Do Blockchain Technologies Make Us Safer? Do Cryptocurrencies Necessarily Make Us Less Safe?

Sarah Jane Hughes

Follow this and additional works at: https://www.repository.law.indiana.edu/facpub

Part of the Banking and Finance Law Commons, and the Internet Law Commons
Do Blockchain Technologies Make Us Safer? Do Cryptocurrencies Necessarily Make Us Less Safe?

SARAH JANE HUGHES*

Abstract

This essay is based on a presentation made on January 24, 2020 at the invitation of the Texas Journal of International Law and the Strauss Center for National Security at the University of Texas. That presentation focused on the two questions mentioned in the title of this essay – Do Blockchain Technologies Make Us Safer? And Do Cryptocurrencies Necessarily Make Us Less Safe? The essay presents answers to the two questions: “yes” and “probably yes.” This essay begins with some level-setting on different types of blockchain technologies and of cryptocurrencies, and gives some background materials on global and national responses to certain cryptocurrencies, such as El Petro sponsored by Venezuela’s PDVSA and Facebook’s Libra.

* Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law at the Maurer School of Law, Indiana University, Bloomington, Indiana. She served as the Reporter for the Uniform Law Commission’s Uniform Regulation of Virtual-Currency Businesses Act (2017) and the Uniform Supplemental Commercial Law for the Uniform Regulation of Virtual-Currency Businesses Act (2018).

Support for this paper came from the Maurer School of Law and from the Program on Financial Regulation & Technology, Law & Economics Center, George Mason University’s Antonin Scalia School of Law. Research for this essay was completed on January 21, 2020.

Professor Hughes thanks the editors of the Texas International Law Journal and the Strauss Center for International Law and Security at the University of Texas for the invitation to participate in their January 2020 conference. Commenters included Professors Thomas Vartanian and Robert Ledig of the Antonin Scalia School of Law, Julie Hill of the University of Alabama Law School, Lawrence J. Trautman of Western Carolina University-College of Business; Elizabeth Rosenberg, Center for New American Security; Peter A. Wayner, technology author and programmer; Brian Brooks, formerly of Coinbase, Inc.; and Richard Levin of Polsinelli, LLP. Despite their helpful comments, she claims all errors in this essay are my own.
INTRODUCTION

Escalations in the tensions around the world and recent cyberwarfare incidents against agencies, businesses, and infrastructure in the United States bring new attention to the adoption of blockchain technologies and cryptocurrencies. Additionally, plans announced by Facebook, the Russian Federation, and China to issue new cryptocurrencies add new urgency to discussion of issues related to the increasingly wider adoptions of cryptocurrencies, including government-issued digital currencies (“central bank digital currencies” or “CBDCs”). Questions about “El Petro”, the cryptocurrency sponsored by the Maduro government in Venezuela and backed by the reserves of the state-owned oil company, raise additional issues. National and regional governments, such as the United States and the European Union, and inter-governmental organizations, such as the Financial Action Task
DO BLOCKCHAIN TECHNOLOGIES MAKE US SAFER?

Force (FATF), have aimed initiatives at the uses of cryptocurrencies to limit their use for laundering monies or financing terrorism.

This essay will offer thoughts on topics intersecting national security and these two emerging technologies – blockchain and cryptocurrencies. Foremost among these topics are:

(1) Are blockchain technologies able to make us safer? and,

(2) Do some or all cryptocurrencies necessarily make us less safe?

Generally speaking, the answer to both questions is “yes.” However, the reasons for each differ significantly. The first question is far easier to answer than the second.

This essay will address both the two basic questions and the two pairs of subsidiary questions. This essay also attempts to tie issues surrounding blockchain and cryptocurrencies to international law and national security by discussing two laws that pose challenges to international law and to national security law. To address these questions, this essay first engages in some level-setting for blockchain and cryptocurrencies. The conclusion will set out subjects for additional research and offer final thoughts on the introductory questions.

I. BACKGROUND INFORMATION ON BLOCKCHAIN TECHNOLOGY AND CRYPTOCURRENCY

The terms “blockchain” and “cryptocurrency” have been around long enough that some of us think we know something about each term. For the purposes of this essay, I want to make clear how I am using these terms, and I invite readers’ comments in response. Readers familiar with this subject matter may wish to move on the sections dealing with the two broad questions posed above.

A. Blockchain

In this article, I use the term “blockchain” to refer to permissionless, decentralized public distributed ledgers—engaging all four of these concepts as prerequisites to the observations I want to make. First, the term “permissionless” describes blockchains like the blockchain that is the authoritative ledger for Bitcoin.

In simplified terms, a blockchain is a method of storing records of ownership or of assets and transactions which uses a version of a distributed ledger. A distributed ledger keeps records “in many different locations simultaneously.” Distributed ledgers theoretically are auditable, verifiable, and transparent.

No one needs “permission” to have an interest or transfer of interest recorded on the Bitcoin blockchain. A user needs instead to create bitcoins through a problem-solving process known as “mining,” which results in the new bitcoin being reflected on the block. Others who earn bitcoins by performing transfer verification services for the Bitcoin blockchain or who purchase or acquire bitcoins from others do not require anyone’s advance permission to participate. None of us would need permission from anyone except a miner or

2. Id.
3. Id.
a counterparty in another transaction to acquire a bitcoin; none of us would need permission to mine a bitcoin—we’d just need the mental, computational, and, in the case of proof-of-work generation, an energy supply fit for the job. Alternatively, one could acquire the funds to buy a bitcoin from a previously recognized owner.

Second, the Bitcoin blockchain is decentralized, which means that no one person, government (yet), or other legal entity is in charge.5 Rather, as noted above, a group of miners acting as the verification and registry team are in charge.

Third, the term “public” is distinct from “private” or fully anonymous in this context because of the chain of transfers that are viewable in a “public” blockchain.6 Bitcoin is a public system: it operates through addresses and nodes. In the basic Bitcoin regime, individual transfers can be associated with prior transactions by tracking backwards through the pseudo-anonymous addresses that the chain reveals.7 The blocks are open-to-view even if no “names” in the traditional sense are associated with the property registered on the block.

The chain of blocks that track the sequence of transactions for cryptocurrencies provide a unique opportunity for public analysis of transaction patterns and deterrence of double-spending.8 Although the nominal identity of each person is not recorded as a human name or by a common identification value like a Social Security number, the public key used to sign the transaction can provide much of the same value.9 All of the transactions associated with the key of a particular person are easy to find on the blockchain in the publicly accessible information.10 Even if the transactions are routed through different exchanges or intermediaries, all of the cryptocoins that flow through the wallet can be flagged.11

The ability to review and essentially trace transfers back to the time of the creation of a bitcoin facilitates identification not just of transfers, but of the actors involved.12 To demonstrate how open-to-view Bitcoin transactions are, in 2018 the Treasury’s Office of Foreign Assets Control (OFAC) placed two Iranian intermediaries and their identified blockchain addresses on OFAC’s “Specially Designated Nationals” list.13 The selected actors had been identified by name as being associated with laundering proceeds from the Sam-Sam ransomware attacks.14

“Distributed ledger” refers, in the first instance, to the manner that proposed entries/transactions are verified before being entered on the Bitcoin blockchain.15 The
authority to verify and authorize entries is distributed among the group of nodes designated for this purpose. These ledgers are decentralized by design. Their decentralization is considered to provide the trust proxy that legacy providers of record systems have long provided.\textsuperscript{16} Carla Reyes explains that distributed ledger technologies

\begin{quote}
[use] the [distributed ledger technology or DLT] to refer generally to “computer software that is distributed, runs on peer-to-peer networks, and offers a transparent, verifiable, tamper-resistant transaction-management system maintained through a consensus mechanism rather than by a trusted third-party intermediary that guarantees execution.”\textsuperscript{17}
\end{quote}

Finally, a \textit{“ledger”} is just a system of records—a source of information or a place to store records.\textsuperscript{18} People have used ledgers since Biblical times.\textsuperscript{19} The bitcoin blockchain as with other distributed ledgers is the location of records that hold a series of increasingly long entries that show the chain of transactions involving a single unit (a bitcoin) and a storage system that is designed to be irreversible.\textsuperscript{20} The first entry in the ever-longer “addresses” on the blockchain stays with the later transactions.\textsuperscript{21} The second entry does as well.\textsuperscript{22} This allows observers to see how the bitcoin has moved through later transactions to the present day. The retention of earlier transactions identifiers is comparable to the requirements of the “Travel Rule” that the U.S. Department of the Treasury imposed on wire transfers in the 1990’s.\textsuperscript{23}

Blockchains perform storage and vault-like protections for many commercial applications. They can replace legacy paper or digital records systems created and maintained by Federal or State agencies relating to who owns which parcels of land, who owns which motor vehicles or watercraft, who is the record owner of intellectual property, or who is the holder of bank or credit-card accounts.\textsuperscript{24} Such systems could be public and distributed as the Bitcoin blockchain is, or could be operated by a centralized manager and lose its distributed character.

\begin{itemize}
\item[17.] Carla L. Reyes, \textit{If Rockefeller Were a Coder}, 87 GEO. WASH. L. REV. 373, 379-380 (2019); see also Carla L. Reyes, \textit{Conceptualizing Crypto Law}, 96 NEB. L. REV. 384, 390-91 (2017) (“Distributed ledger technology (DLT) refers to computer software that is distributed, runs of peer-to-peer networks, and offers a transparent, verifiable, tamper-resistant transaction-management system maintained through a consensus mechanism”).
\item[19.] JP Fabri, \textit{LEDGER-NOMICS}, BITEMYCOIN, https://bitemycoin.com/opinion/ledger-nomics/ (last visited Mar. 8, 2020) (“The first recorded ledgers were found in the city of Mesopotamia, today’s Iraq, around 7000 years ago.”).
\item[20.] See Bitcoin White Paper, \textit{ supra} note 5, at 1 (explaining a new electronic payment system to work based on “cryptographic proof . . . without the need for a trusted third party”)
\item[21.] See generally \textit{Id.} at 3.
\item[22.] \textit{Id.}
\end{itemize}
Ledgers like that undergirding Bitcoin also can help us follow supply chains and guard against counterfeit or “grey market” goods entering the marketplace in place of authorized, compliant, and wholesome goods.\(^\text{25}\)

Blockchain-recorded transactions have the added advantage of being non-reversible.\(^\text{26}\) Blockchain transactions are one-way streets: no one can place a “stop-payment order” against a payment they initiated via a system using the bitcoin blockchain.\(^\text{27}\) The only way to get a refund or reversal of a transfer is to get the transferee to send a new message to the blockchain in favor of the transferor with the same value.\(^\text{28}\) The blockchain then shows both sides of the transaction—the in-bound and out-bound transactions.\(^\text{29}\)

\[\text{B. Cryptocurrency}\]

The term “cryptocurrency” currently describes a class of digital assets that is not designated as legal tender by any national government.\(^\text{30}\) One reason for this framing is that when a national government designates a currency as legal tender and the currency comes into another government’s jurisdiction or is designated by counter parties to a transaction as the pertinent currency for satisfying obligations under contracts, the US government refers to that currency transaction as “foreign exchange.”\(^\text{31}\) The US government applies different standards to “foreign exchange” for purposes of taxation and regulation of intermediaries handling it.\(^\text{32}\) Currency that is regulated as “foreign exchange” is not “legal tender” under the Coinage Act of 1965.\(^\text{33}\)

Its early proponents viewed cryptocurrencies as market-based alternatives to the hegemony of financial services providers.\(^\text{34}\) Other proponents see it as a faster and less costly means of transferring ownership of assets that may either be digital or may be real-world assets.\(^\text{35}\) Yet others see cryptocurrencies as displacing the need for banks or other legacy


\[\text{26. Bitcoin White Paper, supra note 5, at 1.}\]

\[\text{27. See generally U.C.C. § 4-403 (AM. LAW INST. & UNIF. LAW COMM’N 2019).}\]

\[\text{28. Bitcoin White Paper, supra note 5, at 2.}\]

\[\text{29. Id.}\]

\[\text{30. Contra 31 U.S.C. § 5103 (1983) (“United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes and dues[,]”) I do not include cryptocurrencies such as El Petro offered by Venezuela’s state-controlled oil and natural gas company, Petróleos de Venezuela, S.A., because it appears to be more in the nature of a security than of a currency.}\]


\[\text{32. See 31 C.F.R. § 1010.100(ff)(1) (2019) (defining a “dealer in foreign exchange” as “a person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more other countries in an amount greater than $1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery.”); see also I.R.C. §988 (2018) (defining “foreign currency” for purpose of taxing income from sources without the United States).}\]


\[\text{34. Bitcoin White Paper, supra note 5, at 1.}\]

providers of asset-storage or asset-transfer systems, including systems supporting remittances and other cross-border transfers. Some early inventors viewed cryptocurrencies as a means of reducing or eliminating the risk of “double spending” in digital environments. The range of potential uses includes faster and less costly cross-border payments and trade transactions, as well remittance payments.

International organizations and various governments have developed definitions of cryptocurrencies or “virtual currencies” to explain how they fit into their regulatory regimes. One of the earliest definitions is the G-20’s Financial Action Task Force’s (FATF) 2014 definition:

Virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued or guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (i.e., “real currency,” “real money,” or “national currency”), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency — i.e., it electronically transfers value that has legal tender status.

In the United States, the Financial Crimes Enforcement Network (“FinCEN”) had issued its first guidance on cryptocurrencies in March 2013:

“Virtual currency” is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. . . . “Convertible” virtual currency . . . either has an equivalent value in real currency, or acts as a substitute for real currency.

See Emilio R. Coello, Are Cryptocurrencies Useful for Remittances?, COIN CTR. (Jan. 6, 2020), https://coincenter.org/entry/are-cryptocurrencies-useful-for-remittances (explaining significantly lower costs to senders recipients and shorter delivery times of as little as 90 seconds compared with three to five days).


FinCEN’s March 2013 Guidance focused on persons that engage as a business in transactions involving exchange of cryptocurrency for real currency, funds, or other crypto currencies, or that issue and have authority to redeem or withdraw from circulation cryptocurrencies.\(^{41}\) This focus was appropriate because FinCEN was explicating how “virtual currencies” fit into its 2011 Guidance on responsibilities of “money transmitter[s]” and “provider[s] of prepaid access” under Treasury Department rulings.\(^{42}\) FinCEN updated the March 2013 Guidance and its intervening opinions on specific topics in May 2019 without changing the fundamentals of its 2013 Guidance.\(^{43}\)

For the moment, cryptocurrencies can be separated into the eight groupings discussed below. These categories each contain unique features that pose national security risks. Some present very low risks, and others present higher risks, as I explain in Part IV of this article.

1. Permissionless, decentralized and market-based.

Since its introduction in 2009, Bitcoin has spurred the rise of cryptocurrencies. Bitcoin operates on a decentralized basis with verification and blockchain maintenance entrusted to a peer-to-peer network nodes.\(^{44}\) Bitcoin, as previously mentioned, is also permissionless and pseudo-anonymous.\(^{45}\)

On the downside, however, bitcoins are backed only by the blockchain and a market’s willingness to trust it.\(^{46}\) No hard assets or digital assets (other than the blockchain itself) stand behind bitcoins.\(^{47}\)

In a public, permissionless blockchain, such as Bitcoin or Ethereum, all participants are theoretically equal.\(^{48}\) There is no central management or authority that can be compelled to report users’ data or keep records prescribed by a government other than those inherent to their business model, or even a central authority to respond to legal process.\(^{49}\) The exception to this “equality” principle is that some participants play key roles in validating transactions on the blockchain, including “miners” of bitcoins who perform verification and validation functions but are not known to all participants.\(^{50}\) However, their verification-and-validation roles do not necessarily make them persons susceptible to regulatory requirements or to subpoenas or other forms of legal process by governments or counterparties.

Transactions on public blockchains are all open-to-view and relatable to each other in a chain because the “public key” is in fact public. The “private key” that is required to engage

\(^{41}\) Id. at 1–2.
\(^{44}\) Bitcoin White Paper, supra note 5, at 3, 8.
\(^{45}\) Id. at 6.
\(^{46}\) Id. at 1.
\(^{49}\) FinCEN Regulation Application, supra note 43, at 18.
\(^{50}\) Adam Chodorow, Bitcoin and the Definition of Foreign Currency, 19 FLA. TAX REV. 367, 373–74.
in transfers of these cryptocurrencies is private—not visible on the blockchain.\(^{51}\) Transactions are time-stamped and sequential.\(^{52}\) One can follow a chain of transfers from the first entry to the latest entry in time, and can ascribe to the last entry the status of being the “owner” or at least the custodian of the related crypto assets for the owner.\(^{53}\) It also is possible to follow transfers from the original public key address to others in the chain by comparing the relative lengths of the chains with similar initial addresses to the current “owner” or custodian.\(^{54}\)

2. Permissioned, centralized and linked to fiat currencies.

Another form of cryptocurrencies is known as “stablecoins,”\(^ {55}\) To reduce volatility in pricing, stablecoins should be backed by assets having values equal to the number of coins in circulation.\(^ {56}\) These cryptocurrencies are centralized because some entity issues the units of currency against its reserves of the fiat currency or currencies to which the stablecoins are linked.\(^ {57}\) Tether is an example of a stablecoin, despite the allegations over the past 18 months that the existing reserves do not support the number of Tether stablecoins in circulation.\(^ {58}\)

A centralized manager has information about the intermediaries or owners of the coins because stablecoin holders theoretically have redemption rights to the underlying reserve fiat currency or other asset.\(^ {59}\) One might also describe stablecoins as having values dependent on whatever “reserves” support the “stable” claim of stablecoin issuers. Facebook’s Libra appears to be in the stablecoin category, but it has other attributes that I describe in subparagraph 6 of this Part, below.

3. Public, Centrally Validated Blockchains

EOS\(^ {60}\) and Ripple\(^ {61}\) are examples of public, permissioned blockchains. Some participants in this category of blockchains/cryptocurrencies are more equal than others.\(^ {62}\)

\(^{51}\) J. ANTHONY MALONE, BITCOIN AND OTHER VIRTUAL CURRENCIES FOR THE 21ST CENTURY lxxiv (2014).


\(^{53}\) WAYNER, supra note 6, 16–17.

\(^{54}\) Id.


\(^{56}\) Id. (“[I]f there are 500,000 USD-pegged coins in circulation, there should be at least $500,000 sitting in a bank.”).

\(^{57}\) Id.


\(^{59}\) See 31 C.F.R. § 1022.420 (2019) (stating the recordkeeping requirements for providers of prepaid access to enable reconstruction of activation and later prepaid-related transactions).

\(^{60}\) EOS.IO, https://eos.io/about-us (last visited Mar. 29, 2020) (EOS Worldwide, LLC and its Block.One operate blockchain protocols that can be private or public in their operations as businesses building on those systems select).


\(^{62}\) See Angela Walch, Univ. Coll. London Cr. for Blockchain Techs., Intermediaries Who Must not be Named? The Keepers of the Public Blockchain., (Nov. 21, 2019) (unpublished draft paper presented at the Smart Regulation and the Future of Financial Services Public Policy Conference hosted by Antonin Scalia Law School
because the network appoints certain participants to hold privileges over others. These privileges include participating in running the node and keeping certain records, which are not powers shared by the general participants.

These privileges draw criticism for EOS, in part because the privileged, as of the time this article was published, were concentrated in China. The centralization of validation in privilege holders on these networks may be sufficient to impose record-keeping and reporting of specific types of records of customers and transactions to government authorities or counter-parties in discovery or to respond to legal process. However, this may be difficult to achieve with offshore privileged participants.

A public, permissioned blockchain is one source of future public records systems, such as those for recording ownership of tangible property or providing public notice of security-interest claims.

4. Private, Permissionless Blockchains

A private, permissionless blockchain has nodes that “will only acknowledge [other nodes’ existence], but not share any data” with them.

One attraction of the private, permissionless blockchains is that each “smart contract” that may be used “automatically creates a private (side-) chain associated with that contact.”

In addition, although a node may hold more than one “side-chain,” one node will not hold all of those in existence for the larger chain.

Each node still operates as a repository. Only designated persons or organizations get permission to read specific nodes; designated persons will require cryptographic signatures to gain access to reading. To have reading privileges, one needs both the unique identifier (address) and the URL of the node that has a copy of the smart contract and associated chain.

Also, each node will hold only data needed to service its own users—an “agent-centric” solution. These chains inside private chains make the task of ferreting out specific transactions more complicated because they are not visible to the those with a need to know.
In this respect, the ‘permissionless’ concept seems a stretch, but the main point is that access to information is not public in any form.

These blockchains represent more powerful opportunities to hide assets because “smart contracts on these private networks, not only define who is allowed to perform contract actions but also who is allowed to read the contract and all related data.” First, the “smart contract” manages any contract actions required and created by this node, making it an ideal “location” from which to move those assets in the intermediate “layering” steps needed for traditional money laundering. Owners of crypto assets on private, permissionless blockchains are not likely to spend them outside a narrow sphere of prospective counterparties. This narrow sphere of prospective counterparties and the restrictions on permissions help protect the identities of users of these blockchains.

Experimentation with private, permissionless blockchains has been limited. As of October 2018, one commentator, Arnold Daniels, had identified only three chains – the Holochain, LTO Network, and Monet. Holochain allows “users [to] share information peer-to-peer on a need-to-know basis.” The LTO Network is Daniels’ own project: it “run[s] trustless workflows, targeting multinationals and governments . . . . The process has a strong focus on privacy and GDPR compliance.”

The last, as of February 2019, is Monet. Monet may be the most likely to be used to hide proceeds of financial crimes: it allows users to build “ad-hoc, short-lived chains, with mobile devices acting as nodes for the participants.”

Other crypto assets are in existence and development that will enhance privacy protections for users. One later entrant in this category is the LTO Network. Indeed, LTO Network states as a goal both keeping governments away and promoting compliance with the EU’s General Data Protection Regulation (GDPR).

5. Services and Applications that Allow “Mixing” of Bitcoins to Preserve More Privacy for Users

“Mixing” or blending of transactions allows a Bitcoin user to transfer or transact with bitcoins and to have the details of the transaction deleted as soon as the transaction is complete. So that transactions are not linked to the in-bound bitcoins or prior transactions on that bitcoin chain, one or more units of Bitcoin enter the validation process to be “mixed” or “laund[ered]” with other bitcoins, and different bitcoins emerge. This process works like

76. Id.
77. See id. (explaining how one can use a “smart contract” to disguise criminal activity).
78. See generally id. (noting the narrow scope of users on a single permissionless private network).
79. Id.
80. Daniels, supra note 48.
81. Id. For more information on the GDPR, see Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 04.05.2016 [hereinafter EU Regulation 2016/679]. The GDPR went into effect on May 25, 2018.
82. Daniels, supra note 48.
83. See generally id.
84. See generally id.
85. EU Regulation 2016/679, supra note 81.
87. Id.
the stages of laundering “money.” First, the assets are “placed” into a deposit account, securities account, or hard assets with a legitimate entity. Then, in a process to separate the proceeds from the underlying crime called “layering,” the assets are moved around from one or more locations or through one or more person to others. Finally, the assets eventually emerge with the appearance of being clean—free from association with their origins. Fees charged for this bitcoin-mixer-laundry-style service vary considerably by service provider and the number of bitcoins being washed through the provider’s system.

6. The Libra: Facebook’s Cryptocurrency

Facebook announced in June 2019 that it was preparing to launch a global currency built on a self-designed blockchain. The announcement described “a new decentralized blockchain, a low-volatility cryptocurrency, and a smart contract platform that together aim to create an new opportunity for responsible financial services innovation.” Although professedly “decentralized,” Libra will be “governed by the Independent Libra Association tasked with evolving the ecosystem.” Libra has stablecoin features: it will be backed by a “basket of [assets]” designed to give each unit “intrinsic value.” The Libra Association has the purpose of “coordinating and providing a framework for governance for the network and reserve” with membership “formed from the network of validator nodes that operate the Libra Blockchain.” A separate entity, the Libra Reserve, is intended to hold and manage the assets underlying Libra towards low-volatility.

7. Central Bank Digital Currencies (CBDCs)

Conversation about digital currencies issued by central banks has increased over the past year, particularly in France and Germany following the publication of Facebook’s plans for its Libra Cryptocurrency. The most recent development is a call for a Bank for International Settlements’ study of CBDCs.

88. Id.
89. Id.
91. Nine Best Bitcoin Mixers 2020, supra note 86.
94. Id. at 3.
95. Id. at 3; see Jon Fingas, Facebook’s Libra Currency Will Get Half Its Backing from the US dollar, ENGADGET (Sept. 22, 2019), https://www.engadget.com/2019/09/22/facebook-libra-currency-backing/ (reporting that Facebook updated the basket of currencies it intended to include in the Libra Reserve).
97. Christian Catalini et al., LIBRA, The Libra Reserve, https://libra.org/en-US/about-currency-reserve/#the_reserve (describing intentions to fully back each coin “with a set of stable and liquid assets . . . users can have confidence that they will be able to sell any Libra coin at or close to the value of the reserve at any time.”).
99. See generally Libra White Paper, supra note 93.
Central bank digital currencies would not be “virtual currencies” under the definitions adopted by FATF in 2014\(^\text{101}\) or FinCEN in 2013\(^\text{102}\) because they would

(a) qualify as “legal tender” in the jurisdictions whose central banks issue them; and
(b) would be digital representations of fiat or real currency.\(^\text{103}\)

The term “central bank digital currency” in this taxonomy excludes the last category in this section of this paper—government-sponsored cryptocurrencies such as Venezuela’s Petro because, at least initially, such cryptocurrencies are not designated as “legal tender” by sponsoring governments.\(^\text{104}\)

8. Government-sponsored cryptocurrencies or other digital assets designed for disruptive effect

This category of government-sponsored cryptocurrencies appears to be designed—at least initially—for limited types of transactions, such as purchases of oil or oil futures or for use only or primarily by off-shore persons.\(^\text{105}\) Because their announced raison d’etre is to evade sanctions or frustrate operations of normal reserve currencies, we may think of this category as being disruptors of a different dimension than Bitcoin.

i. El Petro

The most visible example of this disruptor category is “El Petro,” the cryptocurrency issued by Venezuela’s state-run oil-and natural-gas company, Petróleos de Venezuela, S.A. (PDVSA).\(^\text{106}\) This cryptocurrency emerged in early 2018.\(^\text{107}\)

One of the stated purposes of El Petro is to enable the Maduro government to sell oil and evade economic sanctions placed on the Maduro government, PDVSA, and representatives of both by the United States.\(^\text{108}\) In March 2018, the Trump Administration imposed economic sanctions that barred US Citizens from purchasing Petros.\(^\text{109}\) Maduro government officials and officials of the PDVSA were named in that and subsequent rounds of economic sanctions.\(^\text{110}\)

\(^{101}\) FATF Definitions, supra note 39, at 4.

\(^{102}\) FinCEN March 2013 Guidance, supra note 40, at 1.

\(^{103}\) Id.


\(^{108}\) Id. (providing a timeline of developments, including imposition of sanctions by President Trump, in El Petro from its announcement to July 2019).

\(^{109}\) Id. (citing backing for El Petro as including diamond and gold reserves as well as oil and gas).

There is evidence that US sanctions have been working, a fact that portends more efforts to evade sanctions and may cause more allies to help the Maduro government and certain individuals against whom the President has imposed sanctions.

Recently, the Maduro government has been encouraging broader internal uses of Petros, which has led to a surge in domestic person-to-person (“P2P”) uses and which has almost equaled the cryptocurrency penetration in the Russian Federation. More recently, the Maduro government is pushing for its people to use Petros to make everyday purchases. P2P volumes in Venezuela are rising and, allegedly, are right behind Russia in cryptocurrency penetration.

To the extent that the Maduro government allows or encourages use of El Petro in domestic transactions, the government appears to be attempting to “regularize” El Petro as fiat currency or as CBDCs. That could lead to greater acceptance of Petros both in Venezuela’s domestic economy and as a medium for payments of oil and natural-gas purchases on a larger scale.

ii. Russia and China and Plans for Gold-Backed Crypto

Russia and China also have announced plans to issue gold-backed cryptocurrencies for their own internal or external trade reasons. Another goal appears to be replacing the US Dollar as the world’s reserve currency. Russia has used cryptocurrencies such as the Venezuelan, government-owned Petro, which is specifically identified on the US Treasury Department’s “Specially Designated Nationals” (SDN) list to help Venezuela evade US economic sanctions, and to assist Russia’s operations in Crimea.

---


112. Haig, supra note 107 (mentioning Maduro’s order in July 2019 to Venezuelan banks to accept Petros in their banking; useful timeline of the emergence).


114. Haig, supra note 107.


The Putin government has spoken publicly of its intentions to create “official cryptocurrencies.”122 Russia’s announced purpose is to thwart economic sanctions imposed on Russian organizations and citizens.123 This puts the forthcoming Russian gold-reserves-backed cryptocurrency both in the disruptor category in this paper’s taxonomy and in the reserves-backed category of cryptocurrencies.

It is unclear whether governments such as Russia that sponsor cryptocurrencies will use their sovereign rights to deem their sponsored cryptocurrencies as “legal tender,” meaning a legal means to pay taxes and debts.124 It certainly appears that the Maduro government is moving in that direction with El Petro. Some of these specialty cryptocurrencies, such as China’s current, external-only version of the yuan or renminbi, referred to as the CYH, are destined to operate only as an external currency, not for domestic purposes.125 It is unclear whether owners of these cryptocurrencies will be allowed to exchange it for rubles, yuan, or pesos, that is, for “real” domestically usable legal tender. What is clear, in the United States at least, is that when a foreign government declares a cryptocurrency “legal tender” for its own internal-domestic-market purposes, that currency will cease to be “virtual currency” as FinCEN has defined it126 and will become “foreign exchange.”127 Does this matter in the short-term to the potential national security threats that these government-sponsored but not CBDCs may pose? I deal with that question in Part IV of this article.

II. CAN BLOCKCHAIN MAKE US SAFER?

Turning now to the first of two questions for consideration: Can blockchain technologies make us safer? I have already stated that the answer is “yes.” The more important questions are how and why blockchains may make us safer. This paper focuses on health care and life science applications as well as on supply-chain applications in food and pharmaceuticals. I previously mentioned but did not elaborate on this topic in my January 24, 2020 presentation on which this essay is based.


124. The Case of Mixed Money in Ireland, Trin. 2 James I. A.D. 1605, reprinted in 2 COBBETT’S COMPLETE COLLECTION OF STATE TRIALS 114–130 (1809) (the earliest reported decision upholding the sovereign’s authority to make, change or debase its money and designate its choice as legal tender for payments of taxes and debts) [hereinafter The Case of Mixed Money]. For a recent discussion of U.S. methods thwarting competition to the dollar, see Stephen T. Middlebrook & Sarah Jane Hughes, Substitutes for Legal Tender: Lessons from History for the Regulation of Virtual Currencies, in RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW (John A. Rothchild, ed., 2016).


126. FinCEN March 2013 Guidance, supra note 40.

127. Id.
A. Blockchain technologies are designed to be tamper-resistant.

Although many experts talk about blockchains being “immutable,” it is preferable to think of blockchains as being “tamper-resistant.” To be more precise, “blockchain” technologies – distributed ledger technology (DLT) – offer a larger set of technologies that are engineered to have certain properties. Professor Carla Reyes offered one of clearest and simplest descriptions of DLTs:

[T]he term distributed ledger technology (DLT) . . . refer[s] generally to “computer software that is distributed, runs on peer-to-peer networks, and offers a transparent, verifiable, tamper-resistant transaction-management system maintained through a consensus mechanism rather than by a trusted third-party intermediary that guarantees execution.”

Building on this definition, there are a few key attributes associated with DLTs that can make us safer, including:

- transparency in transactions,
- verifiable transactions,
- consensus mechanism as a governance principle,
- peer-to-peer networks, and
- no third-party intermediary to introduce cyber-threats or to be the focus of hacking attempts, or fewer opportunities for effective cyber-hacks of the blockchain.

Among the fields in which blockchain technologies are expected to produce gains in safety are healthcare and life sciences. The major areas of predicted utility, some of which will need to be private, permissioned blockchains, include:

- Electronic health records systems,
- Enabling sharing aggregate patient data with privacy protections for patient-level data that can serve larger population studies instead of patient-level data,
- Limitation of single-point of failure episodes,

---


130. Id.

131. Id. (citing ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGY: A COMPREHENSIVE INTRODUCTION (2016)).


133. Id.

134. Id.
DO BLOCKCHAIN TECHNOLOGIES MAKE US SAFER?

Since my January 24, 2020 presentation, we can expand the utility of the second item on the list above: this utility may offer benefits in tracking the spread of infectious diseases, such as the Covid-19 virus, and of contagious diseases. Blockchains may assist us in performing studies on the effectiveness of therapies and of engaging in contract tracing.

B. Blockchain technologies can contribute to safer supply chains, including chains that show origins of foodstuffs and pharmaceuticals.

Because of their general tamper-proof status and of the ability to design private and permissioned blockchain applications, as described in Part II of this essay, blockchains can help protect supply chains in food and pharmaceuticals. With respect to food, blockchains can help us determine the origins of specific batches of food stuffs—namely, whether batches were produced domestically or not. With the added reliability of blockchain technologies, this information can help public-health officials trace back to specific deliveries if a contaminant is detected. For example, this technology could have assisted in discovering Listeriosis in pre-sliced meats and cheeses in 2019 and E. coli bacteria in the notorious 1993 Jack-in-the-Box hamburger episode.

Sourcing and origins of pharmaceuticals are not second-in-fact in the benefits that may flow to the public from blockchain record-keeping. The presence of counterfeit components and useless pharmaceuticals in the pharmaceutical supply chains are sources of significant concerns. Examples of these problems include drugs with no active ingredients, those with the wrong or counterfeit ingredients, and those with the wrong dose of correct active ingredients.
III. WILL CRYPTOCURRENCIES MAKE US LESS SAFE? IF SO, WHY?

First, let me state that I do not believe that all cryptocurrencies make us safer. Second, I do not believe that all cryptocurrencies make all of us less safe. So, it is important to describe “safer” and “less safe” in this context and to explain what factors, features, or arrangements may make persons in the United States less safe than they otherwise might be and what I mean by “safer” or “less safe.” It also is important to appreciate that these are complicated questions because privacy is an important protection for activists and journalists, especially in non-rule-of-law jurisdictions. Cryptocurrency transfers can provide privacy protections. Finally, it is important to identify the spheres in which cryptocurrencies pose risks to safety that are different from legacy, intermediated payments, and payments services.

In highlighting three types of risks in this section, I do not mean to belittle the contributions that well-governed cryptocurrencies and real blockchains can make to economies, trade, and global remittances—the contributions are real. They include potential expansion of financial inclusion, faster delivery of trade payments and remittances, and less costly delivery of payments domestically and internationally.

The three topics I mention in this section may not be in the order in which the specific issues will emerge. The purpose is to begin to identify types of risks that may emerge. In my concluding remarks, I mention other topics where my own research may apply, and as a means of encouraging others to look at the same issues.

A. Risks to “monetary sovereignty”

During the March 1, 2019 Roundtable on the Future of Financial Regulation hosted by George Mason University’s Antonin Scalia Law School, I raised my concern that state-sponsored cryptocurrencies could threat national security because—taken to their logical endpoints—cryptocurrencies challenge the ability of governments to prescribe “legal tender” and, for that reason, to protect national governments’ “monetary sovereignty.”143 I made that comment before Facebook announced its intention to launch its Libra cryptocurrency.144

The connection to concerns about “monetary sovereignty” appear to be animating the objections of governments, such as those in France and Germany—whose finance ministers declared in September 2019 that “[n]o private entity can claim monetary power, which is inherent to the sovereignty of nations.”145 This sentiment is in accord with the outcome of The Case of Mixed Money in Ireland, the 1605 decision upholding the authority of the English sovereign, Queen Elizabeth I to fix the currency and its value within that sovereign’s domain.146 (Despite more than 400 years old, the opinion in Mixed Money explains so much about governments’ insistence on controlling “legal tender.”)

To see one of the logical outgrowths of state-sponsored cryptocurrencies such as El Petro, we can look to the consultation request filed by the Maduro government in Venezuela against the United States in the World Trade Organization in late 2018.147

146. The Case of Mixed Money, supra note 124.
147. General Agreement on Tariffs and Trade, WTO, (1994) [hereinafter GATT].
complaint cited violations of the General Agreement on Tariffs and Trade of 1994 (GATT)\textsuperscript{148} and General Agreement on Trade and Services (GATS) obligations occasioned by Executive Order 13,827 and other actions taken by the United States against El Petro.\textsuperscript{149} More specifically, the Maduro Government charged that the United States was violating GATS Article II Section 1. That Article provides that no member will treat another member less favorably than any other nation.\textsuperscript{150} Exceptions to WTO obligations arise if the member maintains that their actions relate to “essential security interests.”\textsuperscript{151} Executive Order 13827 explicitly references a prior declaration of a national emergency by the United States against Venezuela—Executive Order 13692 of March 8, 2015\textsuperscript{152} and Executive Order 13808 of August 24, 2017.\textsuperscript{153} As of July 1, 2020, there had been no progress to the appointment of the panel to hear Venezuela’s complaint.\textsuperscript{154} President Trump’s Executive Orders against El Petro and its government-operated company sponsor, PDVSA, prohibited “U.S. persons” from transactions “related to, provi[ding] financing for, and other dealings in” digital currency, coins or tokens “issued by, for, or on behalf of the Government of Venezuela on or after January 9, 2018 . . . . “\textsuperscript{155} The President’s sanctions order reached “any digital currency, digital coin, or digital token, that was issued by, for, or on behalf of the Government of Venezuela on or after January 9, 2018 . . . . “\textsuperscript{156} The President’s anti-Petro Executive Order cited the President’s authority to deny access to U.S. markets if the purpose—such as evading economic sanctions—is “unlawful.”\textsuperscript{157}

Other examples showing that cryptocurrencies are designed to enable governments to evade sanctions come from Iran and Russia.\textsuperscript{158} Beyond that, we see evidence that governments aid each other in avoiding sanctions.\textsuperscript{159} Others believe that cryptocurrencies generally may diminish the effectiveness of sanctions.\textsuperscript{160} A decrease in national governments’ monetary policy or control capacities because of an increase in assets placed in cryptocurrencies could decrease the dollar or other reserve currencies that central banks use to respond to crises of

\textsuperscript{148} Id.
\textsuperscript{151} GATT art. XXI. For discussion of how the WTO signatories expected Article XXI to be interpreted, see GATT, ‘Analytical Index, Note by the Executive Secretary’ (MGT/61/52, June 1952).
\textsuperscript{154} United States—Measures Relating to Trade in Goods and Services, World Trade Organization, WTO DS574 (Mar. 14, 2019), https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds574_e.htm (reporting that Venezuela’s request for a panel hearing is pending).
\textsuperscript{155} Exec. Order No. 13827-Venezuela, supra note 110.
\textsuperscript{156} Id.
\textsuperscript{157} Id. at preamble.
\textsuperscript{158} See Manshee Joshi, Iran Proposes Use of Cryptocurrency to Elude Sanctions, CRYPTOPOLITAN (Feb. 27, 2020), https://www.cryptopolitan.com/iran-use-of-cryptocurrency/ (reviewing numerous efforts to bring “mining” and investments to Iran, and the use of resulting cryptocurrencies to evade U.S. sanctions).
\textsuperscript{159} See Shuster, supra note 121 (outlining Russia’s encouragement of Venezuela avoidance of US sanctions).
national, regional, or international dimensions. The Bank for International Settlements has commented on monetary sovereignty risks from cryptocurrencies.

“Monetary policy” capacity enables governments to control inflation and spur economic growth. Use of monetary policy tools such as those that the Federal Reserve System deployed during the 2008–2009 financial crisis both in favor of U.S.-based depository institutions and global institutions enabled its program of “qualitative easing” of the economy through its discount-window lending and other measures.

B. Concerns about cryptocurrencies’ roles in money laundering and terrorist financing

Concerns about the uses of cryptocurrencies as tools in money laundering and terrorist financing caused the G20 to urge member states to adopt regulations compelling cryptocurrency exchanges to collect customer information. The Secretary of the U.S. Department of Treasury noted that Libra could be “misused by money launderers and terrorist financiers.”

C. Deposit volatility – enabling runs and panics in crypto and traditional depository institutions — and enabling fraud and theft

Cryptocurrencies, given the speed at which transfers can be settled compared with legacy bank transfers, also enhance risks associated with rapid movements of values from nation to nation and could contribute to broader instability in world markets and national economies. Use of crypto assets to either avoid national securities regulatory regimes or to engage in market manipulation is also worrisome.

The February 2020 G20 attendees also called for measures to handle consumer and investor protection, following the more than $4.26 billion in cryptocurrency holdings lost to fraud and theft in the first half of 2019.

161. Id.
163. See Monetary Policy Principles and Practice, FED. RESERVE BOARD (Mar. 8, 2018), https://www.federalreserve.gov/monetarypolicy/monetary-policy-what-are-its-goals-how-does-it-work.htm (“In the broadest terms, monetary policy works by spurring or restraining growth of overall demand for goods and services in the economy.”).
164. Id.
165. Gregory Lisa & Hogan Lovells, G20 Calls on Countries to Adopt FATF Crypto Standards, JD SUPRA (Feb. 28, 2020), https://www.jdsupra.com/legalnews/g20-calls-on-countries-to-adopt-fatf-41765/ (referencing the June 2019 FATF Guidelines on cryptocurrencies and the “travel rule” adopted then to require “virtual asset service providers” to collect such information). See also Smith-Meyer, supra note 98, at 2 (describing July 2019 concerns about these topics by G7 finance ministers).
167. See generally, Lawrence J. Trautman & George P. Michaely, Jr., The SEC & The Internet: Regulating the Web of Deceit, 68 CONSUMER FIN. L. Q. REP. 262 (2014).
CONCLUSION

In this essay, I asked and began to answer two questions. The first focused on whether blockchains could provide safer environments for supply chains and beyond. In response, I argue that blockchains generally can increase our collective safety in certain ways. I focus on supply-chains for food and pharmaceuticals and the manner that blockchain, can protect the integrity of information about contents, providers, and purchasers, I note that supply chains can be retraced if problems arise. Additionally, I note that the primary issue with blockchains in this respect is that, if the information sent to the block is garbage, then the information available later will be no better than garbage. This is a challenge that blockchain technology tries to address. However, despite considerable optimism that it can, we do not yet know how successfully it meets this challenge.

The tamper-resistant features of permissionless blockchains provide greater protections from hacking and theft generally and security in the integrity of data from interference by bad actors. Data integrity and data resilience are key aspects of secure supply chains for foodstuffs, pharmaceuticals, and other important manufactured goods and commodities. They also matter enormously in safe-and-sound financial services and to national security.

With the second question I asked, will cryptocurrencies make us less safe? Despite longstanding interests in faster and less costly forms of payment products, I see some of the developments in cryptocurrencies as making individuals less safe for the reasons I have laid out in Part IV of this essay. That does not mean that we cannot avoid increased or increasing risks if we act soon and also if we act in concert with other national governments and international organizations such as the G-7, G-20, and the European Union. One of the means of containing some of the risks that cryptocurrencies may pose to individuals and institutions is to do as the United States, the European Union, and the G-20’s Financial Action Task Force are endeavoring to do, which is to place responsibilities on gatekeepers or the entities that FATF calls “virtual asset service providers” (VASPs). How or why do some of the cryptocurrencies cause or contribute to national security risks as I have described them above? In addition to the three, top-level concerns that I discuss in Part IV, I have identified the following as issues which demand the attention of scholars:

• Will pseudo-anonymous cryptocurrency transactions cause governments and supply-chain financiers a loss of information about trade balances and possibly about trade occurrences?

• Will pseudo-anonymous cryptocurrency transactions cause business and consumers to lose demand deposit features common in commercial banking or assured redemption rights to values transferred in exchange for cryptocurrencies?

• Will cryptocurrency transactions weakening governments’ ability to track transactions for tax purposes? Will this weaken governments generally – even as much as individuals might like it?

• How will businesses and governments manage the loss of government-provided deposit insurance if a cryptocurrency provider fails? Can we fund a new program that ensures speedy resumption of access to deposits when non-insured financial services providers or VASPs fail? How will we manage the potential for disruption to the economy as businesses and consumers lack access to enough fiat currency or fiat-associated deposits to meet their

daily needs including payroll? Lengthy delays are not fictional. Mt. Gox and Quadriga FX customers are waiting for access to their assets today.

• What types of anti-fraud and anti-market manipulation tools will we need to manage different types of service providers than those currently regulated in the U.S. and elsewhere?

These questions are the topics that need future exploration as cryptocurrencies and other blockchain technologies come into wider adoption.