



March 14, 2016

TO: Members, Subcommittee on Commerce, Manufacturing, and Trade

FROM: Committee Majority Staff

RE: Hearing entitled “The Disrupter Series: Digital Currency and Blockchain Technology.”

I. INTRODUCTION

On March 16, 2016, at 11:00 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing entitled “The Disrupter Series: Digital Currency and Blockchain Technology.”

II. WITNESSES

The Subcommittee will hear from the following witnesses:

- John A. Beccia III, General Counsel and Chief Compliance Officer, Circle Internet Financial (on behalf of the Electronic Transactions Association);
- Jerry Brito, Executive Director, Coin Center;
- Jerry Cuomo, Vice President Blockchain Technologies, IBM;
- Matthew Roszak, Chairman, Chamber of Digital Commerce, and Co-Founder, Bloq. Inc.;
- Paul Snow, Chief Architect, Factom;
- Juan Suarez, Counsel, Coinbase; and,
- Dana Syracuse, Counsel, BuckleySandler LLP.

III. BACKGROUND

A. Introduction

Blockchain technology, or distributed ledger technology, generally refers to a protocol that allows peer-to-peer transfer of assets over the Internet.¹ Today, trusted entities are

¹ “Blockchain: Enigma. Paradox. Opportunity” Deloitte LLP, <http://www2.deloitte.com/uk/en/pages/innovation/articles/blockchain.html>. See <http://blog.kpmg.lu/luxembourg-becomes-living-lab-for-blockchain-testing/>; “Simply put, a blockchain is a distributed ledger that maintains a

responsible for verifying and validating transactions online. The disruptive component of blockchain technology is that its core functionality depends on the creation of an immutable ledger of all activity across peer-to-peer transactions for the first time.²

Simply, a blockchain, or distributed ledger, is made up of “blocks” of information tied together cryptographically (i.e. mathematically) one after another for the world to see, but allowing what is inside the block to be protected. The railroad system is another analogy used to describe the relationship between blockchain technology and an application, such as Bitcoin. In this analogy, the blockchain is the network of tracks that connect the system participants, and the Bitcoins are transferred over the blockchain in “blocks” of information. Put another way: “[P]rogrammers can develop alternative protocols on top of the [blockchain] protocol in the same way that the Web and email are run on top of the Internet’s TCP/IP protocol.”³

There are six common features of all blockchains, whether they are public, permissioned, or hybrid systems:⁴

- The blockchain is distributed in real-time between participants in a peer-to-peer network, generally without a centralized authority permitting transactions.
- Authentication and verification of a new entry to the blockchain is determined by consensus of the network to prevent the same digital asset from being duplicated (i.e. double-spent).
- The veracity of the ledger is mathematically provable through the use of cryptography⁵ and digital signatures.⁶
- It is difficult to change historical records, or previous blocks, in the blockchain. The rules for a particular blockchain system determine how difficult this is to achieve.⁷
- Transactions on the blockchain are time stamped.
- Blocks within the blockchain are programmable—allowing future conditions to trigger activity once a block is placed on the blockchain without further action by the user.

continuously growing list of data records that are hardened against tampering and revision, even by operators of the data store’s nodes.”

² *Supra* note 1 at 7.

³ Jerry Brito and Andrea Castillo, “Bitcoin, A Primer for Policymakers,” the Mercatus Center at George Mason University, December 19, 2013, <https://coincenter.org/2013/08/bitcoin-primer-policymakers>.

⁴ *Id.*

⁵ The Economist has put together a helpful diagram explaining “hashing” and how this technique is combined in a cryptographic puzzle that secures the blockchain from tampering. “The great chain of being sure about things” The Economist, October 31, 2015, <http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable>

⁶ While some focus on how blockchains, like Bitcoin, allow for anonymous, or pseudonymous, transactions to occur, the points of entry and exit, i.e. wallets and exchanges, for individuals to use government-backed currencies allow for more information about a transaction to be determined in criminal investigations.

⁷ In the Bitcoin blockchain, one would have to control more than 50 percent of the network at the same time to theoretically change the blockchain. There are reports that this 50 percent threshold was almost reached in 2014 but because of the economic incentives for miners not to destroy all users trust in the system, this control was disseminated quickly. See <http://www.foxnews.com/tech/2014/06/17/bitcoin-faces-previously-unimaginable-threat-takeover-by-pool-miners.html>.

There are several versions of distributed ledgers that may be leveraged by a company working on developing business or consumer applications on top of a blockchain. The main differences between blockchain systems are how many copies of the ledger are created, who controls the copies of the ledger, and how is the authenticity of the ledger verified. The Bitcoin blockchain is a public blockchain because records of the ledger are shared with the entire network without any centralized control over who can enter the network or verify transactions through the mining process. Other blockchains may be developed that limit who may access the network or who validates a user's ability to interact with the system, otherwise referred to as permissioned blockchains.⁸

The most developed and well-known blockchain application is the digital cryptocurrency Bitcoin.⁹ However, the potential of blockchain technology to disrupt sectors including international financial transaction clearing and settlement, health care records management, manufacturing supply chain management, real estate records, and government functions is driving a surge of interest from a variety of players.¹⁰ To date, there is an estimated \$1 billion in venture capital funding for companies in this space.¹¹

According to an analysis by the World Economic Forum “[t]he greatest potential for cryptocurrencies may be to radically streamline the transfer of value, rather than as store of value” and “decentralized payment schemes leverage cryptographic protocols to transfer value virtually in a secure, low cost, near-instantaneous manner.”¹² The immediate applications for this technology are manifesting themselves in transactions that require multiple authentication and verification steps to establish trust including international money transfers.¹³

When all of the potential applications are taken into consideration and compared to the development of other groundbreaking technologies, blockchain technology is still in its infancy. The ban on commerce over the Internet was not lifted until 1991 by the National Science Foundation.¹⁴ The original whitepaper describing the open source software platform, now known as Bitcoin, was published in 2008.¹⁵

⁸ Appendix 1 is a distributed ledger taxonomy flowchart to further explain the distinctions.

⁹ FAQ, <https://bitcoin.org/en/faq#what-is-bitcoin>.

¹⁰ See Robert McMillan, “IBM Bets on Bitcoin Ledger” Wall Street Journal, February 16, 2016, <http://www.wsj.com/articles/ibm-bets-on-bitcoin-ledger-1455598864?cb=logged0.3160805300197209>; Sir Mark Walport, U.K. Government Chief Scientific Adviser “Distributed Ledger Technology: beyond block chain” <https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain>.

¹¹ Jose Pagliery “Record \$1 billion invested in Bitcoin firms so far” CNN Money, November 3, 2015, <http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested/>.

¹² “The Future of Financial Services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed.” World Economic Forum, June 2015, p. 15, 45, http://www3.weforum.org/docs/WEF_The_future_of_financial_services.pdf

¹³ *Id.* at 44.

¹⁴ <http://money.howstuffworks.com/history-e-commerce1.htm>

¹⁵ “An Abridged History of Bitcoin” The New York Times, updated November 19, 2013, http://www.nytimes.com/interactive/technology/bitcoin-timeline.html?_r=0. (The final entry of this piece does not reflect the current price of a Bitcoin, which is closer to \$400 today.)

B. Bitcoin

Bitcoin is one of the best known digital currencies and is illustrative of how the digital currency system works. As of March 7, 2016, there were 15.3 million Bitcoin in circulation with a trading value of \$419.09 per Bitcoin.¹⁶ Anyone with an Internet connection can download a Bitcoin wallet app on their computer or mobile phone. The wallet app connects to a Bitcoin exchange that allows the user to purchase Bitcoin for dollars, euros, or other government-backed currency. The user must open an account with the wallet provider, which is a key point in the transaction for regulators focusing on “know your customer” and anti-money laundering regulations.

Once a user has Bitcoin in their wallet account, they are able to hold the digital currency or spend it where Bitcoin are accepted. Overstock.com accepts Bitcoin for online purchases and the Sacramento Kings will accept Bitcoin for tickets, merchandise, and even concessions inside the arena.¹⁷ Several companies, including Coinbase and Stripe, are offering merchant services for businesses interested in accepting Bitcoin on their e-commerce websites.¹⁸

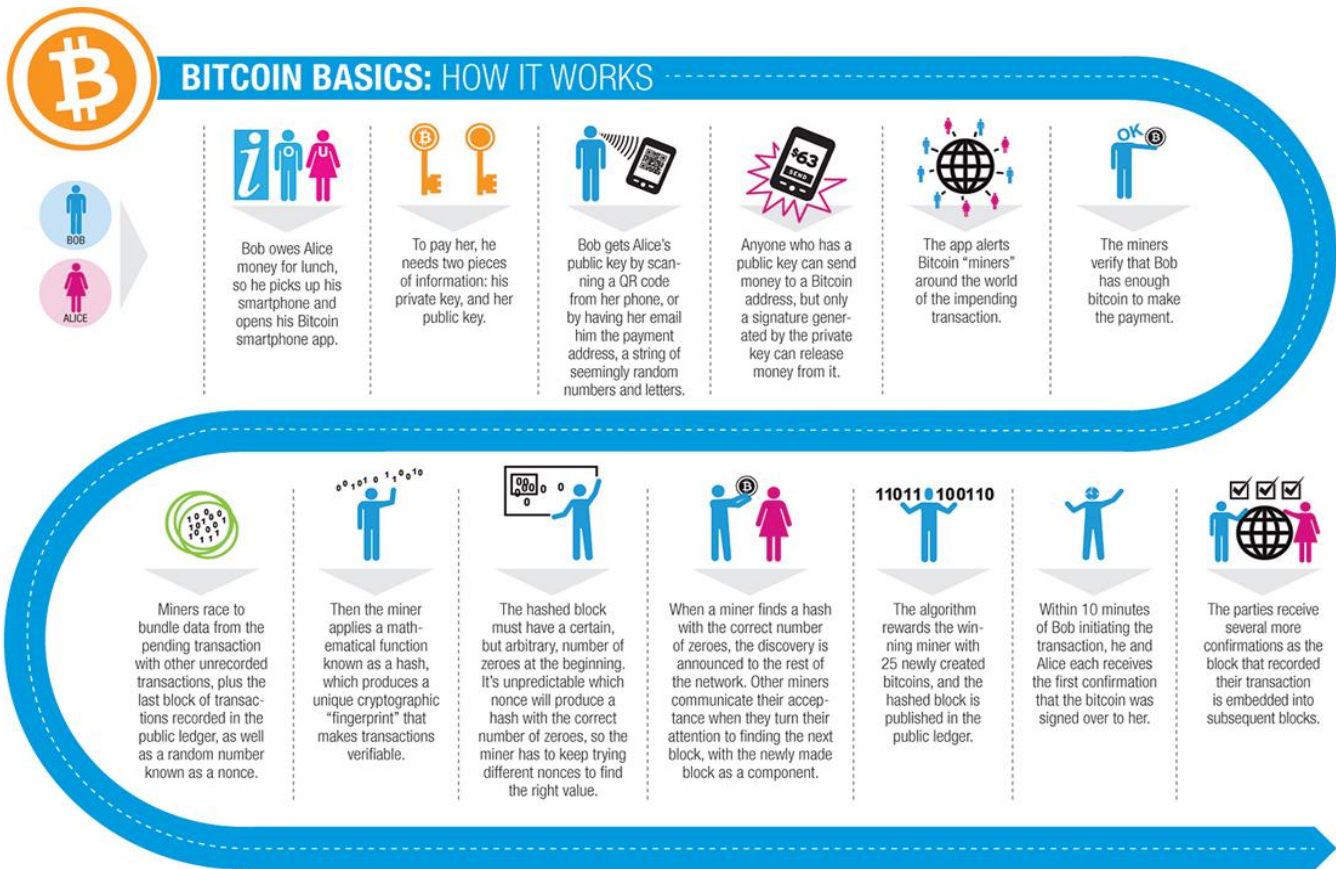
The following diagram explains a Bitcoin transaction:¹⁹

¹⁶ <http://www.coindesk.com/data/bitcoin-total-circulation/> (last accessed March 11, 2016).

¹⁷ <http://www.wsj.com/articles/SB10001424052702304603704579323352532979922>.

¹⁸ <https://stripe.com/Bitcoin>

¹⁹ Marc Hachstein “Why Bitcoin Matters For Bankers” American Banker, March 11, 2016
http://www.americanbanker.com/magazine/124_02/why-bitcoin-matters-for-bankers-1065590-1.html.



The Federal Reserve Bank of Chicago published a primer in 2013 noting “Bitcoin solves two challenges of digital money—controlling its creation and avoiding its duplication—at once.”²⁰ Consumers generally interact with Bitcoin through an exchange that allows the consumer to exchange government-backed currency for cryptocurrencies, including Bitcoin.²¹ The exchanges provide a variety of services, including an easy to use customer interface and private key management.²²

As shown in the figure above, the economic incentive of the mining activity and the miners’ ability to solve the cryptographic puzzles necessary to add another block of transactions to the chain is a key element to its virtue. This process occurs once every 10 minutes and the miner that solves the puzzle is awarded with Bitcoin.²³ The Bitcoin blockchain was written limiting the universe of potential Bitcoin to 21 million and Bitcoin are divisible into units call satoshi.²⁴ Therefore, while the amount of Bitcoin miners are rewarded with is decreasing, the

²⁰ <https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317>.

²¹ See <http://bitcoinexchangeguide.com/>. Major exchanges include Bitstamp, Coinsetter, Coinbase, BTC-e, and Cryptsy.

²² *Id.*

²³ *Supra* note 17.

²⁴ See <http://www.btcsatoshi.com/>.

prevalence of transactions fees that can be attached to a transaction for the miner that “solves the block” fastest is increasing.²⁵

As well as fueling over \$1 billion in venture capital investment in various iterations of blockchain technology, Bitcoin has faced challenges. In August 2015, Mark Karpeles, the CEO of Mt Gox, a bitcoin exchange, was arrested in Japan for embezzlement after allegations surfaced that he “manipulated Mt Gox’s volumes” that resulted in the loss of an estimated \$350 million in Bitcoin.²⁶ The circumstances of how the Mt Gox bitcoin exchange shut down are not clear. This incident was noteworthy because at one point Mt Gox reportedly controlled around 80 percent of Bitcoin trading value. During a bankruptcy proceeding Karpeles acknowledged that 750,000 Bitcoins the company held for users are still missing.²⁷

Money laundering and terrorism financing concerns have been raised with virtual currencies, including Bitcoin, that allow for anonymous, or pseudonymous, transactions to occur. However, the value proposition of these digital currencies is that all transactions are recorded and immutable, which provides a tool to law enforcement that does not exist in the physical world with cash transactions.²⁸ A discussion of the Department of Justice’s activity in this area is included below.

C. Other blockchain applications

While Bitcoin was the first application that used blockchain technology in the market, other major firms have begun investing in the technology.²⁹ For example, on its existing cloud platform, Microsoft provides a “Blockchain-as-a-Service” product that allows organizations to leverage private or semi-public blockchains using their choice of blockchain protocols (i.e. Bitcoin, Ripple, Ethereum, etc.) without having to set up their own network.³⁰ As a result, there is much development across two fronts – developing blockchain technologies and developing applications to run on top of existing blockchains.

The basic characteristics of the blockchain also present the potential to address some long standing issues in intellectual property, health care, supply chain management, identity management, energy exchanges, property rights, and smart contracts. For example, last year the

²⁵ *Supra* note 17.

²⁶ <http://www.coindesk.com/mt-gox-the-history-of-a-failed-bitcoin-exchange/>

²⁷ *Id.*

²⁸ See Testimony of Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, United States Senate Committee on Homeland Security and Governmental Affairs, “Beyond the Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies” November 18, 2013.

<http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies>.

See Jerry Brito and Andrea Castillo “Bitcoin: A Primer for Policymakers” Mercatus Center at George Mason University, December 19, 2013, <https://coincenter.org/2013/08/bitcoin-primer-policymakers/>.

²⁹ *Supra* note 10.

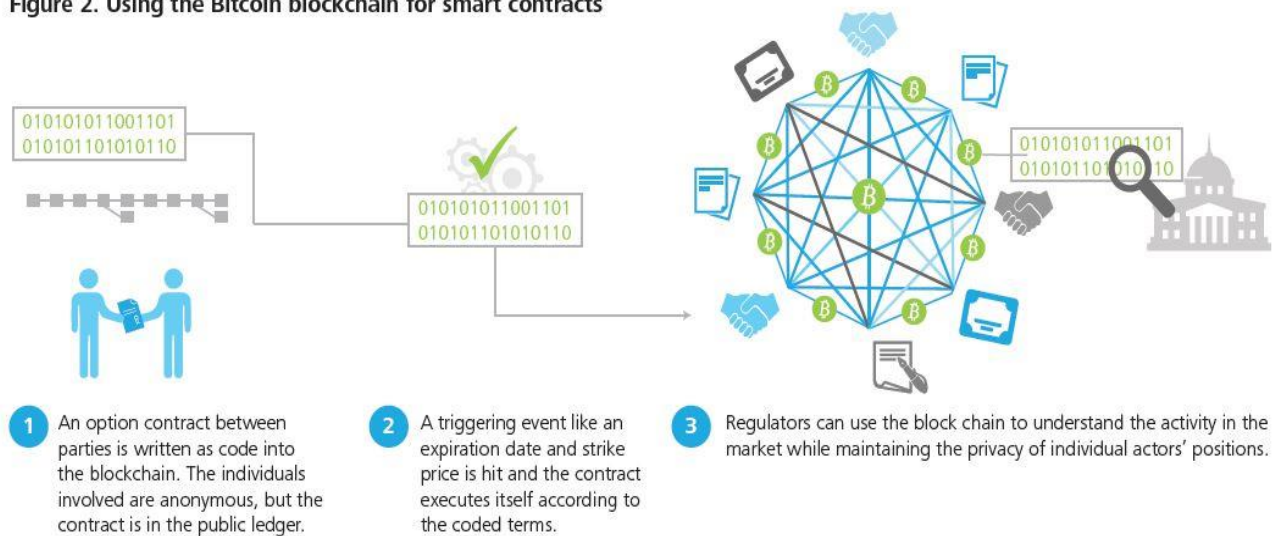
³⁰ *Supra* note 1 at 7.

company Ascribe raised \$2 million in venture capital based on the premise that blockchain allows artists to own digital art in the same way individuals can own Bitcoin today.³¹

Another company, Slock, allows an owner to rent out property by posting rental information on the blockchain, and once a renter pays via the blockchain they are able to open and close the smart lock on the front door with his phone without a middleman.³² This technology is moving quickly to applications in the Internet of Things (IoT).³³ Indeed the distributed nature of IoT and the blockchain could lead to a myriad of applications.

The follow diagram demonstrates how the Bitcoin blockchain could be used for smart contracts:³⁴

Figure 2. Using the Bitcoin blockchain for smart contracts



Graphic: Deloitte University Press, DUPress.com

The future of blockchain technology is by no means certain at this stage. There is a robust debate about the role of the public Bitcoin blockchain, and the development of private or permissioned blockchains for backend business operations, and some hybrid that leverages the benefits of each protocol.

D. Government Perspectives and Oversight

³¹ John Biggs “Ascribe Raises \$2 Million To Ensure You Get Credit For Your Art” Tech Crunch, June 24, 2015, <http://techcrunch.com/2015/06/24/ascribe-raises-2-million-to-ensure-you-get-credit-for-your-art/>.

³² <https://slock.it/>. See Paul Levy “Finally, interesting uses for the blockchain that go beyond bitcoin” Phys.org, December 7, 2015, <http://phys.org/news/2015-12-blockchain-bitcoin.html> and <https://www.quora.com/What-are-non-Bitcoin-applications-of-blockchain-technology>.

³³ Later this month at a conference in Hannover, Germany, Slock.it is demonstrating a new prototype to charge cars. <https://slock.it/>

³⁴ “Blockchain: Enigma. Paradox. Opportunity” Deloitte LLP, <http://www2.deloitte.com/uk/en/pages/innovation/articles/blockchain.html>

1. International Perspectives

Several countries have expressly engaged in an evaluation of the potential benefits and risks of blockchain technology and have encouraged entities within their own governments to evaluate potential use cases for the technology. One of the leading reports was published by the United Kingdom Government Chief Scientific Adviser and it expressly encouraged departments within the government to explore unlocking “the full potential of this technology.”³⁵ Uses cases highlighted in the UK report include financial markets, supply chains, consumer and business-to-business services, and publicly-held registers.³⁶ A number of other governments have engaged and invested in this space.³⁷ Last November, the Estonian government announced a public notary service for e-residents.³⁸

2. U.S. Federal Enforcement Actions and Regulations

A number of Federal enforcement agencies and regulators are engaged in oversight of virtual currencies and general consumer protection for financial transactions, including the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), the Securities and Exchange Commission (SEC), the Financial Crimes Enforcement Network (FinCEN), the Internal Revenue Service (IRS),³⁹ the Commodity Futures Trading Commission (CFTC), the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), the Conference of State Bank Supervisors, and the Uniform Law Commission.

The FTC has brought two enforcement cases against companies in the Bitcoin industry applying traditional consumer protection principles.⁴⁰ In the most recent settlement with Butterfly Labs, Inc., the FTC’s Director of the Bureau of Consumer Protection stated “[e]ven in the fast-moving world of virtual currencies like Bitcoin, companies can’t deceive people about their products.”⁴¹ The allegations against Butterfly Labs centered around the company’s delivery date promises for Bitcoin mining machines to individual consumers when the machines had already been paid for. The computing power necessary to conduct mining operations has exponentially increased over the last few years, and Butterfly Labs’ failure to deliver mining

³⁵ Sir Mark Walport, U.K. Government Chief Scientific Adviser “Distributed Ledger Technology: beyond block chain” <https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain>.

³⁶ See also Ian Allison “Security firm Guardtime courting governments and banks with industrial-grade blockchain” International Business Times, January 4, 2016, <http://www.ibtimes.co.uk/security-firm-guardtime-courting-governments-banks-keyless-blockchain-1535835>.

³⁷ <https://bitcoinmagazine.com/articles/estonian-government-partners-with-bitnation-to-offer-blockchain-notarization-services-to-e-residents-1448915243>

³⁸ *Id.*

³⁹ <https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance>

⁴⁰ See <https://www.ftc.gov/news-events/press-releases/2016/02/operators-bitcoin-mining-operation-butterfly-labs-agree-settle>

⁴¹ *Id.*

machines, or delivery delay for a year or more, fundamentally changed the functionality of the mining machines, rendering them far less valuable for the consumer.⁴²

In 2014, the FTC and CFPB issued separate consumer advisories about virtual currencies and both agencies accept consumer complaints relating to the virtual currency product or service.⁴³

The Department of Justice has testified about its enforcement work with respect to virtual currencies acknowledging “that many virtual currency systems offer legitimate financial services and have the potential to promote more efficient global commerce”; however, [a] convertible virtual currency with appropriate anti-money laundering and know-your-customer controls, as required by U.S. law, can safeguard its system from exploitation by criminals and terrorists in the same way any other money services business could.”⁴⁴ Money transmitters, which include many virtual currency systems and exchanges, are required under 31 U.S.C. § 5330 to register with FinCEN.⁴⁵ General money laundering and spending statutes have been interpreted by the Department of Justice to cover financial transactions involving virtual currencies, and they have successfully prosecuted several cases involving virtual currencies.⁴⁶

3. State Activity

States activity has generally been centered on virtual currencies and the application of existing money transmission licensing requirements. New York, Connecticut, North Carolina, New Hampshire, Kansas, Texas, and Washington have made policy announcements regarding the application of money transmission laws to virtual currency. California and New Jersey are considering proposals that would impose varying levels of regulation on the virtual currency market.

California, Kentucky, Minnesota, Missouri, New Jersey, New York, Washington, and Wisconsin have also made statements regarding the applicability of State tax law to virtual currency.⁴⁷

The most comprehensive proposal that has been finalized was last year in New York with the creation of its BitLicense regulations.⁴⁸ The BitLicense covers “virtual currency business activity” which includes transmitting, storing, holding, maintaining control of virtual currency; buying and selling virtual currency as a customer business; performing exchange services as a

⁴² *Id.*

⁴³ <https://www.consumer.ftc.gov/blog/staying-current-bitcoin-and-other-cryptocurrencies>;
<http://www.consumerfinance.gov/blog/consumer-advisory-virtual-currencies-and-what-you-should-know-about-them/>

⁴⁴ *Supra* note 25 at 1.

⁴⁵ Failure to register with FinCEN or obtain the appropriate state license(s) may be criminally prosecuted under 18 U.S.C. § 1960.

⁴⁶ *Supra* note 25 at 3-5 (E-Gold, Liberty Reserve, and Silk Road). See 18 U.S.C. §§ 1956 and 1957.

⁴⁷ http://www.ncsl.org/documents/task_forces/Waterfield_Virtual_Currency_2015.pdf at 26-40.

⁴⁸ New York State Department of Financial Services “Virtual Currencies” Title 23, Chapter I, Part 200
http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf.

customer business; or controlling, administering, or issuing a virtual currency.⁴⁹ It has been reported that after the finalization of the BitLicense regulations, several Bitcoin companies stopped operating in New York.⁵⁰

IV. ISSUES

The following issues may be examined at the hearing:

- What applications of this technology are most likely to impact consumers and jobs in the near term and the long term?
- What does the regulatory environment look like for Bitcoin and other blockchain applications? What hurdles exist for widespread industry or consumer adoption for blockchain applications, including Bitcoin?
- How has Bitcoin disrupted the traditional payments landscape? How could blockchain technology disrupt non-financial sectors of the economy? What use cases exist for non-financial blockchain applications?
- What benefits and risks exist for consumer information security with wider adoption of the blockchain?
- What privacy considerations should be examined for consumers using digital currency or other blockchain applications? Are there special considerations for financial applications, including Bitcoin?

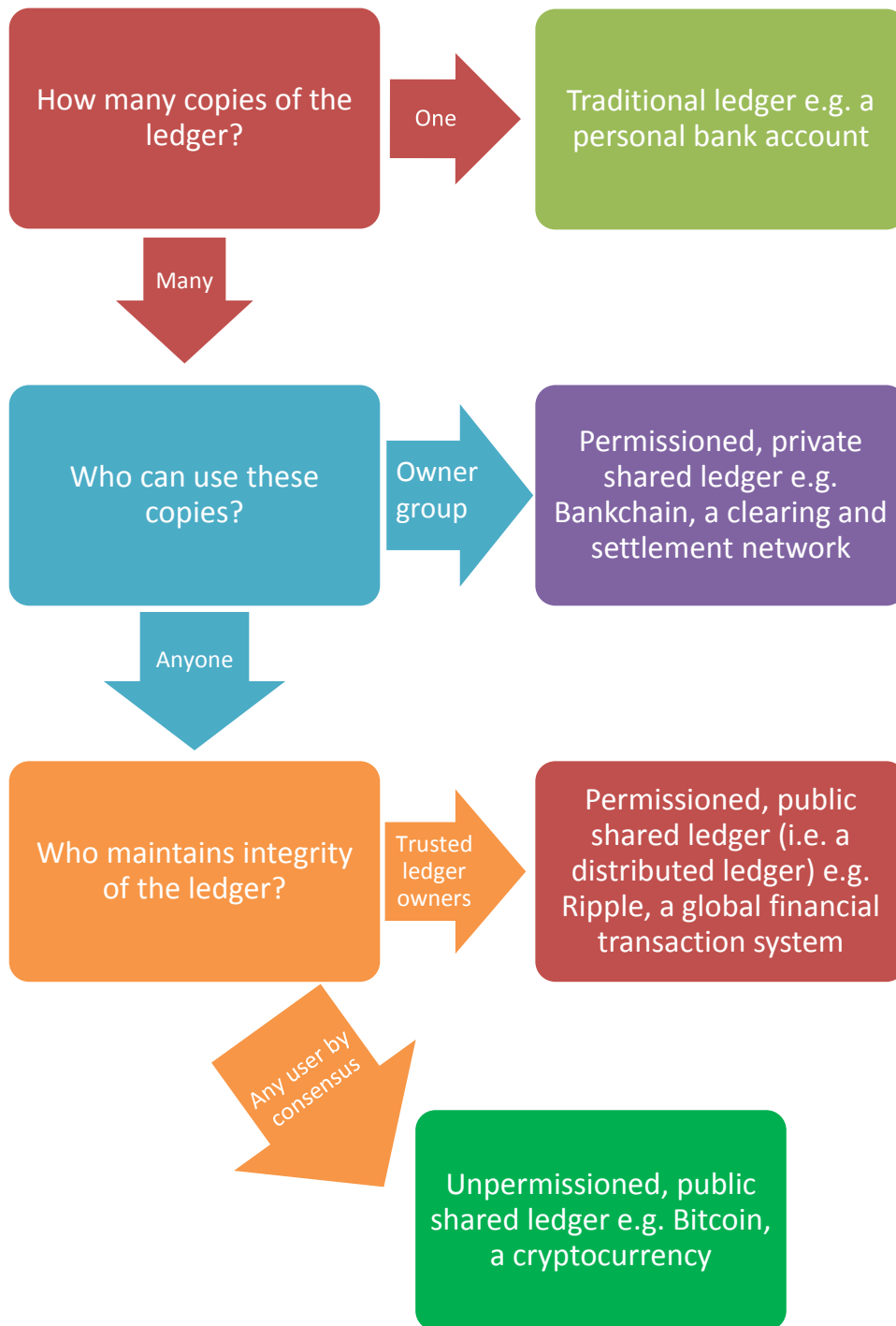
V. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Paul Nagle or Melissa Froelich of the Committee staff at (202) 225-2927.

⁴⁹ *Id.* at 6.

⁵⁰ Yessi Bello Perez “The Real Cost of Applying for a New York BitLicense” CoinDesk, August 13, 2015, <http://www.coindesk.com/real-cost-applying-new-york-bitlicense/>.

Appendix 1
Distributed Ledger Taxonomy⁵¹



⁵¹ Sir Mark Walport, U.K. Government Chief Scientific Adviser “Distributed Ledger Technology: beyond block chain” Figure courtesy of Dave Birch (Consult Hyperion), p. 19 <https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain>.