A Blockchain Bookshelf

[As of 07/12/18; from Blockchainforlawstudents.com]

Professor Walter A. Effross
American University Washington College of Law

[Books not available for free online are identified by * instead of ●]

Philosophical and Political Foundations

● John Perry Barlow, *A Declaration of the Independence of Cyberspace* (1996)- A non-lawyer's (but Grateful Dead lyricist's) famous early manifesto rejecting any governmental regulation of "Cyberspace, the new home of Mind."

Relevant to discussions of blockchain and cryptocurrency because both systems can be used to eliminate the traditional role/requirement of government as a trusted third party. Moreover, though many of Barlow's proclamations may now seem impossibly utopian/naïve, they're worth reading as a product of their time and as a continuing influence on online and offline culture and law.

● Timothy May, *The Crypto Anarchist Manifesto* (1988)- May predicted that the popularization of powerful encryption techniques would "fundamentally alter the nature of corporations and of government interference in economic transactions" and would "create a liquid market" for intellectual property.

● Eric Hughes, *A Cypherpunk's Manifesto* (1993)- Declares that

> We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. . . .
>
> We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.
>
> Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. . . .
>
> . . . . Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.
>
> For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good.

***** Steven Levy, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age* (2001)- An illumination account of the independent rediscovery and dissemination, by a group of cypherpunks operating in the 1970s through the 1990s, of the "public key encryption" technology (which would later underlie blockchain) then closely-held by the intelligence community. Of particular interest: pages (in the Penguin edition) 69-73, 84-88, 102-105, 201-203, and 215-219.

***** Steven Levy, *Hackers: Heroes of the Computer Revolution* (1984)- Like *Crypto*, emphasizes the emergence of communities, connections, and cultures in the context of developing technology; but, unlike that book, chronicles the rise of a proprietary, as opposed to literal and figurative free-sharing, model of software development. (A watershed moment was the 1976 dissemination of a letter signed by Bill Gates as a "General Partner, Micro-Soft," protesting the unauthorized copying of its BASIC software: "As the majority of hobbyists must be aware, most of you steal your software.")

Levy revisited many of his profile subjects twenty-five years later in the Wired magazine article, *Master Minds* (May 2010).

● Eric S. Raymond, *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (1999)- An illuminating collection of essays contrasting proprietary, restricted-access methods ("cathedrals") with transparent, universally-accessible methods ("bazaars") of software development, and emphasizing the virtues of the latter's "hacker" culture.

Prefigures the "open-source" nature of blockchain, the creation of "permissioned" or "private" blockchains, and the "strong social pressure against forking projects. It does not happen except under plea of dire necessity, with much public self-justification, and with a renaming."

"Here, I think, is the core difference underlying the cathedral-builder and bazaar styles. In the cathedral-builder view of programming, bugs and development problems are tricky, insidious, deep phenomena. It takes months of scrutiny by a dedicated few to develop confidence that you've winkled them all out. Thus the long release intervals, and the inevitable disappointment when long-awaited releases are not perfect.

"In the bazaar view, on the other hand, you assume that bugs are generally shallow phenomena—or, at least, that they turn shallow quickly when exposed to a thousand eager co-developers pounding on every new release. Accordingly you release often in order to get more corrections, and as a beneficial side effect you have less to lose if an occasional botch gets out the door. . . . "

However, "[i]t's fairly clear that one cannot code from the ground up in bazaar style. One can test, debug, and improve in bazaar style, but it would be very hard to *originate* a project in bazaar mode."

● Vitalik Buterin, *The Meaning of Decentralization* (posted on Medium site, February 6, 2017). A founder of the Ethereum platform explains that "When people talk about software decentralization, there are actually *three separate axes* of centralization/decentralization that they may be talking about. While in some cases it is difficult to see how you can have one without the other, in general they are quite independent of each other."

Buterin discusses "Three Reasons for Decentralization" and notes that "[a]ll three arguments are important and valid, but all three arguments lead to some interesting and different conclusions once you start thinking about protocol decisions with the three individual perspectives in mind."

Overviews- Blockchain and its Applications

● Jamie Berryhill et al., *Blockchains Unchained: Blockchain Technology and Its Use in the Public Sector*, OECD [Organisation for Economic Co-operation and Development] Working Papers on Public Governance No. 28 (2018)

Summarizes blockchain technology, definitions, and uses; discusses public-private partnership, and governmental, applications of blockchain; and provides a useful review of the possible disadvantages of such applications. Includes an appendix with eight "case studies."

● Angela Walch, *The Path of the Blockchain Lexicon (and the Law)*, 36 Rev. Banking & Fin. L. 713 (2017). Focuses on "the technology's fluid, contested vocabulary[, which] can cause a variety of problems for regulators." Offers practical suggestions ("Seek to Separate Hype from Reality"; "Consider the Source (and the Source's Incentives)"; "Seek Diverse Perspectives'); "Doubt Everything and Trust No One"; "Resist Peer Pressure") relevant not just to regulators but to researchers generally.

● Center for Digital Commerce, *Blockchain and Financial Inclusion* (March 2017). This white paper examines the advantages and risks of using blockchain in this context; notes Anti-Money Laundering (AML), Know Your Customer (KYC), and consumer protection concerns; presents three case studies (Coins.ph, BitPesa, and Unocoin); and concludes that "collective action from private sectors and government is required to provide innovative solutions within a supportive ecosystem. Blockchain is not the only answer, but it can be part of the solution and requires partnerships with existing [financial institutions]."

***** Michael J. Casey & Paul Vigna, *The Truth Machine: The Blockchain and the Future of Everything* (2018)

* Don Tapscott & Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World* (2016)

Both books discuss the operation of blockchain, and its potential-- beyond enabling Bitcoin and other cryptocurrencies—to revolutionize financial, contracting, voting, distribution of intellectual property, and other processes.

The Tapscotts' book is organized more around lists (*e.g.*, "Seven Design Principles of the Blockchain Economy"; "The Twelve Disruptions"' "Ten Implementation Challenges"), and features several useful diagrams (including "The Golden Eight: Blockchain Transformations of Financial Services."

Casey & Vigna warn (at 223), that "the legal industry is . . . in for a huge shakeup. Lawyers who don't understand code are likely going to be valued far less than those who do."

***** Daniel Drescher, *Blockchain Basics: A Non-technical Introduction in 25 Steps* (2017)

***** Shawn Amuial et al., *The Blockchain: A Guide for Legal and Business Professionals* (2016)

Both present user-friendly, non-mathematical guides to the technology—and both contain helpful diagrams.

● The Center for Legal Innovation of Vermont Law School, *Financial Technology Report* (December 7, 2017). A wide-ranging analysis, commissioned by the Vermont Legislature, of "possible legal and regulatory actions that could, on the one hand, create a hospitable climate for blockchain and other financial technology developments, while, on the other hand, protecting Vermonters from risks created by these innovations."

Citing many online resources, the document "provide[s] a summary-level description of a range of possibilities" but "do[es] not advocate for or against the adoption of any of [them]."

Among the more interesting suggestions: the introduction of a new specialized form of business organization, such as a Digital Currency LLC ("DLLC"), for use by the operators of blockchain and cryptocurrency networks; and the creation of "a framework for recognizing autonomous agent corporations via a sub-chapter of the Vermont corporate code."

<u>Overviews- Cryptocurrency</u>

***** Paul Vigna & Michael J. Casey, *The Age of Cryptocurrency* (revised ed. 2016)

***** Nathaniel Popper, *Digital Gold* (reprint ed. 2016)

***** Brian Patrick Eha, *How Money Got Free* (2017)

Three accounts of the development and refinement of Bitcoin and other cryptocurrencies, including the effects of: the 9/11 attacks; the financial crisis of 2007-2008; the Occupy Wall Street movement (2011); the hacking of and ultimate bankruptcy of the pioneering Bitcoin exchange, Mt. Gox (2014); and the swift rise and sudden government shutdown of the outlaw Silk Road online marketplace (2011-2013).

Eha's book may be of most use to law students, because of its deep profiles of cryptocurrency entrepreneurs, of the tensions among them and between them and their investors and regulators, and of the firms' designing their business models to meet (or bypass) existing and emerging laws and regulations. One entrepreneur told the author, "If you're just starting up, you're almost forced to break the [criminal] law and hope that you can get away with it long enough to produce some traction" to secure investors' money, after which you can try to meet regulatory requirements. Another concurred, "We're all forced to break the law until someone calls us out."

The Vigna/Casey book provides particularly good discussions of the ways in which cryptocurrency differs from traditional "fiat currencies," of the blockchain mechanism underlying cryptocurrency, and of the ways in which the new technology can be used to provide funds and a fund-transfer mechanism to "unbanked" individuals in developing areas.

<u>Technical Foundations</u>

As Steven Levy (above) discusses, two of the seminal papers in public key encryption are:

● Whitfield Diffie & Marin E. Hellman, *New Directions in Cryptography*, IEEE [Institute of Electrical and Electronics Engineers] Transactions in Information Theory, IT-22(6) (November 1976), pp. 644-654

● R. L. Rivest, A. Shamir & L. Adleman, *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Communications of the ACM [Association for Computing Machinery], 21(2), pp. 120-126 (February 1978)

● Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008). The pseudonymous nine-page "White Paper" that started it all when posted online in November 2008, outlining the design of "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." Technical. For amplification and commentary by the author, see *The Book of Satoshi*, below.

***** *The Book of Satoshi* (Phil Champagne, ed.) (2014) A collection, classified by subject and with some editorial commentary (and the editor's very useful practical introduction), of Satoshi Nakamoto's listserv postings and e-mails between late 2008 and late 2010, most in answer to other cryptographers' questions about the technical operations of his system.

Towards the end of his "public period," when PayPal declined to serve as a conduit for donations to the controversial WikiLeaks site, Nakamoto opposed proposals to encourage Bitcoin donations: "The [Bitcoin] project needs to grow gradually so the software can be strengthened along the way. I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage."

Six days later, in response to a computer magazine's suggestion that the WikiLeaks situation could encourage the use of cryptocurrency, Nakamoto posted, "It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us."

At one point, Nakamoto wrote, "I'm better with code than with words, though." But as this book proves, he was very good with words, and certainly not (so to speak) cryptic in many of his posts.

● National Institute of Standards and Technology, *Blockchain Technology Overview* (2018)- A great introduction, with diagrams. (Also helpful: NIST's *Introduction to Public Key Technology and the Federal PKI Infrastructure* (2001).)

● American Council for Technology-Industry Advisory Council, *Enabling Blockchain Innovation in the U.S. Federal Government: A Blockchain Primer* (2017)- Focuses on current and potential applications of blockchain.

● Rebecca Lewis et al., *Blockchain and Financial Market Innovation, Federal Reserve Bank of Chicago, Economic Perspectives*, Vol. 4, No. 7 (2017)- Offers "a brief overview of what

blockchain technology is, how it works, and some potential applications and challenges," including a set of diagrams.

● David Mills et al., *Distributed ledger technology in payments, clearing and settlement*, Finance and Economics Discussion Series 2016-095, Divisions of Research & Statistics and Monetary Affairs, Federal Reserve Board (2016)- Concludes that the technology

> has the potential to provide new ways to transfer and record the ownership of digital assets; immutably and securely store information; provide for identity management; and other evolving operations through peer-to-peer networking, access to a distributed but common ledger among participants, and cryptography. . . . Nonetheless, the industry's understanding and application of this technology is still in its infancy, and stakeholders are taking a variety of approaches toward its development. Given the technology's early stage, a number of challenges to development and adoption remain, including in how issues around business cases, technological hurdles, legal considerations, and risk management considerations are addressed.

*****Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (2016) [Hardcover published in 2016, but a draft dated February 9, 2016 is available online at no charge.]

Useful but somewhat technical— the authors did not use the word "comprehensive" loosely.

● Ian Grigg, *Financial Cryptography in Seven Layers* (1998-2000). Identifies and discusses the interactions of seven "critical disciplines" in the design and operation of financial cryptography: finance, value, governance, accounting, rights, software engineering, and cryptography. Readers might consider, where and how the law does, or should, fit into this framework.

***** Andreas M. Antonopoulos, *The Internet of Money*, Vol. 1 (2016) & Vol. 2 (2017)

Brief collections of edited transcripts of the author's presentations on Bitcoin and blockchain, videos of which are available online.

Volume 1 is particularly useful in dispelling some of the fuzziness of easy metaphors for cryptocurrencies (see pp. 81-82, concerning misleading references to "wallets" and "coins," and p.92, "The Problem with Traditional Banking Metaphors").

Volume 2 identifies "proof of work" as a central characteristic of blockchain, and attacks many "permissioned 'distributed ledgers'" as mere "databases" constructed by participants who simply "assemble transactions and sign them. . . . It's not a blockchain anymore, because there are no blocks and there is no chain." Permissioned blockchains are also, asserts the author, more likely to be vulnerable to cyberattacks than those, like Bitcoin, that are publicly available.

While decrying the recent tendency to characterize everything as a "dapp" (or, "decentralized application"), Antonopoulos identifies smart contracts, and particularly the articles of organization of a decentralized autonomous organization (DAO), as the "killer app" for Ethereum.

***** Henning Dietrich, *Ethereum* (2016)

Many short chapters, including discussions of 85 pithy pronouncements (such as "Blockchains collapse agreement and execution" and "You can't defeat a protocol") and overviews of 30 key elements ("What is Ether?"; "What is a Mirror Asset?") An easily-accessible overview of and perspective on blockchain, smart contracts, and their strengths and limitations.

Regulation

● Lawrence Lessig, *Code: And Other Laws of Cyberspace* (version 2.0) (2006)- An update of the law professor's pioneering 1999 work. Lessig warns, "We can build, or architect, or *code* cyberspace to protect values [including online privacy/anonymity] that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no middle choice that does not include some kind of building."

And: "If some architectures are more regulable than others—if some give governments more control than others—then governments will favor some architectures more than others."

Of particular interest: the discussion (pp. 120-137) of the "regulation" of an individual's activities as the net effect of four interacting "constraints": "the law, social norms, the market, and architecture."

***** Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* (2018)- In 210 pages (followed by 75 pages of notes), the authors describe the operation and applications of blockchain and the regulatory questions that they raise.

De Filippi and Wright discuss in detail the way in which blockchain-enabled systems can be developed to "operate autonomously,. . . and designed in such a way that they cannot be altered by any single party. . . . These systems can be designed to undermine and erode existing social structures or enhance and protect them. . . . Traditional legal doctrines, especially those focused on regulating middlemen, will not easily translate to these. . . systems, and the broader adoption of blockchain technologies may ultimately require the development of alternative mechanisms of regulation. . . ."

● Don Tapscott & Alex Tapscott, *Realizing the Potential of Blockchain: A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies,* World Economic Forum White Paper (June 2017)

The Tapscotts argue that "this blockchain era should not be governed by nation states, state-based institutions or corporations," but instead "through a multistakeholder approach" involving networks that develop and provide: standards, knowledge, products and services, policy, advocacy, scrutiny of participants, and combinations thereof.

"By governance, we mean stewardship, which involves collaborating, identifying common interests and creating incentives to act on them. We do not mean government, regulation, or top-down control. We explore governance needs at three levels: platform, application, and the ecosystem as a whole."

Smart Contracts

● Smart Contracts Alliance (Chamber of Digital Commerce), *Smart Contracts: 12 Use Cases for Business & Beyond* (December 2016)

Identifies the building blocks of smart contracts, and reviews twelve applications: digital identity; records; securities; trade finance; derivatives; financial data recording; mortgages; land title recording; supply chain; auto insurance; clinical trials; and cancer research. Provides an overview of legal and regulatory issues.

● Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, First Monday, Vol. 2(9) (Sept. 1, 1997)

The computer scientist, lawyer, and digital currency pioneer (and, in the eyes of some, a candidate for the person behind "Satoshi Nakamoto") clarifies that "[t]he contractual phases of search, negotiation, commitment, performance, and adjudication constitute the realm of smart contracts. This article covers all phases, with an emphasis on performance. Smart contracts utilize protocols and user interfaces to facilitate all steps of the contracting process."

Szabo concludes, after examining topics including "Contemporary Practice,' "Dimensions of Contract Design," "Building Blocks of Smart Contract Protocols," that "[s]mart contracts reduce mental and computational transaction costs, imposed by either principals, third parties, or their tools."

● Nick Szabo, *A Formal Language for Analyzing Contracts* (Preliminary Draft, 2002)

Offers "a mini-language for professionals and researchers interested in drafting and analyzing contracts. It is intended for computers to read, too. The main purpose of this language is to specify, as unambiguously and completely and succinctly as possible, common contracts or contractual terms. These include financial contracts, liens and other kinds of security, transfer of ownership, performance of online services, and supply chain workflow."

Should be of special interest to those concerned with creating "smart contracts."

● Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform* (2014)- The "white paper," posted on coding site GitHub, that envisioned what became the Ethereum blockchain.

Decentralized Autonomous Organizations (DAOs)

● Vitalik Buterin, *DAOs, DACs, DAs and More: An Incomplete Terminology Guide,* posted on Ethereum Blog, May 6, 2014: warns that "no one even knows what all of these individual terms mean. What exactly is a decentralized organization, what is the difference between an organization and an application, and what even makes something autonomous in the first place? . . . . The intent of this article will be to delve into some of these concepts, and see if we can come up with at least the beginnings of a coherent understanding of what all of these things actually are."

Blockchain in Voting

● Democracy Earth Foundation, *The Social Smart Contract: An Open Source White Paper* (Version 0.2; January 25, 2018). Discusses the political need for, and the technological operations of, "Sovereign, a blockchain liquid democracy that enables direct voting on issues as well as the ability to delegate voting power on specific topics to peers over a secure network without central authority. By operating with tokens signaled on a blockchain all votes become censorship resistant and immediate audit rights can be granted to every voter without needing to provide access to servers or private infrastructure, thus making the system open and transparent for all."

Cryptocurrency Concerns

● Consumer Financial Protection Bureau, *Consumer Advisory: Risks to Consumers Posed by Virtual Currencies* (August 2014). Nineteen practical warnings, such as "Know who you're dealing with if you decide to buy," and "Bitcoin transactions may not be entirely anonymous."

Also see North American Securities Administrators Association (NASAA), *Informed Investor Advisory: Initial Coin Offerings* (April 2018)

● U.S. Commodities Futures Trading Commission, *A CFTC Primer on Virtual Currencies* (October 17, 2017)- A deck of slides discussing the basics of virtual currencies and the Commission's role in their regulation.

● Brett Scott, *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?*, United National Institute for Research and Social Development Working Paper 2016-1 (February 2016). Reviews technical principles and critically discusses social justice applications. Scott concludes,

> The technology is still new, but it is apparent that there are potentially empowering uses of it in certain contexts. Nevertheless, while the community around this technology is enthusiastic and experimental, it is still prone towards the elitist, tech-centric outlook of disruptive technology start-up culture. A key role for [social justice] practitioners then, is to consider how blockchain technology could be implemented with sensitivity to the real struggles people face in implementing technology within diverse cultural and political contexts. One blockchain does not fit all.

Also of possible interest:

***** Nick Bilton, *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road* (2017). An account of the activities, apprehension, and sentencing (to life

imprisonment) of libertarian Ross Ulbricht, the creator and operator of the Silk Road website that connected buyers and sellers of narcotics, weapons, and hacking software.

Portrays Bitcoin as the crucial "missing piece Ross had been waiting for to build his experimental world with no rules." However. Ulbricht himself lost Bitcoins to a hacker stealing them from Ulricht's account; to a rogue law enforcement agent using an informant's identity to withdraw funds from users' accounts; and to a hacker who demanded payment in order to restore the site's operation. He also used Bitcoin to pay a rogue law enforcement agent for information.

Blockchain Law Blogs

Baker Hostetler- The Blockchain Monitor
https://www.theblockchainmonitor.com/

Burr Forman
http://www.burr.com/blogs/blockchain-law/#

CKR Law Blockchain Blog
https://www.ckrlaw.com/blockchain-blog

Covington- Cov Financial Services
https://www.covfinancialservices.com/

Frost Brown and Todd
https://www.frostbrowntodd.com/services-practices-blockchain-and-digital-currency.html
{Click on "In the News"]

Goodwin Procter LLP Digital Currency + Blockchain Perspectives
https://www.digitalcurrencyperspectives.com/

Gordon Law Group Blog
https://gordonlawltd.com/blog/

K&L Gates FinTech Law Watch
https://www.fintechlawblog.com/

Michael Best & Friedrich LLC
https://blockchainplusthelaw.com

Murphy & McGonigle Blockchain Law Center
https://blockchainlawcenter.com

Perkins Coie Virtual Currency Report
https://www.virtualcurrencyreport.com

Proskauer
https://www.blockchainandthelaw.com/

Related Sites

Bitcoin Magazine
https://bitcoinmagazine.com

CoinDesk, A Beginner's Guide to Blockchain Technology
https://www.coindesk.com/information/