



TESTIMONY OF

Peter Van Valkenburgh

Director of Research of Coin Center

BEFORE THE

**United States House of Representatives Committee on Financial Services
Subcommittee on Capital Markets, Securities, and Investment**

“Examining Cryptocurrencies and ICO Markets”

March 14, 2018

I am Peter Van Valkenburgh, Director of Research at Coin Center, an independent nonprofit focused on the public policy questions raised by cryptocurrencies and open blockchain networks.¹

The fundamental achievement of Bitcoin² and follow-on cryptocurrencies³ is digital scarcity. We know there are only 16.9 million bitcoins in the world right now because their distribution and movements are described with perfect fidelity on a public ledger that anyone can independently read and mathematically authenticate.⁴ That ledger is called the Bitcoin blockchain.⁵ Just as anyone who owns an ounce of gold can independently assay the metal and

¹ Based in Washington, D.C., Coin Center is the leading independent non-profit research and advocacy center focused on the public policy issues facing cryptocurrency and decentralized computing technologies like Bitcoin and Ethereum. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using permissionless 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. See Coin Center, *Our Work*, <https://coincenter.org/our-work>.

² Bitcoin was first described in a white paper circulated over Internet mailing lists in late 2008. The author(s) used a pseudonym, Satoshi Nakamoto. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), <https://bitcoin.org/bitcoin.pdf>. The Bitcoin network itself did not begin running on the Internet until January 3, 2009 when the first block in the bitcoin blockchain was mined. See "Block 0" Bitcoin Block Explorer, (last accessed Dec, 2015) <http://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>

³ The software that powers the Bitcoin network is open source. That means that it can be freely copied and modified without seeking a copyright license or paying the original creators. Because of this openness, several thousands of cryptocurrency and token projects have emerged by borrowing software code or developing new software inspired by Bitcoin. While there are now thousands of cryptocurrency projects, only a handful are actively used online and have more than a trivial total value. See https://en.wikipedia.org/wiki/List_of_cryptocurrencies.

⁴ The total supply, distribution, and full history of all bitcoin transactions can be observed by running the bitcoin core software client on an Internet connected computer. Alternatively, one can visit a website that publishes the data in the blockchain in a more convenient and easy to access format. See, e.g., <http://blockchain.info>. See <https://blockchain.info/charts/total-bitcoins> for an up to the minute accurate tally of the total number of bitcoins in circulation. New bitcoins are released to network participants who perform verifiable work securing the blockchain according to a diminishing schedule that is described in the bitcoin software. Ultimately, this schedule dictates that there will only ever be 21 Million bitcoins in circulation.

⁵ The bitcoin blockchain is broken up into blocks. Each block comprises the authoritative list of bitcoin transactions that settled in a given period that is, on average, 10 minutes long. For an up to date list of recent blocks and the transactions included within them, see <https://blockchain.info/blocks>.

have proof that what they hold is real, scarce, and valuable, anyone can check the data in the Bitcoin blockchain and verify that bitcoins they've received are provably scarce and valuable.⁶

An open set of computers running the free Bitcoin software works together to store, update and verify that blockchain 24 hours a day, 365 days a year. Anyone can join that network of computers and independently check the work of every other participant, independently store their own copy of the blockchain, and independently contribute computing power to validate the integrity of that data.⁷ Honest and verifiable contributions to help secure the network are rewarded with automated payments in bitcoins, and attempts at fraud are revealed and punished by automatically withholding bitcoin-denominated rewards and ignoring fraudulent transactions. This is how these networks establish trust in the integrity of the record, and, by extension, trust in the inherent scarcity of bitcoins or any other token, coin, or unit whose distributions and movements are tracked on an open blockchain.

This digital scarcity can enable a wide variety of new, follow-on innovations:

- A scarce token can be developed to be nothing more than *scarce* and *transferrable* person to person. That, in a nutshell is Bitcoin.⁸ Because it is transferable and scarce it can be used as money just like other portable and scarce goods throughout history have been used as money—from gold to seashells.

⁶ Truly verifying that data requires familiarity with cryptographic functions used to sign and chain together the relevant transaction data going back to the beginning of the network in 2009. This is not easy for a lay person, however it is a deterministic technical process that any expert in the field of cryptography can perform, much like any expert metallurgist could verify the quality of an ounce of gold via chemical analysis.

⁷ Participating in this verification is known as mining. For a comprehensive explanation of the mining process *See infra* Attachment 2, *Framework for Securities Regulation of Cryptocurrencies*, Appendix 1. The Bitcoin Mining Mechanism: Proof of Work Consensus.

⁸ To quote François Velde of the Chicago Federal Reserve, “Bitcoin is a system for securely and verifiably transferring bitcoins.”

- A scarce token can be developed that is *automatically* redeemable for a digital good or service (like cloud storage or digital identity credentialing) that is provided by the same open network that keeps the blockchain. Projects like Ethereum, Filecoin, or Blockstack follow this model and they may soon challenge centralized computing service providers like Amazon, Facebook, and Google that specialize in the provision of services like cloud storage, social networking, or digital identity.⁹
- A scarce token can be developed as a representation of a legal agreement or financial asset: a public company could track its shares as tokens on a blockchain,¹⁰ or a network of banks could settle accounts by trading tokens that represent debt obligations on their balance sheets.¹¹
- A scarce token could even represent a real world identity document like a diploma, a driver's license, or a deed to land.¹²

Looking at it one way, these blockchains are just records, whether they be records about money, assets, identity, or computation. But rather than relying on a variety of major corporations or institutions to keep track of these important records in data centers that each have the potential to go offline or get hacked, a token-powered blockchain version of the record relies on an open network of thousands or potentially millions of economically motivated participants. Those records will be available until every participant goes offline. In other words,

⁹ See *infra* Attachment 1, *What are Appcoins?*

¹⁰ See, e.g., Cade Metz, "Overstock Begins Trading its Shares via the Bitcoin Blockchain" *Wired* (Dec. 2016) <https://www.wired.com/2016/12/overstock-com-issues-stock-via-bitcoin-blockchain/>.

¹¹ See, e.g., Adam Kissack, *Utility Settlement Coin: A Pioneering Form Of Digital Cash* (Sep. 2017) <https://www.clearmatics.com/utility-settlement-coin-pioneering-form-digital-cash/>.

¹² See, e.g., Laura Shi, "The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project" *Forbes* (Feb. 2017) <https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#4b232e1f4dcd>.

they will likely always be available. Additionally, those records will have fidelity unless every participant has their individual computer hacked and compromised. In other words, they will likely always have perfect fidelity. It's this revolutionary architecture that makes these systems effectively unhackable, at least using traditional methods of attack.

Especially pertinent to today's hearing, these technologies have also been employed for capital formation.¹³ Scarce tokens like bitcoin and ether already exist in the world and are used as currencies or to obtain computing resources and services from the decentralized networks that power them. Other scarce tokens, however, are merely theoretical, because the software that will enable them has yet to be built. Recently, various developers have raised money to fund the development of their new blockchain software projects, by selling a promise of future scarce tokens to willing investors in a so-called initial coin offering or "ICO." The pitch is simple: If you give me money today, I'll give you a blockchain token in the future that will be redeemable for valuable computing services.

From a regulatory standpoint there is a fundamental distinction to be made between, on the one hand, scarce tokens that exist today and are used for payment or to obtain computing services, and, on the other hand, *promises* of future scarce tokens that represent the hopefully profitable efforts of a developer. The former (things like bitcoin and ethereum) are effectively digital commodities: scarce items that may have value on open markets as money, investments, or inputs for valuable commercial and industrial processes. They are commodities, just digital.

¹³ By some estimates, ICOs raised a cumulative \$5.6 billion last year for early stage blockchain software companies. See Fabric Ventures and Token Data, *The State of the Token Market* (Jan. 2018) <https://static1.squarespace.com/static/5a19eca6c027d8615635f801/t/5a73697bc8302551711523ca/1517513088503/The+State+of+the+Token+Market+Final2.pdf>.

The latter, tokens promised in so called initial coin offerings, are securities: promises from issuers to investors that efforts will be put forward to create a profitable enterprise.¹⁴

Both have investor protection risks, but distinct risks that are best addressed in different ways. A commodity-like token has no issuers upon whom investors rely, but it trades on speculative spot markets. Policing these markets for fraud and market manipulation is critical for investor protection. A promise of future tokens is a security with an issuer upon whom investors rely. Mandating accurate risk disclosures and transparency from these issuers is critical for investor protection. The sensible and emerging investor protection regime is nothing new even though the underlying assets may seem like science fiction: it is the existing investor protection authority of the CFTC to supervise commodities derivatives markets and police spot markets for fraud and manipulation,¹⁵ in conjunction with the existing authority of the SEC to mandate disclosure from issuers making public securities offerings.¹⁶

Where there are frictions and a mismatch between new technologies and old regulatory structures, is state-by-state money transmission regulation. Today, commodity-like token spot markets, known generally as cryptocurrency exchanges, are in some states regulated as money transmitters like Western Union or Paypal. This is not ideal for entrepreneurs because

¹⁴ For a comprehensive look at why some cryptocurrencies and tokens likely don't qualify as securities under the relevant legal tests while others do qualify as securities, see Attachment 2, *Framework for Securities Regulation of Cryptocurrencies*.

¹⁵ “[T]he CFTC DOES have enforcement jurisdiction to investigate through subpoena and other investigative powers and, as appropriate, conduct civil enforcement action against fraud and manipulation in virtual currency derivatives markets and in underlying virtual currency spot markets.” Chairman J. Christopher Giancarlo, *Written Testimony of Chairman J. Christopher Giancarlo before the Senate Banking Committee, Washington, D.C. (Feb. 2018) available at <http://www.cftc.gov/PressRoom/PressReleases/opagiancarlo37>*.

¹⁶ “There should be no misunderstanding about the law. When investors are offered and sold securities – which to date ICOs have largely been – they are entitled to the benefits of state and federal securities laws and sellers and other market participants must follow these laws.” Chairman Jay Clayton, *Chairman Jay Clayton Testimony before the Senate Banking Committee on Virtual Currencies: The Roles of the SEC and CFTC (Feb. 2018) available at <https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission>*.

obtaining money transmission licenses from 53 states and territories is costly and duplicative. This is also not ideal for consumers or investor protection, because money transmission regulation focuses only on the risks of custodial customer funds while in transmission, not in running highly liquid markets in commodity-like assets. As Chairman Giancarlo and Chairman Clayton have both suggested, it may be time to revisit the wisdom of a state-by-state approach.

¹⁷ A federal solution might be desirable both to reduce barriers to entry and enhance competition amongst exchanges, and also to better protect investors.

Thank you and I look forward to your questions.

¹⁷ “[C]onsideration should be given to shortcomings of the current approach of state-by-state money transmitter licensure that leaves gaps in protection for virtual currency traders and investors. Any proposed Federal regulation of virtual currency platforms should be carefully tailored to the risks posed by relevant trading activity and enhancing efforts to prosecute fraud and manipulation. Appropriate Federal oversight may include: data reporting, capital requirements, cyber security standards, measures to prevent fraud and price manipulation and anti-money laundering and ‘know your customer’ protections. Overall, a rationalized federal framework may be more effective and efficient in ensuring the integrity of the underlying market.” Chairman J. Christopher Giancarlo, *Written Testimony of Chairman J. Christopher Giancarlo before the U.S. Senate Agriculture, Nutrition, and Forestry Committee, Washington, D.C.* (Feb. 2018) available at <http://www.cftc.gov/PressRoom/PressReleases/opagiancarlo38>. See also Chairmen Jay Clayton and J. Christopher Giancarlo, “Regulators Are Looking at Cryptocurrency” *Wall Street Journal* (Jan. 2018) <https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363>.

Attachment 1:

Peter Van Valkenburgh and Jerry Brito, “What are Appcoins?” *Coin Center* (Oct. 2016)

What are Appcoins?

Cryptocurrencies and open blockchain networks have created a new way to raise money to develop and maintain novel products and services—whether devices on the Internet of Things, new cloud services on the Internet, or even financial products and investments. This is an unprecedented form of crowdfunding that may raise various legal and policy questions. Developers and investors are eager to have answers to these questions so that they can safely take advantage of this innovative model.

How It Works

Let’s take a common web service as an example: cloud storage. The traditional model for building this service is Dropbox, which allows users to pay Dropbox a monthly fee to store their files on the company’s Internet-connected hard drives so that the files can be available anywhere. Dropbox is a private company that raised money from private investors to finance the development of the service, and the service is built on private company-owned infrastructure (e.g. server farms) that connects to the open Internet.

Two things can be different than this traditional model when an open blockchain network is employed. (1) Developers get paid differently. Instead of raising money from investors, developers can use a blockchain to keep track of a scarce token, sometimes called an “appcoin” (short for application coin). Developers can sell or give away that token to people who want to use the storage service or those who want to support its development. The sale of these tokens can finance the development or maintenance of the service, and that sale can happen before, during, or after the development of the service. (2) The service is peer-to-peer. The users of the cloud storage service, themselves, comprise the infrastructure that powers the service (there is no server farm) and individual users can be rewarded for their contributions to that infrastructure (e.g. the spare space on their individual Internet-connected hard drives) with the token.

These Tools Offer a New Way to Fund Open Platforms

A closed platform for messaging (e.g. Apple’s iMessage or Google’s Hangouts) only allows users to message other registered users of the service while an open platform (e.g. email or SMS text messaging) allows users to message anyone with an Internet- or cellular-connected device. With closed platforms necessary software may be proprietary, access may come with a fee, and various services may not interoperate (e.g. music purchased on iTunes can not be moved to Google Play if the user decides to switch from one music store platform to the other). A

traditional company, once built, may not have a motivation to open up their platform.

Open platforms have proved difficult to create because it has been historically difficult to monetize them even if they become successful—by nature they are public goods. Now, however, the developers of a cloud storage service can incorporate a scarce access-token, an appcoin, into the design, distribute that token to users, retain some amount of the token for themselves, and if the platform proves popular, the token (alongside the holdings of the developers) will grow in value and remunerate the developers for providing a public good. This new model challenges the concept of equity as traditionally understood, and carries entirely different risks and rewards.

Appcoin Crowdfunding is Happening Now

Developers of these services and their potential investors are already moving to take advantage of these new opportunities. Services for cloud storage are being developed by [IPFS](#), [Storj](#), [Swarm](#), and may be supported by tokens (Filecoin, Storjcoin, or Ether respectively). Services for cloud computing power are being developed by [Ethereum](#), [Counterparty](#), and others, while utilizing tokens (Ether and XCP respectively). Services for content-curation and attribution are being developed by [Steemit](#), [Mediachain](#), and others (some, like Steemit, are already supported by a token, others are not but may wish to include tokens in the future). This list is incomplete and new projects and new developers emerge weekly. Simultaneously, investors interested in helping finance applications built on open networks have begun looking at whether they can buy and hold tokens rather than take ownership interests in the firms developing these networks.

Attachment 2:

Peter Van Valkenburgh, "Framework for Securities Regulation of Cryptocurrencies" *Coin Center* (Jan. 2016).

Omitted from Print Copy to Save Paper. Please see electronic copy or visit:
<https://coincenter.org/entry/framework-for-securities-regulation-of-cryptocurrencies>