COIN CENTER

TESTIMONY OF

Jerry Brito

Executive Director of Coin Center[1]

BEFORE THE

United States Senate Committee on Banking, Housing, and Urban Affairs

"Cryptocurrencies: What are they good for?"

July 27, 2021

Cryptocurrencies receive much attention these days, but even so, the real use cases of these new technologies are often glossed over. Much cryptocurrency discussion unfortunately leaves the reader with too much breathless hype or knee-jerk condemnation and not enough measured analysis. It is not surprising, then, that some people may walk away with the impression that cryptocurrency is little more than a new iteration of the dot com bubble, without any real value add. Some will say, "There is nothing that can be done with cryptocurrency that cannot be done with sovereign currency that is meritorious and helpful to society."[2]

This is unfortunate, because cryptocurrency technologies have a wide range of use cases that extend far beyond the cloistered circles of Silicon Valley and Wall Street. What's more, cryptocurrencies' technological innovations allow a much broader range of unique applications that traditional sovereign currencies could never provide.

[1] Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain technologies.We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy. *This testimony is based on*: Andrea O'Sullivan, "Cryptocurrency: What is it good for? (A lot, actually.)" *Coin Center*, July 30, 2018, https://www.coincenter.org/cryptocurrency-what-is-it-good-for-a-lot-actually/ and Jerry Brito and Peter Van Valkenburgh, "The ideal regulatory environment for Bitcoin," *Coin Center*, August 25, 2020, https://www.coincenter.org/the-ideal-regulatory-environment-for-bitcoin/.

[2] Quotation from Rep. Brad Sherman, U.S. House Financial Services Committee, Subcommittee on Capital Markets, Securities, and Investment, "Cryptocurrency Markets," *Hearing*, March 14, 2018, *clip available a*t: https://twitter.com/coincenter/status/976182050616152064.

At its core, a cryptocurrency allows any individual to transfer value directly to a recipient anywhere in the world, without needing to rely on a trusted third party in the middle to facilitate the exchange.[3] This seemingly simple function introduces possibilities for a great variety of solutions and improvements in areas of payments, law, security, business processes, and much more.

Here are just a few of the meritorious cryptocurrency applications that will be quite helpful to society—that is, if we allow them to grow.

Direct digital payment

Let's start with the simplest use case. We may take it for granted that we can make payments online, but this state of affairs is neither evenly distributed nor always guaranteed. For one, not everyone in the world has access to a bank account or credit card with which they can engage in online commerce. Furthermore, the current system, which relies on third parties to facilitate exchange, is only as good as the trust that we can place in them. Such providers could conceivably go offline due to technical or cybersecurity difficulties,[4] or governments could push them to prevent certain transactions,[5] or they could mismanage[6] or improperly direct user funds.[7] Whatever the hypothetical, the point is that customers must place considerable trust in the third party to be a responsible and faithful steward of those funds, assuming that individuals have access to those services in the first place.

Cryptocurrencies remove the need to rely on any single trusted third party to make a transaction. In effect, a cryptocurrency replaces a third party like Bank of America or PayPal with the network itself, which is managed by a distributed web of computers all across the world. This means that Alice can make a payment online directly to Bob whenever and wherever she wants, without needing to introduce another party that may be cumbersome or costly. This also means that people without access to banking services globally can now take part in digital commerce.

In the U.S. we take it for granted that we can send each other funds effortlessly with our smartphones, but this is not the case everywhere in the world—especially where authoritarian

[3] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, October 31, 2008, https://bitcoin.org/bitcoin.pdf.

[4] Nicole Perlroth, "Attacks on 6 Banks Frustrate Customers," *New York Times*, September 30, 2012, https://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html.

[5] Victoria Guida, "Justice Department to end Obama-era 'Operation Choke Point,'" *Politico*, August 17, 2017, https://www.politico.com/story/2017/08/17/trump-reverses-obama-operation-chokepoint-241767.

[6] Kurtis Ming, "Safe Boxes May Not Be Safe After All," *CBS Sacramento*, July 26, 2018, https://sacramento.cbslocal.com/2018/07/26/safe-boxes-stolen-drilled/.

[7] Anna Tims, "Redundancy payout nightmare after bank transfer error sends stranger money," *The Guardian*, September 25, 2017, https://www.theguardian.com/money/2017/sep/25/worker-loses-home-car-bank-money-transfer-error.

governments block payments to and from reformers. Just last year, pro-democracy activists in Belarus and anti-police-violence protesters in Nigeria successfully turned to the Bitcoin network to accept donations because local banks would not bank them.[8]

This kind of direct digital exchange is not possible with traditional sovereign currencies. To make a *direct* exchange with sovereign currencies, individuals will need to meet in person to transact, which can be inconvenient or dangerous. To make a *digital* payment, they will need to rely on a trusted third party, which can be expensive or unavailable. There is no way to combine direct exchange and digital exchange using a traditional sovereign currency, which is why cryptocurrencies are so unique and value-generating.

Secure store of value

Cryptocurrencies are useful beyond their application as a medium of exchange. By eliminating the need to rely on a third party for the issuance and transfer of value, cryptocurrencies empower users to take control of their finances. Transfers can only be made when a user cryptographically approves a specific transaction—an action known as "signing with a private key." This means that the user who holds the private key, and only that user, can control where and when their money is spent.

This use case is crucial in environments where citizens cannot trust that institutions will be responsible stewards of their hard-earned money. Consider the tragic case of a country like Venezuela, where individuals' property and savings can be confiscated by authorities through law or inflation.[9] Many Venezuelans are unfortunately unable to access traditional forms of exit such as emigration or stealthily accruing more stable sovereign currencies. With cryptocurrency, more Venezuelans have an alternative: They can opt to purchase or mine a secure store of value that cannot be confiscated or inflated away by their government because they alone control their

[8] Anna Baydakova, "Belarus Nonprofit Helps Protestors With Bitcoin Grants," *CoinDesk*, September 9, 2020, https://www.coindesk.com/belarus-dissidents-bitcoin; Yomi Kazeem, "How bitcoin powered the largest Nigerian protests in a generation," *Quartz Africa*, October 26, 2020, https://qz.com/africa/1922466/how-bitcoin-powered-nigerias-endsars-protests/.

[9] Nick Miroff, "How to fight hyperinflation in Venezuela? By seizing massive amounts of cash," Washington Post, December 13, 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/12/13/how-to-fight-hyperinflation-in-venezuela-by-seizing-massive-amounts-of-cash/; Matt O'Brien, "Venezuela could have one million percent inflation. How is that even possible?" *Washington Post*, July 26, 2018, https://www.washingtonpost.com/business/2018/07/26/good-news-is-venezuela-wont-have-million-percent-inflation-soon-bad-news-is-it-might-later/.

private keys.[10] Indeed, cryptocurrencies are especially popular in Venezuela for precisely this reason.[11]

There is a use for this property for people living in more responsibly-managed monetary systems as well. As cybersecurity incidents continue to affect more and greater financial institutions, more people will find their personal information vulnerable to hostile actors.[12] After all, in order to engage with the traditional system of personal finance, we must give over considerable information to banks which are then tied to our credit and debit card numbers. Cryptocurrencies require no such personal information in order to engage in online commerce, and users do not need to trust that financial institutions and their vendors will be able to thwart all of the many daily attacks on their systems.

Microtransactions and metering

Removing the middleman can also do more than just remove a threat point; it can also reduce the cost to send a transaction. By allowing people to send value directly to another person, cryptocurrencies may prove to be an affordable alternative to other forms of transfer. This means that transactions that may have not made economic sense due to the fees imposed by third parties in the past may now be feasible, which unlocks a range of possibilities.

One of these is microtransactions, which is just what it sounds like: the ability to make tiny transfers of only a few cents (and perhaps fractions of a cent) at a time.[13] When you walk by a gumball machine and decide you want a little treat, it takes very little effort to just whip out a quarter and receive your desired confection. But when you want to purchase the digital equivalent of a gumball online—say, a single music video, or WiFi coverage to check an email for a few minutes, or an in-game upgrade—things quickly become not worth the hassle. You would likely have to create an account with the service in question and would need to have access to some kind of credit card and link it to the service. And because the fees to actually undertake a 25 cent transaction will be greater than the transaction itself, you won't have the option to buy just one item, say, but instead have to pony up for a month's worth of access. This

[10] Rene Chun, "Big in Venezuela: Bitcoin Mining," *The Atlantic*, September 2017, https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177/.

[11] John Detrixhe, "Bitcoin trading in Venezuela is skyrocketing amid 14,000% inflation," *Quartz*, June 8, 2018, https://qz.com/1300832/bitcoin-trading-in-venezuela-is-skyrocketing-amid-14000-inflation/.

[12] Major hacks on entities such as Equifax, Anthem, Marriott, and the Office of Personnel Management are only a few of the high-profile data breaches that have exposed millions of Americans to outside parties. Hacked datasets can be combined to provide an even fuller picture of individual information. *See*: Garrett M. Graff, "China's Hacking Spree Will Have a Decades-Long Fallout," *WIRED*, February 11, 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

[13] Steve Glassman, et al., "The Millicent Protocol for Inexpensive Electronic Commerce," Proceedings of the 4th International World Wide Web Conference, December 1995, https://www.w3.org/Conferences/WWW4/Papers/246/.

kind of arrangement is obviously just not worth it, so there are a lot of transactions that aren't happening because the existing payments system can't facilitate them.[14]

Cryptocurrencies can, for the first time, make microtransactions for many services economically feasible.[15] Let's say that someone wants to view a paywalled article online, but does not want to purchase a full subscription to that outlet. That person could send a microtransaction to the newspaper's cryptocurrency wallet, which would automatically unlock the article to the payer. The reader benefits by only paying for the content they want, and the newspaper benefits because expanded price discrimination can lead to greater overall engagement. Additionally, microtransactions present an alternative to the advertising model of monetizing content on the web and all the attendant privacy-encroaching tracking it brings with it.[16]

Metering is a special kind of microtransaction. Rather than a per unit price, metered microtransactions allow users to purchase access to a service for an unspecified amount of time. WiFi access provides a good example. Right now, if people want to purchase public WiFi access, they have to purchase a set unit of time for a set price, regardless of whether they only need to send a quick email or check on some data for work. This can be costly and obnoxious to the user, but there is no easy way to meter microtransactions using traditional credit and debit cards for the reasons mentioned above. Cryptocurrency provides a solution for low-to-no fee metering to access these kinds of club goods.

Smart contracts

People who say that cryptocurrency can't do anything that 'sovereign currency' can't also do probably don't understand that cryptocurrencies aren't just a kind of money; they are a kind of programmable money. While our examples so far have focused on simple currency storage and transfers between parties, cryptocurrencies also include scripting capabilities that allow for more complex transactions to occur. These kinds of transactions are known as "smart contracts," and they work because all of the elements of the exchange to take place are entirely digitized.[17]

For example, let's say that Alice would like to gift her granddaughter, Erin, with a sum of money upon her 18th birthday. Today, Alice's option is basically to hire a lawyer to create a trust that will hold the funds and disburse them on the appointed date. Being a technologically-savvy

[14] "Electronic commerce with microtransactions," Computer Weekly, July 22, 1999, https://www.computerweekly.com/feature/Electronic-commerce-with-microtransactions.

[15] Coin Center demonstrated this capability for Congress using the bitcoin lightning network and a lightning-enable candy dispenser that was built by a swiss developer, David Knezić, out of off the shelf hardware and open source software. Transactions could be made for fees less than 1/250th of a penny. https://www.coincenter.org/we-demonstrated-the-bitcoin-lightning-network-in-congress/

[16] Brave Software, "Basic Attention Token (BAT): Blockchain Based Digital Advertising," White Paper, February 10, 2021, https://basicattentiontoken.org/static-assets/documents/BasicAttentionTokenWhitePaper-4.pdf.

[17] Nick Szabo, "The Idea of Smart Contracts," 1997, https://nakamotoinstitute.org/the-idea-of-smart-contracts/.

grandmother, however, Alice knows that she can simply program a smart contract to do the same thing without having to employ an intermediary. Alice creates a cryptocurrency wallet for herself and another for her granddaughter Erin. Alice sends the equivalent of $10,000 to her wallet and programs a smart contract. The contract is set up so that on the day of Erin's birthday—let's say January 3, 2027—the contract will automatically move the funds from Alice's wallet directly to Erin's, where she will have complete control of those funds. Once Alice sets the transaction in motion, she no longer has access to the funds, just as if she had created a trust.

And that is just the simplest example. Smart contracts can be deployed any time that a set of digital promises can be enforced by a protocol through which the parties to the promises operate. There are a wide range of hypothetical and currently-used applications in the fields of finance,[18] law,[19] and identity.[20]

However, smart contracts are not a kind of magic wand. It is crucial that the parties to a smart contract are absolutely certain that their code will function the way that they intend, and will not be susceptible to attack. There have been high-profile smart contract failures, resulting in millions of dollars in losses.[21] With that caveat in mind, it is likely that routine and simple smart contracts—like the illustration with Alice and Erin above—will be ironed out relatively quickly, and more experience will improve the quality and range of smart contracts available.

Extra-monetary applications

The examples above show just a few of the ways that cryptocurrency offers a great expanse of currency-based applications that traditional sovereign currencies simply cannot. But one of the really neat things about cryptocurrencies is that they and the open blockchain networks that underpin them have uses that primarily have little to do with "money" at all.

Our previous examples illustrated how blockchain tokens can be directly transferred in different kinds of ways. But those tokens don't necessarily need to only represent a currency. After all, at the end of the day, it's all just zeros and ones on a computer. So a blockchain token can hypothetically represent anything that can be digitized. And because blockchains are censorship-resistant, any entry added to a blockchain can be thought of as a persistent, public, and verifiable

[18] Thaddeus Dryja, "Discreet Log Contracts," *MIT Digital Currency Initiative*, https://adiabat.github.io/dlc.pdf.

[19] Max Raskin, "The Law and Legality of Smart Contracts," 1 *Geo. L. Tech. Rev*. 304 (2017): pgs. 305-341, https://dx.doi.org/10.2139/ssrn.2842258.

[20] Affan Yasin and Lin Liu, "An Online Identity and Smart Contract Management System," 2016 IEEE 40th Annual International Computer Software and Applications Conference (COMPSAC), June 2016, https://ieeexplore.ieee.org/document/7552202.

[21] Andrea O'Sullivan, "Bot-Run Company of the Future Gets Hacked," *Reason*, August 16, 2016, https://reason.com/2016/08/16/dao-gets-hacked/.

record online. This tamper-resistant recordkeeping, however, is only present in open networks with a cryptocurrency or scarce token component.

Consider this story from China: In 2018, a pseudonymous blogger reported that a major pharmaceutical company had been manufacturing and selling unsafe vaccines.[22] Although the story went viral on social media, government censors went about removing any posts about it online. How could the blogger make sure that his posts would not be blotted out? He put it on an open blockchain network; in this case Ethereum. By sending a small transaction worth a few pennies of ether to their wallet, the blogger was able to attach his exposé to the metadata of the transaction, thus immortalizing the report's existence on the internet.

This kind of application is especially crucial in situations where the public must know of some kind of high-level corruption. But there are a number of blockchain efforts to record data for commercial and legal applications as well. Some people envision a title registration service that is entirely or mostly-blockchain-based, which would cut down on the need for costly administration and title insurance.[23] Others are working on projects to offer Dropbox-like services, where a blockchain would facilitate storing users' files in a decentralized manner.[24]

Perhaps more relevant to average Americans are the potential applications of cryptocurrency tamper-resistance to enable identity solutions for cybersecurity. The root cause of many data breaches—such as those at Experian,[25] Equifax,[26] OPM[27]—is the fact that if an attacker can compromise the password of one individual he may gain access to the personal information of millions of others.

Microsoft is a company that is painfully aware of this vulnerability as it provides the identity infrastructure for over 90 percent of Fortune 500 companies.[28] This is why Microsoft spent years helping develop a decentralized identity standard built on top of Bitcoin. It is called the ION

[22] Kristin Houser, "Chinese Citizens Are Using Blockchain to Warn Each Other of Unsafe Vaccines," *The Byte*, July 25, 2018, https://futurism.com/the-byte/unsafe-vaccines-china-blockchain.

[23] Avi Spielman, "Blockchain : digitally rebuilding the real estate industry," *MIT Center for Real Estate*, 2016, https://dspace.mit.edu/handle/1721.1/106753.

[24] *For examples, see*: https://www.storj.io/, https://ipfs.io/, and https://sia.tech/.

[25] Brain Krebs, "Experian API Exposed Credit Scores of Most Americans," *Krebs on Security,* April 28, 2021, https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans/.

[26] Alfred Ng, "How the Equifax hack happened, and what still needs to be done," *CNet*, September 7, 2018, https://www.cnet.com/tech/services-and-software/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/.

[27] Brendan I. Koerner, "Inside the Cyberattack That Shocked the US Government," *WIRED*, October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[28] Apron Shah, "Microsoft Azure: The only consistent, comprehensive hybrid cloud," Microsoft Azure blog, September 25, 2018, https://azure.microsoft.com/en-us/blog/microsoft-azure-the-only-consistent-comprehensive-hybrid-cloud/.

network, it was launched in March, is live and operational, and is now a candidate W3C standard.[29]

By replacing usernames and passwords with decentralized identifiers,[30] the ION network will allow individuals to control their own identities rather than trust data brokers that can be compromised at root. This means that an attacker would no longer be able to compromise just one credential in order to gain access to everyone else's, but would instead have to hack each individually—a massive improvement to cybersecurity.

Other benefits of decentralized identifiers include the ability to verify credentials—helping, for example, to combat disinformation. For example, with ION it will be trivially easy to verify that a photo you're looking at was signed as authentic by a photographer credentialed by the Associated Press.[31] Additionally, because you own your own identity and network of relationships to other identities, we will be able to see the emergence of an open, portable social graph that will allow for competition with incumbent social networks.

What about regulation?

A cursory review of just a handful of the most high-profile applications of cryptocurrency technologies reveals that these innovations can yield benefits that traditional sovereign currencies never could. It is never a bad thing to wait to get involved with a new technology until you feel that you really understand it—especially when that technology can also be a kind of financial investment. The great thing about cryptocurrencies is that they are entirely voluntary: If a person feels uncomfortable using them, they are in no way obligated to get involved.

There are a lot of very good reasons that cryptocurrency enthusiasts spend so much time improving and building out new infrastructure to bring these innovations to more and more people. And while there are certainly illicit uses of cryptocurrency, that is par for the course for new technologies: from automobiles to the internet. The solution to that is not to throw out the baby with the bath water. A policy environment that preserves for tinkerers and innovators the greatest possible space to develop new and better applications of cryptocurrency technologies will ensure that society gets the most value possible.

What would such an environment look like?

[29] "Decentralized Identifiers (DIDs) v1.0," *W3C Candidate Recommendation Draft*, July 20, 202, https://www.w3.org/TR/did-core/.

[30] *Ibid*.

[31] "Tangents from Coin Center: Daniel Buchner," Podcast, October 21, 2020, https://www.youtube.com/watch?v=VMzJ3AdhDtI.

As it turns out, with the notable exception of tax policy, the prescription for an enlightened policy environment that balances the risks and benefits of cryptocurrency is essentially the regulatory regime at which the United States has arrived after years of policy evolution. The U.S. regime is not perfect, it can improve, but it gives regulators and law enforcement the tools they need to sensibly address risks and criminal behavior. We divide the policy areas into four general categories of regulation: consumer protection, investor protection, financial surveillance, and tax. We'll go through them one at a time.

Consumer Protection

The purpose of consumer protection regulation is to ensure that businesses who take custody of consumer cryptocurrency for any purpose—whether it is for safekeeping, to provide payments or exchange services, or anything else—are sound and law-abiding. This is typically done through licensing. That is, a business cannot legally offer a service to the public that involves taking custody of consumer funds without first acquiring permission (a license) from the state. The state gives a license to any business that meets certain criteria, including passing a background check, posting a bond, satisfying minimum capitalization requirements, and offering specific disclosures to customers.[32]

The key to a sensible consumer protection licensing regime is twofold. First, and most important, it should be clear that the licensing requirement is triggered by custody and nothing else. Second, licensing requirements should be reasonable and non-duplicative.

Taking custody of consumer funds is the activity that creates a risk to consumers (for obvious reasons), and it is that risk that licensing aims to ameliorate. Therefore, if a business provides cryptocurrency services to consumers (possibly including payments or exchange services) but does not take custody of consumer funds, it should be excluded from any licensing requirement. Only if a firm has the ability to lose or steal or otherwise risk consumer funds should it be required to be licensed.

In contrast to this, some foreign governments have made the mistake of requiring a license from any business that engages in cryptocurrency services, even if no risk to consumer funds can be identified. This is pernicious because it places a burden on firms that have innovated in such a way to provide services to consumers without creating the kind of risk that licensing is meant to address in the first place. The way to avoid that is to have any licensing law turn exclusively on whether the business has "control" of consumer cryptocurrency, and the best statutory definition

[32] *See, generally*: Marco Santorini, "What is Money Transmission and Why Does it Matter?" *Coin Center*, April 7, 2015, https://www.coincenter.org/education/policy-and-regulation/money-transmission/; *See also*, e.g. Coinbase license list, accessed June 28, 2021, https://www.coinbase.com/legal/licenses.

of "control" available is found in the Uniform Law Commission's Regulation of Virtual-Currency Businesses Act (RVCBA):

> "Control" means … [the] power to execute unilaterally or prevent indefinitely a virtual-currency transaction[33]

For firms that do take custody (control) of consumer cryptocurrency, licensing criteria should be clear and sensible. First, in contrast to the United States where a business must acquire dozens of licenses in each state in which it does business, an ideal regulation would be national or transnational (*e.g.* the E-Money License in the European Union) in scope.[34] Second, the level of regulation imposed by the license should be calibrated to the level of custody risk posed to customers by the business. For example, the RVCBA includes a provision that allows firms to operate without a license (simply by registering) until their business activity exceeds $35,000 annually.[35]

Investor Protection

The purpose of investor protection regulation is to ensure that investors do not face information asymmetries that would put them at a disadvantage. This means ensuring accurate financial reporting issuers of equities, as well as ensuring the fairness of markets. Bitcoin and cryptocurrencies like it are not securities, in part because there is not a firm or person who runs the Bitcoin network or issues bitcoins. It is instead more accurately classified as a commodity.[36] Therefore, regulations that apply to securities and securities markets should not apply to Bitcoin and cryptocurrencies like it. In contrast to the United States, which employs a court-made test for determining whether an asset qualifies as an "investment contract," most other countries list in statute what assets are securities. The ideal regulatory policy should simply ensure that Bitcoin and cryptocurrencies are not treated as securities.

[33] "Uniform Regulation of Virtual-Currency Businesses Act," National Conference of Commissioners on Uniform State Laws, drafted at the ULC Annual Conference, San Diego, CA, July 14-20, 2017, https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=bd2ebf37-48a6-1d1e-8644-a9869bb-4f0e7&forceDialog=0.

[34] Peter Van Valkenburgh, "The Need for a Federal Alternative to State Money Transmission Licensing," *Coin Center*, January 2018, https://www.coincenter.org/the-need-for-a-federal-alternative-to-state-money-transmission-licensing/.

[35] *Supra* at 33.

[36] This has been stated policy at both the SEC and the CFTC. *See*: Neeraj Agrawal, "SEC Chairman Clayton: Bitcoin is not a security," *Coin Center*, April 27, 2018, https://www.coincenter.org/sec-chairman-clayton-bitcoin-is-not-a-security/; William Hinman, "Digital Asset Transactions: When Howey Met Gary (Plastic)," *Remarks at the Yahoo Finance All Markets Summit: Crypto*, San Francisco, CA, June 14, 2018, https://www.sec.gov/news/speech/speech-hinman-061418; "CFTC Statement on Self-Certification of Bitcoin Products by CME, CFE and Cantor Exchange," *Commodity Futures Trading Commission*, December 1, 2017,

As far as market regulation is concerned, an ideal policy would be to simply ensure equal treatment between markets in cryptocurrency and commodities. Typically, it is not markets for commodities themselves that are regulated, but commodity derivatives markets that are subject to regulation. Alternatively, foreign exchange market regulation could serve as a model for cryptocurrency exchange regulation or new authority could be given to a federal supervisor, such as that proposed in the Digital Commodity Exchange Act.[37]

Financial Surveillance

The purpose of financial surveillance laws (better known as anti-money-laundering regulation) is to deputize private businesses as criminal investigators for the state.[38] Generally these laws apply only to a defined class of business referred to as "financial institutions."[39] Regulated financial institutions must collect identifying information about their customers, as well as surveil their customer's activities and report detailed information about certain specified transactions (or potentially all transactions) to the financial surveillance regulator, which will in turn share that information with law enforcement and national security agencies.[40] Throughout this process customer information is collected and transmitted to the government without a search warrant, and, in some cases, without any independent legal process whatsoever.[41] Persons engaged in a variety of cryptocurrency activities may or may not be classified as financial institutions and be obligated to surveil their customers or transactional counterparts.[42]

As far as financial surveillance is concerned, an ideal policy would be to require a warrant for any state collection of personal financial data from a financial institution including businesses facilitating cryptocurrency activities. This, however, would be an extreme shift in policy; banks have been subject to financial surveillance laws in the U.S. since the 1970s, and the Supreme Court found long ago that bank customers have no reasonable expectation of privacy over

[37] Rep. Michael K. Conaway, "Digital Commodity Exchange Act of 2020," H.R. 8373, House Agriculture Committee, 116th Congress, introduced September 24, 2020, https://www.congress.gov/bill/116th-congress/house-bill/8373.

[38] Peter Van Valkenburgh, "Electronic Cash, Decentralized Exchange, and the Constitution," *Coin Center*, March 2019, https://www.coincenter.org/electronic-cash-decentralized-exchange-and-the-constitution/#iii-electronic-cash-decentralized-exchange-and-the-fourth-amendment (*Section III: Electronic Cash, Decentralized Exchange, and the Fourth Amendment*).

[39] *31 U.S.C. § 5312*.

[40] *Id*.

[41] *Supra* note 38.

[42] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," *Financial Crimes Enforcement Network*, FIN-2013-G001, March 18, 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf; *and* "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," *Financial Crimes Enforcement Network*, FIN-2019-G001, May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

records that they willingly hand over to banks while transacting.[43] Similar regimes have proliferated across the world thanks to international standards-setting bodies such as the Financial Action Task Force.[44] Short of reviving judicial oversight and a warrant requirement for the mass collection of customer financial data by law enforcement, a pragmatic policy is to seek equal treatment as between cryptocurrency businesses and traditional financial institutions. This means that only those businesses that hold and control customer cryptocurrency (as in our definition from consumer protection above) should be classified as regulated financial institutions. Non-controlling cryptocurrency businesses such as miners, node-operators, software developers, or minority key-holders in a multi-sig arrangement, should never be classified as financial institutions. Individuals transacting on their own behalf (buying and selling, donating, or paying for goods and services) should also never be classified as financial institutions. Generally speaking, this is the current policy of FinCEN.[45]

Taxation

Ideally, the IRS should state clearly and in detail how cryptocurrency transactions will be taxed as this may not be intuitive given the novelty of cryptocurrencies as assets including how to account for basis in calculating capital gains.[46] There should also be a threshold in the amount gained below which no tax is due. Without such a *de minimis* exemption from capital gains taxation, a cryptocurrency user could trigger a taxable event every time she pays for a good or service rendering cryptocurrencies too complicated for micropayments or other simple payments use.[47]

Cryptocurrency block rewards from mining or staking on cryptocurrency networks should not be taxed as income when they are created. These rewards are best analogized to fruit that has ripened on the taxpayer's land, crops grown in her fields, or precious metals mined from her soil. Applying a tax liability at the moment the new value is created generates extreme accounting

[43] *Supra* note 38 and *California Bankers Assn. v. Shultz*, 416 U.S. 21 (1974).

[44] "About," Financial Action Task Force, accessed July 24, 2021, https://www.fatf-gafi.org/about/.

[45] "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," Financial Crimes Enforcement Network, FIN-2019-G001, May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[46] James Foust, "A Duty to Answer: Six Basic Questions and Recommendations for the IRS on Crypto Taxes," *Coin Center*, April 2019, https://www.coincenter.org/a-duty-to-answer-six-basic-questions-and-recommendations-for-the-irs-on-crypto-taxes/.

[47] There is already a de minimis exemption from capital gains taxation for foriegn currencies and legislation has been introduced to apply a similar sensible standard to cryptocurrencies. See: Mike McSweeney, "New Congressional Bill Seeks De Minimis Tax Exemption for Smaller Crypto Transactions," Office of Congressman David Schweikert, January 16, 2020, https://schweikert.house.gov/media-center/in-the-news/new-congressional-bill-seeks-de-minimis-tax-exemption-smaller-crypto.

difficulties and overtaxes the citizen. Instead, should a country wish to collect taxes related to mining or staking activities, it should tax them when they are sold by the miner or staker.[48]

Conclusion

As the above lays out, there are many use cases for cryptocurrencies that can be beneficial to society. Allowing this technology to flourish can also help maintain the position of the United States as the home to global innovation. In order for us to achieve this promise we must also carefully consider the ideal regulatory environment that both fosters innovation and adequately protects consumers. As noted at the outset, the regulatory regime in the United States goes in the right direction.

Like the early internet, there are real, live uses of cryptocurrency networks today, but we can only see glimpses of the truly world-changing applications to come. The Clinton administration successfully pursued a deliberate policy of avoiding undue restrictions of the Internet.[49] To reap the benefits of cryptocurrency networks we should have the wisdom to do the same today.

[48] Mattia Landoni, "Dilution and its discontents: Quantifying the overtaxation of block rewards," *Coin Center*, August 2020, https://www.coincenter.org/dilution-and-its-discontents-quantifying-the-overtaxation-of-block-rewards/.

[49] Jerry Brito, "How the SEC and CFTC can address cryptocurrency while preserving US innovation," *Coin Center*, January 25, 2018, https://www.coincenter.org/how-the-sec-and-cftc-can-address-cryptocurrency-while-preserving-us-innovation/.