Over time, the widespread deployment of smart contracts, smart property, and other cryptographically-activated assets will raise a series of important challenges to the current legal framework. Yet, the blockchain is—and will fundamentally remain—a regulatable technology. While states initially had a hard time grasping how to regulate a global and decentralized network like the Internet, they eventually came to the understanding that, as long as there are centralized chokepoints, regulation can be achieved, through the indirect regulation of the various intermediaries and online operators that actually run the network[185]—a task which has been greatly facilitated by growing concentration and centralization of Internet services in recent years.[186]

An analogous situation will likely take place in the context of blockchain technology. Even in a world dominated by decentralized data and organizations, powerful intermediary will still remain. If threatened, states and governmental actors could adopt a series of draconian measures to regulate the emerging online ecosystem and to retain control over the blockchain ecosystem. First, Internet service providers could be pressured to block encrypted data passing through their network, preventing Internet service providers from transmitting any traffic from or to a decentralized (autonomous) organization.[187] Second, regulations could be passed to

---

[185] *See* GOLDSMITH & WU, *supra* note 82, at 65-86.

[186] *Id.* at 71-81 (analyzing the main intermediaries that governments target enforce control over Internet activity including ISPs, financial intermediaries, Domain Name Systems, and information intermediaries such as search engines and social networks).

[187] There is some precedent for this. Internet service providers have previously blocked traffic, most notably traffic related to the BitTorrent protocol. *See* Peter Svensson, *Comcast Blocks Some Internet Traffic*, NBC NEWS (Oct. 19, 2007), http://www.nbcnews.com/id/21376597/ns/technology_and_science-internet/t/comcast-blocks-some-internet-traffic/ (noting that "Comcast Corp. actively interferes with attempts by some of its high-speed Internet subscribers to share files online, a move that runs counter to the tradition of

require that corporate or human-run online intermediaries, such as search engines, purposefully avoid indexing any blockchain-based applications in order to push this technology to unregulable black markets.[188] Third, centralized authorities could attempt to chill the development of unlawful blockchain based organizations by seeking to prosecute software developers or the users of blockchain based institution. Fourth, pressure could be applied to hardware manufacturers—like Apple or Dell—mandating that these organizations purposefully break their products to prevent the use of certain encryption techniques or to implement measures to track.[189]

The result would be a gross abuse of government power, and many of these approaches would likely chill the economic gains that permissionless blockchain technology offers. It would represent a retreat from current attempts to support the free exchange of information, ideas, and commerce on the Internet, which might ultimately raise significant constitutional issues.[190] By imposing requirements on software developers, the government would in effect mandate the code that software developers

---

treating all types of Net traffic equally"). However, it is also worth noting that, over time, Internet service providers may be themselves decentralized through the use of widespread mesh networking. *See* Ryan Paul, *The Darknet Project: netroots activists dream of global mesh network*, ARS TECHNICA (Nov. 7, 2011), http://arstechnica.com/information-technology/2011/11/the-darknet-plan-netroots-activists-dream-of-global-mesh-network/.

[188] Again, this has already happened in the context of websites believed to have engaged in copyright piracy. *See* Christian Bautista, *Google Search Algorithm Changes Demote Piracy Sites From Page Rankings*, Tech Times (Oct. 22, 2014), http://www.techtimes.com/articles/18334/20141022/google-search-algorithm-changes-demote-piracy-sites-from-page-rankings.htm (reporting that Google "in an effort to appease copyright holders, will start taking out websites with pirated content from its search results.").

[189] Such a law was recently suggested by the British Prime Minister. David Cameron. Cameron sought to ban encryption in end-to-end communications. Shortly after the proposal, the plan was dropped. *See* James Ball, *Cameron Wants To Ban Encryption – He Can Say Goodbye To Digital Britain*, THE GUARDIAN (Jan. 13, 2015), http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror.

[190] These were the same issues raised during the "cryptowars." *See* Henry Corrigan-Gibbs, *Keeping Secrets*, STANFORD ALUMNI MAGAZINE (Nov. 2014), https://alumni.stanford.edu/get/page/magazine/article/?article_id=74801. ("At the time, knowledge of how to encrypt and decrypt information was the domain of government; the NSA feared that making the secrets of cryptography public would severely hamper intelligence operations. But as the researchers saw it, society's growing dependence on computers meant that the private sector would also need effective measures to safeguard information. Both sides' concerns proved prescient; their conflict foreshadowed what would become a universal tug-of-war between privacy-conscious technologists and security-conscious government officials.").

can write.[191] Similarly, laws requiring the development of broken hardware to prevent encryption would violate fundamental human rights by forcing citizens to communicate in a way that limits their ability to protect their own privacy.

In this sense, the implementation of blockchain technology could eventually fall into the same trap as the original Internet. The Internet was originally regarded as a source of individual freedom and emancipation. Today, while it unquestionable that it has enhanced the expression of free speech, it has also become a tool for surveillance and control. Governments use Internet technology to conduct mass surveillance. Internet advertisers track users across websites to better target ads. Google records every click on thousands of websites across the Internet, only disclosing how it uses user data with vague proclamations in its privacy policy.

Without appropriate legal safeguards, it is plausible that the development of blockchain technology could follow a similar path, leading to increased surveillance. In spite of the opportunities for the development of worldwide systems, the state or other centralized bodies could, indeed, use the technology to exercise a significant degree of control over people's interactions and online communications.[192] As more and more of our economic transactions and social interactions occur in a networked environment, the technology could increasingly be used to regulate people's behavior, to ensure that they remain consistent with the law or with the contractual obligations that they have entered into. The blockchain could be used, for instance, to manage identity, making it easier to monitor, surveil,[193] or simply keep track of various online activities. Every transfer,

---

[191] *See* Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996) (mathematician sought declaratory and injunctive relief against enforcement of the Arms Export Control Act and the International Traffic in Arms Regulations on the grounds that they were unconstitutional on their face and as applied to mathematician's cryptographic computer source code. The District Court held that cryptographic computer source code is "speech" protected by First Amendment, and colorable constitutional challenges to statute and regulations were justiciable).

[192] Although the blockchain is inherently decentralized and cannot be controlled by any single entity, in practice, the situation is quite different. As the Bitcoin network has shown, substantial power dynamics might emerge with this technology. For example, blockchains that use a Proof of Work consensus mechanism can have computational power concentrated into the hands of a few large mining pools that could conceivably collude and cheat the network. *See* Bonneau, *supra* note 22, at 11.

[193] Even considering the pseudonymous nature of the blockchain, it is already possible to trace back certain transactions to a particular identity, or even just to infer the identity of the person associated with a particular address by means of big data analysis over the blockchain (so-called blockchain analytics). *See* Sarah Meiklejohn et al., *A Fistful of*

vote, purchase can be recorded on the blockchain, creating a permanent record that will potentially push the boundaries of privacy law. Regulators might further require that online operators within the blockchain ecosystem to refuse to deal or transact with unidentified parties that have not satisfied AML or KYC requirements,[194] undermining the pseudonymous nature of the blockchain and turning it into a powerful tool of surveillance and control.

Beyond the evolving dynamic between law and architecture, blockchain-based applications could also raise interesting and novel legal questions concerning the regulation of decentralized (autonomous) organizations. As opposed to traditional online applications, which are ultimately stored on a server at a particular location, decentralized organizations are deployed directly on the blockchain. They do not subsist at any given geographic location, but rather operate transnationally regardless of any national boundaries or jurisdictions. While decentralized organizations, which are actively managed by online users, could be regulated much like a limited liability corporation or another corporate form, the same cannot be said of decentralized autonomous organization. As opposed to traditional corporations or organizations, decentralized autonomous organization are not owned nor controlled by any single corporate or governmental agency, nor any individual person; yet they can interact with the public in a way that might give rise to specific rights and obligations. Decentralized organizations can thus have a significant effect on third parties, and might even be at the source of certain torts or wrongdoings.

Bitcoins: Characterizing Payments Among Men with No Names, UNIV. OF CAL., SAN DIEGO (2013), https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf. Several initiatives have already been deployed to explore the Bitcoin blockchain in order to get a better understanding of the leading forces within its ecosystem. Coinalytics, for instance, analyses the Bitcoin blockchain through sophisticated data analytics techniques, as an attempt to build up identifiable profiles. *See* COINALYTICS, http://coinalytics.co/ (last accessed Mar. 4, 2015) (Coinalytics builds tools that aggregate data from the Bitcoin blockchain and analyze trends to provide answers for compliance, business intelligence and finance). Coinalytics works by aggregating all sorts of transaction data into specific clusters of Bitcoin addresses, which can be subsequently connected to real-world identities. Another similar initiative is BlockTrail whose objective is to unravel hidden blockchain information by providing insights into Bitcoin transactions and network data. *See* BLOCTRAIL, https://www.blocktrail.com/ (last accessed Mar. 4, 2015) (BlockTrail provides secure Bitcoin application program interface for developers and enterprises). Today, it is already possible to identify certain Bitcoin addresses which are the most likely to be involved in the process of mining, as well as to keep track of those which have been associated with illicit transactions, such as gambling or money laundering.

[194] *See* notes 95-96, *supra* for an overview of AML and KYC rules.

This raises new fundamental questions such as how can the law determine who is in charge of, and who is responsible for the activities of these new organizations? A plausible answer would be to adopt *the nearest person theory* and assume that the creator of a decentralized autonomous organization should be held jointly liable for any foreseeable damages it might cause under product liability law. Compensation would therefore have to be paid for by the creators, possibly by divesting the funds that the decentralized autonomous organization uses to operate. Such an answer assumes, however, that the creators of a decentralized autonomous organization can always be identified, whereas such an organization could potentially be created by hundreds, if not thousands of anonymous individuals, or even other decentralized autonomous organizations.

Alternatively, one might argue that the users of a decentralized autonomous organization should be held vicariously liable for the services they are paying for, if they in some way can control and receive direct or indirect financial benefit from the decentralized autonomous organization's operation. Again, however, holding users liable presents causation issues. It would be unjust to hold a user liable for a third party's actions, which the user did not know, or did not have a good reasons to believe could potentially cause harm to someone.

Perhaps, the decentralized autonomous organization itself should be held liable for its own misdemeanors. Yet, given the properties of smart contracts and distributed blockchains, it is virtually impossible to recover damages, or to obtain an injunction against a decentralized autonomous organization, unless these measures have been specifically encoded into the contract or the organizational structure of the decentralized autonomous organization.

As a result, because decentralized organizations will be difficult to shut down, the role of laws that directly ban certain online activity may narrow. If decentralized autonomous organizations accommodate unmet consumer demand, or act as an attractive alternative to consumers by offering, for example, lower prices, regulators will have a hard time stopping these services without resorting to measures that are highly coercive and likely violative of fundamental rights, such as the right to privacy and freedom of expression.

Thus, unless these organizations have been designed to cooperate with the regulatory framework in which they operate, states and regulators might actually lose their ability to regulate them by relying exclusively on

the law. To regulate society, laws may need to be directly embedded into code or laws may need to shape social norms, structure markets, and influence architectural design in order to incentivize the proper deployment of decentralized organizations. Left without such alternatives, governments could attempt to preserve their hegemony by resorting to draconian measures, such as filtering internet service providers, blacklisting malicious decentralized autonomous organizations and criminalizing software developers, introducing back doors on everyone's computer to monitor citizen behavior, or adopting more extreme coercive measures. New regulatory approaches therefore need to be taken, else the fundamental principles of an open Internet and permissionless innovation could eventually disintegrate.

CONCLUSION

The rise of *Lex Cryptographia* presents a world where ideals of individual freedom and emancipation might come true. The blockchain could offer people access to alternative currencies, global markets, automated and trustless transactions systems, self-enforcing smart contracts, smart property and cryptographically activated assets, and innovative models of governance based on transparency and corruption-free voting. Combined, these elements could be used to promote individual freedoms and user autonomy. Regardless of nationality, people could be granted equal access to basic digital institutions and infrastructure such as decentralized laws, markets, judiciaries, and payment systems, which can be customized to each country's, group's, and individual's needs. Decentralized institutions and governance models could be designed and constructed iteratively, through use and experimentation of emergent blockchain-based applications, rather than being imposed by centralized legal edicts. This could significantly contribute to the process of disintermediation that has characterized the online world.

Yet, as with every technology, cryptographically secured blockchains can be used for both good and evil. In spite of its benefits, many of the emerging applications also come with important drawbacks. Given the transnational, encrypted, and decentralized nature of blockchain-based applications, ill-intentioned individuals can use it for illicit transactions. This, along with the pseudonymity provided by the blockchain, may make it increasingly difficult for law enforcement agencies to identify and prosecute the users of these emergent technologies.

With the growth of blockchain technology, the role of middleman and other centralized gatekeepers may narrow, requiring a recalibration as

to how we regulate individual behavior. As more and more communities form (and formalize) their own values, transposing community practices and social norms into the code governing decentralized organizations, individual behavior will become more difficult to mold through external forces imposed by third parties, such as national laws and regulations. If law becomes less efficient in its capacity to regulate individual behavior, governments and other state actors will be forced to regulate individuals indirectly by shaping social norms, intervening into markets, and regulating the design of the architecture or code.

Further frustrating regulation, in a decentralized environment, governments and states may need to adopt a different approach to shape markets. Markets and marketplaces created or maintained by decentralized autonomous organizations will not readily allow for government intervention. Laws trying to avoid market manipulation, price cutting, or other anticompetitive practices, as well as regulations banning marketplaces from selling a good or product will, therefore, become much harder to enforce.

Finally, the open nature of blockchain-based architecture means that most, if not all of the applications deployed on the blockchain could be reproduced and adjusted by anyone, in order to fulfill different functions and satisfy the needs of different groups and communities. As a result, dictating the manner in which software developers design a particular application protocol, or forcing software developers to introduce a particular feature into the code will only work to the extent that the user-base actually agrees to switch to the new protocol. Failure to reach consensus amongst users means that software will remain in use.

Of course, states can always adopt coercive measures in order to force users to update their clients. Yet, in this context, regulating architecture can be a treacherous task and, without careful contemplation, runs the risk of undercutting the powerful interconnectivity of the Internet and traditional notions of free expression.

Thus, if we want to preserve the opportunities provided by emerging blockchain technologies—in terms of individual freedoms and emancipation, democratic institutions, and creative expression—while avoiding or reducing to the minimum the possible drawbacks that they might introduce in society, the time has come to start thinking about a new paradigm of law that could balance the power of blockchain technology and

emerging autonomous systems in ways that promote economic growth, free speech, democratic institutions, and the protection of individual liberties.