AN EMERGING POLITICAL ECONOMY OF THE BLOCKCHAIN: ENHANCING REGULATORY OPPORTUNITIES*

John W. Bagby,** David Reitter,*** and Philip Chwistek****

I. INTRODUCTION

New technologies seldom integrate immediately, well or even ultimately into existing public policy. Existing law, regulations and prevailing contracting practices are largely the product of traditional, fairly well-understood technologies, social mores and customs. Policy adjusts slowly to change, and, too often, it adjusts excruciatingly so. This delay tolerates the largely unimpeded disruptive introduction of technologies, permitting the transformation of institutions in unexpected ways. The delay often fails to compel public policy to operate ex ante, possibly enabling the prevention of future externalities during a technology's early stages of introduction. Blockchain exhibits these characteristics.

The institutional framework of public policy necessarily adapts slowly in response to changing technologies. This is perhaps the most fundamental feature of laissez-faire, democratic capitalism. Such matters are complicated by the novel ontologies developed by technologists. Their taxonomies are inadequately reflected in the public policy lexicon.[1] But the difficulties do not stop at policy makers misunderstanding of technology. Technologists regularly assume away regulation if their inventions are designed to skirt regulation. Indeed, blockchain regulation is also complicated by *Internet Exceptionalism*, the fairly accurate observation that technology can avoid policy influence, particularly in the near term. This is an impudent form of laissez-faire that taunts public choice advocates about the latter's difficulties in exercise of control over often anonymous actors

---

* Blockchains are inherently secure, encrypted technologies, enabling electronic transaction processing, communications, authentication, and recordkeeping. Blockchain circumvents traditional (banking) systems, promising transaction cost savings and speculative profits. Blockchain is an open, encrypted and distributed ledger system underlying cryptocurrencies (Bitcoin) and initial coin offerings (ICO). Both masquerade as media of exchange. Future blockchain applications include supply chains, identity management and healthcare information exchange. Blockchains' technical complexity obscure comprehension by many legislators, regulators, lawyers and judges. Libertarian technologists cheer these barriers to regulation. This paper explores blockchain operations, reviews evolving cryptocurrency policies, and proposes regulatory approaches, urging expanded jurisdiction over blockchain bubbles.

** Professor Emeritus, College of Information Sciences & Technology & Smeal College of Business, The Pennsylvania State University, jbagby146@outlook.com

*** Associate Professor of Information Sciences and Technology, The Pennsylvania State University.

**** Schreyer Honors College candidate, College of Information Sciences & Technology, The Pennsylvania State University.

[1] *See*, Walch, Angela, *The Path Of The Blockchain Lexicon (And The Law)*, 36 REV.BANK.& FIN.L.713 (2016-2017) *accessible at*: http://www.bu.edu/rbfl/files/2017/09/p729.pdf (arguing blockchain nomenclature is ill-defined contributing to regulatory challenges, such as how it is esoteric controversy that is "notoriously confusing, with disputes over whether a blockchain is the same as a distributed ledger, or whether an appcoin is the same as a protocol token").

residing in secret, temporary and/or obscure (cyber-)locations.[2] The jurisdiction of courts and the authority of government over online activities is too often weak given the mobility of servers to easily "forum shop" by crossing borders, sometimes instantaneously or even frequently, to reside in more friendly venues or domiciles.[3]

A. The Interdisciplinary Problem

The blockchain is a large data set of every transaction ever consummated on this distributed network of independent nodes or computers. Transactions are authenticated, or proven valid, but not duplicated, by the use of public-private key encryption to validate and anonymize the connections between each component of a transaction data. In some cryptocurrency applications of blockchain technology, unique software resides on each node to permit various actions like recording transactions, proving ownership or mining (creating) new money. These blockchain descriptions point to the unique perspectives of several disciplines that show interest in blockchain architecture and applications.

At least two regulatory difficulties arise with blockchain: (1) the policy wonk views of technology and (2) technologists views of policy. But these two perspectives may only be the start of the problem. At least four additional bilateral misunderstandings should be considered. When blockchain involves virtual money, then monetary economics must be introduced. Technologists generally appear to understand a few major aspects of monetary economics, but in their zeal to create cool new technologies, they neglect to recheck with economists as their technologies are designed, coded (manufactured), promoted (hyped), deployed and maintained (adapted to marketplace demands and policy demands). By contrast, monetary economists are intrigued but discouraged by cryptocurrencies as they speculate how the most basic assumptions of monetary economics could be dismantled. Relations among public policy wonks and monetary economists is a mixed bag: there is some substantial overlap, both sides embrace the inevitability, even interdependency with each other, but safe zones also exist for each side to operate limited monopolies on certain functions in managing how new forms of money work.[4] All these fields have become smitten by FinTech, an emerging form

---

[2] *See e.g.,* Bagby, John W. (special issue editor), *Cyberlaw: A Forward, Special Issue on Cyberlaw*, 39 AM.BUS.L.J. 521, 523 (Summer 2002) (arguing (1) anarchy in cyberspace retards effective regulation, (2) that some theorists argue for forbearance in regulating transformational, nascent institutions to encourage their development, and (3) that the resulting tension between evolutionary and revolutionary forces requires more methodical, thoughtful reconsideration of first principles before the rush to regulation). *See also,* Post, David G., *What Larry Doesn't Get: Code, Law and Liberty in Cyberspace*, 52 STAN. L. REV. 1439 (2000), Samuelson, Pamela, *Five Challenges for Regulating the Global Information Society*, in REGULATING THE GLOBAL INFORMATION SOCIETY (Chris Marsden ed., 2000), Lessig, Lawrence, CODE AND OTHER LAWS OF CYBERSPACE (1999), Easterbrook, Frank H., *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL FOUND. 207.

[3] *See generally*, Bagby, John W., ECOMMERCE LAW: ISSUES FOR BUSINESS at 29-32 (West 2003).

[4] Of course, financial economists specialize in investment and commodity market aspects of these fields. Along with accountants who have managed most ledgers for centuries, these financial

of financial engineering in which new instruments, markets and trading strategies are developed, many scarcely disguise their potential for evasion of taxes, detection and regulation.[5]

Thus, in this article, for the perspective that blockchain regulation is feasible, but challenging, it is important to recognize the depth and limitations to the domain specific expertise of the three (or five) primary scholarly perspectives. First, technologists have the expertise and drive to develop new technologies that can evade clear understanding and, consequently, evade effective regulation. Second, at least some public policy wonks are neither deterred by the challenge of regulating amorphous technologies ("like nailing jelly to the wall")[6] nor are they all incapable of understanding the technology's design architectures or their next-most feasible alternatives. Third, economists have much to contribute to the design of both technologies and their regulation. For example, blockchain enabled cybercurrencies or cryptocurrencies could be banned if they are too successful at defeating public policy. As discussed later, several governments, at both the national and provincial levels, weaken cryptocurrency operations. The full embrace of blockchain by governments is an opposite strategy, an approach succinctly embraced by the old adage: "if you can't beat them join them."[7] Such difficulties lead some observers to abandon the skirmish and embrace technologies on their own terms, urging armistice to such battles before they much start.[8]

This article recognizes these policy response limitations in the fast-paced diffusion of blockchain technologies and the predictable reactions by pro-regulatory advocates. This article reveals the architecture and operations of existing blockchain applications (e.g., Bitcoin, Initial Coin Offerings (ICO)) because it is necessary to enable thoughtful and balanced regulation. We review various prospective applications of blockchain while using cross-cutting, and increasingly evident, blockchain legal challenges (tax evasion, money laundering, challenging forensics) to develop solutions. The technical complexity of

---

professionals have additional perspectives that are important in understanding the "regulability" of blockchain.

[5] *See e.g.*, Marr, Bernard, *The Complete Beginner's Guide To FinTech In 2017*, FORBES (Feb.10, 2017) *accessible at*: https://www.forbes.com/sites/bernardmarr/2017/02/10/a-complete-beginners-guide-to-fintech-in-2017/#6b9437a43340 (arguing FinTech, Financial Technologies, are more than just "technologies used and applied in the financial services sector, chiefly used by financial institutions themselves on the back end of their businesses," FinTech are evolving to "represent technologies that are disrupting traditional financial services, including mobile payments, money transfers, loans, fundraising, and asset management.) *See also*, Lin, Tom C. W., *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643 (2015) *accessible at*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711379.

[6] *Teddy Roosevelt's Metaphor*, NY TIMES (March 9, 1986) *accessible at*: https://www.nytimes.com/1986/03/09/magazine/l-teddy-roosevelt-s-metaphor-605086.html (discussing idiom's origin from letter written by Theodore Roosevelt to William Roscoe Thayer on July 2, 1915 describing difficulties in acquiring Panama Canal rights from the government of Columbia).

[7] *See generally*, *Atlantic Monthly*, Feb. 1932.

[8] *See e.g.*, Werbach, Kevin D., *Trust, But Verify: Why the Blockchain Needs the Law* 33 BERK.TECH.L.J. 487 (2016) *accessible at*: https://ssrn.com/abstract=2844409 (arguing for adoption of blockchain as major control over contracting).

blockchains tend to obscure comprehension by many public policy operatives: legislators, regulators, lawyers and judges.[9]

The first major section of this paper defines the architecture of blockchain in non-technical language. We also provide technically-equivalent terminology to enable rigorous public policy analysis of alternative technical descriptions by legislatures, regulatory agencies, judges and public policy scholars. Regulation that is under-informed by the general design of blockchains runs the risk of unintended consequences, including, inflicting damage to useful innovations, inadequately achieving regulatory objectives and negatively externalizing the regulated activity's harmful side effects.

The second section examines proven advantages and predicted benefits of blockchain applications: increased privacy, security and the disintermediation that promises economic efficiency. The third section then turns to the proven disadvantages and predicted burdens of blockchain applications in particular domains: weakening central banking, currency manipulation, fraud in the commodity and investment markets, tax evasion, illegal gambling, money laundering, frustration of forensics and shielding from transparency and lawful authority a range of illegal and unethical activity. Analysis of regulatory enforcement experience informs this scrutiny. The fourth section dissects blockchain architecture into some of its recurring components to enable understanding of the regulatory challenges. The final three sections attempt to add value to the blockchain regulation debates by illuminating blockchain regulation challenges with a view to informing the development of proposals balancing the remediation of blockchain externalities while designing policy incentives that encourage useful blockchain applications.

II. INTRODUCTION TO BLOCKCHAIN ARCHITECTURE

The first implemented blockchain appeared as the infrastructure to support the digital currency Bitcoin. The inventor, an unknown individual simply known under the likely pseudonym as "Satoshi Nakamoto," wished to create a peer-to-

[9] Increasingly, a growing literature demystifies blockchain, some to promote the author/sponsor's products and services and others to maintain their role as interpreter of emerging practices, *see e.g.*, Lawrence J. Trautman & Mason J. Molesky, *A Primer for Blockchain*, UMKC L. REV. (forthcoming 2019), https://ssrn.com/abstract=3324660, Gupta, Manav, BLOCKCHAIN FOR DUMMIES, (2017 John Wiley) *accessible at*: https://bertrandszoghy.files.wordpress.com/2017/05/ibm-blockchain-for-dummies.pdf, Iansiti, Marco & Karim R. Lakhani, *The Truth About Blockchain*, 95 HARV.BUS.REV. 118-127 (Jan. Feb. 2017) *accessible at*: https://hbr.org/2017/01/the-truth-about-blockchain, Shackelford, Scott J., & Steve Myers, *Block-By-Block: Leveraging The Power Of Blockchain Technology To Build Trust And Promote Cyber Peace*, 19 YALE J.L.& TECH. 334 (2017), Peters, Gareth and Panayi, Efstathios and Chapelle, Ariane, *Trends in Cryptocurrencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective* 3 J.FIN. PERSP. 92-113, (Nov.7, 2015) *accessible at*: https://ssrn.com/abstract=3084011, Walch, Angela, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk* 18 NYU J. LEGIS.& PUB.POL'Y 837 (2015) (March 16, 2015). Congress may be learning of cryptocurrency foibles, *see generally*, Sykes, Jay B., *Securities Regulation and Initial Coin Offerings: A Legal Primer*, No. R45301 CONG. RES. SERV. (Aug.31, 2018) *accessible at*: https://fas.org/sgp/crs/misc/R45301.pdf.

peer electronic cash system that could exist outside of traditional financial institutions.[10] Although Nakamoto's exact motivations are unclear, it is generally understood that Nakamoto's disagreement with the government bailouts following the 2008 financial crisis played a significant role in Bitcoin's conception.[11]

Although Bitcoin and similar cryptocurrencies have no material worth (intrinsic value), this fact only disqualifies them from being classified as "exchange-commodities" (e.g. silver). However, whether an item becomes a "means of payment"[12] is entirely dependent on social consensus. A precious metal, for instance, despite being materially valuable and "real," cannot be circulated as a general means of payment if it is not socially agreed upon as such. Even in the cases when a precious metal is used as a means of payment, it is because of the properties that qualify a precious metal as an effective item of exchange.[13]

Therefore, the entry requirements for an item to become socially recognized as an item of exchange are (1) scarcity and (2) verifiable authenticity. Fiat currencies[14] maintain these qualities with the support of the governments. A cryptocurrency is backed by a blockchain that digitally replicates these two conditions using a combination of cryptography, game theory, and computer networks.

A. Blocks and Nodes

A blockchain, at its core, is a database. Specifically, it is a database that tracks transactional data between individuals–a public ledger. In this overview, we will examine the Bitcoin blockchain. Unlike traditional databases, there is no company or individual who administers the blockchain. Instead, thousands of independent computers work together to maintain it.

Each of these computers, called *nodes,* has a local copy of the blockchain. When someone desires to send Bitcoin to another individual, these nodes are responsible for validating the transaction.[15] In simpler terms, these computers check against their own local copies of the ledger to confirm that the sender has enough Bitcoins in their possession to complete the transaction. When the nodes are in agreement, the transaction can be *mined*, or executed.

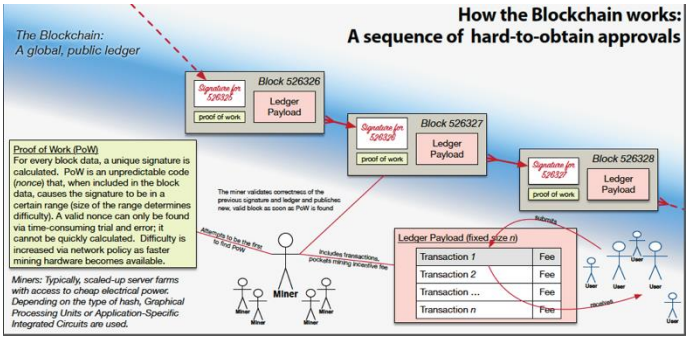
---

[10] Nakamoto, Satoshi, *Bitcoin: A peer-to-peer electronic cash system.* Whitepaper (2009) *accessible at*: https://Bitcoin.org/Bitcoin.pdf.
[11] Davis, Joshua. T*he Crypto-Currency and its Mysterious Inventor*, NEW YORKER (Oct. 11, 2011).
[12] Knapp, Georg Friedrich, H. M. Lucas, & James Bonar, THE STATE THEORY OF MONEY (London: Macmillan & Co. Ltd (1924).
[13] *Id.*
[14] Fiat money or fiat currency are not backed by assets with intrinsic value (e.g., gold) and are usually issued by a government, *Definition of Fiat Money*, FIN. TIMES LEXICON *accessible at*: http://lexicon.ft.com/Term?term=fiat-money.
[15] Orcutt, Mike, *How Secure is Blockchain Really?*, MIT.TECH.REVIEW (April 25 2018) *accessible at: https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/.*

B. Hash Connections

Collections of recently validated transactions are packaged into what are called *blocks* by special nodes called *miners*. Miners are in competition with one another to generate a block in accordance with a *consensus algorithm*, a shared protocol of how to generate the block's digital fingerprint, known as a *hash*. Bitcoin's consensus algorithm is known as "proof of work" (PoW) and requires significant computational power.[16] Figure I below illustrates PoW function in blockchain operations.

Figure I: How Blockchain Works



C. Chain Accumulates to a Ledger for Recordkeeping

Each block also contains the hash of the previous block, a reference that creates a chain that represents the entire transactional history of the ledger (hence block-chain).[17] The "tamper-proof" property of the blockchain is a product of these hashes. If any of the blocks is retroactively tampered with, then the block's hash will no longer correspond to that of the block that follows it, thus breaking the chain and requiring all the blocks ahead of the tampered block to be re-hashed. In order to have a chance at disrupting other miners and re-writing the blockchain from this point, the attacking agent would need to have computational power equivalent to 51% of all Bitcoin miners, which is incredibly unlikely considering the scale of the network.[18] Consequently, a blockchain only becomes more secure as the number of nodes increases.

---

[16] *The Great Chain of Being Sure about Things*, THE ECONOMIST (Oct. 31, 2015) *accessible at:* https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things.

[17] Narayanan, Arvind & Joseph Bonneau, BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION at 11 (Princeton University Press July 19, 2016).

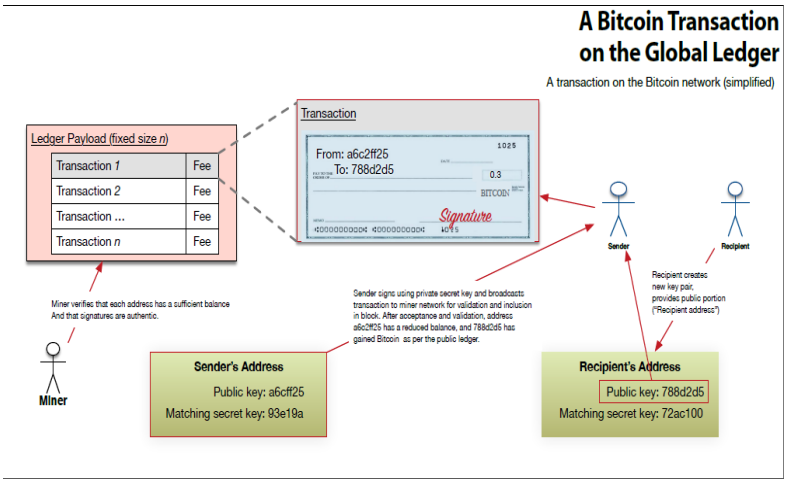
[18] Bitcoin Wiki, *Majority Attack* (Feb. 10, 2018) *accessible at: https://en.Bitcoin.it/wiki/Majority_attack*.

D. Mining as Manufacturing the New Cryptocurrency

The first miner to create a hash that fulfills the protocol's requirements is rewarded with newly minted Bitcoins. This reward not only serves as an incentive for miners to maintain the blockchain, but also as a way for the cryptocurrency to scale. Furthermore, every Bitcoin can have its origin traced back to the block where it was minted, this serves as a form of authentication.[19] When the other nodes in the network recognize that the block's hash is appropriate, they append this block to their local blockchain, effectively executing the transactions within the block by recognizing it as shared history.

It is important to consider that transactions are not necessarily mined in exact chronological order, but according to a fee the sender is willing to pay. This fee is known as a *network fee* and goes to the miner that places the transaction in the block.[20] After all, there are more transactions taking place than can be placed in the block currently being mined. The higher the fee the sender is willing to pay, the faster the transaction will be executed by being placed in the block. The price of this fee is determined by the amount of traffic on the network and can vary wildly. Currently, the average network fee is approximately 19 cents. In 2017, during a period of extremely high traffic, the network fee rose up to nearly 55 dollars.[21] Figure II depicts how Bitcoin utilizes blockchain.

Figure II: Bitcoin Transaction on Global Ledger



---

[19] *The Magic of Mining*, THE ECONOMIST (Jan. 8, 2015) *accessible at:* https://www.economist.com/business/2015/01/08/the-magic-of-mining.
[20] *Id.*
[21] *Bitcoin Avg. Transaction Fee Historical Chart, accessible at:* https://bitinfocharts.com/comparison/Bitcoin-transactionfees.html.

E. Validation, Encryption, Public Forensics

In order for transactions to be validated, all transactional information on the blockchain is public. Otherwise, each node would not be able to keep track of how many Bitcoins are in circulation and whether an individual actually has any Bitcoin to spend. To keep transactions private, individuals are represented by numerical addresses on the blockchain. An address is composed of two cryptographically generated numbers that can be generated for free: a public key and a private key.[22] The public key is used as an identifier on the blockchain, while the private key is only known by the owner of the address. However, this system is "pseudononymous." Addresses can be tied to a particular person if the address's transactions can be associated with an identity, such as in the case of paying bills.[23]

Bitcoins are registered to these addresses and are inseparable from the blockchain. When someone "owns" Bitcoins, in reality, they own the private key to an address that has some number of Bitcoins registered to it. Possession of the private key grants the user the "rights" to send Bitcoin from the corresponding address.

F. Vulnerability to Theft

Most individuals have multiple addresses that are generated by a piece of software external to the blockchain called a *wallet*.[24] Wallets are responsible for managing the private keys associated with each address, as well as displaying transactional history and wallet balance to the user.

Bitcoins can be "stolen" when an address's private key is exposed, as somebody besides the owner gains rights to send funds from the address. If private keys are lost in any way, the funds in the address become completely inaccessible. The blockchain has no way of recognizing ownership of an address beyond the private key. Therefore, keeping private keys secret and secure is paramount.

Most cryptocurrency heists occur at points of centralization, such as at a cryptocurrency exchange, where people exchange fiat currencies for cryptocurrencies. When someone buys Bitcoin at an exchange, the Bitcoin is placed in an address generated by the exchange. Thus, the exchange has possession of the address's private keys. Hackers target these exchanges knowing that if they can break through the service's security, they could potentially have access to thousands of private keys. Therefore, it is advised to send the purchased

---

[22] Antonopoulos, Andreas M, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* at 62 O'REILLY MEDIA (Dec. 20, 2014).

[23] Emerging Technology from the arXiv, *Bitcoin Transactions Aren't as Anonymous as Everyone Hoped*¸ MIT.TECH.REVIEW (August 23, 2017) *accessible at*: https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/.

[24] Gerard, David. ATTACK OF THE 50 FOOT BLOCKCHAIN: BITCOIN, BLOCKCHAIN, ETHEREUM & SMART CONTRACTS, (CreateSpace, July 24, 2017).

cryptocurrencies to another address, preferably one managed by wallet software on the buyer's hard drive, or even better, an external drive (e.g. USB) that is disconnected from the internet.[25]

G. Competing Cryptocurrency Architecture Enable Smart Contracts

The other most significant blockchain other than the Bitcoin blockchain, architecturally speaking, is Ethereum, and its corresponding cryptocurrency, Ether. Ethereum supports all the same functions as the Bitcoin protocol with the added ability of appending pieces of code, called *smart contracts*, to the blockchain.[26] Like transactions, smart contracts are a part of a block and are executed on each local node. Smart contracts also have their own address and can receive Ether payments. However, smart contracts are significantly more computationally expensive to execute than regular transactions. Therefore, the creators of Ethereum established *gas*, a unit of computational work. Each smart contract is measured in terms of gas-expenditure. In order to run the code on the contract, an address on the Ethereum blockchain must pay the miner in Ether for the amount of gas the contract consumes. In this way, Ether is like a digital exchange-commodity in addition to being a means of payment. Paying for gas expenditure is not only a way to compensate miners, but also a method to prevent inefficient, or even maliciously designed code from clogging up the mining process and disrupting the whole network.[27]

Smart contracts have a variety of applications. Most notably, smart contracts are used to create new cryptocurrencies that run on top of Ethereum. This functionality allows a cryptocurrency to exist without a dedicated community of miners to support it and can instead depend on the underlying Ethereum network. Cryptocurrencies that run on Ethereum are called *tokens* as a way to distinguish them from cryptocurrencies that have their own blockchain.[28] Furthermore, Ethereum addresses support Ethereum tokens natively, allowing tokens to be exchanged like Ether.

H. Tokens

Tokens frequently appear in conjunction with *decentralized applications*. A decentralized application, or "dapp" for short, is an application that makes use of smart contracts to store its data, or handle peer-to-peer interactions.[29] The

---

[25] Takashima, Ikuya, ETHEREUM: THE ULTIMATE GUIDE TO THE WORLD OF ETHEREUM, (CreateSpace, March 13, 2018).
[26] Buterin, Vitalik, *A Next-Generation Smart Contract and Decentralized Application Platform*, GitHub repository (2018) *accessible at:* https://github.com/ethereum/wiki/wiki/White-Paper.
[27] Chow, Joseph, *Ethereum, Gas, Fuel & Fees,* CONSENSYS (June 23, 2016) *accessible at: https://media.consensys.net/ethereum-gas-fuel-and-fees-3333e17fe1dc*.
[28] Ethereum Foundation, *Create Your Own Crypto-Currency with Ethereum,* (2018) *accessible at: https://www.ethereum.org/token*.
[29] *What's a DApp?* STATE OF THE DAPPS (2018) *at:* https://www.stateofthedapps.com/whats-a-dapp.

application is considered decentralized because significant parts of its code are distributed across all the mining nodes. It is important to remember that smart contracts, like transactions, are public. This transparency means that all the code in the smart contract as well as the stored data (unless encrypted before being placed in the smart contract) is visible. For some applications, this transparency is desired. For example, gambling applications have found a home on Ethereum, as anyone could theoretically examine the code that is generating the odds. Other decentralized applications simply use the infrastructure available on Ethereum for payments, and store all other information in traditional, centralized databases.

Tokens offer alternative methods of funding and revenue for developers of decentralized applications. For instance, a gambling dapp may require all of its users to gamble with its token. In turn, the gambling dapp will charge no fees. The developers themselves own a significant amount of the token, so as traffic to the application rises, the value of the token appreciates, and the developers can sell their tokens at exchanges to fund their day-to-day operations.

I. Initial Coin Offerings (ICO)

Similarly, developers may raise funds for their application through a process called an Initial Coin Offering (ICO), otherwise known as a token sale. To launch an ICO, a team of developers writes a white paper, share their credentials, and market their idea. Then, investors have the chance to purchase the application's tokens with a more stable cryptocurrency (such as Ether) before the application's launch, essentially speculating on whether the token will have any value in the future.[30] As one might one suspect, this controversial method of crowdfunding has proved to be sometimes incredibly lucrative, most frequently a disappointing investment, and other times completely fraudulent.[31]

However, it is worth noting that the developers of successful ICOs typically place their new-found funds into a smart contract called a *multi-signature wallet*.[32] This type of smart contract stores Ether and is mutually owned by multiple parties. Although the actual rules of the wallet vary per case, the general premise is to prevent one party from embezzling small amount without consent once per day/week/month, and larger withdrawals must receive the consent of the other parties.

---

[30] Biggs, John, *How to Run a Token Sale*, TECHCRUNCH (Sept. 22, 2017) *accessible at: https://techcrunch.com/2017/09/22/how-to-run-a-token-sale/*.

[31] Clayton, John, *Statement on NASAA's Announcement of Enforcement Sweep Targeting Fraudulent ICOs and Crypto-asset Investment Products* (May 22, 2018) *accessible at: https://www.sec.gov/news/public-statement/statement-nasaas-announcement-enforcement-sweep-targeting-fraudulent-icos-and*.

[32] George, Stefan, *Release of New Multsig Wallet* GNOSIS BLOG (Feb. 23, 2017) *accessible at: https://blog.gnosis.pm/release-of-new-multisig-wallet-59b6811f7edc*.

J. Private Blockchain Features

Different blockchains, which have different cryptocurrencies tied to them, differ in terms all the funds. Typically, each party can withdraw a of consensus algorithm, block size, mining rewards, and other properties. Both Bitcoin and Ethereum blockchains are considered public blockchains, meaning anyone can potentially become a node in the network. However, blockchains can also be permissioned,[33] meaning that every node must be verified before joining the network, effectively forming a "private" blockchain. Private blockchains can be used within large organizations as a common database and can provide certain levels of privacy that is difficult to achieve on a public blockchain. The primary trade-off of a private blockchain is security, as it naturally has less nodes than its public counterparts. For this reason, permissioned blockchains have relatively niche uses. One example of a private blockchain is Ripple, a proprietary cryptocurrency used as an intermediary currency for international bank transfers.[34] Although Ripple can be purchased at cryptocurrency exchanges and used as a means of payment between individuals, it cannot be mined by public nodes.

III. POLITICAL ECONOMY OF MONEY

Since the decline of the barter trades,[35] money has ascended as the predominant medium of exchange to become the primary payment performance method.[36] Money has a long history that both informs the design of electronic payment systems as well as the critique of failed forms of electronic money. Successful forms of money were well-known hundreds of years B.C.[37] With some significant exceptions, most forms of money have been created, controlled and

---

[33] Boinodiris, Phaedra, *Who Has the Power in Enterprise Blockchains?* IBM BLOCKCHAIN BLOG (Feb. 20, 2018) *accessible at: https://www.ibm.com/blogs/blockchain/2018/02/who-has-the-power-in-enterprise-blockchains/.*

[34] https://ripple.com/.

[35] Barter is a system of voluntary exchange in which the value tendered is composed of goods, services or real property without involvement of money as a medium of exchange, *see generally* Keynes, John Maynard, THE MONETARY THEORY OF PRODUCTION (1933) *accessible at*: http://zimmer.csufresno.edu/~sasanf/135Documents/Keynes.doc The initial decline of barter accompanied the widespread adoption of currencies after the middle ages. However, barter periodically reemerges as competitive to other money forms at other times, such as in periods of hyperinflation, when currency becomes scarce, if central banks weaken or when governments become incapable of backing their fiat currencies.

[36] Smith, Adam, *The Origin and Use of Money*, Ch.4 in AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS, (1776, London) *accessible at*: http://www.earlymoderntexts.com/assets/pdfs/smith1776_1.pdf (denigrating barter as "higgling, haggling, swapping, dickering"); *but see*, Strauss, Ilana E., *The Myth of the Barter Economy*, ATLANTIC MONTHLY (Feb 26, 2016) *accessible at*: https://www.theatlantic.com/business/archive/2016/02/barter-society-myth/471051/.

[37] Due to religious sensitivities, particularly outside the U.S., it is becoming more acceptable to refer to the era before the birth of Christ as the BCE, Before the Common Era, *see generally*, Riggs, John W., *As I See It: Whatever happened to B.C. and A.D., and why?* United Church of Christ (Dec. 31, 2002) *accessible at*: http://www.ucc.org/whatever-happened-to-bc-and.

regulated by government, the *coinage prerogative*.[38] Most of the world's money supply is firmly under the control of national, central banks, which developed at the close of medieval times to enable the expansion of international trade.[39]

Economics generally recognizes that money provides two socially beneficial functions. First, money constitutes a *storehouse of value*, a form of wealth that typically does not depreciate quickly or unpredictably. Second, money serves to facilitate contractual exchange in modern economies as a *medium of exchange*, that is, money is an intermediate asset generally accepted as having reliable value in which buyers offer money to persuade sellers to take money in exchange for land, goods or services.

A. Issuers of Money in American History

Some forms of money historically had intrinsic value, that is, coin with precious metal content actually stored its face value, such as from the reliable value of its constituent gold or silver. Of course, in modern economies few circulating coins are struck from precious metal, except as an investment or hedging device.[40] Furthermore, paper currencies replaced bulky and awkward coin, by substituting, for intrinsic value, the issuing government's promise to redeem the paper with precious metals, like gold or silver. Today, money functions as a storehouse of value and medium of exchange so long as its users have confidence that the money will maintain value. History illustrates that no form of money can become a dominant medium of exchange unless there is a sufficient supply, it is widely available and it is accessible to most users. Thus, any particular form of money

---

[38] Coinage prerogative is the sovereign right to design and mint coins. In the past, this was the right of the state ruler (e. g. the king). Today, the coinage prerogative lies with the government or the government established central bank, *see e.g.*, Deutsche Bundesbank, Glossary, *accessible at*: https://www.bundesbank.de/Navigation/EN/Service/Glossary/Functions/glossary.html.
As fiat currencies developed, the coinage prerogative was largely supplanted by monetary sovereignty, the power of government to exercise exclusive powers over that nation's legal tender, *see* Mann, Frederick A., THE LEGAL ASPECT OF MONEY at 460-78 (5th ed. Oxford, 1992).
Coining, printing or otherwise manufacturing money can be a profitable proposition, that is, most nations with fiat currencies retain the right of *seigniorage*, to make a profit from creating money. Some nations also appoint and license private sector businesses to coin or print currency. For example, commemorative coins are struck in base, semi-precious and precious metals by non-government mints, which generally are granted only limited seigniorage rights. Some economists argue seigniorage constitutes a hidden tax. *See generally*, Neumann, Manfred J.M., *Seigniorage in the United How Much Does the U.S. Government Make from Money Production?* Fed. Res. Bank of St. Louis. (Mar.April,1992) *accessible at*: https://files.stlouisfed.org/files/htdocs/publications/review/92/03/Seigniorage_Mar_Apr1992.pdf.

[39] Of course, private banks create money, taking in deposits and making new loans, the deposited money plus the loaned money nearly doubles the money supply. Central banks exert limitations on this form of new money created by these loans with reserve requirements.

[40] These coins include, *inter alia*, Krugerrands, Eagles, Maple Leafs, Libertads, Pandas and a wide variety of commemoratives. By contrast, junk silver (low grade) coins with little numismatic value nevertheless can be generally accepted for trade as a quasi-barter/medium of exchange by weight due to its assay value, the quantity and quality of the ore's valuable constituent precious metals.

will have limited success without sufficient *critical mass*[41] to enable transactions by a large portion of the user population.

Early in U.S. history, there was considerable experience with competing currencies issued by the private banks and government entities.[42] Paper currency notes were issued by governments (e.g., England, most colonies, the states, U.S. federal), by private banks and even some private parties. Some early competing currencies were backed by assets, meaning that note holders could demand payment (exert claims to redeem or exchange) for something of tangible value (asset named on the note) such as agricultural products or precious metals, (e.g., tobacco, gold bullion).

B. Decline of Currencies Competing with Government Backed Monies

In Colonial times, private currencies proliferated leading to rampant inflation. Furthermore, many early currencies failed to achieve critical mass, leading to mistrust that prevented universal acceptance as payment. The framers of the U.S. Constitution, and many other nations' founding documents and later policies, reacted to the ensuing inflation and economic instability allegedly caused by competing currencies by consolidating the establishment of a monetary system into a government agency, typically the national or central bank. The results are that single, predominant currencies exist in most nations.[43] The U.S. Congress eventually consolidated the authority to coin and print money to the U.S. Treasury

---

[41] *Critical mass* in monetary economics is a sufficient supply of an asset or media of exchange (money) that enables economic actors to utilize that asset for regular activity. In this context of electronic payment systems, this means there is a sufficient money supply to support the majority of transactions sought to be conducted by the user base, *see generally*, Bagby, John W., *Performances and Payments*, Ch 9 in ECOMMERCE LAW: ISSUES FOR BUSINESS at 401 (West 2003).

[42] The U.S.'s experience may be sufficient background for understanding the blockchain for purposes of financial regulation. To satisfy this need for experience as instruction, this history arguably needs to include the evolution of U.S. experience with barter, the heritage of English money, the establishment of colonial monies, the transition from barter to monies, the consolidation of private and regional governmental monies to a national currency, the role of the U.S. Treasury and the failures of new monies. However, as this article's research is generalized beyond American borders, it may be necessary to more fully establish other nations' historical struggles with money and other media of exchange. To better match blockchain regulation to those other nations' culture and commercial practices, a broader understanding of the history of world monies seems appropriate. All nations can generally benefit vicariously from the experiences, struggles and successes of other nations.

[43] A few nations use the currency of other nations. For example, the U.S. dollar is either the government anointed currency (e.g., Ecuador, East Timor, El Salvador, Marshall Islands, Micronesia, Palau, Turks and Caicos, British Virgin Islands, Zimbabwe) or a dominant currency due to an erratic or untrustworthy home currency (e.g., Philippines, Panama, Bahamas, Viet Nam, Cambodia, Nicaragua, Belize, Myanmar (Burma), Liberia, Old Jerusalem) *See e.g.*, Chibber, Kabir, *Here Are All The Countries That Don't Have A Currency Of Their Own*, QUARTZ (Sept.15, 2014) *accessible at*: https://qz.com/260980/meet-the-countries-that-dont-use-their-own-currency/ The U.S. Dollar is the most used currency in the world, followed by the Euro, Yen, Pound Sterling, Canadian Dollar and Swiss Franc. Currency hedging and foreign currency translations measure speculative and manipulative activity as well as actual use in transactions after conversions.

as regulated by the Federal Reserve Board.[44] Furthermore, to exert control over monetary policy, these powers were prohibited by the Constitution to the U.S. states.[45] This essentially established a federal government monopoly over money. While states chartered (licensed) banks and currency was issued by both federally chartered banks and by some state chartered banks, eventually the taxes levied on non-federal notes diminished their use. Public confidence in money is enhanced when control is concentrated in a trusted government entity like the U.S. Treasury and Federal Reserve Bank.

In 1996, Federal Reserve Board Chairman Alan Greenspan predicted, at the onset of the electronic commerce era, that history teaches that electronic money will not quickly gain critical mass.

> In conclusion, electronic money is likely to spread only gradually and play a much smaller role in our economy than private currency did historically. Nonetheless, the earlier period affords certain insights on the way markets behaved when government rules were much less pervasive. These insights, I submit, should be considered very carefully as we endeavor to understand and engage the new private currency markets of the twenty-first century.[46]

In Greenspan's opinion, some limited success is possible in the U.S. and some other world economies for electronic money. However, the long history of experience with competing currencies does not signal a successful proliferation of totally alternative payment schemes. Electronic payments that develop must largely rely, at least in part, on the existing monetary system's components of coin, paper currency, bank transfers, credit and debit cards, account transfer documents (checks, notes), electronic funds transfer (EFT), and points of sale infrastructure.

---

[44] Various provisions of the U.S. criminal code forbid unauthorized counterfeiting, coinage, banknote printing or the possession of equipment adaptable to counterfeiting (counterfeit paraphernalia) or other unauthorized money/currency creation. *See e.g.*, 18 U.S.C. §§485 & 486 (prohibiting counterfeiting as utterance of coin), 18 U.S.C. §§481 (prohibiting counterfeiting of bank notes), 18 U.S. Code §474 (prohibiting control, custody, or possession of any plate, stone, or other thing adaptable to printing various government obligations or other securities, counterfeit paraphernalia), 18 U.S.C. §491 (prohibiting tokens or paper used as money). Obligations or other securities of the United States" includes all bonds, certificates of indebtedness, national bank currency, Federal Reserve notes, Federal Reserve bank notes, coupons, United States notes, Treasury notes, gold certificates, silver certificates, fractional notes, certificates of deposit, bills, checks, or drafts for money, drawn by or upon authorized officers of the United States, stamps and other representatives of value, of whatever denomination, issued under any Act of Congress, and canceled United States stamps. 18 U.S.C. §8.

[45] U.S. Const. Art. I §10. No State shall enter into any Treaty, Alliance, or Confederation; grant Letters of Marque and Reprisal; coin Money; emit Bills of Credit; make any Thing but gold and silver Coin a Tender in Payment of Debts; pass any Bill of Attainder, ex post facto Law, or Law impairing the Obligation of Contracts, or grant any Title of Nobility.

[46] Greenspan, Alan, *Regulation Of Electronic Payment Systems*, Remarks of Federal Reserve Board Chair, U.S. Treasury Conference on Electronic Money & Banking: The Role of Government, (Washington DC, Sept. 19, 1996) *accessible at*: https://www.federalreserve.gov/boarddocs/speeches/1996/19960919.htm.

Indeed, PayPal and Venmo have gained some critical mass, arguably, due largely to their reliance directly on some services provided by the banking system as well as being denominated in units defined by government monetary mediums of exchange (e.g., dollar denominated rather than unique units or points). Even Bitcoin's success today as a medium of exchange relies on its dollar denomination as the definition of its value equivalence.[47]

C. Contemporary Use of Electronic Payment Systems

Electronic payments existed long before the Internet. Indeed, wire (telegraph) transfers of funds have been successfully made for almost a hundred and fifty years. The first international wire transfer of funds utilized the new trans-Atlantic telegraph cable, initially laid in the 1880s between the U.S. and the U.K.[48] Few people today could operate successfully in the modern economy without some brush with electronic payments. Cash withdrawals from bank accounts or credit card accounts using automated teller machines (ATMs) are a frequently-used common practice. Credit card charges use electronic account verification and transaction processing. Physical handling of credit card carbon impressions is nearly extinct but can be resurrected temporarily when electronic networks fail to function. Point of sale (PoS) transaction processing for debit and ATM cards use electronic networks similar to credit card networks.

Electronic payments systems take on various other forms: toll tag use at turnpikes, bridges and tunnels or electronic token-readers for charging fuel purchases at the pump. Electronic processing of payments, at the wholesale level, requires that nearly all inter-bank transactions (between banks) be processed electronically including the total fund transfers clearing all paper checks, direct deposits, and clearance of credit card or debit transactions by ATM or PoS. Thus, information exchange between the buyer's bank and the seller's bank are part of the electronic payment system.

D. Controversy over New Monies

Network effects[49] are among the major obstacles to successful innovations in electronic payments. The challenges of introducing new currencies are similar.

---

[47] Of course, cryptocurrencies fluctuate in value, largely as a speculative market in them develops as quasi-commodities. Bitcoin success as a speculative device is discussed *infra*.

[48] Western Union provided a broadly successful wire transfer business in the U.S. and between the U.S. and other nations since the 1870s using Western Union's telegraph network. To a much more limited extent, this system was used among foreign nations, many of which developed their own telecommunications infrastructure that have been adapted to wire transfers.

[49] Network effects are the natural result of adding or subtracting nodes and links to a growing network. The whole system becomes more valuable as links and nodes are reliably added to become active users. The system loses value as links and nodes are eliminated. *See generally*, Shapiro, Carl, & Hal R. Varian, INFORMATION RULES A STRATEGIC GUIDE TO THE NETWORK ECONOMY. (Harvard Business Press, 1998) *accessible at*: https://www.researchgate.net/publication/200167344_Information_Rules_A_Strategic_Guide_to_T

Switching costs are the first barrier: before a payment innovation will succeed, people must believe the new system will be as convenient and reliable as existing money without becoming more costly. New currencies often fail to become as stable as the replaced system(s). Consider that the Euro (€) sustained considerable losses after its initial introduction.

The second barrier is network economics more generally. Network effects are economies of scale derived from standardization and widespread to universal acceptance. Success of payment innovations seems unlikely until critical mass is achieved.[50] The same holds true for money and payment systems. As more consumers and merchants learn to trust particular currencies ($) or forms of payment (checks, credit cards), they become the standard mechanisms of payment.

The implication of network economics for innovative payment systems is that critical mass must be achieved to become successful. This means that enough customer subscribers, participating merchants and infrastructure must come on line to facilitate frequent and reliable use. Critical mass is the essence of network effects, many systems must achieve very wide acceptance before they will be financially successful. Of course, not all markets are controlled by network effects to the same extent as are communications, payments and computer compatibility. Indeed, the measure of success for many tangible products is the achievement of small but profitable market niches. For example, the electronic currency, Venmo reportedly relies more on payment volume derived from transactions among social networks of friends (clusters) than it does on direct, individual payments made from the general population of consumers to the general population of retailers.[51]

E. Early Electronic Money Failures

Hype about experimental consumer electronic payment systems attracts inventors to patent new forms of payment system, venture capitalists and the attention of regular investors.[52] The majority of these systems eventually fail or become part of the "living dead," continuing only at bare subsistence levels. None has yet achieved widespread success or critical mass to serve in most forms of exchange (purchases nearly anywhere from buyers nearly anywhere). Some successes include ancillary services such as peer-to-peer (P2P) payments systems (e.g., PayPal), smart cards, electronic customer loyalty point systems, escrow services, electronic bill presentment and electronic access/manipulation of account records at banks and vendors. Successful systems rely on computerized, electronic

---

he_Network_Economy.

[50] Consider the ubiquitous fax machine. It was nearly worthless until all fax machines used the same communications protocol and only then did most offices install them. As the fax network expanded, the value of the fax technology expanded.

[51] *See e.g.,,* Moorthy, Neelesh, *Cash, credit or mobile app: the rise of Venmo*, (Duke) CHRONICLE (March 25, 2015) *accessible at*: http://www.dukechronicle.com/article/2015/03/cash-credit-or-mobile-app-rise-venmo#.VTIK-eGzn6o.

[52] *See e.g.*, Lawrence J. Trautman & Alvin Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV. 1041 (2017) *accessible at*: http://ssrn.com/abstract=2730983.

tele-communications to do one or more of the following: authorize or order payments, verify customer identity and availability of account status and funds availability, create backup documentation and provide archival record-keeping.

While secure electronic packets of value may someday actually transfer electronic currency without the assistance of trusted third party intermediaries (e.g., banks), third parties are likely to remain involved with any form of payment until payment innovations become much more reliable, secure from tampering, and are specifically legalized. Electronic payment systems must mimic advantages and safeguards of the more commonplace, traditional payment methods. Credit card could remain "king of payments" for at least part of most consumer transactions until the usage of "plastic" is abandon for deposits of electronic payments into user accounts accessed with electronic mechanisms other than "plastic."

More widespread electronic payments using electronic money are constrained by numerous barriers. Uncertainties, outright fraud and speculative bubbles illustrate profound lack of safety and security slowing further public and business acceptance. Most successful electronic payment and money systems largely extend or piggy-back to some extent on existing payment system architectures. This reinforces two immutable observations. First, new payment system acceptance squarely rests on proven security and system reliability. Second, trusted third parties are still required for payment system success. Commercial banks and other time-honored financial system intermediaries are among the early adopters of electronic payment schemes that become successful so they will likely continue exerting their control over the payment process handling.[53]

F. CryptoCurrency's Role in Electronic Payment Systems

The terms virtual currency or virtual money, digital currency and cryptocurrency are widely used interchangeably but have distinguishing differences that are important only to some groups. They are differentiated in (at least) two ways, first, when they were introduced and when they are used significantly, and, second, by differences in their architecture and evolving conceptualization. The choice and stability of terms defining various forms of electronic money evolve as their forms change and as broader understanding expands.

The term virtual money or virtual currency probably dates to 2009.[54] *Virtual currency* was defined in 2012 by the European Central Bank as "unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community."[55] The European Central Bank defined three types of virtual currency.

---

[53] Of course, not all bank adopted new technologies survive or prosper.

[54] *See e.g.*, Sutter, John D., *Virtual Currencies Power Social Networks, Online Games* CNN (May 19, 2009) *accessible at*: http://www.cnn.com/2009/TECH/05/18/online.currency/index.html.

[55] *Virtual Currency Schemes*, European Central Bank (Oct.2012) at 6, *accessible at*: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

Type 1 prevails in closed systems (e.g., Linden Dollars in online games like Second Life). Type 2 has only unidirectional flow (typically inflow) for which there is a conversion rate for purchasing the virtual currency, which can subsequently be used to buy virtual goods and services. Type 3 has bidirectional flows. This allows Type 3 to behave like any other convertible currency because it can potentially have different buy and sell exchange rates. Type 3 virtual currencies are generally usable to buy virtual or real goods or services.[56]

In 2015, the European Central Bank clarified its 2012 report by redefining virtual currency as "digital representation of value, not issued by a central bank, credit institution or e-money institution . . . ."[57] Note this reconsideration dropped the unregulated aspect as well as the apparent requirement for users to be members of some specific virtual community. The characteristics eliminated were indicative of the virtual gaming prevailing during the first decade of the 21st Century and are becoming obsolete.[58]

Digital currency is a broad term encompassing both virtual currencies and cryptocurrencies. Digital currencies can be centrally controlled by a government or by a private issuer. Alternatively, they can be distributed, such as where control is dispersed; the situation possible under the blockchain. Control generally signifies that a balance amount is recorded in a user account residing in a single location as is envisioned by a stored value card. Alternatively, control can be distributed as is envisioned by the blockchain.

Cryptocurrency is a currently popular buzzword most associated with initial coin offerings (ICO). It is characterized as a distributed, blockchain-derived architecture that is equipped with encryption-based security that operates during the transmission/communication of all transaction data and the encryption is also operative to protect data confidentiality while the data is at rest. Generally, ICO are created in a "mining" process that "coins," that is, initially produces new units of the currency. Mining is generally constrained by an amount determined mathematically by specified restrictions. Bitcoin[59] is generally recognized as the

---

[56] *Id.*

[57] *Virtual Currency Schemes – a Further Analysis*, European Central Bank (OFeb.2015) at 33 *accessible at*: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[58] *See generally*, Bagby, John W., *Imagining How to Exploit w00t from Virtual Environments to Inform Real World Public Policy*, No.74 TPRC 2008, 36th Research Conference on Communication, Information, and Internet Policy, Arlington VA, Sept. 2008.

[59] The capitalized word "Bitcoin" refers to its network enabling cryptocurrency transactions. The lower case "Bitcoin" is used when speaking of actual units of the cryptocurrency. Symbols for Bitcoin units are at early stages of standardization and have varied with the capitalized three characters BTC, the most common usage. The symbol, a capital B with two falling strokes at the top and bottom (but not through the middle), is becoming common. The double vertical slash symbol has been widely set in a gold coin-like medallion to serve as the Bitcoin logo and is used with increasing frequency. A competing standard shows a horizontal cross through the lower half bulge of the rising vertical of a capital B. Keyboards and character sets containing the Bitcoin symbol did not become standardized until 2015. Unicode 10.0 (released June, 2017) defines the Bitcoin symbol as U+20BF which has gained widespread support in various operating systems since June 2017. The ISO 4217 currency code for Bitcoin is XBT. *See e.g.*, Bitcoin Symbol, BITCOINWIKI *accessible at*: https://en.Bitcoin.it/wiki/Bitcoin_symbol.

leading cryptocurrency; it was both the earliest cryptocoin developed and it remains the most successful over the time during which true cryptocurrencies have existed.

Fiat currency is a term relevant throughout this discussion because it will remain the standard against which cryptocurrencies are judged for their success and for the challenges they impose on law enforcement. Fiat somewhat belies its own name. Fiat currencies are generally recognized in monetary economics as traditional forms of money, issued by the central bank of a nation, they are authorized by that nation's government, and they are intended to become the standard medium of exchange in the initiating jurisdiction.[60] Currently, the U.S. dollar is, perhaps, the most successful fiat currency and the EU's Euro is the second most successful. Fiat is a pejorative label because, as governments transitioned from tangible coins struck from precious metals with intrinsic value, money supply growth was constrained only by the nation's printing press capacity, not the government's supply of precious gold or silver. Successful fiat monies are generally backed by the full faith and credit of the issuing government, at least in the U.S. By some accounts, the Chinese Yuan Dynasty was the first government to issue paper banknotes in the 13th Century A.D. as fiat currencies.

IV. BLOCKCHAIN COULD PROMOTE PUBLIC POLICY

Blockchains are transparent record-keeping systems secured through means of encryption, redundancy, and financial incentives, allowing them to effectively manage digital assets without a central authority. This decentralization allows for individuals to have more control over their personal information. Internet merchants that accept cryptocurrency payments, for instance, are only ever exposed to the public address of a buyer. No sensitive data, such as a credit card number, needs to be maintained by the vendor. For similar reasons, there have been a number of proposed blockchain-based electronic medical records (EMR) solutions.[61] A blockchain EMR solution could provide patients with better control of their private medical information and might be designed to empower patients to specify exactly which individuals have permission to view their records. These records, furthermore, would need not be housed within one health system, facilitating access to medical information when patients seek treatment outside of their usual providers. For example, Blockstack, aims to implement a blockchain-based architecture for decentralized applications, one that prevents user data from

---

[60] *See generally*, Goldberg, Dror, *Famous Myths of "Fiat Money,"* 37 J.MONEY, CREDIT & BANK. 957–967 (2005).

[61] McFarlane, Chrissa, *Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.1* (May 2017) *accessible at:* https://patientory.com/patientory_whitepaper.pdf.

ever reaching a centralized server, while simultaneously keeping that information off the blockchain.[62]

Blockchains are generally successful in maintaining the integrity of the information they manage. By tracking a history of transactions, only appending new information, and having thousands of copies of the ledger dispersed through the network, blockchains are frequently seen as "immutable." Once something is placed on the blockchain, it is virtually impossible to erase–making blockchains effective tools for identity management or electronic voting.[63]

The financial sector has embraced blockchain technology as a way to promote transparency and eliminate expensive intermediaries, such as clearinghouses. Blockchains support direct peer-to-peer (P2P) transactions, making it cheaper for both businesses and individuals to transfer funds, and potentially rendering payment processing, as a business model, obsolete.[64] Similarly, smart contracts can be developed to perform notary and escrow services. Because smart contracts are also public, this transparency means parties can examine a smart contract before initiating a transaction. Some of the most significant blockchain projects in development include the new blockchain-based infrastructure for the Australian Securities Exchange (ASX)[65] and JP Morgan's Ethereum-inspired payment system, Quorom.[66] Both of these projects allow for more transparency in financial systems, while still protecting, to a degree, the privacy of involved parties.

V. BLOCKCHAIN SUBVERTS PUBLIC POLICY

Consider this public policy advocacy scenario advocating laissez-faire approach to the blockchain:

> What's all this fuss about blockchain, it provides safe, secure and reliable transaction processing and verifiable records. These advantages have always been a primary objective of justice systems. They are integral to the law of evidence and contracts. Public policy should just embrace the technology, then eventually tamp down whatever unlikely negative side effects arise, but only when appropriate and convincing circumstances arise.[67]

---

[62] Ali, Muneed, *Blockstack: A New Internet for Decentralized Applications* (October 17, 2017) accessible at: *https://blockstack.org/whitepaper.pdf.*

[63] Biggs, John, *Sierra Leone Just Ran the First Blockchain-based Election*¸ TechCrunch (March 14, 2018) *accessible at: https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/.*

[64] Holotiuk, Friedrich, Francesco Pisani, and Jurgen Moorman, *The Impact of Blockchain Technology on Business Models in the Payments Industry* (Feb. 12, 2017) *accessible at https://wi2017.ch/images/wi2017-0263.pdf.*

[65] Meyer, David, *The Australian Securities Exchange Just Made Blockchain History*, FORTUNE (Dec. 7, 2017).

[66] https://www.jpmorgan.com/global/Quorum.

[67] The indented excerpt is composed by this article's authors to serve as straw man for the laissez-faire line of argument. *See e.g.*, de Filippi, Primavera, *Bitcoin: A Regulatory Nightmare To A*

Such is the essence of argument by proponents, inventors, owners, consultants and suppliers of many new technologies for much of history.[68] However, in most instances, these supporters' conflicts of interest make their arguments both predictable and suspect.[69] Therefore, to many involved in new technologies like blockchain, any balanced and timely integration of new technologies into the social fabric remains elusive without balance between blockchain incentives and negative externalities and only if based on fundamental understandings of blockchain architecture.[70]

Despite the advantages touted in the section above for wholesale deployment of blockchain transaction processing, the potential for blockchain to enable mischief, specifically money laundering and theft, has been recognized for several years.[71] Other key areas of blockchain-enabled mischief include illegal gambling (online and offline wager settlements), manipulation of currency, commodity and investment markets, insider trading, identity theft, financial fraud, and tax evasion.

The U.S. federal government may have first become seriously interested in Bitcoin as a form of virtual money when it seized 179,000 Bitcoin units as part of a takedown of the Silk Road black market.[72] Silk Road facilitated the sale of

---

Libertarian Dream, 3 INTERNET POL'Y. REV. No.2 (July 24, 2014) *accessible at*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468695 (arguing for blockchain self-regulation to avoid harsher regulation that might stifle innovation in this nascent ecosystem).

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

[69] *See e.g.*, Walch, Angela, *The Path Of The Blockchain Lexicon (And The Law)*, 36 REV.BANK.& FIN.L.713 (2016-2017) *accessible at*: http://www.bu.edu/rbfl/files/2017/09/p729.pdf (arguing blockchain technology has advocates that lobby for favorable treatment by regulators and wide adoption including by governments. Lobbying groups like Chamber of Digital Commerce, Global Blockchain Business and Council Coin Center exert influence on government entities, including formation of the Congressional Blockchain Caucus. Such advocacy predictably highlights alleged blockchain advantages while advocating laissez-faire or even favorable treatment). *See generally*, Rand, Ayn, ATLAS SHRUGGED, (Random House 1957) (arguing the crush of regulation stifles technology) and Prentice, Robert, *Enron: A Brief Behavioral Autopsy*, 40 AM. BUS.L.J. 417-444 (2002) (arguing self-interest compromises disclosure accuracy).

[70] Werbach, Kevin D., *Trust, But Verify: Why the Blockchain Needs the Law* 33 BERK.TECH.L.J. 487 *accessible at*: https://ssrn.com/abstract=2844409 or http://dx.doi.org/10.2139/ssrn.2844409 (arguing that "Excessive or premature application of rigid legal obligations will stymie innovation and forego opportunities to leverage technology to achieve public policy objectives. Blockchain developers and legal institutions can work together.").

[71] *See e.g., Bitcoin Virtual Currency Unique Features Present Distinct Challenges for Deterring Illicit Activity. Intelligence Assessment*, Cyber Intelligence and Criminal Intelligence Section, Federal Bureau of Investigation (Apr. 24, 2012) *accessible at*: https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf (advising that Bitcoin use risks enabling money laundering and Bitcoin theft) and Nigh, Brett & C. Alden Pelker, *Virtual Currency-Investigative Challenges and Opportunities*, L.ENF.BULL. Federal Bureau of Investigation (Sept. 8, 2015) *accessible at*: https://leb.fbi.gov/articles/featured-articles/virtual-currency-investigative-challenges-and-opportunities.

[72] U.S. Attorney's Office, Southern District of New York, *Manhattan U.S. Attorney Announces The Indictment Of Ross Ulbricht, The Creator And Owner Of The "Silk Road" Website* (U.S. Dept. of

hundreds of millions of dollars worth of narcotics, stolen identities, and numerous other illegal goods and services. All transactions were conducted exclusively in Bitcoin.[73] The adage "follow the money"[74] is both precisely the point and precisely addressed to obfuscate money laundering forensics due to the strong anonymity that blockchains enable.

VI. "WHERE" BLOCKCHAIN SUBVERTS PUBLIC POLICY: THE SUBSTANTIVE DOMAINS

Substantive law establishes the rights and duties of individuals and legal entities. Generally these criminal, tortuous and contractual duties are the precise injustices that public policy seeks to (1) deter ex ante as well as (2) punish ex post or (3) compensate victims ex post. This section discusses these "predicate"[75] offenses: currency violations, investment and commodities violations, illegal gambling, tax evasion, theft, embezzlement, mail and wire fraud, and computer fraud, in all four major contexts of (1) criminal wrong, (2) civil regulatory violation and civil wrongs, both (3) tortuous and (4) contractual.

A. Currency Violations: Protecting Central Banking

By some accounts,[76] blockchain's raison d'être closely tracks the "cypherpunk" secessionist movement, a group of crypto-anarchists bent on disaffiliating with national governmental control. These libertarians intended to use technologies like blockchain to deploy distributed ledger to enable their economic withdrawal from government control, irrespective of their physical domicile.

Nations seek control over currencies to avoid hyperinflation, economic aggression from rival nations and to maintain valuation and trust essential to the success of their economies. Central banks developed first among mercantilist nations of the post-middle ages to standardize conduct of trade. These nations prospered as their private citizens and anointed trading companies increased volume and variety of international trade. Trading companies were essentially

---

Justice, February 4, 2014), *accessible at*: http://www.justice.gov/usao/nys/pressreleases/February14/RossUlbrichtIndictmentPR.php.

[73] *Id*.

[74] While the precise origins of the term remains elusive, it is generally attributed to William Goldman's screenplay "All the President's Men" derived from the underlying non-fiction work, Woodward, Robert & Bernstein, Carl, ALL THE PRESIDENT'S MEN at 248 (Simon & Schuster, 1974) (screenplay paraphrasing book's "The key was the secret campaign cash, and it should all be traced").

[75] The term predicate offenses may be best known as the focus of the underlying racketeering crimes that compound into patterns further outlawed under the federal Racketeering Influenced and Corrupt Organizations of 1970 (RICO), 18 U.S.C. §§1961–1968 discussed infra. In the context here, predicate offenses is a term used to signify substantive unlawful acts that can be compounded with evasive techniques that are also unlawful, such as obstruction or spoliation.

[76] *See e.g.*, Berg, Chris, Sinclair Davidson & Jason Potts, *Some Public Economics of Blockchain Technology* (Mar. 2, 2018) *accessible at*: https://ssrn.com/abstract=3132857.

government-granted monopolies intended to increase trade among existing nations. Trading companies also expanded their home country's reach through colonization of the new world and other underdeveloped areas.[77] Widely regarded currencies simplified trade and reduced transaction costs democratizing trade and creating efficiencies in trade that prospered home nations as well as other nations.

Central banking serves as the major controlling authority on economic system operations[78] by manipulating various chokepoints that manage their nation's economy through the mechanism of conducting monetary policy and promoting financial stability. Central banks adjust interest rates that encourage or discourage lending; they change bank reserve requirements (required minimum money on hand) to improve solvency and adjust the overall lending; they provide commercial bank access to loans to achieve temporary-immediate liquidity; they control an economy's liquidity by serving as market makers to purchase or sell bonds; they directly supervise banks and share with other government agencies and private entities[79] the supervision of private banks; and they adjust the money supply. The development of cryptocurrencies threaten central banking control over national and world economies.

The first, and most basic criticism of blockchain-enabled cryptocurrencies is that they subvert government monopolies over money and that this threatens central bank powers to control economies.[80] This condition has divided central banks into hawks, like China and Russia, that seek strong regulation of cryptocurrencies, and doves, like Canada, that apparently seek to enable cryptocurrencies A second, set of additional criticisms focus on other financial

---

[77] The northern European nations of Holland, Spain and England were particularly successful at this form of Imperialism. However, a pejorative vision of the colonial movement is condemned in the more modern use of the term Imperialism. Imperialism is argued to arise when developed nations colonize and control under-developed nations with a singular view of exploiting them economically. The U.S. is very frequently cast in this latter role, particularly in the Western Hemisphere and Pacific Islands. Clearly, Imperialism has had many other objectives and results that this modern usage ignores. Consider that the American colonies chafed under British rule before the American Revolution. Since Colonial times, the U.S. has become a most stellar success, perhaps THE most stellar success, of colonialism. Of course, there are many less virtuous historical and contemporary examples where indigenous peoples are exploited. Areas in Africa and South America are the most frequently used exemplars.

[78] The U.S. Federal Reserve sponsors and conducts research that supplies scholarly understanding of economic and monetary phenomena.

[79] Comptroller (OCC), Treasury, State Banking Regulators, FCIC, UCC, Various standards development organizations (SDO).

[80] McWhinney, James E., *Can Bitcoin Kill Central Banks?* INVESTOPEDIA *accessible at*: https://www.investopedia.com/articles/investing/050715/can-Bitcoin-kill-central-banks.asp and Davies, Howard, *Hawk Or Dove? Bitcoin Is Forcing Central Banks To Take Sides*, GUARDIAN (Feb. 27, 2018) *accessible at*: https://www.theguardian.com/business/2018/feb/27/hawk-or-dove-Bitcoin-is-forcing-central-banks-to-take-sides (arguing blockchain enabled cryptocurrencies are too powerful to be regulated, discussing unlikely success of the newly minted Venezuelan Petro, a petroleum backed cryptocurrency); *but see*, Ellworth, Brian, *Special Report in Venezuela, new cryptocurrency is nowhere to be found*, REUTERS (Aug. 30, 2018) *accessible at* https://www.reuters.com/article/us-cryptocurrency-venezuela-specialrepor/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF15U.

matters such as investment market manipulations, speculative bubbles in currency and commodities markets, and illegal gambling. These matters are discussed next.

B. Money Service Business: Transmission Violations

The potentially greatest threat of cryptocurrency flows directly from its originally most fervently touted, but now curiously muted, claim of advantage: secretive money transmission.[81] Money movements in furtherance of illicit schemes undermine law enforcement, counter-terrorism and the control governments exercise on their economies (through central banking). In response to a long history of illicit money flows undermining law and order, the U.S. enacted the Bank Secrecy Act[82] requiring, among other matters relevant to this paper, the registration of money transmitters. Money transmitters engage in the money service business (MSB). It seems unlikely that there is any current form of "Total Information Awareness"[83] that, in real time, analyzes every money transmittal performed by licensed money transmitters.[84] Nevertheless, the licensing and recordkeeping duties of the MSB enable law enforcement and counter-terrorism forces to subpoena, issue search warrants or otherwise eventually discover such

[81] Some observers argue that cryptocurrencies ability to create a larger money supply also undermines central banking's traditional roles. However, this paper argues, that money supply manipulation remains an unrealized threat from cryptocurrencies. The time has not yet come at which (1) the volume of cryptocurrency in relation to traditional fiat currencies and private bank expanded money supply, and (2) the velocity of money supply turnover, has risen so significantly in relation to traditional money supply so as to undermine central banking. Thus, this article's critique suggests some uncertain future calamity and not the immediate threats cryptocurrencies impose on public policy, is already the driving factor in cryptocurrency regulation, *see e.g.*, Fraser, *The Turnover of Money*, St. Louis Federal Reserve (1959) *accessible at*: https://fraser.stlouisfed.org/files/docs/publications/frbatlreview/pages/64115_1955-1959.pdf.

[82] Pub.L.91-508, 84 Stat. 1114-2, 12 U.S.C. chs.13, 16 & 15 U.S.C. ch.2B (91st Cong, Oct.26, 1970).

[83] Total Information Awareness (TIA) was a post-9.11 defensive scheme advocated by Admiral John Poindexter. He spearheaded U.S. government eavesdropping on all communications, transaction records and messaging traffic of every kind to ferret out terrorists that many argued hid behind anonymity, encryption, the Fourth Amendment or any other protection of privacy or confidentiality (technical, contractual, legal). *See e.g.*, Poindexter, John (Dir.), *Overview Of The Information Awareness Office*, Information Awareness Office of DARPA, Speech to the Defense Advanced Research Projects Agency's DARPATech 2002 Conference, Anaheim, Calif., (Aug. 2, 2002) *accessible at*: https://fas.org/irp/agency/dod/poindexter.html.

[84] This is not to argue that total information awareness of all licensed money transmitters would be successful in capturing any significant volume of money transmittal activities performed by unlicensed money transmitters. Indeed, the major point of this discussion is that blockchain enablement of cryptocurrencies facilitates secretive money transmissions that already facilitate a thriving black market, yet remain generally undetected by government much of the time.

records that help uncover transfers, usually once probable cause is established or litigation commences.

Most states likewise control money transmitters through licensure.[85] The USA PATRIOT Act also criminalizes unlicensed money transmission to prevent its use in terror financing.[86]

> **Money transmitter**: A person that provides money transmission services. The term "money transmission services" means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, fund, or other value that substitutes for currency to another location or person by any means. 'Any means'' includes, but is not limited to, through a financial agency or institution; a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both; an electronic funds transfer network; or an informal value transfer system;[87]

Blockchain enabled cryptocurrency transactions should be easily seen as coming within the ambit of the regulated money transmission services defined just above. This bank secrecy regulation's catch all phrases, "other value" and "by any means" are likely be interpreted to include cryptocurrency transmissions in whatever currency chosen - dollar, Bitcoin, etc. "Other value that substitutes for currency" should be read to include known or invented media of exchange, including cryptocurrencies. The transmission methods listed should include existing and legally recognized financial transmission systems as well as any future[88] similar system developed. The Bank Secrecy Act seems broadly worded enough to immediately capture transfers using cryptocurrencies processed through their systems. However, while plausible, it seems unlikely any node or cloud location in any non-governmental operated blockchain will actively seek designation as a quintessential money transmitter. Indeed, just the opposite seemed intended ab initio.

Cryptocurrency designers, participants and promoters are likely to seek exemption from state or federal control over MSB or will argue their unique peer-to-peer design is well outside MSB regulations.[89] The Financial Crimes

---

[85] *See e.g.*, Brown, Thomas, *50-State Survey: Money Transmitter Licensing Requirements, accessible at*: http://abnk.assembly.ca.gov/sites/abnk.assembly.ca.gov/files/50%20State%20Survey%20-%20MTL%20Licensing%20Requirements(72986803_4).pdf.
State licensure are consumer protection measures. They generally operate without deposit insurance for banks (FDIC) or credit unions (NCUA).

[86] 18 U.S.C. §1960.

[87] 76 Fed.Reg. 43596, Bank Secrecy Act Regulations; Definitions and Other
Regulations Relating to Money Services Businesses"; (July 21, 2011) *accessible at*: https://www.govinfo.gov/content/pkg/FR-2011-07-21/pdf/2011-18309.pdf.

[88] The rule of statutory interpretation, *ejusdem generis*, may apply, literally of the kind in the list. Here, these catch all phrases append to include new inventions intended to operate like the specifically listed items.

[89] *See*, Brito Jerry & Andrea Castillo, *Bitcoin-A Primer for Policymakers*, MERCATUS CENTER at 25-

Enforcement Network (FinCEN), a bureau within the U.S. Department of the Treasury, is responsible to monitor financial transaction data to service the enforcement of (1) anti-money laundering (AML) law, (2) terror finance, and (3) financial crimes. FinCEN is the U.S.'s Financial Intelligence Unit (FIU), one of 155 worldwide.[90]

Early on in the cryptocurrency "revolution," FinCEN interpreted the Bitcoin phenomenon to exempt "users" from MSB regulations.[91] Users merely obtain or dispose of virtual currency if done for personal use to purchase goods or services; users are not MSB. Users includes both natural persons and organizations, like companies, corporations and unincorporated entities. Remarkably, exempt users can include those who create cryptocurrencies through mining, if for personal use.[92] This FinCEN guidance would also appear to exempt cryptocurrency software developers.[93] However, administrators and exchangers of convertible virtual currency are money transmitters under MSB regulations requiring registration, recordkeeping and reporting.[94] This distinction parallels the scope of MSB regulations regarding the traditional money supply.

1. Ripple Labs

The first real test of FinCEN's Virtual Currency regulations it coordinated with the U.S. Attorney for the Northern District of California. The settlement establishes a pattern framework for remedial undertakings by unregistered virtual

---

28 (2013, George Mason Univ.) *accessible at*: https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf.

[90] The Egmont Group of FIU is a Toronto-based network of 155 FIUs intended to facilitate international cooperation in money laundering and terror finance enforcement. *See Financial Intelligence Units: An Overview*, Int'l Monetary Fund (2004) *accessible at*: https://www.imf.org/external/pubs/ft/FIU/fiu.pdf.

[91] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, (U.S. Dept. Treasury, Mar. 18, 2013) *accessible at*: https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (interpreting FinCEN regulations of "money transmitter" duties for participants in cryptocurrency operations). "A user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is not an MSB under FinCEN's regulations." *Id*. at 2.

[92] *Id*. at n.7. "How a person engages in "obtaining" a virtual currency may be described using any number of other terms, such as "earning," "harvesting," "mining," "creating," "auto-generating," "manufacturing," or "purchasing," depending on the details of the specific virtual currency model involved. For purposes of this guidance, the label applied to a particular process of obtaining a virtual currency is not material to the legal characterization under the BSA of the process or of the person engaging in the process."
Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Virtual Currency Mining Operations* (U.S. Dept. Treasury, Jan. 30, 2014), *accessible at*: https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R001.pdf.

[93] *Id*. *See also*, Van Valkenburgh, Peter, *The Bank Secrecy Act, Cryptocurrencies, and New Tokens: What is Known and What Remains Ambiguous*, COIN CENTER RPT., at 9 (May 2017) *accessible at*: https://coincenter.org/entries/aml-kyc-tokens.

[94] *Id*. MSB are required to make currency transaction reports (CTR) of suspicious transactions to inform FinCEN and other law enforcement of possible illegal activities or terror financing transactions. 31 C.F.R. §§1010.300 – 1010.370.

currencies.[95] *In re Ripple Labs*,[96] involves the wholly owned subsidiary of XRP II, Ripple Labs, which built products supporting XRP, a decentralized cryptocurrency.[97] XRP was the second largest currency network to Bitcoin in 2015.[98] Ripple admits facts recounted in the Statement of Facts and Violations, essentially that, after publication of FinCEN's 2013 interpretive guidance, Ripple continued to sell XRP for legal fiat currency without MSB registration.

While violations like Ripple's seem widespread, the undertakings Ripple agrees to are not. The three year agreement with Justice requires Ripple to offload much of its currency transmission business to a separate legal entity, requires cooperation in other investigations, forfeiture and civil penalties totaling $700,000 and extensive remediation steps to prevent future violations. These include:

> (1) promises to transact XRP and "Ripple Trade" activity through a money services business registered with FinCEN;
> (2) implement and maintain an effective AML program, with required internal controls, training programs, risk assessments, and other requirements;
> (3) comply with the Funds Transfer and Funds Travel Rules, which were issued to ensure that essential information can be made available to law enforcement to trace the flow of dirty money;
> (4) conduct a three-year "look-back" review of their records to identify and provide overdue reports of suspicious activity;
> (5) retain external independent auditors to review their compliance every two years, up to and including 2020;
> (6) require the auditors' reports be provided to FinCEN and the U.S. Attorney's Office; and
> (7) undertake certain enhancements to the Ripple Protocol to appropriately monitor all future transactions.[99]

---

[95] "Unregulated, virtual currency opens the door for criminals to anonymously conduct illegal activities online, eroding our financial systems and creating a Wild West environment where following the law is a choice rather than a requirement." News Release, *Ripple Labs Inc. Resolves Criminal Investigation*, Dept. of Justice (May 5, 2015) *accessible at*: https://www.justice.gov/opa/pr/ripple-labs-inc-resolves-criminal-investigation.

[96] Settlement Agreement, *Ripple Labs*, Dept. of Justice (N.D.Cal. May 5, 2015) *accessible at*: https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/05/05/settlement_agreement.pdf.

[97] NewCoin and OpenCoin are predecessors to XRP. XRP is "pre-mined" in that it was fully-generated prior to distribution, *Id*. at 6.

[98] Ripple differs in architecture from Bitcoin underscoring how each cryptocurrency must be compared to the "standard design" for similarities as well as key differences. For example, Ripple uses gateways to move XRP and other currencies through its network as a business for customers. This seems clearly within the MSB ambit. *See*, Van Valkenburgh, Peter, *The Bank Secrecy Act, Cryptocurrencies, and New Tokens: What is Known and What Remains Ambiguous*, COIN CENTER Rpt., at 10 (May 2017) *accessible at*: https://coincenter.org/entries/aml-kyc-tokens.

[99] *Id*. at Attachment B: Remedial Framework.

2. Canton Business Corporation (BTC-e)

A 2017 FinCEN enforcement action exercises extra-territorial jurisdiction over Canton Business Corporation (BTC-e) and one of its operators, a Russian national Alexander Vinnik who was arrested in Greece.[100] BTC-e operated a money transmitter and currency exchanges business servicing both fiat currency, such as U.S. dollars, Russian Rubles & Euros, as well as the convertible virtual currencies Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash.[101] BTC-e facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. It also processed transactions of proceeds derived from funds stolen from bankrupt Mt.Gox, at one time the largest Bitcoin exchange. Jurisdictional requirements of FinCEN are clearly satisfied because some BCT-e transactions involved customers residing in the U.S.

C. Gambling

Cryptocurrencies and blockchain communications would appear to be perfect mechanisms for the conduct of illegal online gambling. Legal, casino-style gambling is transparent; open casinos permit onlookers to witness the scale of winnings and the identity of gamblers. Online gambling generally camouflages both scale and identity. Cryptocurrency seems a likely medium to settle bets. Thus, secretive and mostly illegal gambling can be blockchain based, first and foremost, for the settlement of gambling debts. Furthermore, a virtual gambling casino can also communicate all other matters not involving final gambling debt settlements using blockchain technologies.[102]

Gambling has existed since ancient peoples believed the practice expressed supernatural powers. Similarly, today many gamblers believe in luck. Gambling is a widespread pastime but was sullied in the 19th century U.S. wild west when considered alongside three other socially unacceptable saloon activities: violence, alcohol consumption and prostitution. Indeed, the financial ruin suffered by many naïve, "cowboy-era" gamblers also burdened their frontier families. By the 20th century organized crime and the manipulation of sporting events further sullied gambling. Some forms of legalized gambling proliferates in

---

[100] *See* News Release, In re BTC-e, FinCEN, *accessible at*: https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware and https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf.

[101] In re BTC-e, FinCEN Assessment of Civil Money Penalty, No.2017-03 (July 26, 2017) *accessible at*: https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf.

[102] Pressures to expand illegal online sports gambling may ease somewhat as gambling debt settlement payments become state regulated. Legal sports gambling is quickly becoming sanctioned by a rush of states to legalize the practices, following the Supreme Court invalidation of the Bradley Act.

many nations and in most U.S. states, including, e.g., native indigenous casinos, riverboat gambling, state-run lotteries, state licensed casinos, and, increasingly, onshore sports betting.[103] Still, much gambling remains illegal and remains unenforceable as an illegal form of contract.

> Gambling is the creation of a risk with no prior existence primarily for the purpose of shifting the risk to expose the parties to gain or loss. These risks are usually based on uncertain events that solely rely on chance (simple card games, dice, roulette), rely entirely on external factors (sports outcomes) or are based on a combination of chance and the gambler's skill (complex card games).[104]

Gambling likely proliferates on the Internet because local law enforcement is underfunded, predominately focuses on "street crime," and, despite developing some online forensic expertise, largely remains ill-equipped to shift primary focus to online forensics. Gamblers' private homes are their primary gambling venues shielding their gaming activities from law enforcement or the discipline from censure by peers. Furthermore, gambling at work is a likely growth area but is poorly policed by corporate network administrators except in university communities or where online gambling migrates from PCs to hand-held devices operating off employer-operated networks. Cryptocurrencies used for gambling debt settlement are resistant to forensics. Furthermore, offshore gambling sites can operate beyond U.S. jurisdiction further frustrating regulation as well as debt settlement. This will be a particular problem if offshore casinos or counter-parties become big losers willing to suffer goodwill loss from non-payment or if the casinos become insolvent.

VII. INVESTMENT MARKET REGULATION

Bitcoin, and by clear implication most all other current and future cryptocurrencies, continually exhibit the volatility of commodities, rather than the stable conditions for successful currencies: sovereign-backing, governance standards, accountability, oversight, and reliable reporting of financial data such as trading. Cryptocurrency volatility and tenuous connection to currencies could make commodity regulation appropriate. Cryptocurrencies unique character make

---

[103] The Bradley Act prohibited sports betting except in the four grandfathered states of Nevada, Deleware, Montana and Oregon, *see* Professional and Amateur Sports Protection (PASPA) Act of 1992, Pub.L.102–559, 106 Stat. 4227, *codified as* 28 U.S.C. §§3701-04. PAPSA was invalidated as unconstitutional in Murphy v. National Collegiate Athletic Association, No. 16-476 584 U.S. – (May 14, 2018) *accessible at*: https://www.supremecourt.gov/opinions/17pdf/16-476_dbfi.pdf (holding PASPA failed to validly pre-empt state sanctioned gambling under any of three prevailing pre-emption theories because states cannot be the pre-emption object under the anti-commandeering rule of the 10th Amendment, only private actors can be targeted).

[104] Bagby, John W., ECOMMERCE LAW: ISSUES FOR BUSINESS at 113-114 (West 2003) (arguing costs of enforcement outweigh most benefits of illegal gambling, indeed legalizing gambling would weaken organized crime and the negative social context of gambling has changed).

them vulnerable to falling between the cracks separating regulatory schemes of commodities, securities and currencies. This seemingly un-regulable situation is one that many cryptocurrency participants likely prefer.[105] Nevertheless, both regulatory schemes have broad regulatory purviews and sufficiently open-ended jurisdictional boundaries, security[106] and commodity,[107] to implicate one or more investment market regulatory schemes for cryptocurrencies.

All this makes investment market regulation a more immediate and appropriate channel for blockchain regulation. Unless specifically exempt, and, depending on the method of initial distribution, the pool of traders and the modes of trading, cryptocurrencies are possibly classified as either commodity futures contracts and/or securities. Cryptocurrencies exhibit group participation aspects such as distributed (blockchain) participants engaged in a common enterprise or scheme with strong expectation of profit from future efforts, both internal and external, making many such systems closely resemble the traditional catch-all "investment contracts" regulated in *Howey*.[108]

Cryptocurrencies could be regulable under the Commodity Exchange Act (CEA) by the Commodity Futures Trading Commission (CFTC). Alternatively, cryptocurrencies could constitute securities regulable by the Securities and Exchange Commission (SEC). Perhaps aspects of cryptocurrencies and their markets could be regulable by both agencies. An exclusive, binary jurisdictional choice may be unnecessary for blockchain "tokens" or other cryptocurrency instruments representing value, despite a history of these two agencies'

---

[105] *See e.g.,* Schäfer, Daniel & Michael Maisch, *The pros and cons of Bitcoin regulation*, HANDELSBLATT TODAY (Dec.21, 2017) *accessible at*: https://www.handelsblatt.com/today/flip-sides-the-pros-and-cons-of-bitcoin-regulation/23573506.html.

[106] SEC v. Howey, 328 U.S. 293 (1946) *accessible at*: https://caselaw.findlaw.com/us-supreme-court/328/293.html.

[107] The definition of a commodity is complex, having endured tortured revision since the passage of the Commodity Exchange Act in 1936, Pub.L.74-675, 49 Stat. 1491 *codified as* 7 U.S.C. §§1-27:
The term "commodity" means wheat, cotton, rice, corn, oats, barley, rye, flaxseed, grain sorghums, mill feeds, butter, eggs, Solanum tuberosum (Irish potatoes), wool, wool tops, fats and oils (including lard, tallow, cottonseed oil, peanut oil, soybean oil, and all other fats and oils), cottonseed meal, cottonseed, peanuts, soybeans, soybean meal, livestock, livestock products, and frozen concentrated orange juice, and all other goods and articles, except onions (as provided by section 13–1 of this title) and motion picture box office receipts (or any index, measure, value, or data related to such receipts), and all services, rights, and interests (except motion picture box office receipts, or any index, measure, value or data related to such receipts) in which contracts for future delivery are presently or in the future dealt in. 7 U.S.C.§1a.
The CFTC regulates most futures contracts covering commodities and a variety of non-agricultural commodities and financial interests. Over time, these commodity futures markets, known as designated contract markets (DCMs) regulated by the Commission, have grown to include those for energy and metals commodities such as crude oil, heating oil, gasoline, copper, gold, and silver. The agency now also oversees DCMs for financial products such as interest rates, stock indexes, and foreign currency.
CFTC Mission Statement, *accessible at*: https://www.cftc.gov/About/MissionResponsibilities/index.htm.

[108] SEC v. Howey, 328 U.S. 293 (1946).

competition to exert jurisdiction over whatever was the latest new investment vehicle.[109]

A. CFTC Jurisdiction over Commodities

The CFTC has brought enforcement actions arguing that cryptocurrencies are commodities.[110] Furthermore, the CFTC and the SEC have argued to Congress,[111] that cryptocurrencies must be included in their jurisdictions given the impact of cryptocurrencies on investors and financial markets.[112]

1. CFTC v. McDonnell

The CFTC won an early skirmish in this battle to regulate cryptocurrencies in C*FTC v. McDonnell*.[113] The CFTC alleged that defendants misappropriated investor funds by operating a fraudulent trading scheme in virtual currency making these activities fall under CFTC supervision. In *McDonnell* the CFTC had standing because virtual currencies are commodities within the CFTC's jurisdiction and the

---

[109] The SEC and CFTC jurisdictional disputes are longstanding due to the vagueness of their statutory enablements, the creativity of financial engineers throughout the 20th century and the totally unforeseen developments by FinTech entrepreneurs in the 21st century. *See e.g.,* Loss, Louis, FUNDAMENTALS OF SECURITIES REGULATIONS, (6th ed. 2013 supp) at 303-305 (detailing a long jurisdictional battle triggered by the two agency's enabling acts and revisions, resulting in a temporary "treaty" largely codified in the Futures Modernization Act, 96 Stat.2294 (1983)); Charter of the Joint CFTC-SEC Advisory Committee on Emerging Regulatory Issues (May 11, 2010) *accessible at*: https://www.cftc.gov/sites/default/files/idc/groups/public/@aboutcftc/documents/file/cftc-sec-joint_charter.pdf (establishing joint efforts to manage regulatory challenges within or close to the two agencies' missions, initially conducting inquisition into market illiquidity crisis concerning interactions between equity and derivatives markets occurring on May 6, 2010) and Memorandum of Understanding Between the SEC and CFTC Regarding Coordination in Areas of Common Regulatory Interest, (Mar.11, 2008) *accessible at*: https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/cftc-sec-mou030608.pdf.

[110] See e.g., In re BXFNA Inc., CFTC Docket No. 16-19 (June 2, 2016); In Re TeraExchange LLC, CFTC No.15-33, 2015 WL 5658082 (Sept. 24, 2015); CFTC v. Gelfman Blueprint, Inc., Case No. 17-7181 (S.D.N.Y. filed: Sept. 21, 2017) (alleging ponzi scheme purporting to trade Bitcoin); CFTC v. The Entrepreneurs Headquarters Limited, Case No. 2:18-cv-00345 (E.D.N.Y. filed: Jan. 18, 2018) (alleging misappropriation of Bitcoins to trade in commodities); see generally, CFTC Launches Virtual Currency Resource Web Page, Press Release (Dec. 15, 2017) *accessible at*: https://www.cftc.gov/PressRoom/PressReleases/pr7665-17.

[111] Lumb, David, *U.S. Regulators Are Trying To Figure Out What To Do With Cryptocurrency*, ENGADGET (Feb. 5, 2018) *accessible at*: https://www.engadget.com/2018/02/05/us-regulators-are-trying-to-figure-out-what-to-do-with-cryptocur/.

[112] *See*, Clayton, Jay & J. Christopher Giancarlo, *Regulators Are Looking at Cryptocurrency*, WALL ST. J., (Jan. 24, 2018) *accessible at*: https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363.

[113] CFTC v. McDonnell, 18-CV-361 (E.D.N.Y. Mar.6, 2018) *accessible at*: https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoindroporder030618.pdf (holding that cryptocurrencies (Bitcoin in particular) are commodities subject to CFTC regulation under CEA).

agency is enabled to police fraud or manipulation in commodity futures markets.[114] Virtual currencies are commodities, a classification that includes: '*all other goods and articles . . . and all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in.*'[115] With cryptocurrencies within the regulatory ambit, the CFTC's enabling statutes recognize the agency as having "broad authority [that] extends to fraud or manipulation in derivatives markets and *underlying spot markets*."[116] "Where a futures market exists for a good, service, right, or interest, it may be regulated by CFTC, as a commodity, without regard to whether the dispute involves futures contracts."[117] While *McDowell* appears to confirm the CFTC's broad regulatory exercise over cryptocurrencies, other cases percolating could undermine this.[118]

B. SEC Jurisdiction Over Cryptocurrencies as Securities

The U.S. federal securities laws target investments known as "securities." Virtual currencies, whether designated as tokens or offered for sale in an initial coin offering (ICO), are susceptible to masquerade as "investment contracts." Furthermore, federal securities laws are implicated when cryptocurrencies are assets held by public companies or flow as consideration in securities trading. Once a cryptocurrency, or any other blockchain inspired investment scheme, is designated a security, a whole panoply of regulable activities are triggered: initial public offerings, exempt offerings, reduced registration requirements such as crowdfunding, duties of involved registered broker-dealers, licensed exchanges, online trading portals, disclosure duties, antifraud provisions, market manipulation or IPO stabilization, and SEC enforcement including remedies such as cease and desist or disgorgement.

A security may be considered an intangible transaction or contract right requiring one party to make payments or future performances to another party. While "security" can also mean contract rights (lien) on particular collateral or even a reduced risk of danger, the narrower meaning encompasses investment schemes and the attendant professional services regarding investment schemes

---

[114] CFTC's jurisdiction does not likely preclude other agencies, like the SEC, IRS or banking regulators, from regulating cryptocurrencies, *see*, Benjamin, James Joseph Jr., Jan-Paul Bruynes, Peter I. Altman, Nicholas C. Adams & Kelly Handschumacher, *Federal Judge Adopts CFTC Position That Cryptocurrencies Are Commodities*, BUS.L.TODAY (Apr. 20, 2018) *accessible at*: https://businesslawtoday.org/2018/04/federal-judge-adopts-cftc-position-cryptocurrencies-commodities/.

[115] *Id*. at 18, *citing* 7 U.S.C. §1(a)(9) emphasis in original.

[116] *Id*.

[117] *Id*. at 22 *citing* U.S. v. Brooks , 681 F.3d 678, 694 (5th Cir. 2012), cert. denied, 133 S. Ct. 839 (2013) (noting futures contracts dependant on pricing of natural gas as commodity moving through Louisana's Henry Hub would also be commodity if passing through any other pipeline or transportation conveyance).

[118] *See e.g.*, CFTC v. My Big Coin Pay, Inc. No. 1:18-cv-10077 (D. Mass. Filed: Jan. 16, 2018) *accessible at*: https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfmybigcoinpaycomplt011618.pdf.

when brought within the SEC's jurisdiction:

> The term security means any note, stock, treasury stock, bond, debenture, evidence of indebtedness, transferable share, **investment contract**, voting trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, stock option, warrant, or in general, any interest or instrument commonly known as a "security."[119] (emphasis added)

Instruments on this statutory list are regulable securities and there are only a few exceptions: short-term commercial paper, notes that facilitate trade credit and credit sales of consumer assets,[120] securities issued by banks, government agency securities and the securities issued by charities.

Scholars opine, the SEC brings charges and the courts have designated schemes as investment contracts when new forms of investments become regulable as securities. For example, securities include limited partnership interests, equipment trust certificates, some franchises, time-shares, variable annuity insurance policies and pyramid/Ponzi selling schemes. The catch all "investment contracts" emphasized above in the quoted statutory definition is generally used to capture new forms of security. Clearly, tokens and ICO are ripe for this analysis.

1. Fitting ICO into the *Howey* "Investment Contract" Regime

There are four elements first established in *SEC v. Howey*[121] of investment contracts relevant to capturing blockchain managed tokens however, labeled - cryptocurrencies or other forms of virtual money:

> (1) an investment of money,
> (2) into a common enterprise or scheme,
> (3) from which the investor is led to expect profits, which are

---

[119] 15 U.S.C. §77b *accessible at*: https://www.law.cornell.edu/uscode/text/15/77b.

[120] Notes are exempt from securities regulations if they bear a "family resemblance" to the commercial transactions above. *Reves v. Ernst & Young* held that notes are securities depending on the following four factors: (1) the parties' purposes, (2) the seller's distribution plan, (3) the public expectation for securities law protection, and (4) whether another factor reduces the instrument's risk so the protection of the securities laws becomes unnecessary, 494 U.S. 56 (1990).

[121] 328 U.S. 293 (1946). Recall the *Howey* story: vacationers largely from the northeast to Florida were solicited by Howey to purchase precise fractional interests in land on which there were producing citrus groves. All were offered and most investors also purchased ten year term cultivation, harvesting and marketing service contracts from Howey's affiliate, Howey in the Hills. Profits were shared proportionately from the whole mass as produced, none from the actual production of the investors' separate individual plots. The SEC challenged these separate land sale and share cropping service contracts as combining together into an unregistered security. In 1946, the Supreme Court held the Howey scheme constituted the offer and sale of "investment contracts." The four part *Howey* analysis was created. The substance, not the form as designated, of transactions is the true test of the jurisdictional bounds of the federal securities laws. Investment contract is a flexible concept that adapts to novel forms of contract and investment when they take on the features of a security.

(4) derived solely (primarily) from the efforts of others.

The application of the *Howey* elements to ICO seems straightforward.[122]

First, persons solicited by the near standardized ICO "white papers" are clearly expected to invest their money, time, effort and/or MIPS[123] to engage in the offering, satisfying the first *Howey* element.[124]

Second, and perhaps the most challenging aspect of satisfying the *Howey* regime, is the common enterprise or scheme element. Nevertheless, ICOs appear to fit in a straightforward way. Any cryptocurrency is a standardized token issued, traded, redeemed, and valued or understood by the public and analysts is a unit of trade inhabiting a single cryptocurrency system potentially encompassing all such identical tokens. Tokens or coins are fungible interests similar to shares or other participation units or certificates. Even if a particular coin can be traded or otherwise given value in various markets, it is the system's community of interest that endow cryptocurrency with like value. Bitcoin and other cryptocurrencies illustrate that fractional interests are needed when a single unit's value rises significantly, thereby permitting "de-scaling" to each particular transaction's size.[125] Thus, a unified, common enterprise is involved in an ICO.

Commonality is assessed two ways, and either is sufficient to satisfy the common enterprise element. Pooling the coin holder's interests into a market for fungible and identical interests is key to existence of a common enterprise. Coin holders need not be inter-related, except in their interest that any identically denominated token in the system will have similar value. Of course, identical value is elusive because cryptocurrencies experience very significant volatility in price, supply and demand, just as do other investment contracts. Commonality emerges most clearly from the promoter's efforts in designing and promoting the investment, a condition shared by ICO as well as traditional securities. The issuer's fortunes generally dictate the investment's success.

Vertical commonality is present when the investors fortunes rise and fall with the issuer's fortunes. In the ICO context, coin holders wealth represented by coin holdings rise or fall with the issuer's fortunes in mining and distributing coin.[126] Alternatively, horizontal commonality is present when similarly situated

---

[122] *Digital Asset Transactions: When Howey Met Gary (Plastic),* Remarks of William H. Hinman, Director, SEC Division of Corporation Finance, at the Yahoo Finance All Markets Summit: Crypto, San Francisco, CA (June 14, 2018) (recounting Howey elements in most ICO as observed by SEC Division of Enforcement investigations and actions), accessible at: https://www.sec.gov/news/speech/speech-hinman-061418.

[123] MIPS is a 1970s era, standard measure of computer performance processing, literally "million instructions per second."

[124] ICO white papers serve as initial offering documents, prospectuses, offering memoranda, red herring (preliminary) prospectus and the like. Online repositories offer free access to previously used white paper (forms) so some standardized boilerplate is emerging.

[125] Securities and currencies frequently exhibit fractional interests.

[126] *See generally*, Klayman, Elliot, John W. Bagby & Nan Ellis, IRWIN'S BUSINESS LAW-CONCEPTS, ANALYSIS, PERSPECTIVES, Ch.44 *Regulation of the Investment Markets: Public Offerings and Private Placements*, at 949-951 (Richard D. Irwin 1994).

investors, here coin holders, enjoy gains or suffer loss, that is rise or fall, together. While the size of their holdings may differ, just as particular shareholders own different numbers of shares, their percentage gain or loss is identical. This creates a common enterprise derived from a shared community of interest.

As to *Howey's* third element, the expectation of profits, it is clear from ICO "white papers" that ICOs conform to *Howey*. Investors are attracted primarily for the speculative profits possible.[127] The profitability of fungibles is achieved substantially when secondary trading markets are envisioned. Organized secondary trading markets further increase liquidity, enabling the expectation of profitability from appreciation. ICO offering documents regularly tout healthy secondary market liquidity. Indeed, a fundamental factor in any currency is potential for network effects as a medium of exchange to purchase land, goods, and services of for the payment of debts as well as how readily speculative trading markets will successfully clear cryptocurrencies transactions.

Finally, the fourth *Howey* element, profits derived solely (primarily)[128] from the efforts of others, seems easy to satisfy. Except for the miners who create new coins, investors' profits come from the system's success, the efforts of ICO promoters. Of course, ICO and cryptocurrencies are highly speculative instruments whose value is far less dependent on the issuer's performance in markets for products or services, a key distinction between ICO enterprises and the primary lines of business conducted by industrial or service firms that have classes of securities traded on a securities exchange.

---

[127] *See* Statement on Cryptocurrencies and Initial Coin Offerings, SEC Chairman Jay Clayton (Dec. 11, 2017): "many token offerings appear to have gone beyond [a simple book of the month club style] construct and are more analogous to interests in a yet-to-be-built publishing house with the authors, books and distribution networks all to come. It is especially troubling when the promoters of these offerings emphasize the secondary market trading potential of these tokens. Prospective purchasers are being sold on the potential for tokens to increase in value – with the ability to lock in those increases by reselling the tokens on a secondary market – or to otherwise profit from the tokens based on the efforts of others. These are key hallmarks of a security and a securities offering." *Accessible at*: https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

[128] Later cases illustrate that the term "solely" was probably a prematurely conceived modifier to the "efforts of others" limitation. The Supreme Court likely sought to permit development of novel investment schemes without triggering securities laws jurisdiction when purchasers were intimately involved in operations and thus the success of the investment depended on the purchaser's efforts in addition to efforts of some others. However, over time, some investor participation has been allowed in novel investment contracts without negating status as a security. Consider that employee stock ownership plans permit employees to share in their employer's profitability while contributing to the firm' s success and these interests are still classified as securities. It is even more convincing that the alternative limiting principle of "primarily" used here is more suitable in executive options. While stock and options are on the statutory list already, arguably not to be removed easily, the nominal participation in "efforts" by investors should not negate designation as an investment contract in a compelling case. This may be important in ICO, token sales and other cryptocurrency situations where an investor participates in mining new coins or making markets by spending, accepting or redeeming coins. Larger markets of increasing numbers of coin holders also increases the network effects of the whole system, liquidity is form of participation effort.

C. SEC Cryptocurrency Enforcement History

As of this writing, the SEC has released over two dozen enforcement actions since 2013 when cryptocurrency problems began to fester. Most ICO situations fall within the ambit of a security. However, in addition, ancillary activities that facilitate trading or the development of cryptocurrency markets also implicate the securities laws. Cryptocurrencies implicate regulable transactions, regulated institutions, trading platforms as national securities exchanges, regulated disclosures and the prohibition of fraudulent statements. SEC enforcement activity in these matters is growing steadily.

The North American Securities Administrators Association (NASAA) has been actively engaged in a "Crypto Crackdown" by conducting over 200 investigations with several states and Canadian provinces bringing 76 ICO enforcement actions, most resulting in some form of cease and desist, demand letter, show cause demand, or emergency action.[129] The following subsections focus on the SEC's cryptocurrency and ICO administrative record since 2013.

1. Trendon T. Shavers & Bitcoin Savings & Trust

In *SEC v. Trendon T. Shavers & Bitcoin Savings & Trust*,[130] the SEC charged Shavers, allegedly used the Internet monikers of "Pirate" and "pirateat40," along with his company, with defrauding investors in a Bitcoin-denominated Ponzi scheme. Various securities law provisions were alleged.[131] More than 700,000 Bitcoins were raised from investors in Shavers' Bitcoin Savings & Trust (BTCST). Shavers allegedly falsely promised up to 7% weekly returns based on BTCST's purported Bitcoin market arbitrage activity. At the time, the Bitcoin were valued at $4.5 million based on 2011 and 2012 trading values. However, this case illustrates Bitcoin's wild volatility - the value of the 700,000 Bitcoin in this case, when valued at its high on Dec. 17, 2017, was $13 trillion. After Bitcoin's most recent and precipitous fall, the value of this 700,000 Bitcoin fraud today exceeds $5 billion. BTCST was allegedly a Ponzi scheme, Shavers used Bitcoin from new investors to make purported interest payments and cover investor withdrawals. The Shavers case prompted the SEC to issue the first of several Investor Alerts warning of cryptocurrency fraud.[132]

---

[129] *See, State and Provincial Securities Regulators Conduct Coordinated International Crypto Crackdown, accessible at*: http://www.nasaa.org/45121/state-and-provincial-securities-regulators-conduct-coordinated-international-crypto-crackdown-2/ and http://www.nasaa.org/regulatory-activity/enforcement-legal-activity/operation-cryptosweep/.

[130] SEC v. Trendon T. Shavers and Bitcoin Savings and Trust, SEC Enf.Act.No.2013-132 (E.D.Tex. July 23, 2013) *accessible at*: https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf.

[131] Offer and sale of investments in violation of anti-fraud registration provisions §§ 5(a), 5(c) and 17(a) of the Securities Act of 1933, Section 10(b) of the Securities Exchange Act of 1934 and Exchange Act Rule 10b-5.

[132] *Investor Alert - Ponzi Schemes Using Virtual Currencies*, SEC Pub. No 153 (July 2013) *accessible at*: https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf (listing common fraud red flags: 1.

2. In re Erik T. Voorhees

A second SEC Investor Alert[133] detailing Bitcoin architecture was precipitated by the cease and desist order, In re Erik T. Voorhees.[134] Voorhees reportedly co-owned two websites for unregistered public offerings in Bitcoin by allegedly publishing prospectuses on the Internet, through Bitcoin-related websites, and on Facebook. Voorhees allegedly solicited investors to buy 13 million shares raising 50,600 Bitcoins in SatoshiDICE and raised 2,600 Bitcoins selling 30,000 shares in FeedZeBirds. Bitcoin were received for shares offered.[135] Voorhees settled SEC charges of violating security registration provisions of the 1933 Act[136] by disgorging almost $16,000 profits including the payment of a $35,000 civil penalty. Additionally, Voorhees is disqualified as a bad actor[137] from participating in virtual currency offerings for five years barring participation in Reg.D exempt offerings.[138]

3. In re BTC Trading, Corp. & Ethan Burnside

Burnside, an online gaming venue, allegedly operated unregistered BTC Virtual Stock Exchange and LTC-Global Virtual Stock Exchange from August 2012 to October 2013.[139] Burnside was a computer programmer traded securities using virtual currencies Bitcoin or Litecoin.[140] He significantly cooperated with the SEC's investigation, is barred from the securities industry and settled by

---

High returns with low risk, 2. overly consistent returns, 3. unregistered investments, 4. unlicensed sellers, 5. secretive, complex strategies, 6. no minimum investor qualifications, 7. disclosure deficiencies, 8. unreliable payments, 8. shared affinity).

[133] *Investor Alert: Bitcoin and Other Virtual Currency-Related Investments*, SEC Pub. No -- (May 7, 2014) *accessible at*: https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-Bitcoin-other-virtual-currency (explaining Bitcoin workings and limitations, reiterating *Shavers* ponzi scheme criteria).

[134] In re Voorhees, SEC Rel. No. 33-9592, SEC Admin.Proc.No.3-15,902, *accessible at*: https://www.sec.gov/litigation/admin/2014/33-9592.pdf.

[135] The value of Bicoins in the cases chronicled varies widely as evident using various Bitcoin historical trading records; one website, CoinDesk, is used here, *accessible at*: https://www.coindesk.com/price/ Commentary in this text, footnotes and discussion of enforcement records is generally valued at the time of sale of securities. In addition, at Bitcoin's high on December 17, 2017 was $19,340. As of this writing, the price had fallen to just over $3,800. Given this wild volatility, this narrative will hereinafter omit the historical high and current price in analyzing the enforcement case history. Nevertheless, Bitcoin price history reveals very significant stakes in the recorded wrongdoing.

[136] §§5(a) & 5(c), 15 U.S.C. §77e.

[137] 17 C.F.R. §230.507.

[138] 17 C.F.R. §§230.500-508.

[139] In re BTC Trading, Corp. and Ethan Burnside, SEC Rel.No.33-9685, SEC Rel.No.34-73783, SEC Rel.No.40-31,866, SEC Admin.Proc.3-16,307 (Dec.8, 2014) *accessible at*: https://www.sec.gov/litigation/admin/2014/33-9685.pdf.

[140] *Id.* 2,655 users opened online accounts with LTC-Global exchange, executing approximately 60,496 trades and paying a total of 12,081 in Litecoins. Approximately 7,959 users opened online accounts with the BTC exchange and executed approximately 366,490 trades through the website, paying a total of 2,141 Bitcoins.

disgorging his total profit of more than $68,000. He was barred from operating unregistered online environments as a stock exchange or from serving as a stock broker.[141]

4. In re Sand Hill Exchange

In the June 2015 cease and desist order, In re Sand Hill Exchange,[142] the SEC settled Dodd-Frank violations[143] with two entrepreneurs who allegedly offered and sold security-based swaps through defendants' Sand Hill website by seeking either dollars or Bitcoins to fund these accounts. Dodd-Frank requires transparency of swap positions to permit evaluation of systemic risk.[144] Investors/users were allegedly not queried about their financial holdings nor were the offerings limited to users with "accredited" minimum amounts of assets. The Sand Hill website read: "We accept everybody regardless of accreditation status." Sand Hill allegedly offered, bought, and sold contracts through the website in violation of the Dodd-Frank provisions that limit security-based swaps transactions with unaccredited investors who failed as eligible contract participants. Sand Hill operatives Hall and Ou allegedly exaggerated Sand Hill's trading, operations, controls, and financial backing. Sand Hill agreed to pay a $20,000 penalty without admitting or denying the findings, and agreed to cease and desist from committing or causing any future securities laws violations. Sand Hill precipitated yet another SEC Investor Alert on the avoidance of fantasy stock trading websites.[145]

5. SEC v. Homero Joshua Garza

In late 2015, two Bitcoin mining companies were charged in Connecticut federal court with operating Ponzi schemes.[146] The SEC provisionally defined

---

[141] The SEC alleged violation of §§5(a) & 5(c) of the Securities Act of 1933 and willfully violated §§5 and 15(a) of the Securities Exchange Act of 1934.

[142] In re Sand Hill Exchange et. al., SEC Rel.No.33-9809, SEC Rel.No.34-75,187, SEC Admin.Proc.3-16598 (June 17, 2015) *accessible at*: https://www.sec.gov/litigation/admin/2015/33-9809.pdf.

[143] Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, 15 U.S.C. §§77e(e), 15 U.S.C. § 78f(l).

[144] 17 C.F.R. §45 (swap data reporting). The 2018 Dodd-Frank reform enacted as the Economic Growth Regulatory Relief and Consumer Protection Act (Pub.L. 115-174, S. 2155) did not repeal the CFTC's swap reporting regulations involved in this case, *see generally* Perkins, David W., Darryl E. Getter, Marc Labonte, Gary Shorter, Eva Su & N. Eric Weiss, *Economic Growth, Regulatory Relief, and Consumer Protection Act (P.L. 115-174) and Selected Policy Issues*, R45073 Cong.Res.Serv. (June 6, 2018) *accessible at*: https//fas.org/sgp/crs/misc/R45073.pdf.

[145] *See*, *Investor Alert: Beware of Fantasy Stock Trading Websites Offering Real Returns*, (June 17, 2015) *accessible at*: https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-beware-fantasy-stock-trading (warning of online offerings and trading in swaps, derivatives, pay-to-play competitions, and Bitcoin prizes).

[146] SEC v. Homero Joshua Garza, Civ.Act. No. 3:15-cv-01760 (D. Conn., Complaint filed Dec. 1, 2015) *accessible at*: https://www.sec.gov/litigation/complaints/2015/comp23415.pdf.

Bitcoin mining as "applying computer power to try to solve complex equations that verify a group of transactions in that virtual currency. The first computer (or collection of computers) to solve such an equation is awarded new units of that virtual currency."[147] Garza allegedly defrauded investors because he lacked sufficient computing power to legitimately mine Bitcoin. In last 2014 Garza and his companies sold $20 million worth of purported shares in a digital mining contract they called a "Hashlet" to more than 10,000 investors. Hashlets were represented as physical products or pieces of mining hardware and GAW Miners allegedly promised to entitle each investor to control a share of computing power. GAW Miners and other defendants allegedly violated various securities laws and regulations.[148]

6. SecondMarket, Inc. & Bitcoin Investment Trust

The Commission filed a settled administrative proceeding against SecondMarket, Inc.,[149] a New York broker-dealer registered with the Commission, and Bitcoin Investment Trust (BIT), a Delaware trust whose sole assets are Bitcoins. The defendants allegedly violated Rules 101 and 102 of Regulation M[150] that prohibit issuers and participants in a public distribution from purchasing any security that is the subject of that distribution during the restricted period. BIT began offering its shares to accredited investors on a continuous basis under Reg.D Rule 506(c) but the offerings size and the special selling efforts and methods, the offering constituted a distribution. BIT announced a shareholder redemption program. Through BIT's affiliate and SecondMarket, BIT began redeeming shares purchasing 85,721 BIT shares from BIT shareholders in violation of 17 C.F.R §242.101. Without admitting or denying the findings, SecondMarket and BIT agreed to a cease-and-desist order against future violations and paid disgorgement with interest.

7. SEC v. Renwick Haddow

In SEC v. Renwick Haddow, et al.[151] the SEC charged the founder of a Bitcoin platform with operating as an unregistered broker-dealer cold calling investors to sell shares in Bitcoin Store Inc. and Bar Works Inc. Promotional materials allegedly touted non-existent executives and claimed that the companies were secure ways to hold and trade Bitcoin. Proceeds from these sales were diverted to offshore accounts. In addition, the enterprise allegedly sold space in

---

[147] *Id.* at 1.
[148] Sections 5(a) and 5(c) of the Securities Act of 1933; Section 10(b) of the Securities Exchange Act of 1934 (Exchange Act) and Rule 10b-5, violating Sections 17(a)(1) and (3) of the Securities Act.
[149] Admin.Proc.No. 3-17,355 (July 16, 2016) *accessible at*: https://www.sec.gov/litigation/admin/2016/34-78282-s.pdf.
[150] 17 C.F.R. §§242.100-242.105.
[151] SEC v. Renwick Haddow, et al., Civ.Act. No. 17-cv-4950 (S.D.N.Y., filed June 30, 2017). *Accessible at*: https://www.sec.gov/litigation/complaints/2017/comp-pr2017-123.pdf.

converted former bars and restaurants conceived as leases sold coupled with sub-leases that together functioned like investment notes, a security. An emergency asset freeze was ordered and the U.S. Attorney for the Southern District of N.Y. filed criminal charges arising from these facts.

8. The DAO

In subsequent enforcement actions, the SEC frequently refers to its first Investor Alert concerning ICO,[152] which was precipitated by this case, a § 21(a) Report of Investigation of The Dao.[153] The SEC investigation states that offers and sales of digital assets by virtual organizations are subject to federal securities laws. When conducted using distributed ledger or blockchain technology, these are often called "initial coin offerings" (ICO) involving "Token Sales." Whether ICO or tokens constitute securities depends on the facts and economic realities of the transaction. Unless exempt, issuers of distributed ledger or blockchain technology-based securities must register such securities. Securities exchanges trading tokens must register. Furthermore, despite The DAO allegedly describing itself as a "crowdfunding contract" it failed to satisfy the Regulation Crowdfunding exemption:[154] it was not a registered broker-dealer or a funding portal or Financial Industry Regulatory Authority (FINRA).

9. SEC v. REcoin Group Foundation

Fraud in ICOs purportedly backed by diamonds and real estate allegedly occurred in SEC v. REcoin Group Foundation.[155] Defendants allegedly sold unregistered securities and the tokens sold failed to exist. REcoin was touted as "The First Ever Cryptocurrency Backed by Real Estate" but misrepresented to investors that "a team of lawyers, professionals, brokers, and accountants" would invest the proceeds in real estate. Similarly, the Diamond Reserve Club misrepresented the diamonds as that company's assets. In addition to disgorgement and interest penalties for the misrepresentation violations, the SEC sought an

---

[152] Investor Bulletin: Initial Coin Offerings, (July 25, 2017) *accessible at*: https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings (provisionally defining blockchain, virtual currencies, tokens, virtual currency exchanges, issuers of virtual coins; warning of limited remedies in ICO fraud or theft; and opining that some ICO constitute the initial offering of securities). *See also*, Statement by the Divisions of Corporation Finance and Enforcement on the Report of Investigation on The DAO, SEC Divisions of Corporation Finance and Enforcement, *accessible at*: https://www.sec.gov/news/public-statement/corpfin-enforcement-statement-report-investigation-dao (arguing DAO tokens are securities).

[153] SEC Rel.No.34-81,207 (July 25, 2017).

[154] 17 C.F.R §§227.100-227.503; *see* Jumpstart Our Business Startups Act (JOBS) Pub. L. 112-106, 126 Stat. 306 (2012).

[155] SEC v. REcoin Group Foundation, DRC World and Maksim Zaslavskiy, (E.D. N.Y. Sept. 29, 2017) *Accessible at*: https://www.sec.gov/litigation/complaints/2017/comp-pr2017-185.pdf.

officer-and-director bar and a bar from participating in any offering of digital securities.

10. SEC v. PlexCorps

The SEC obtained an emergency asset freeze to halt a fast-moving ICO perpetrated by the alleged recidivist and Quebec securities law violator, Dominic Lacroix, and his company, PlexCorps.[156] PlexCorps marketed and sold securities called PlexCoin on the internet to investors in the U.S. and elsewhere, promising a yield of 1,354 percent profit in less than 29 days. This is the first case initiated by the SEC's new Cyber Unit.[157]

11. In re Munchee

The last enforcement action of 2017 settled a cease and desist voluntarily with a California-based company about to go live with an ICO of unregistered digital tokens.[158] Munchee was seeking $15 million capital to improve an existing iPhone app centered on restaurant meal reviews and create an "ecosystem" in which Munchee and others would buy and sell goods and services using the tokens.

12. SEC v. AriseBank

In SEC v. AriseBank[159] a successful asset freeze halted an allegedly fraudulent ICO based on false and misleading statements in connection with an unregistered offering of securities. The asset freeze succeeded on order to AriseBank to protect the digital assets before they could be dissipated, enabling the receiver to immediately secure AriseBank's various cryptocurrencies including Bitcoin, Litecoin, Bitshares, Dogecoin, and BitUSD. AriseBank allegedly sold unregistered investments in their purported "AriseCoin" cryptocurrency. AriseBank was allegedly held out as a first-of-its-kind decentralized bank offering a variety of consumer-facing banking products and services using more than 700 different virtual currencies. AriseBank claimed that it developed an algorithmic trading application that automatically trades in various cryptocurrencies. Individual defendants Jared Rice Sr. and Stanley Ford, consented, without

---

[156] SEC v. PlexCorps, Case No. 1:17-cv-07007-DLI-RML *accessible at*: https://www.sec.gov/litigation/complaints/2017/comp-pr2017-219.pdf.

[157] The unit was created in September 2017 to focus the Enforcement Division's cyber-related expertise on misconduct involving distributed ledger technology and initial coin offerings, the spread of false information through electronic and social media, hacking and threats to trading platforms, *see* Press Release- SEC Emergency Action Halts ICO Scam, *accessible at*: https://www.sec.gov/news/press-release/2017-219.

[158] In re Munchee, SEC Rel.No.33-10445, SEC Admin.Proc.No.3-18304 (Dec. 11, 2017) *Accessible at*: https://www.sec.gov/litigation/admin/2017/33-10445.pdf.

[159] SEC v. AriseBank (N.D.Tex.-Dallas Div. Jan. 30, 2018) (filed under seal) *accessible at*: https://www.sec.gov/litigation/complaints/2018/comp-pr2018-8.pdf.

admitting or denying the complaint's substantive allegations, to a final judgment of restraining order, bar from violating various securities laws and regulations,[160] disgorgement of $2,259,543.83, civil penalty of $184,767.00, and bar from practicing before the SEC. [161]

As a result of the AriseBank case, the SEC's Office of Investor Education and Advocacy again published a follow-on supplement to its Investor Alert series that is accumulating understanding of unique, developing cryptocurrency problems, this time about ICO[162] and related trading suspensions.[163]

13. SEC v. Jon E. Montroll & Bitfunder

The SEC charged Montroll and Bitfunder, an unregistered Bitcoin-demoninated securities exchange, in the Southern District of New York, of defrauding exchange users by misappropriating their Bitcoins and failing to disclose a cyber-attack on the exchange's system that resulted in the Bitcoin theft of over 6000 Bitcoins.[164] Defendants were charged with false and misleading statements in connection with an unregistered securities offering. The SEC argues that: Platforms that engage in the activity of a national securities exchange, regardless of whether that activity involves digital assets, tokens, or coins, must register with the SEC or operate pursuant to an exemption.[165] The SEC continues to refer to blockchain enabled cryptocurrencies as based on distributed ledger

---

[160] *Inter alia*, 15 U.S.C. § 78j(b)] and Rule 10b-5(b), 5 U.S.C. § 77q(a), 15 U.S.C. §§ 77e(a) and 77e(c), 15 U.S.C. § 78u(d)(2), and 15 U.S.C. § 77t(e).

[161] SEC v. AriseBank, No. 3:18-cv-00186-M (N.D.Tex.-Dallas Div. Dec.11, 2018) *accessible at*: https://www.sec.gov/litigation/complaints/2018/finaljudgment-pr2018-280.pdf.

[162] *See*, Investor Alert: Public Companies Making ICO-Related Claims, (August 28, 2017) *accessible at*: https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-public-companies-making-ico-related (warning of trading suspensions in , pump-and-dump schemes and social media transmitted rumors).

[163] *See e.g.*, ICO related trading suspensions in: In re Sunshine Capital, SEC Re. No. 34-80435 (April 11, 2017) *accessible at*: https://www.sec.gov/litigation/suspensions/2017/34-80435-o.pdf (suspending trading for insufficient information in Sunshine Capital (SCNP), its asset holdings were largely DIBCOINS); In re Strategic Global Investments, SEC Re. No. 34-81314 (August 3, 2017) *accessible at*: https://www.sec.gov/litigation/suspensions/2017/34-81314-o.pdf (suspending trading for misrepresentations involving Strategic Global Investments (STBV) for questionably ICO activities); In re CIAO Group, SEC Re. No. 34-81367 (August 9, 2017) *accessible at*: https://www.sec.gov/litigation/suspensions/2017/34-81367-o.pdf (suspending trading for alleged misrepresentations in its telecommunications business plans and forthcoming ICO); and In re First Bitcoin Capital, SEC Re. No. 34-81474 (Aug. 23, 2017) *accessible at*: https://www.sec.gov/litigation/suspensiins/2017/34-81474.pdf (temporarily suspending trading due to alleged inaccuracy and inadequacy of information on trading in securities of Canadian corporation, First Bitcoin Capital Corp. (BITCF)).

[164] SEC v. Jon E. Montroll & Bitfunder, Case No. 18-cv-01582 (S.D.N.Y. February 21, 2018) *accessible at*: https://www.sec.gov/litigation/complaints/2018/comp-pr2018-23.pdf.

[165] SEC Press Release: SEC Charges Former Bitcoin-Denominated Exchange and Operator With Fraud, *accessible* at*: https://www.sec.gov/news/press-release/2018-23*.

technology. The SEC published an accompanying specialized resource, titled, Spotlight on Initial Coin Offerings and Digital Assets.[166]

14. In re Centra Tech

An administrative proceeding and criminal case[167] were brought charging two co-founders of Centra Tech with misrepresentation and the conduct of an unregistered ICO,[168] and a third co-founder added later.[169] Centra Tech allegedly raised more than $32 million from thousands of investors in 2017. Centra Tech claimed the proceeds would fund the build out of a suite of financial products, such as Visa and MasterCard debit cards that would allow instant conversion of hard-to-spend cryptocurrencies into U.S. dollars or other legal tender. No relations allegedly exist with the credit card issuers. Defendants allegedly created fictional executives with impressive biographies, posted false or misleading marketing materials to Centra's website, and paid celebrities to tout the ICO on social media.

15. SEC v. Longfin

The SEC obtained another successful court ordered asset freeze and preliminary injunction concerning over $27 million in trading proceeds from allegedly illegal distributions and sales of unregistered restricted shares of Longfin Corp. stock.[170] After Longfin began NASDAQ trading and announced the acquisition of a purported cryptocurrency business, its stock price rose dramatically and its market capitalization exceeded $3 billion. Allegedly Longfin insiders then illegally sold large blocks of their restricted Longfin shares to the public while the stock price was highly elevated.

---

[166] *Accessible at*: https://www.investor.gov/additional-resources/specialized-resources/spotlight-initial-coin-offerings-digital-assets (further indexing online investor alert resources including SEC Chairman's Congressional Testimony and warnings about potentially unlawful online platforms for trading digital assets).

[167] In a parallel action, the U.S. Attorney's Office for the Southern District of New York today announced criminal charges against Sharma and Farkas U.S. v. Sharma & Farkas, No.18 MAG 2695 crim *accessible at*: https://www.justice.gov/usao-sdny/press-release/file/1048231/download (releasing sealed complaint charging all three Centra Tech co-founders with conspiracy to commit securities fraud, wire fraud,).

[168] SEC v. Sharma & Farkas (Centra Tech), 18-cv-02909 (E.D.N.Y April 2, 2018) *accessible at*: https://www.sec.gov/litigation/complaints/2018/comp-pr2018-53.pdf.

[169] SEC v. Sharma, Farkas & Trapani (Centra Tech), 18 Civ. 02909 (DLC) (E.D.N.Y April 20, 2018) *accessible at*: https://www.sec.gov/litigation/complaints/2018/comp-pr2018-70.pdf.

[170] SEC v. Longfin Corp., 18 CV 2977 (S.D.N.Y April 6, 2018) *accessible at*: https://www.sec.gov/litigation/complaints/2018/comp-pr2018-61.pdf order issued May 1, (complaint) *accessible at*: https://www.sec.gov/litigation/litreleases/2018/lr24130-order.pdf (order).

16. SEC v. Titanium Blockchain Infrastructure Services

A court ordered emergency ICO halt and preliminary injunction was ordered in SEC v. Titanium Blockchain Infrastructure Services.[171] SEC alleged that self-proclaimed "blockchain evangelist," Michael Alan Stollery, a/k/a Michael Stollaire, lied about business relationships with the Federal Reserve and dozens of well-known firms, including PayPal, Verizon, Boeing, and The Walt Disney Company. Titanium's website allegedly contained fabricated testimonials from corporate customers and that Stollaire publicly–and fraudulently–claimed to have relationships with numerous corporate clients and that Stollaire promoted the ICO through videos and social media and compared it to investing in "Intel or Google."

The Titanium case prompted the SEC's Office of Investor Education and Advocacy to design and build a mock ICO website. This appears intended to educate investors by illustrating the similarity of promotional "white papers" and the extravagant claims they make about high short term ICO returns.[172]

17. SEC v. Jesky and DeStefano

The SEC charged an attorney and law firm with illegal sales above the $3.70/share registration statement restriction of UBI Blockchain stock.[173] The SEC alleged that Jesky and DeStefano unlawfully sold their restricted shares at much higher market prices–ranging from $21.12 to $48.40–when UBI Blockchain's stock experienced an unusual price spike. Without admitting or denying the allegations in the SEC's complaint, Jesky and DeStefano agreed to disgorge approximately $1.4 million, pay $188,682 in penalties, and be subject to permanent

---

[171] SEC v. Titanium Blockchain Infrastructure Services, No. CV18-4315-DSF (C.D.Cal. (LA Div.) May 29, 2018) *accessible at*: https://www.sec.gov/litigation/complaints/2018/comp-pr2018-94.pdf; *see also*, Litig. Rel. No. 24160 (June 7, 2018) *sub.nom* Securities and Exchange Commission v. Titanium Blockchain Infrastructure Services, Inc., EHI Internetwork and Systems Management, Inc. aka EHI-INSM, Inc., & Michael Alan Stollery aka Michael Stollaire, Civ.Act. No. 2:18-CV-04315-DSF (JPRx) (C.D. Cal. filed May 22, 2018) *accessible at*: https://www.sec.gov/litigation/litreleases/2018/lr24160.htm.

[172] The SEC Has an Opportunity You Won't Want to Miss: Act Now! *accessible at*: https://www.sec.gov/news/press-release/2018-88 Additional information about ICOs is available on Investor.gov *accessible at*: https://www.investor.gov/additional-resources/specialized-resources/spotlight-initial-coin-offerings-digital-assets and SEC.gov/ICO *accessible at*: https://www.sec.gov/ICO Farcically, the SEC's ICO is denominated in HoweyCoins, *accessible at*: https://www.howeycoins.com/index.html and users duped into action by clicking "buy coins now" are transported to a finger-wagging red-flags lecture on the recurring characteristics of fake ICOs *accessible at*: https://www.investor.gov/howeycoins *See also Digital Asset Transactions: When Howey Met Gary (Plastic)*, Remarks at the Yahoo Finance All Markets Summit: Crypto William Hinman, Director, Division of Corporation Finance, *accessible at*: https://www.sec.gov/news/speech/speech-hinman-061418 (discussing challenges of applying *Howey* to ICO and Bitcoin).

[173] SEC v. Jesky and DeStefano, No. 18 CIv. 5980 (S.D.N.Y July 2, 2018) *accessible at*: https://www.sec.gov/litigation/complaints/2018/comp-pr2018-126.pdf.

injunctions. This case prompted yet another update to the SEC's information barrage to investors to avoid fraudulent and get-rich-quick ICOs.[174]

18. Blockvest

An emergency ICO trading ban and order freezing the defendants' assets was issued in Blockvest.[175] Blockvest, and its promoter Ringgold, a/k/a Rasool Abdul, allegedly made false claims in its ICO that it had regulatory approval as "licensed and regulated" by a fake agency Ringgold called the "Blockchain Exchange Commission." Defendants allegedly used a graphic similar to the SEC's seal. The National Futures Association (NFA) also issued a cease-and-desist letter to halt use of the NFA's seal.

19. Tomahawk Exploration

Permanent SEC practice bars were issued against David T. Laurance and Tomahawk Exploration who allegedly perpetrated a fraudulent ICO, to ostensibly fund Tomahawk Exploration's petroleum drilling.[176] In a failed ICO, Blockchain based digital tokens, called "Tomahawkcoins," which were to be sold based on promotional materials citing inflated projections of oil production and nonexistent drilling leases. Offering documents misleadingly described Laurance as having a "flawless background" without disclosing a criminal conviction for a prior fraudulent securities offerings.[177]

20. Airfox and Paragon

SEC administrative orders against Airfox[178] and Paragon[179] were the first issued solely for ICO civil penalties citing violations of failure to register an ICO. Airfox allegedly raised approximately $15 million in cryptocurrency for the development of a token-denominated "ecosystem" and mobile application in advertising tokens. Paragon allegedly raised approximately $12 million in

---

[174] *See* Spotlight on Initial Coin Offerings (ICOs) *accessible at*: https://www.sec.gov/ICO.

[175] SEC v. Blockvest, LLC and Reginald Buddy Ringgold, III a/k/a Rasool Abdul Rahim El, No. 18-CV-2287-GPC (BLM) (S.D. Cal. filed Oct. 3, 2018) *accessible at*: https://www.sec.gov/litigation/complaints/2018/comp24314.pdf SEC Litig.Rel. No. 24314 (Oct.11, 2018) *accessible at*: https://www.sec.gov/litigation/litreleases/2018/lr24314.htm.

[176] In the Matter of Tomahawk Exploration LLC & David Thompson Laurance, Admin.Proc.No. 3-18641 (Aug.14, 2018) *accessible at*: https://www.sec.gov/litigation/admin/2018/33-10530.pdf.

[177] This case precipitated yet another SEC investor advisory (warning) urging background checks of brokers, dealers, and promoters investment schemes, *see* Investor Alert: Check the Background of Anyone Selling You an Investment, *accessible at:* https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-check-background-anyone-selling-you.

[178] In the Matter of Carriereq, Inc., d/b/a Airfox, SEC Admin.Proc. No.3-18898 (Nov.16, 2018) *accessible at*: http://www.sec.gov/litigation/admin/2018/33-10575.pdf.

[179] In the Matter of Paragon Coin Co., SEC Admin.Proc. No 3-18897 (Nov.16, 2018) *accessible at*: http://www.sec.gov/litigation/admin/2018/33-10574.pdf.

cryptocurrency to fund its business plan to add blockchain technology to the cannabis industry and lobby for cannabis legalization.

21. Mayweather and Khaled

Allegations of compensated celebrity promotional endorsements touting ICO were settled in SEC administrative orders in November 2018. This case precipitated yet another SEC investor advisory on celebrity endorsements.[180] Maryweather had approximately 21 million Instagram followers, 7.8 million Twitter followers and 13.4 million Facebook followers. Well-known music producer DJ Khaled allegedly posed in a photo on his Instagram and Twitter accounts a picture of himself holding a Centra Card, captioned, "I just received my titanium centra debit card." In both cases, these celebrities allegedly failed to disclose their compensation for endorsement for posting promotions of Centra Tech's ICO. Both celebrities settled these cases, without admitting or denying the SEC's allegations, by paying disgorgement, penalties and interest. Both agreed not to promote securities.[181]

22. Coburn

Zachary Coburn, founder of the cryptocurrency trading platform EtherDelta, settled SEC charges in November, 2018, alleging that the platform constituted an unregistered national securities exchange.[182] The platform allegedly traded 3.6 million orders for ERC20, blockchain-based tokens frequently offered in ICOs. EtherDelta combined an order book, a website that displayed orders, and a "smart contracts" run on the Ethereum blockchain, the latter validated order messages, confirmed order terms and conditions, executed paired orders, and caused the distributed ledger to record such transactions on the blockchain. Without admitting or denying the findings, Coburn consented to disgorge $300,000 plus $13,000, prejudgment interest and pay a $75,000 civil penalty.

23. Gladius Network

An unregistered ICO was self-reported by Gladius Networks after allegedly raising approximately $12.7 million in digital assets to finance its plan to develop a network for renting spare computer bandwidth to as a computer

---

[180] *See also, SEC Statement Urging Caution Around Celebrity Backed ICOs,* SEC Div. of Enf.& SEC Ofc.of Compliance Inspect. & Exam. (Nov. 1, 2017) *accessible at*: https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos (warning about the weight too often given paid and biased celebrity endorsements in ICO and other investment schemes).

[181] SEC Press Rel.No.018-268 *accessible at*: https://www.sec.gov/news/press-release/2018-268

[182] In the Matter of Zachary Coburn, SEC Rel.No. 34-84553 (Nov.8, 2018) *accessible at*: https://www.sec.gov/litigation/admin/2018/34-84553.pdf.

security defensive strategy.[183] Likely due to its prompt cooperation, the SEC orders against Gladius required no penalties but required the return of funds to investors, registration of tokens and file periodic reports to the SEC.

VIII. "HOW" BLOCKCHAIN ENABLES PUBLIC POLICY SUBVESRION: COLLATERAL MEANS

This section discusses procedural and practical enforcement challenges in blockchain related activities. This discussion includes forensic challenges, cryptocurrency as the object of money laundering used in other criminal activities, compound crimes, secondary liability for some participants throughout the blockchain supply chain, mail and wire fraud and racketeering.

A. Forensic Resistance and Seizure Difficulties

Computer crimes are difficult to detect because the more artful "hackers" carefully cover their tracks to conceal any "audit trail." Vigilance in deploying effective security controls (e.g., encryption, restricting access to computer hardware, firewalls, passwords, ID codes) can assist in protecting victims from exposure. While much of the enforcement of computer crime is simply accomplished by extending existing laws, nevertheless, governments in many nations are now customizing criminal, contract and tort laws to accommodate the unique problems of unlawful acts hiding behind online anonymity and the forensic resistance of cryptocurrencies.[184]

B. Money Laundering

Money laundering is a diverse collection of acts that disguise the proceeds of criminal activities. Cryptocurrencies with robust security, strong encryption, and diffuse recordkeeping are ideal instruments to obfuscate almost any transfer of value. Money laundering is actually a large and secretive set of practices that

---

[183] In the Matter of Gladius Networks, Admin.Proc.No. 3-19004 (Feb.20, 1019) *accessible at*: https://www.sec.gov/litigation/admin/2019/33-10608.pdf.

[184] A complete discussion of computer forensics applicable to blockchain operations is well beyond the scope of this article. However, FinTechs such as blockchain-based cryptocurrency transactions, create big data accumulations from which analytics can be deployed to produce circumstantial evidence, that can be harvested to provide investigatory leads. In some cases, direct evidence is accessible from such big data, *see generally* Schwerha, Joseph J. IV, John W. Bagby & Brian W. Else, *United States of America*, Ch. 19 in ELECTRONIC EVIDENCE, Stephen Mason (ed.) LexisNexis UK (Butterworths, 2012).

create the illusion of transaction legitimacy by providing plausible explanations for illegal cash flows and cash reserves.[185]

In "following the money," law enforcement examines the finances of suspects, extends this inquiry to their accomplices and this may include deceived, but related parties. When transactions are suspicious, law enforcement probes further to find either a legitimate purpose or a money laundering purpose. Suspicion rises when transactions appear to have no genuine economic substance, are consummated at a scale larger than anticipated for the participants themselves (beyond their means) or are not equivalent in value to the goods, services or land transacted (they paid way too much). The additional value flow produced becomes suspect as possible illicit proceeds accompanying a seemingly legitimate transaction. Of course, paying too little is a reverse variant; it moves value back to the payment maker rather to the payment recipient.

Cryptocurrencies are likely deployed because they can be structured to avoid the ruse typical of traditional money laundering of "creating the appearance of legitimate transactions" because blockchain transactions are resistant to forensic discovery. Indeed, a wholly opaque, underground black market in money movements, unknown and unobserved by law enforcement, would be a money launderers delight. This is precisely why cryptocurrencies appear to be perfect means for money laundering. Furthermore, traditional money laundering typically requires the costly establishment of "fronts," businesses used to create the appearance of legitimacy to conceal money movements. The cost of front operations requires considerable overhead expense. Thus, fronts impose a "laundering fee" and this fee appears to free ride on the cryptocurrency's legitimate infrastructure overhead. The advantages of circumventing fronts are particularly heightened for moving large sums over great distances, such as in international transactions.

Money laundering literally cleanses, that is legitimizes, the appearance of "dirty" money derived from the proceeds of crimes or other illicit activities or intended to fund illegal activities (e.g., bribes, terror finance). Sources ascribe the term money laundering to the gangster era. The movement of fungible coins, with no serial numbers or other unique identifiers, was legal from slot machine gambling and from coin-operated laundries. Large volumes of coin movements provided plausible and practically untraceable excuses for handling the coins or for conversion into currency. Money laundering is likely a very old activity, perhaps 4000 years old. Money laundering was originally used to hide legitimate earnings from taxation or from unfair confiscation by oppressive governments.

1. Cryptocurrencies Enhance Laundering Methods

Cryptocurrencies vastly expand the tools of money launderers.[186] Many tools continue to be well-known but are forensically resistant to detection and

---

[185] *See generally*, Bagby, John W., ECOMMERCE LAW: ISSUES FOR BUSINESS at 118-120 (West 2003).
[186] Online gaming environments create their own centralized unique currencies, *see e.g.,* Bagby,

enforcement is costly. Basic laundering tools include (1) minimization of records, (2) laundering through one or more legitimate front businesses presumed to have cash flows, (3) use of unmarked cash, (4) minimal or no use of checks, recorded wire transfers or traceable credit card usage,[187] and (5) the conversion of criminal proceeds into gold, diamonds or other valuable hard assets that already have (intrinsic value), thereby eluding the forensic tracking of money.

Money laundering is seen as an indispensable component of many illegal schemes: terrorism, organized crime, gambling, human trafficking, the illegal drug trade, and smuggling. Anti-money laundering (AML) laws and regulatory requirements to provide assistance to AML investigations seek to: (1) identify criminals and accomplices, (2) reveal criminals' accessories and co-conspirators to gain incriminating evidence against criminal organizations, (3) seize money and freeze assets in accounts holding laundered money, and (4) deter crimes when the incentives are reduced as risk rises with the spending of laundered money.[188] Cryptocurrencies lower the costs and risks of laundering while raising the enforcement costs and decreasing the likelihood of detection.

Under one general model money laundering has three basic stages, and cryptocurrencies may vastly simplify the process while simultaneously complicating enforcement. The three steps are: (1) placement, (2) layering, and (3) integration.[189] Placement or promotion includes most efforts to initially make the funds less suspicious. This is when funds become somewhat more convenient because they enter the financial system after initial acquisition in an unlawful act. This first step hides the funds following their acquisition in an unlawful activity, an initial concealment. The second stage is layering, the second significant concealment process, characterized by movement. Layering separates the illegal proceeds from their source. In successful schemes, layering can be composed of multiple, complex financial transactions including wire transfers, monetary instruments, and asset purchases or sales. Layering obscures any links between placement and integration. For example, any alteration of the lump sum amount by combining with other funds or dividing it into several smaller amounts obfuscates an audit trail. Successful layering frequently involves multiple iterations of obfuscation. The third stage of integration reintroduces the funds into the economy for ultimate use, such as when they are spent or invested, essentially a reentry into the legitimate economy.

John W., *Imagining How to Exploit w00t from Virtual Environments to Inform Real World Public Policy*, Paper#: 174 TPRC 2008, 36th Research Conference on Communication, Information, and Internet Policy, Arlington VA, Sept. 2008.

[187] Pre-paid cash cards may be becoming popular as a money laundering device, *see e.g.*, Debter, Lauren, *The Idiot's Guide To Laundering $9 Million*, FORBES (Jan 11, 2017) *accessible at*: https://www.forbes.com/sites/laurengensler/2017/01/11/gift-cards-money-laundering.

[188] *See generally* Bagby, John W., *Protecting Critical Infrastructure through Effective Money Laundering Enforcement*, vol.8, no.8, pp.6-8, 22, CIP REPORT, George Mason Univ-Law School (Feb.2010).

[189] Report To Congress, In Accordance with §356(C) Of The USA Patriot Act, Secretary of the Treasury, Board of Governors of the Federal Reserve System, Securities and Exchange Commission, Dec. 31, 2002 at 7, *accessible* at http://www.fincen.gov/news_room/rp/files/356report.pdf.

Cryptocurrencies can abbreviate complex and iterative layering because the appearance of further legitimizing can be unnecessary. The overhead costs of complex traditional money laundering are mostly illuminated by using undetectable money transfers using obscure currencies that largely avoid detection. Indeed, scrip, virtual money, goods, or even services may constitute a sufficient flow of "value" to or from criminals back through the illegal organization sponsoring or assisting in the money laundering. Consider how diamonds, gold, or other precious and valuable assets might be used as laundering flows. Indeed, *counter-trade*, a multifaceted form of international barter, can be a particularly insidious money laundering method. Counter-trade moves goods as non-monetary value through complex, multi-party loops, which give the appearance of pursuing, usually humanitarian motives.[190]

C. Compound Crimes & Secondary Liabilities

Cryptocurrencies require large networks of willing participants to succeed.[191] Criminal law can address illegal activities of blockchain operators by identifying additional persons allegedly participating in illegal schemes. Corporate families implicate all members, particularly if the crime does not require specific intent. Indeed, large organizations committing complex acts with various participants obscure clear proof of criminal intent. However, secondary liability includes some legal doctrines that assign criminal liability for major and minor participants in group crimes. Parent corporations are occasionally held liable for the crimes of subsidiaries. When the law pierces the corporate veil to reach a parent that significantly controls the subsidiary's decision-making, the law lowers the limited liability shield exposing the parent to responsibility.

When crimes are committed by groups there are additional doctrines available to broaden the risk perimeter. An accessory is someone who aids the perpetrator of a crime but is not present at its commission. An accessory before the fact provides assistance before the commission of the illegal acts and an accessory after the fact provides assistance after the commission. A conspiracy is an agreement among two or more persons who plan the commission of a crime. A criminal attempt includes all the activities of the perpetrator(s) to plan and carry out a criminal act, such that if successful, would result in the criminal act. All these are separate crimes for which additional convictions and penalties can be assessed if adequately proven. Use of blockchain enabled cryptocurrencies are vulnerable to allegations of violating one or more of these secondary liabilities when successful forensics identifies the participants.

---

[190] *See, e.g.*, Klayman, Elliot I., John W. Bagby, & Nan Ellis, Ch, 34 *International Sales Transactions* in IRWIN'S BUSINESS LAW - CONCEPTS, ANALYSIS, PERSPECTIVE, p.680-85 (1994, Richard D. Irwin Pub. Burr Ridge IL).

[191] Of course, smaller networks may be effective too, such as when some participants are not willing, instead duped into donating their computers as unintentional recruits in zombie networks.

D. Mail & Wire Fraud

Cryptocurrency use, whether directly connected to predicate wrongs or used in furtherance of predicate/substantive wrongs, likely can violate the federal mail and wire fraud statutes.[192] It is a federal criminal offense in the U.S. to communicate misrepresentations in the mail or over a wire and thereby perpetrate a fraud.[193] The conduct of an intentional scheme or artifice to defraud in order to obtain money, property or deprive another of honest services is prohibited.[194] Even incidental use of mail or wire communications implicates liability under these statutes. Furthermore, elaborate fraudulent schemes likely constitute numerous predicate offenses comprising a pattern that is illegal as racketeering. Mail and wire fraud are classic "pile on" crimes accompanying other underlying predicate offenses because communication is essential in most attempts and conspiracies or to direct the activities of accessories.

In one blackmail scheme, the perpetrator allegedly demanded (ostensibly untraceable) payment of the hush money in Bitcoin.[195] Blackmailers delivered the demand letter via U.S. Postal Service largely to married men claiming possession of evidence of their unfaithful cheating on their spouses. Hundreds of similar victims surfaced when one recipient posted his letter to his own obscure blog revealing a large scope to the extensive scheme. Blackmailers initial solicitation demanded $2,000 in Bitcoin but later waves quadrupled the demand to $8,000. The case provides a how-to guide for the acquisition of Bitcoin wallets informing victims unfamiliar with cryptocurrency operations.

Bitcoin scams proliferate on social media (SM).[196] Mail and wire fraud is implicated in a bevy of SM frauds involving Bitcoin, including, *inter alia*, malware downloads where Bitcoin is bait, Bitcoin impersonators phishing to free ride on Bitcoin's reputation, Bitcoin flipping seeking Bitcoin denominated startup fees for non-existent investments, and Bitcoin pyramid schemes.[197] Cloud mining scams offer to share Bitcoin mining earnings with duped investors.[198] Additional cases potentially unlawful under the mail and wire fraud statutes are discussed supra as securities or commodities fraud.

---

[192] 18 U.S.C. §§1341, 1343.

[193] Including, *inter alia*, telephone, telegraph, radio, television, Internet, electronic data interchange, computer modem, satellite, e-Mail, Internet, cell phone, pager, social media.

[194] 18 U.S.C. §1336.

[195] *See e.g.*, Schlesinger, Jennifer & Andrea Day, "*I Know You Cheated On Your Wife." Growing Blackmail Scam Demands Payment In Bitcoin*, CNBC (Jan.22, 2018) *accessible at*: https://www.cnbc.com/2018/01/22/growing-blackmail-scam-demands-payment-in-Bitcoin.html.

[196] *Bitcoin Scams on Social Media: The Dark Side of Digital Currency*, ZEROFOX RESEARCH *accessible at*: https://www.zerofox.com/blog/Bitcoin-scams-social-media/.

[197] Wasik, John, *How To Spot A Bitcoin Scam*, FORBES (Apr 26, 2017) *accessible at*: https://www.forbes.com/sites/johnwasik/2017/04/26/how-to-spot-a-Bitcoin-scam.

[198] Complaint, SEC v. Garza, Gaw Miners, Zenminers, No. 3:15-cv-01760 (Dec.1, 2015) *accessible at*: https://assets.documentcloud.org/documents/2630336/comp23415.pdf and Farivar, Cyrus, *GAW Miners founder owes nearly $10 million to SEC over Bitcoin fraud* ARSTECHNICA (Oct.5, 2017) *accessible at*: https://arstechnica.com/tech-policy/2017/10/Bitcoin-fraudster-hit-with-9-1m-civil-judgment-on-top-of-criminal-guilty-plea/.

E. Racketeering

Regulation of unlawful blockchain activities and cryptocurrency use is well enabled when expressed as racketeering, permitting Justice Department (DoJ) referral of investigations to regulatory agencies, DoJ criminal prosecutions and civil private rights of action. Racketeering is prohibited under 31 states' laws[199] and the federal statute, the U.S. the Racketeering Influenced and Corrupt Organizations Act of 1970[200] (RICO) as well as statutes in some other nations Racketeering is a compound, pattern-based crime. That is, RICO is violated when underlying, predicate offenses are repeated. RICO is criticized as it has been used to target many activities not traditionally part of organized crime, e.g., malpractice cast as accounting fraud.

RICO under the U.S. federal scheme requires proof that: (1) the defendant committed at least two prohibited acts (2) the acts constitute a pattern (3) of racketeering activity (4) by which the defendant (5) invested in, maintained an interest in, or participated in (6) an enterprise (7) that affects interstate or foreign commerce. Unlawful applications of blockchain activities, like many unlawful Internet activities, are prime subjects for racketeering claims. Computers and networks enable large numbers of similar illegal activities that form patterns. The statute is violated when at least some of the acts perpetrated are listed as predicate acts under RICO.[201] RICO makes it unlawful to invest proceeds derived from racketeering activities, a practice used by organized crime to strengthen its organization while also laundering its illegal profits. RICO provides for treble damages in civil cases, attorney's fees to civil plaintiffs, asset seizure and forfeiture in criminal cases, regulatory enforcement and criminal penalties of potentially long prison terms and large criminal fines.

IX. CONCLUDING OBSERVATIONS-AN EVOLVING EPOLOG

This article recognizes that blockchain schemes are clearly susceptible to regulation. However, we demonstrate that various agencies' regulatory enforcement and private plaintiffs rights vindication continue at considerable disadvantage in confronting the wrongs of blockchain activities. Attempts to

---

[199] State Racketeering Laws, FIndlaw *accessible at*: https://statelaws.findlaw.com/criminal-laws/racketeering.html; Floyd, John E. (ed.), *RICO State by State: A Guide to Litigation Under the State Racketeering Statutes*, (2nd ed.) Am. Bar Assn.-Section of Antitrust Law; and *National State Law Survey: Racketeering*, *accessible at*: http://sharedhope.org/wp-content/uploads/2016/03/NSL_Survey_Racketeering.pdf.

[200] Pub.L. 91-452, Stat. 922-3, *codified as* 18 U.S.C. §§1961–1968.

[201] Under 18 U.S.C §1961*accessible at*: https://www.law.cornell.edu/uscode/text/18/1961 predicate acts include these and other offenses too numerous to list here: bribery, counterfeiting, theft, embezzlement, fraud, obscenity, obstruction of justice, slavery, racketeering, gambling, money laundering, murder-for-hire, murder, kidnapping, extortion, arson, robbery, bribery, controlled substance under Controlled Substances Act, bankruptcy or securities fraud, drug trafficking and certain acts of terrorism.

remain current in combating fraud and overreach in almost any of the developing blockchain schemes is demanding and daunting. Indeed, incremental and transformative blockchain innovations nearly always outpace public understanding, policy development or balanced implementation of regulatory control. This "regulatory lag" problem is exacerbated by the pace of deployment of FinTech innovations.[202] Mostly harmful externalities take hold well before effective counter-measures become feasible.

Four observations as to the future of blockchain innovations are evident. First, blockchains are inherently stealthy, making them somewhat impervious to detection. As a single blockchain record system proliferates, the communications, stored records and implemented transactions (e.g., payments, contracts, actions) will accumulate to become "big data" susceptible to forensic analytics. This opens opportunities for enhancing public security but at the expense of individual privacy. Regulation of public blockchains such as Bitcoin or Ethereum is feasible and potentially valid under privacy law and the Fourth Amendment.

Second, blockchain schemes are based on unstable and evolving technologies. The blockchain "are" FinTechs based on changing designs that challenge regulatory principles. These are, all too often, based on particular existing or past designs that have or will evolve. Any resulting regulations addressing a past "instantiation" of blockchain design may lack generalizability as to future blockchain embodiments. Indeed, to maintain relevance and success, any blockchain instance must rapidly evolve as security flaws are identified and resolved to address new security vulnerabilities. This is a perpetual cat and mouse game of fixing security flaws.[203] Furthermore, blockchain purveyors devise workarounds to maintain their stealth as forensic vulnerabilities are identified. For example, new eco-sub-systems are now emerging driven by the availability of APIs to imbed blockchain functionality into other applications.

Third, blockchain applications in cryptocurrencies, Bitcoin in particular, are not as scalable as widely touted. Indeed, Bitcoin's capacity constraints may be a major factor in the proliferation of other competing cryptocurrencies. Traditional monetary policies that promote economic stability presume fewer, more voluminous and stable currencies. By contrast, cryptocurrency proliferation undermines this key factor in traditional visions of successful forms of money.

Finally, the current form of design upon which many cryptocurrencies are based use blockchain technologies. These proof-of-work cryptocurrencies generally require the mining of new blocks to expand that cryptocurrency's money supply or simply to sign (authenticate) transactions. Each cryptocurrency is mathematically limited to a maximum number of coins none of which could amount to sufficient supply for a major nation's economy. Mining is a large-scale

---

[202] *See e.g.*, Lawrence J. Trautman, *Bitcoin, Virtual Currencies and the Struggle of Law and Regulation to Keep Pace*, 102 MARQ. L. REV. 447 (2018).

[203] Orcutt, Mike, *Once hailed as unhackable, blockchains are now getting hacked*, MIT TECH.REV. - (Feb.2019) *accessible at*: https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.

computer process that requires increasing computer energy consumption.[204] This process is arguably unsustainable because it externalizes crypto-miners' social cost to other customers in those franchise areas of the electrical grid where mining occurs.

Blockchain technology may endure in the near to medium term, although the hype is palpable.[205] Regulation of blockchain externalities are destined to experience regulatory lag. Nevertheless, it remains possible that this lag can be reduced as regulators and policymakers expend resources and creative intelligence to better understand, address and resolve blockchain characteristics. Blockchain shows some promise to revolutionize transaction processing in several fields so regulators should attempt to avoid classic overreach by throwing out the baby with the bathwater.[206]

---

[204] *Bitcoin Energy Consumption Index*, DIGICONOMIST (2019) *accessible at*: https://digiconomist.net/Bitcoin-energy-consumption.

[205] Carson, Brant, Giulio Romanelli, Patricia Walsh, & Askhat Zhumaev, *Blockchain beyond the hype: What is the strategic business value?* (June 2018) *accessible at*: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.

[206] *See generally*, *Virtual Currency*, Written Testimony of Chairman J. Christopher Giancarlo before the Senate Banking Committee, Wash., D.C. (Feb. 6, 2018) *accessible at*: https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo37.