

Framework for Securities Regulation of Cryptocurrencies

Version 2
Peter Van Valkenburgh
August 2018

Coin Center Report



COIN CENTER

coincenter.org

Peter Van Valkenburgh, *Framework for Securities Regulation of Cryptocurrencies v2.0*, Coin Center Report, Aug. 2018, available at <https://coincenter.org/entry/securities-framework/>

Abstract

This report presents a framework for securities regulation of cryptographic assets, cryptocurrencies, and so-called tokens, including—e.g. Bitcoin, Ethereum, and derivative projects. The framework is based on the Howey test for an investment contract, as well as the underlying policy goals of securities regulation. We find that three key variables within the software of a token project and the community that runs and maintains that software are indicative of investor or user risk: distribution, decentralization, and functionality. These variables are explained in depth and mapped to the four prongs of the Howey test in order to create a framework for determining when a cryptocurrency resembles a security and might therefore be regulated as such. We find that larger, more decentralized token projects—e.g. Bitcoin—and functional decentralized computing services—e.g. Ethereum—do not easily fit the definition of a security and also do not present the sort of investor risk best addressed through securities regulation. We do find, however, that several smaller, questionably marketed or designed tokens may indeed fit that definition. We also discuss how pre-sales of tokens may be securities issuance even if the resultant token, once built, and the subsequent trading of that token, may not benefit from securities regulation.

Author

Peter Van Valkenburgh
Director of Research
Coin Center
peter@coincenter.org

About Coin Center

Coin Center is a non-profit research and advocacy center focused on the public policy issues facing open blockchain technologies such as Bitcoin, Zcash, 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 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.

Credits

Thank you to Kathleen Moriarty, Gregory Xethalis, and Jason Somensatto for taking the time to review this report and offer such valuable feedback. Additionally, thanks to Houman Shadab, Joel Dietz, and Chris Crawford whose discussion of these topics formed the genesis of this work.

Table of Contents

Introduction	3
Bitcoin, Cryptocurrencies, and Tokens: What are they to Regulators?	3
I. A Primer on Forks, New Cryptocurrencies, Tokens, and Tokens on Top of Tokens.	7
Forking Software	7
Forking Blockchains	9
Developing New Software from Scratch and Airdrops	10
Tokens on Top of Tokens	10
II. Token Project Variables that can Affect User and Investor Risk	11
A. Distribution	11
Pre-Mines and Pre-Sales (Initial Coin Offerings)	12
Proof-of-Burn	13
Airdrops	14
Sidechains	15
Private Sales	16
Traditional Capital Formation and Release by Mining or Dividend	17
Distribution and Risk	17
B. Decentralization	17
Consensus	18
Scarcity	26
Transparency	27
Abundance and Diversity of Developers and Validators	33
Profit-Development Linkage	35
C. Functionality	38
Functionality Contingent on Scarcity and Decentralization	39
Functionality Beyond Scarcity and Decentralization	40
Non-Functional Tokens	43

III. A Rubric for Securities Regulators	44
The Howey Test	44
Investment of Money	46
Distribution	46
Common Enterprise: Horizontal and Vertical Commonality	48
Scarcity	50
Decentralization	51
Profit-Development Linkage	52
Expectation of Profits	52
Distribution	52
Functionality	53
Efforts of a Third Party	53
Consensus	55
Transparency	56
General Policy Goals Based on the Howey Test	57
Chilling Innovation vs. Protecting Investors	58
Separate the Analysis for Pre-sale Agreements and Derivative Tokens	58
Conclusion	60
Appendix	60
1. The Bitcoin Mining Mechanism: Proof of Work Consensus	60
2. Digital Signatures and Bitcoin Transactions	61
3. Sidechains	62

Introduction

Bitcoin and follow-on cryptocurrencies or tokens are open source innovations. There is no gatekeeper determining who may and who may not build these networks, and modifying them or building them from scratch requires nothing more than an Internet-connected computer. This permissionless ecosystem for invention is one of the reasons we should celebrate and support the technology: it helps to break down many of the structural barriers that divide us, whether as producers and consumers, banked and unbanked, or rich and poor. The openness of the ecosystem also means that many will misuse the technology for selfish and malicious reasons. It is the goal of this report to help regulators, in particular securities regulators, identify the scams from the true innovations.

Part I of this report will give securities regulators, and anyone else interested, an overview of the large and ever expanding landscape of cryptocurrencies and derivative innovations (e.g. decentralized computing systems and tokens). Part II will break down the salient variables that could make a token look more or less like a security and the relevant risks to investors, and Part III will offer policy goals that a regulator in this space may wish to pursue. Before delving into these details, however, some background on Bitcoin and tokens generally may be helpful. Persons well-acquainted with the technology may, however, wish to skip ahead to Part II.

Bitcoin, Cryptocurrencies, and Tokens: What are they to Regulators?

It's prudent to start with a brief overview of Bitcoin. Bitcoin is the *original* cryptocurrency; the first truly decentralized network for sending and receiving value over the Internet. Since Bitcoin's invention in 2008,¹ several "forks" (modified versions) and derivative innovations have emerged. Rather than refer to these derivatives as cryptocurrencies (a limiting term that implies use as currency) we shall generally use the broader term "token" unless speaking specifically about currency-focused projects. Irrespective of terminology, the fundamentals of these new tokens can vary, and some may functionally resemble securities when marketed and sold to investors.

Cryptocurrencies and tokens, broadly, are truly innovative. That is to say, they present an arrangement of technological components that is so novel and varied as to defy categorization as any traditional asset, commodity, security, or currency.

At root, units of a cryptocurrency are scarce items that can be exchanged and may have market value despite the fact that they have no institutional issuer or legally-promised redemption. In this sense, cryptocurrencies are somewhat like valuable commodities (e.g. gold or platinum). However, unlike gold or platinum, cryptocurrencies are entirely non-tangible. That is not to

¹ 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. "Block 0" Bitcoin *Block Explorer*, (last accessed Dec, 2015) <http://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>

say, however, that they exist only in the minds or promises of men and women. In a literal sense, a bitcoin is a unique answer to a math problem and proof that you solved that problem² or else had the unique record of the solution transferred to your control.³ There are a finite number of solutions to the math problem as it has been devised,⁴ and finding those solutions takes genuine effort.⁵ This too can be analogized to a precious metal: there is a finite amount of gold to be found and effort is required to find it.

The decision to value these finite solutions and therefore make the effort to uncover them can also be analogized to gold. Men and women need not seek gold. The value placed on gold by society is largely a sort of mutually shared desire or—less charitably—illusion. We could, instead, seek platinum or silver for use as a medium of exchange, store of value, or decorative object. Similarly, those interested in cryptocurrencies could seek answers to alternative math puzzles. A particular cryptocurrency, say Bitcoin, could even change its underlying math puzzle. However, such a change would be more like the collective actions of gold miners choosing to instead mine silver, and less like a single government choosing a different asset, or no asset, to back its paper currency.

Regardless of the particular analogies used to explain the technology, regulators will continually look at *how* a token is employed, *what* work it helps a user accomplish, and they will thus classify these activities as within or without their regulatory purview. The “*how* it is employed” question will always be more significant to any regulatory policy than the abstract and metaphysical “*what* is it” question. The unintended result, however, will necessarily be a confounding cavalcade of seemingly contradictory conclusions: “bitcoin is a commodity” (*per* a 2015 CFTC ruling⁶) “bitcoin is property” (*per* IRS guidance⁷) “bitcoin is virtual currency” (*per*

² See *infra* Appendix 1. The Bitcoin Mining Mechanism: Proof of Work Consensus.

³ See *Id.*

⁴ There is no line of code in the Bitcoin reference client that specifically says, “there will only ever be 21 Million bitcoins” corresponding to some number of— what we have termed—“finite solutions to a math problem.” Instead, there is language that describes the permissible size of the reward of new bitcoins that miners who mine new blocks can claim in a coinbase transaction. This reward is referred to as a “block subsidy” and it is coded to start at 50 bitcoins per block and decrease by half on a schedule that would result in a final total supply of roughly 21 million total bitcoins at some point in the year 2140. See Bitcoin Core, “main.cpp,” <https://github.com/bitcoin/bitcoin/blob/master/src/main.cpp>, lines 1380-1391 (“Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years.”). See also “Controlled supply,” *Bitcoin Wiki*, https://en.bitcoin.it/wiki/Controlled_supply (last accessed Dec. 2015).

⁵ Mining bitcoins is a process of guess and check. The speed at which miners can make these guess and check calculations is dependent on the processing power of their hardware. Faster calculations means a greater chance you will find a solution before other miners on the network. As more computing power is leveraged by miners, blocks will be solved at a faster rate. The software is pre-programmed to retarget the difficulty of finding new blocks by requiring more or fewer leading zeros in acceptable hashes. This retargeting is based on a formula that looks at difficulty over the previous 2,016 blocks and seeks to keep the rate of new block discovery at roughly one block every 10 minutes. See “Bitcoin Difficulty Made Easy” <http://bitcoin-difficulty.com/> (last accessed Dec. 2015); “Difficulty” *Bitcoin Wiki*, <https://en.bitcoin.it/wiki/Difficulty> (last accessed Dec. 2015).

⁶ *In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan*, CFTC Docket No. 15-29 (Sep. 2015) available at

FinCEN guidance⁸) “bitcoin is money used for money transmission.” (*per* various state money transmission regulators⁹).

Compounding the complexity of this analysis is the fact that Bitcoin’s underlying blockchain—the shared ledger that lists all transactions on the network—can also be used as an irreversible public broadcast channel for any recordkeeping or recordkeeping-related purpose.¹⁰ The original and still primary use of the Bitcoin blockchain is moving scarce tokens, or to quote François Velde of the Chicago Federal Reserve, “Bitcoin is a system for securely and verifiably transferring bitcoins.” Blockchains, however, can and are beginning to be used for securely and verifiably transferring other financial assets (by, *e.g.*, Nasdaq¹¹), identity credentials (by *e.g.* Blockstack¹²), automobile loans (by *e.g.* Visa¹³), document notarizations (by *e.g.* Proof of Existence¹⁴), machine-to-machine messages on the Internet of Things (by *e.g.* IBM¹⁵), and more.

<http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf>.

⁷ *Notice 2014–21 IRS Virtual Currency Guidance*, Internal Revenue Bulletin: 2014-16 (Apr. 2014) *available at* https://www.irs.gov/irb/2014-16_IRB/ar12.html.

⁸ *Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 2013) *available at* https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

⁹ While this may not be the formal conclusion of various states now regulating bitcoin businesses, it is the basic substance: bitcoin businesses are increasingly being regulated under the same prudential framework as money transmission activities. See New York Department of State Department of Financial Services, New York Codes, Rules and Regulations Title 23. Department of Financial Services Chapter 1. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies (Jan. 2015) *available at* <http://www.dfs.ny.gov/legal/regulations/adoptions/dfs200t.pdf>; Pennsylvania House Bill 850 (March 26, 2015) *available at*

<http://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2015&sessInd=0&billBody=H&billType=B&billNbr=0850&pn=1029> (a proposed amendment to the PA money transmission law that would include virtual currencies in the definition of money). See also CSBS

¹⁰ The Bitcoin Blockchain is a public record of all bitcoin transactions (and some associated metadata) redundantly stored across all full nodes on the peer to peer network, and easily available for download. Data in that chain can be independently validated and the pseudonymous identity of the person who inserted that data can be proven (to the extent that we believe that a given Bitcoin address has a matching private key within the exclusive control of a given person).

¹¹ See Michael Casey, “A Bitcoin Technology Gets Nasdaq Test” *Wall Street Journal* (May 2015) http://www.wsj.com/article_email/a-bitcoin-technology-gets-nasdaq-test-1431296886-1MyQjAxMTE1MzEyMDQxNzAwWj

¹² “About,” *Blockstack.org* (“Blockstack uses the lower layers of the traditional internet and focuses on decentralizing the application layer. Blockstack provides key tools and infrastructure to developers enabling decentralized storage and decentralized authentication & identity.”). <https://blockstack.org/about/> (last accessed Aug. 2018).

¹³ Sophie Curtis “Visa uses bitcoin’s blockchain technology to cut paperwork out of car leasing” *The Telegraph* (Oct. 2015) <http://www.telegraph.co.uk/technology/news/11961296/Visa-uses-bitcoins-blockchain-technology-to-cut-paperwork-out-of-car-rental.html>.

¹⁴ “About” *Proof of Existence* <https://www.proofofexistence.com/about> (“Use our service to anonymously and securely store an online distributed proof of existence for any document. Your documents are NOT stored in our database or in the bitcoin blockchain, so you don’t have to worry about your data being accessed by others. All we store is a cryptographic digest of the file, linked to the time in which you submitted the document. In this way, you can later certify that the data existed at that time. This is the

And even if the Bitcoin blockchain is being used for these alternative purposes, some amount of bitcoin will always be involved in order to write to the ledger, even if it is a nominal amount.¹⁶ Within these various uses will lie some obviously regulated activities, such as platforms for trading securities, but also many generally unregulated activities, such as trading and transferring tickets to a concert or keeping records of online video views and charging for access.

As a final complication, Bitcoin is an open source innovation; its codebase can be “forked”¹⁷ in order to make derivative tokens, similarly it can be a source of inspiration for all manner of new projects. These projects may simply use the scarce, fungible, and transferrable nature of a Bitcoin-like token to represent a legal right. For example, the token may represent a claim on the issuer’s future revenue or a claim to valuable physical assets or funds that the issuer secures. Many of these issuer-backed tokens may, transparently, be securities. Other token projects seek to decentralize an online service, just as Bitcoin effectively decentralizes online money transmission, and the tokens that power these networks may more closely resemble valuable commodities used within the ecosystem

At a conceptual level, Bitcoin is a network of strangers who provide an online service — electronic money transmission and value storage. The bitcoin software (specifically its consensus mechanism) and its verifiable public ledger (the blockchain) ensure that participants perform this service faithfully, thus obviating the need for service-users to trust any particular service-provider within the network. The Bitcoin “cryptocurrency” or “token,” itself, is simply a scarce unit of value, and the blockchain is a public ledger that accounts for the global distribution and transfer of this scarce unit amongst participants. This scarce unit is algorithmically and automatically awarded to the participants based on their efforts to power

first online service allowing you to publicly prove that you have certain information without revealing the data or yourself, with a decentralized certification based on the bitcoin network.”

¹⁵ “Device democracy: Saving the future of the Internet of Things” *IBM Institute for Business Value* (July 2015) available at

http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03620USEN&attachment=GBE03620USEN.PDF

(“In our vision of a decentralized IoT, the blockchain is the framework facilitating transaction processing and coordination among interacting devices. Each manages its own roles and behavior, resulting in an “Internet of Decentralized, Autonomous Things” – and thus the democratization of the digital world.”).

¹⁶ There’s no way to write to the Bitcoin blockchain without including transaction inputs, amounts of bitcoin you control. Users hoping to add verifiable data to the blockchain can write by spending very small amounts of bitcoin. Bitcoins are divisible down to 8 decimal places.

¹⁷ This use of “fork” comes from the larger world of free and open source software development, particularly the communities developing Linux, the open source and oft-forked operating system that powers many enterprise computing systems. Forking refers to a decision amongst some developers within an open source project to duplicate the code of that project and maintain it separately in order to create some derivative invention. See Benjamin Mako Hill, “To Fork or Not To Fork: Lessons From Ubuntu and Debian” (May 2005) https://mako.cc/writing/to_fork_or_not_to_fork.html (“The act of taking the code for a free software project and bifurcating it to create a new project is called “forking.” There have been a number of famous forks in free software history. One of the most famous was the schism that led to the parallel development of two versions of the Emacs text editor: GNU Emacs and XEmacs. This schism persists to this day.”).

the service, thus incentivizing and rewarding honest participation in the open network. The scarce unit is also the medium of exchange that users of the service must obtain and then utilize in order to pay for that service. If I want to pay a friend by making a Bitcoin transaction I will need to attach a bitcoin-denominated fee to my transaction that will incentivize miners to put my transaction into the blockchain, thus indicating to the world that I've paid my friend.

That conceptual model can then be applied to other online services beyond money transmission. For example, a network of strangers organized through software and public ledgers could be incentivized to provide cloud storage services or cloud computing services, and a scarce unit inherent to that network could be used as a medium of exchange and an automatic reward for honest participants who help provide the service by offering storage or computational power to the network.

"Scarce unit" is an unwieldy phrase to say the least. Because cryptocurrency development is an open source movement, no one has the last say regarding what anyone of these things *should* be called, and several terms are used reflecting the various purposes that any particular scarce unit might service within a decentralized service, most prominently: cryptocurrency, token, or coin. These terms are used without precision and interchangeably. The particular term is immaterial as compared with the general idea represented: a scarce unit used as a medium of exchange and reward for participation amongst a network of strangers that collaborate to provide a service. Again, for the remainder of the report we shall use the term broader term "token" to describe the scarce-units in both currency-focused projects as well as non-currency focused projects.

The first section of this report will further explain "forking" and new tokens. The second section will identify distinctions amongst various types of tokens and the risks suggested by these distinctions.¹⁸ The final section will offer a rubric that securities regulators may find instructive when determining whether a particular token *is or is not being used as* a security or investment contract.¹⁹

I. A Primer on Forks, New Cryptocurrencies, Tokens, and Tokens on Top of Token Networks

Forking Software

Fundamentally, Bitcoin or any other token network is merely *software* running across a *network of peers*²⁰ that creates and maintains a *shared ledger*²¹ accounting for holdings of a *scarce token*.²²

¹⁸ See *infra* at p.11.

¹⁹ See *infra* at p. 44.

²⁰ The Bitcoin network is built to work within the existing Internet protocol suite. It uses a peer-to-peer structure to broadcast transaction messages through the connected computers of Bitcoin users. See Joseph Bonneau, Andrew Miller, et al. "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies" IEEE Security & Privacy (2015), <http://www.jbonneau.com/doc/BMCNKF15-IEEEESP-bitcoin.pdf>

²¹ This "shared ledger" is a database of all past bitcoin transactions, it is referred to as "the blockchain." See *Id.* at 3.

Bitcoin's network software is open source, so it can be duplicated and modified without seeking a license from the copyright holder.²³ Most other token networks also utilize open source software, meaning that they too can be copied and modified to create derivative innovations. These modifications can result in software that remains compatible with the parent network or ceases to be compatible. Changes that do not break compatibility are sometimes referred to as changes to the software's *policy rules*. Changes that do break compatibility will necessarily be changes to the software's *consensus rules*—referring to the rules upon which the entire network must agree.

An example of a *policy* rule could be: refuse to relay transactions sending less than a certain amount of bitcoin.²⁴ Some examples of the *consensus* rules within the Bitcoin core software are:

- Miners of new blocks may only create a certain number of new bitcoins; currently 12.5.²⁵
- Transactions must have correct ECDSA signatures²⁶ for the bitcoins being spent.²⁷
- Transactions/blocks must be in the correct data format.
- Within a single blockchain, a transaction output cannot be double-spent.²⁸

Creating any custom modification of core protocol software is called “forking the code.”²⁹ The term “forking” can be tricky to understand in the context of tokens because the term is also used to refer to a split in the network's shared ledger—a “fork in the blockchain.”³⁰

²² These scarce tokens, bitcoins, are really just a human-friendly shorthand for amounts listed in past transactions that have yet to be utilized (spent) in future transactions. To explain, in order to send bitcoins one actually signs a transaction message that references past transactions that will fund the new transaction. Input transactions must be larger—in total—than the desired output transaction, and any excess is specified to return to the user as change (a transaction to and from the same user). The full transaction message—references for all past transactions used as inputs, all output addresses and amounts sent to each output (both the addresses controlled by the recipient(s) and the change address)—is signed with the sender's private key (to prove that she was the recipient of referenced input transactions). This signed message is then broadcast to the network, and—if the signatures are valid—added to the blockchain by miners. That transaction can then be referenced by the recipient in order to fund future transactions. See *id.*

²³ The core software that makes up the bitcoin protocol was released by developers under an open source software license that allows for reproduction, distribution, and the making of derivative works without seeking permission. Specifically, it is released using the MIT license. See <https://github.com/bitcoin/bitcoin/blob/master/COPYING>

²⁴ See Bonneau *supra* note 20 at 6 (“default nodes refuse to relay more than a few thousand transactions below B0.001 per minute as a penny-flooding defense.”).

²⁵ These are created in coinbase transactions—transactions with no sender or inputs (funding transactions). See *infra* Appendix 1. The Bitcoin Mining Mechanism: Proof of Work Consensus.

²⁶ ECDSA stands for elliptic curve digital signature algorithm. It is a widely used digital signature algorithm. See *infra* Appendix 2. Digital Signatures and Bitcoin Transactions.

²⁷ See *id.*

²⁸ See *id.*

²⁹ See *infra* note 17.

³⁰ A fork in the blockchain means that for some period there exist two alternative versions of the transaction history. The authoritative history will be the “longest” of any possible chain (measured by the amount of mining work put into finding the constituent blocks). Blockchain forks can occur for various reasons. The simplest example is when two miners on opposite sides of the world find a new

Forking Blockchains

Running forked software that does not alter the consensus rules *does not* “fork” the blockchain; users of this software will agree with the parent network over the state of transactions on the ledger. To give an example, if someone wants to develop new Bitcoin mining software that is compatible with the existing Bitcoin network but better utilizes her own particular mining hardware, then she may fork the original Bitcoin core software and take care to not alter the consensus rules. She is running forked software but her mining activity does not fork the Bitcoin blockchain.

By contrast, developing and running forked software that *does* alter the parent network’s consensus rules will result in either a brand new blockchain or a fork of the parent blockchain (depending on whether the fork is backwards compatible—*i.e.* the software recognizes previously mined blocks in the parent blockchain as authoritative). Peers running this new software will recognize an alternative set of confirmed transactions (as compared with the list of transactions on the parent blockchain) on their own new network as authoritative.

Whenever a group of networked peers persist in running forked software with alternative consensus rules that—therefore—create an alternative blockchain, then these peers will effectively be creating a new token network and new tokens. The new blockchain will account for holdings of the new scarce token, and participants will be able to use the new network software to send these tokens to each other. Some early examples of token networks whose underlying software was forked from Bitcoin’s codebase include Litecoin,³¹ Dogecoin,³² and Peercoin.³³ New token networks have also forked off from projects other than Bitcoin. For example Paycoin forked from Peercoin and Ethereum Classic forked from Ethereum.

Some varieties of forked token software recognize a common transaction history with their parent chains up until the moment of the fork. For example, Ethereum Classic forked from

block nearly simultaneously. If there is latency in the network, peers near each miner may disagree over which block came first and until another block is built atop one or the other in the fork. For that period (~10 minutes) there are two alternative states of the ledger. This is statistically unlikely to perpetuate beyond one or two blocks because it would be extraordinary (to the point of probabilistic impossibility) for two miners to happen upon solutions simultaneously twice or three times in succession. Longer forks (sometimes referred to as deeper forks because they go further into the transaction history) can occur when some part of the network follows different consensus rules because of a bug in a upgraded version of the network software (see Joseph Bonneau, “How long does it take for a Bitcoin transaction to be confirmed?” *Coin Center* (Nov 2015)

<https://coincenter.org/2015/11/what-does-it-mean-for-a-bitcoin-transaction-to-be-confirmed/>.) or because of a deliberate desire to separate from the legacy network (*i.e.* create a token).

³¹ “What is Litecoin?” *Litecoin.org* (last accessed Dec. 2015) <https://litecoin.org/>. See also, “litecoin-project/litecoin” (last accessed Dec. 2015) <https://github.com/litecoin-project/litecoin>, where the current reference client for the litecoin network is developed. Note particularly that this software repository is listed as forked from the bitcoin github repository.

³² Dogecoin is a fork of Litecoin that is branded with an image of a Shiba Inu dog, a popular meme within Internet message board communities. See “Dogecoin” *Dogecoin.com* (last accessed Dec. 2015) <http://dogecoin.com/>. See also the Dogecoin github repository at <https://github.com/dogecoin/dogecoin>.

³³ See “Why Peercoin?” *Peercoin.net* (last accessed Dec. 2015) <https://peercoin.net/>.

Ethereum and Bitcoin Cash forked from Bitcoin and both forks recognize pre-fork transactions from their parent blockchains as valid. Other forked token software starts from scratch with a new blockchain that does not include historical transactions from the parent chain. For example, Litecoin and Paycoin are forks of Bitcoin and Peercoin respectively but they did not adopt their parent chain's transaction history.

When a forked token network recognizes a parent chain's transaction history, users of the parent network, if they choose to also use the new network, will find that they have an equal number of the new-network tokens as they had tokens on the parent network at the time of the fork. Users can spend or use these new tokens without affecting the disposition of their tokens on the original network and vice versa.

Developing New Software from Scratch and Airdrops

Rather than fork a version of an existing token network's software, a developer may also start truly from scratch in order to create a new network, selectively borrowing elements of prior cryptocurrency software or writing the code anew. A notable example of a from-scratch cryptocurrency is Ethereum.³⁴

The first block in a from-scratch network's blockchain would typically be empty because at the inception of the network no one yet has any tokens with which to transact. Alternatively, the developers of the new network could hard-code their own desired set of initial transactions and account balances into the first block. This could list certain amounts of tokens as belonging to addresses already generated by the developers as a reward for their work to develop the new network software, or it could assign new tokens to addresses created for investors who financed these development efforts. Releasing cryptocurrency software with a hard-coded first block and some initial distribution of tokens is referred to as a "pre-mine" and will be discussed further in the section on distribution.³⁵

Developers could even set the first block to initiate with a transaction history copied from a moment in some other blockchain. A developer could, for example, decide that the first block of NewCoin will have the exact same set of positive balances corresponding to addresses on the Bitcoin blockchain at midnight Jan 1, 2018. This mode of distribution is referred to as an "airdrop" because users of the parent blockchain suddenly have access to a corresponding number of tokens on the new network as if they'd been airdropped onto them. As with a forked blockchain, users of the parent chain can, if they so choose, freely spend or utilize the airdropped tokens without affecting the disposition of their tokens on the parent chain.

Tokens on Top of Token Networks

Further complicating matters, several networks, most prominently Ethereum, are designed to empower their users to create further bespoke tokens "on top of" the parent network. The

³⁴ See "What is Ethereum?" *Ethereum.org* (last accessed Dec. 2015) <https://www.ethereum.org/>.

³⁵ See *infra* at p. 11.

minting and transmission of these new tokens and their use is policed and described by the consensus mechanism and blockchain of the underlying network. For example, a random Ethereum user can create 20 units of their own RandomCoin on top of the Ethereum network and send them to Ethereum addresses controlled by her friends. There is no RandomCoin blockchain; the original creation of RandomCoin by our random user and any subsequent transactions to her friends and beyond are recorded in the Ethereum blockchain. Ethereum is not the only token network that has this functionality, but it is presently the largest.³⁶

II. Token Project Variables that can Affect User and Investor Risk

When token software is forked or developed from scratch many key attributes may change as compared with Bitcoin—the original cryptocurrency. What implications will these changes have for investor protection policy, for securities regulation, or regulation generally? Three key questions can help assess whether these changes pose heightened risks for potential users:

- How is the initial distribution of the token achieved?
- How decentralized is the community that powers the token?
- What functionality does possession of the token afford a holder?

From these questions we can arrive at three key variables: distribution, decentralization, and functionality. Each will be addressed in turn.

A. Distribution

Back in 2009, the very first bitcoins made it into the wild through mining. At this point in time, the only “person” running Bitcoin mining software was the man, woman, or group of people pseudonymously identified on mailing lists and Internet forums as Satoshi Nakamoto.³⁷ Eventually, more individuals joined and obtained bitcoins either by mining or having bitcoins sent to them by friends for fun, as gifts, or in early exchanges or purchases, e.g. two pizzas were purchased in 2010 for 10,000 bitcoins.³⁸

Bitcoin represents a particularly special case when it comes to distribution. As the first cryptocurrency—really a first running proof of concept for peer-to-peer Internet cash—very few individuals knew about it, and many of those who did, approached it with hearty skepticism. It would not be until two years later that bitcoin would reach parity with the dollar.³⁹ In these early years it was not uncommon for people to actually lose track of the bitcoins they had been

³⁶ For more background on creating tokens on top of ethereum see

³⁷ See Timothy B. Lee, “12 questions about Bitcoin you were too embarrassed to ask” *Washington Post* (Nov. 2013)

<https://www.washingtonpost.com/news/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/>.

³⁸ Three years later, that amount of bitcoin would be worth three-quarters of a million dollars. See Brian Merchant “This Pizza Cost \$750,000” (Mar. 2013)

<http://motherboard.vice.com/blog/this-pizza-is-worth-750000>.

³⁹ See sapiophile & Brother Bitcoin, “Bitcoin Price Chart with Historic Events” *Bitcoin Help* (Aug. 2014) <https://bitcoinhelp.net/know/more/price-chart-history>.

playing with as a hobby. For example, somewhere more than four feet deep in a Welsh landfill is what remains of James Howells's hard drive.⁴⁰ Howells was an early enthusiast who mined bitcoin for a few weeks in 2009. Later, after losing interest in the technology, he spilled lemonade on the laptop that stored the private keys to his mined tokens. Unaware of the value he was throwing away, he broke his laptop down for scraps and took the hard drive out with the trash. Later, at the height of the price rally, the bitcoins controlled by keys on Howells's lost hard drive were worth as much as \$7.5 Million dollars.⁴¹

Without online exchanges capable of matching interested buyers and sellers or being market makers themselves, the early spread of bitcoins was primarily through mining, gifting, and the occasional over-the-counter exchange. This stands in stark contrast to how many tokens are, today, distributed. Following the meteoric rise of Bitcoin's price in 2011 and onward,⁴² several new token projects were developed.⁴³ Many exchanges quickly offered markets in these new tokens⁴⁴ so that token miners could quickly liquidate their mined tokens into bitcoins or dollars, and interested buyers could obtain new tokens without dealing with a complicated mining setup. In short, today much of the early distribution of a token will often go to those intending to speculate on future value, rather than participate in the platform via mining or software development.

Pre-Mines and Pre-Sales (Initial Coin Offerings)

Developers of tokens are faced with a distributional choice: should we release the token's software at the point when no tokens yet exist and allow supply to grow as people run the software and mine the tokens (as it was with Bitcoin)? Or, should we internally mine or create some number of the total tokens that will ever exist before releasing the software publicly by hard-coding an initial distribution in the first block of the blockchain? This latter strategy is known as pre-mining.⁴⁵ A developer planning to pre-mine will often sell off the pre-mined

⁴⁰ See Kate Seamons, "\$7.5M Bitcoin fortune buried in landfill" *USA Today* (Nov. 2013) <http://www.usatoday.com/story/news/world/2013/11/28/newser-bitcoin-landfill/3775271/>.

⁴¹ *Id.*

⁴² See sapiophile & Brother Bitcoin, "Bitcoin Price Chart with Historic Events" *Bitcoin Help* (Aug. 2014) <https://bitcoinhelp.net/know/more/price-chart-history>.

⁴³ See e.g., Cyrus Farivar, "Behold Arscoin, our own custom cryptocurrency!" *Ars Technica* (Mar. 2014) <http://arstechnica.com/business/2014/03/behold-arscoin-our-own-custom-cryptocurrency/>. ("While the creator of Bitcoin remains a mystery, the currency's digital underpinnings are open to anyone to learn about; it's famously open source. One of its first major competitors, Litecoin, used the Bitcoin source code in late 2011, changing a few key parameters before releasing its own source code. That, in turn, has spawned more recent clones like BBQCoin and Dogecoin. According to Coinmarketcap.com, 75 mineable tokens currently exist, with market capitalizations ranging from \$38,000 (FedoraCoin) to \$10.3 billion (Bitcoin).").

⁴⁴ See e.g., *Shapeshift*, <https://shapeshift.io/> (last accessed Jan. 2016).

⁴⁵ See David Morris, "Beyond bitcoin: Inside the cryptocurrency ecosystem" *Fortune* (Dec 2013) <http://fortune.com/2013/12/24/beyond-bitcoin-inside-the-cryptocurrency-ecosystem/> ("It certainly hasn't been the M.O. of the flood of bad actors looking to make a quick buck by starting bogus cryptocurrencies. This is usually accomplished through what's known as a "pre-mine," in which the founders of a currency generate a large chunk of currency for themselves before releasing the mining code to the public. Those founders will then undertake a big marketing push, including, it is rumored, the occasional payoff to a prominent spokesman and bribes in exchange for listing on cryptocoin trading

tokens to the general public at a set price in order to fund future development. She may even sell tokens long before any mining, either private or public, takes place. This is referred to as a pre-sale.⁴⁶ Buyers may line up for this so-called “initial coin offering” under the assumption that they will be obtaining tokens at the earliest possible point, and, should the token turn out to be useful and/or popular, with the largest possible upside. However, should the token network fail to develop into a useful platform, any initial investment can and will, of course, come to naught.

In the most questionable examples of a pre-mined and pre-sold token, one will often find promises of a future guaranteed price floor for the token.⁴⁷ This could, for example, be a promise that six months after the pre-sale the developer will offer to buy back the tokens from all willing sellers at \$20 a piece. This may be rationalized or marketed by suggesting that each token is linked to some underlying reserve asset, perhaps a precious metal or partitions of a profitable fruit grove.⁴⁸ Alternatively, the developer may claim to have integrations or partnerships with prominent retailers or online service providers, and may guarantee that the token will soon be accepted by these partners for certain real goods.⁴⁹ Experience thus far has indicated that these sorts of hard sell arrangements are almost always scams.⁵⁰

Recognizing the community-wide reputational and regulatory risk posed by pre-sale offerings,⁵¹ as well as the risk to users within token development generally, some cryptocurrency enthusiasts sought and developed alternative modes of initial distribution: proof-of-burn, airdrops, sidechains, private sales, and traditional capital formation.

Proof-of-Burn

In a proof-of-burn system, new tokens are distributed to those who provably destroy bitcoins by visibly sending them to a Bitcoin addresses known to have no known matching private key (making them unspendable).⁵² The motivation behind this scheme is to achieve a fair distribution of the new tokens, based on the relative desire of users to sacrifice bitcoins. It is believed that such a distribution scheme does not unfairly enrich the developers with

exchanges, which can confer a sheen of legitimacy. Then, when the hyped, bogus coin is released, adoption by cryptocoin enthusiasts can give its value a brief bump, and unscrupulous founders can unload their pre-mined loot. ‘In excess of 80% of tokens are pump-and-dump schemes in the most traditional sense of the term,’ says Antonopoulos.”).

⁴⁶ See, e.g., Michael Casey, “BitBeat: Ethereum Presale Hits \$12.7 Million Tally” *Wall Street Journal* (Aug 2014) <http://blogs.wsj.com/moneybeat/2014/08/05/bitbeat-ethereum-presale-hits-12-7-million-tally/>.

⁴⁷ See suchmoon *supra* note 153.

⁴⁸ See “SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds” *U.S. Securities and Exchange Commission* (Sep. 2017) <https://www.sec.gov/news/press-release/2017-185-0>.

⁴⁹ *Id.*

⁵⁰ See Morris *supra* note 44.

⁵¹ See, e.g., “Viacoin Distribution Model” *Viacoin Blog* (Jul. 2014) <http://blog.viacoin.org/2014/07/07/viacoin-distribution-model.html> (“There will be no developer pre-mine because we think that ‘pre-mines’ in general harm the market by creating uncertainty (that developers may exit at an unknown time in the future).”).

⁵² See Meni Rosenfeld, “How does proof of burn work?” *Quora* (Nov. 2014) <https://www.quora.com/How-does-proof-of-burn-work>.

speculative profits before any real progress on the platform has been achieved. The most notable example of proof-of-burn came during the initial release of the Counterparty token XCP. The motivation behind this distribution, as described on the Counterparty website, was fairness:

By opting to distribute all XCP by proof-of-burn, the Counterparty developers eliminated any speculation that they planned to get rich quick or redistribute risk unequally. On the contrary, they put themselves in the same position as everyone else, backing their ideas with destroyed bitcoin to obtain XCP in the hope of eventually benefiting financially from their own project and hard work.

It is hard to overstate how far removed Counterparty is from almost any other altcoin.

The strategy of taking on more personal risk than developers of competing projects and forcing themselves to produce results before they could see any benefits is already bearing fruit. Counterparty is the first (and so far the only) protocol to have a working distributed exchange, built in record time despite having no outside funding of any kind.

⁵³

There are, however, notable downsides to a proof-of-burn distribution. If the tokens obtained via bitcoin burning are the total supply of the token then the token economy will be inherently deflationary. This static supply can mean that rapid shifts in demand can create large spikes in the price of the token, which could leave investors or users vulnerable to a pump and dump scam perpetrated by larger investors. Additionally, if the token fails, the user will be unable to recover her burned bitcoins; it is a total loss.⁵⁴

Airdrops

A token airdrop is an alternative method of distribution that some believe can achieve a more equitable distribution of new tokens while avoiding any potential misaligned incentives between developer and user that might be inherent in a lucrative token pre-sale.

Key to the airdrop method is the fact that the cryptographic addresses on a blockchain tend to be generated using well-understood cryptographic functions.⁵⁵ Every bitcoin address on the Bitcoin blockchain was generated by a user of the network as a place to be paid or receive mining rewards. In that process the user also generated a corresponding private key. Making a successful bitcoin transaction necessitates digitally signing a message with the private key corresponding to the bitcoin address that will fund the transaction. Users should keep their private keys secret to ensure no one else can spend their bitcoin. Bitcoin's core software uses a

⁵³ "Why Proof-of-Burn" *Counterparty* (Mar. 2014) <https://counterparty.io/why-proof-of-burn/>.

⁵⁴ See cbeast "Pegged vs. Destructive Side Chains" *Bitcoin Talk* (Nov. 2014) <https://bitcointalk.org/index.php?topic=844617.0>.

⁵⁵ For a detailed description of these cryptographic addresses see *infra* Appendix 2. Digital Signatures and Bitcoin Transactions.

well known cryptographic function to generate these addresses, keys, and signatures (the ECDSA) and most other cryptocurrencies have followed suit.

Developers who wish to airdrop their token at the start of their new network simply take a snapshot of some existing blockchain and use it to create the first block of their own blockchain. For example, the developers of a hypothetical AirdropCoin could copy the Bitcoin blockchain as it exists right this moment, and they could craft the first block of AirdropCoin's blockchain such that the same cryptographic addresses have the same positive AirdropCoin balances as they had bitcoin balances on the bitcoin blockchain. Now a Bitcoin user, should she choose to install and use the new AirdropCoin software, can import her existing bitcoin private keys into the new software and, from there, spend her AirdropCoins. Typically, all blocks subsequent to the first block in the airdropped token's chain would be composed organically of transactions initiated by users or miners of that new token; only the first block is hard-coded by the developers to match a moment in time from the parent chain.

Networks that support consensus over multiple user-generated tokens apart from the foundational token, e.g. ERC20 tokens built on top of Ethereum,⁵⁶ may make airdrops even easier. The developer merely creates a smart contract on the network that allows anyone with a positive balance of the foundational token, say Ether, to claim some corresponding amount of the new token, gratis.

As with a proof-of-burn distribution, the developer of an airdropped token does not achieve a large windfall at the moment of distribution, but she is nonetheless able to bootstrap her network by gaining new users who will have tokens to use and a stake in the network's longer-term success.

Unlike proof-of-burn, however, token holders do not have to give anything up to obtain the new token. If they had X number of Bitcoins (or whichever parent chain the developers choose to recognize) at the moment the new network was created, then they'll have X number of new tokens without having to take any action or make any sacrifice. Recipients of airdropped tokens would therefore lose nothing if the new network was to come to naught.

Sidechains

Another method of releasing tokens into the hands of the public is via sidechain.⁵⁷ A sidechained token is like a token with a pegged exchange rate to Bitcoin. To utilize a sidechain, a user need only send bitcoins to a special address which will temporarily lock those funds out of her control. Simultaneously an equivalent nominal amount of sidechain tokens will be released into her control and she will have access to whatever functionality the sidechain offers. The peg also works in reverse, releasing bitcoins back to the user's control. This peg works algorithmically through verification of cryptographic commitments on the blockchains of the

⁵⁶ See Peter Van Valkenburgh, "What does it mean to issue a token "on top of" Ethereum?" *Coin Center* (May 2017) <https://coincenter.org/entry/what-does-it-mean-to-issue-a-token-on-top-of-ethereum>.

⁵⁷ For a more detailed explanation of sidechained tokens, see *infra* Appendix 3. Sidechains.

two pegged tokens. Therefore, the user of the sidechain does not need to rely on a trusted third party to guarantee the peg.

Again, a primary motivation behind this innovation is fairness and the avoidance of volatility risk native to simple tokens. As described in the sidechains white paper, the developers also sought to create an interoperable ecosystem where several blockchains (developed for different specialized purposes) could be knit together:

By reusing Bitcoin's currency, these systems can more easily interoperate with each other and with Bitcoin, avoiding the liquidity shortages and market fluctuations associated with new currencies.⁵⁸

Unlike proof-of-burn or air-dropped tokens, sidechain tokens can always be redeemed for tokens from the parent chain (likely Bitcoin). If the sidechain proves useless, users are not stuck with a valueless investment. The primary downsides to the sidechain approach are technical challenges. Ensuring that pegged bitcoins can be recovered by honest sidechain users, and never dishonestly recovered by interlopers, requires a sophisticated setup,⁵⁹ and—for the most secure implementation—minor adjustments to the Bitcoin protocol itself—something that will ultimately require the political will of the community (or an economic majority at least) to enact.⁶⁰

Private Sales

Rather than freely selling pre-mined tokens to the general public, a developer concerned with regulatory risk may choose to have a more limited sale. She may sell promises of her future tokens only to accredited investors or sell them to the public but only in dollar-value-limited amounts. Assuming full compliance with the relevant requirements in U.S. securities laws, these sales may then take advantage of JOBS Act safe-harbors from securities registration rules.

⁶¹

This approach concedes that the initial agreement between the developer and her purchasers is, in fact, an investment contract and, therefore, a security. It, however, generally assumes that the token, once delivered to the investors pursuant to the terms of that investment contract,

⁵⁸ *Id.* at 1.

⁵⁹ Two potential schemes could enable movement from one chain into another. The first is the Federated Peg system which relies on a group of unaffiliated functionaries who are specified in advance of the conversion and instructed to validate movements from one chain to another through some form of majority voting rule. *See id.* at 17. The second is an automated scheme that avoids placing trust in any particular entity or group of entities to validate the conversion and instead relies on provable statements (SPV proofs) from both blockchains involved in the peg. *See id.* at 9.

⁶⁰ It is trivially easy to design a new sidechain that can utilize SPV proofs in order to lock or release tokens as part of a two way peg. Bitcoin, however, does not currently have this ability and sidechains to bitcoin must therefore rely on the Federated peg mechanism described in the previous note. This is because Bitcoin was designed long before sidechains had been conceived and because the necessary changes would require coding, testing, and ultimately adoption from the larger bitcoin community (which tends to be reticent to change). *See id.* at 20.

⁶¹ *See, e.g.*, 17 C.F.R. §230.506.

will not itself be a security. Future sales or re-sales of that token would not, therefore, be subject to securities regulation. Several lawyers and developers have sought to create a standard version of this limited token pre-sale instrument and have branded that standard agreement as a “Simple Agreement for Future Tokens” in reference to the “Simple Agreement for Future Equity” developed by Y Combinator as an alternative to convertible debt in late 2013.

62

Traditional Capital Formation and Release by Mining or Dividend

Finally, some early stage token projects may eschew any of these public sales or distribution methods, choosing instead to raise funds solely from accredited private investors at least until the protocol is fully fleshed out, publicly released, and open for all interested users to begin mining or providing other such proofs of participation.⁶³

Distribution and Risk

Rounding up these various distribution schemes we can imagine a hierarchy in terms of risk to the public. On the riskier end of that continuum would be pre-mined tokens offered for sale with attendant guarantees of future redemptive value or other hard-sell marketing tactics. Less risky would be tokens offered to the general public without any promise of future value, and ideally with some transparency as to who is working on the project, what the project intends to build, and how new tokens will enter circulation. Less risky still would be tokens distributed using a proof-of-burn or airdrop system. Finally, least risky would be a sidechained coin where users can freely move between the new currency and the long-established Bitcoin network at a known pegged exchange rate.

Token projects that eschew public distribution during early development represent a different species of risk with an alternative mode of controlling for that risk. They are financed following the traditional venture capital method. These projects have formal, accredited investors and are structured like any other early stage technology corporation. Token projects selling via a limited sale or SAFT agreement represent a hybrid approach. Initial investors are accredited or else capable of making only dollar-value-limited investments. This is a traditional approach to mitigating early-stage investor risk. If the project matures as planned, the tokens pre-sold in these agreements will ultimately be delivered and should be functional and decentralized. Their subsequent resale from the initial investors to the public at large removes the mitigating controls of accreditation or dollar-value caps, ideally in exchange for an asset that is less risky being as it is no longer merely a promise of some developer but, in fact, a functional token that can be used within a decentralized network.

⁶² “Startup Documents” *Y Combinator* (Feb. 2016) <https://www.ycombinator.com/documents/>

⁶³ Early development of Zcash (formerly Zerocoin), for example, was funded entirely through traditional private investment. See Andy Greenberg, “Zerocoin Startup Revives the Dream of Truly Anonymous Money” (Nov. 2015) <http://www.wired.com/2015/11/zerocoin-startup-revives-the-dream-of-truly-anonymous-money/>.

B. Decentralization

Decentralization is, perhaps, and overused term in the cryptocurrency and token community. However, there are certain fundamental qualities that differentiate a service, such as money transmission, that is provided by a company, e.g. paypal, and a similar service that is provided by an open group of participants working together via a peer-to-peer networking protocol, consensus software, and a blockchain, e.g. Bitcoin. This section will explain varying degrees of decentralization as exhibited by various token projects, and it will highlight where risks to users do and do not exist with respect to a decentralized network. We will proceed with five subtopics: (1) **Consensus**, the rules that govern participation in a decentralized network and the process by which those rules are enforced by miners or validators; (2) **Scarcity**, a particular rule within any consensus mechanism that establishes key economic relationships between participants; (3) **Transparency**, the degree to which the software establishing the consensus rules is developed in an open and auditable process; (4) the **Abundance and Diversity of Developers and Validators**, whether several unaffiliated persons are developing the software or, merely, a select few; and (5) the **Profit-Development Linkage**, the degree to which a handful of developers or validators are incentivized to take quick profits by encouraging investment in the token.

Consensus

As discussed in the first section, all cryptocurrency software will have policy rules and consensus rules. Policy rules are settings that an individual can choose to alter on her individual running instance of the software (e.g. I'd like my software client to refuse to relay transactions smaller than a certain amount of bitcoin). Consensus rules, by contrast, are those aspects of the software that must remain unchanged for the network to recognize the individual's participation as legitimate. These are, in some sense, the constitutional rules of a cryptocurrency, setting fundamental variables like the total supply of the coin, rules for acceptable and unacceptable transactions, and rules for how the authoritative ledger of transactions—its blockchain—is assembled and maintained.

Again, within Bitcoin's software, examples of these consensus rules are:

- Miners of new blocks may only create a certain number of new bitcoins; currently 12.5 and set to decrease by half every 210,000 blocks.
- Transactions must have correct ECDSA signatures for the bitcoins being spent.
- Transactions/blocks must be in the correct data format.
- Within a single blockchain, a transaction output cannot be double-spent.

For Bitcoin, the consensus rules can be found in the *reference client* version of the software, which is publicly shared on a website known as GitHub,⁶⁴ and maintained by a loosely-defined

⁶⁴ Github is an online tool for version control (monitoring, reviewing and accepting changes to software code under development). It is social, allowing multiple users to join and contribute to a project, and transparent, keeping a fully auditable record of who contributed what. Repositories (bins for particular software projects) on Github are public by default (even those not contributing can view all changes), but

group of unaffiliated developers colloquially known as core devs or core contributors. This software, often referred to as *Bitcoin Core*,⁶⁵ is, however, merely an artifact of the “true,” binding, or de facto consensus rules as they exist in the network. The actual binding rules themselves are whatever actual participants on the Bitcoin network say they are, effectively voting by running their choice of software.⁶⁶ It just so happens that, as of this report and for the foreseeable future, the consensus rules described in the Bitcoin Core software are identical to the rules that exist in the software run by network participants, but this need not always be true.

Changes that relax the consensus rules or remove certain rules (meaning that a wider range of blocks and transactions are now valid on the network) require a so-called “hard-fork.” This means that the new software will be incompatible with the existing software employed on the network and miners and nodes who have not upgraded will not recognize the participation of those who have upgraded. The two factions recognize different and irreconcilable ledgers from the fork onward.⁶⁷

can be made private. Bitcoin’s repository is public. For more on Github see generally Ferdian Thung, David Lo and Lingxiao Jiang, “Network Structure of Social Coding in GitHub” *CSMR 2013: Proceedings of the 2013 17th European Conference on Software Maintenance and Reengineering* 323 (Mar. 2013) available at http://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=2686&context=sis_research (“GitHub is a social coding site that uses Git [an open source version control system for software development originally created for use within the Linux open source operating system project] as its distributed revision control and source code management system. It implements a social network where developers are enabled to broadcast their activities to others who are interested and have subscribed to them. GitHub currently hosts over three million projects maintained by over one million registered developers. A given developer can participate in multiple projects and each project may have more than one developer. The GitHub social coding site is a developer friendly environment integrating many functionalities, including wiki, issue tracking, and code review.”).

⁶⁵ See “README.md” *Github:Bitcoin/Bitcoin* (last accessed Dec. 2015) <https://github.com/bitcoin/bitcoin> (“Bitcoin Core is the name of open source software which enables the use of this currency.”).

⁶⁶ The functional particulars of this emergent voting rule are difficult to pinpoint. For changes that loosen the consensus rules unanimity is required (although those that do not adopt the change would continue to run legacy software and two networks could persist with neither group able to “vote” in each other’s affairs). For changes that tighten the consensus rules a simple majority of miners is required (because all participants would accept the blocks generated by the new software even if they, themselves do not update their own software. For more, see the following footnote on hard and soft forks.

⁶⁷ *Hard forks* can be contrasted with *soft forks*, where the consensus rules become stricter rather than looser (fewer types of transactions or blocks are recognized by the new software as valid). Miners who upgrade their software to the strict client will refuse to accept any blocks that conform to the older, looser consensus rules. However, their blocks (conforming to stricter rules) will continue to be accepted as valid by legacy users whose software is less discerning. If the majority of miners upgrade, the chain they produce (only strict/upgraded blocks) will always be recognized as valid (even by those who do not upgrade) because it will be the longest. Because they will not break compatibility, changes made via soft forks are preferable. However, this limits the types of changes that can be easily made. It’s much easier to add or strengthen a consensus rule (e.g. previously valid transactions must now also have some additional information in order to be processed) than it is to loosen or remove a consensus rule (e.g. coinbase transactions awarding 500 new bitcoins to the miner—previously set to 25 on a decreasing schedule—are now valid). See Joseph Bonneau, Andrew Miller, et al. “Research Perspectives and

Effectively, a contested hard fork is the creation of a new token that shares a common transaction history with the legacy Bitcoin network up until the point that consensus rules were changed. This new network will include all users running the new software, and will not consistently recognize the contributions or participation of legacy users. The question of which side of the fork is the “real” Bitcoin, is basically subjective. Some may suggest that the legacy software represents the true Bitcoin and the new fork is a new currency that should brand itself differently. Others, however, might suggest that the new version is authoritative and represents the latest version of Bitcoin. Still others may argue that the network with more computing power, mining effort, is authoritative. Ultimately, however, both networks will be judged by the purchasing power that they retain. If real merchants refuse to sell goods or other currencies in exchange for either the new or the old network’s putative “bitcoins,” then that time of the fork will stand no chance, rewards to miners working on that network will be useless.

Bitcoin relies on miners in order to enforce constitutional rules because there simply is no other authority within the system. The blockchain is the authoritative state of the network and permission to alter that state in the next block (roughly a ten minute interval of time) is limited to the network participant who (a) solves an open-ended math problem by using guess and check,⁶⁸ (b) broadcasts that solution to the network, *and* (c) whose solution is then built on (because some previous block solution must be used as an input to create future blocks) by sufficient other miners such that this chain of new blocks is the longest chain—has the most computing effort dedicated to it—as compared with any possible alternative states (forks) of the network.⁶⁹

This is why a single individual, by marshalling as much computing power as the rest of the network combined, could, in theory, block future transactions (by refusing to put them in new blocks) or attempt to convincingly double-spend new transactions.⁷⁰ Because this neerdowell has more computing power than the rest of the network combined she will, on average, be able to write new blocks faster, add them to the chain she prefers, and always have that chain remain the longest chain in the network—the authoritative state of Bitcoin.

Challenges for Bitcoin and Cryptocurrencies” *IEEE Security & Privacy*, p. 10 (2015),
<http://www.jbonneau.com/doc/BMCNKF15-IEEE-SP-bitcoin.pdf>

⁶⁸ See *infra* Appendix 1. The Bitcoin Mining Mechanism: Proof of Work Consensus.

⁶⁹ See Joseph Bonneau, “How long does it take for a Bitcoin transaction to be confirmed?” Coin Center (Nov 2015)

<https://coincenter.org/2015/11/what-does-it-mean-for-a-bitcoin-transaction-to-be-confirmed/>.

⁷⁰ Effectively the dishonest miner starts compiling a secret, private blockchain all her own. Meanwhile she sends, for example, 100 bitcoins to an exchange and cashes out in dollars. This bitcoin transaction is incorporated into the public blockchain, but she does not include the transaction in her own private version. Once she is certain she has the dollars she then broadcasts her private chain to the network. If she truly had more computing power than the rest of the network combined then her chain will be “longer” (more difficult math problems solved) and the rest of the network will recognize this new—until recently private—blockchain as the authoritative ledger. The exchange that accepted the 100 bitcoins for dollars no longer has those bitcoins according to this new reorganized chain and has lost the dollars as well. Note, however, that such an attack is far more difficult than merely attempting to steal poorly secured bitcoins from an exchange.

This is referred to as “a 51% attack.” It’s important to point out that such an attack does not give the attacker the ability to spend any funds sent to Bitcoin addresses for which she does not have the corresponding private keys, nor does it give her the ability to create new bitcoins out of thin air. Any miner, even a miner who had a majority share of the network’s computing power, who attempts to change or break these basic consensus rules, is effectively advocating for a hard fork of the network, and she takes the risk that the network writ-large, miners as well as users, would refuse to treat tokens on her new fork as valid currency. While the revisionist miner may create new blocks that reward her with new tokens, if those tokens are not accepted in exchange for real goods or other currencies, then she will fail to profit from her actions.

Therefore, to reiterate, a 51% attack does not enable the attacker to fundamentally change Bitcoin; it merely enables the attacker to block new transactions and, potentially, double-spend transactions that were initiated after she obtained majority control. Moreover, the cost of such an attack is, necessarily, massive. There is fierce competition amongst Bitcoin miners, and specialized hardware components—application-specific integrated circuits or ASICs for short—have come to dominate the field.⁷¹ These ASIC chips have effectively no valuable application outside of cryptocurrency mining, therefore any attacker seeking to perform a 51% attack would need to make a very sizable investment in otherwise useless hardware merely to initiate the attack.⁷² Additionally, given the transparent nature of the blockchain, such double-spend attacks would be immediately visible and, if sufficiently large, would likely lead to a rapid collapse in the price of Bitcoin, leaving the perpetrator with little or no reward as measured in purchasing power.⁷³ Given the high cost and uncertain benefits, a 51% attack against Bitcoin would not be a likely strategy for a rational actor seeking to commit fraud.⁷⁴

⁷¹ See, for example, Motherboard’s report on a large Chinese Bitcoin mine and the technology employed. Erik Franco, “Inside the Chinese Bitcoin Mine That’s Grossing \$1.5M a Month” *Motherboard* (Feb. 2015) <http://motherboard.vice.com/read/chinas-biggest-secret-bitcoin-mine>.

⁷² See, e.g., *id.*, See also David Chernicoff, “Bitcoin miner BitFury looks to invest \$100 million in next data center” *ZDNet* (Sep. 2015) <http://www.zdnet.com/article/bitcoin-miner-bitfury-looks-to-invest-100-million-in-next-data-center/>.

⁷³ According to Bitcoin Core Developer Gavin Andresen, the visibility of the attack would also make finding a fix easier. See Gavin Andresen, “Re: Taking Down Bitcoin” *Bitcoin Talk* (Apr. 2012) <https://bitcointalk.org/index.php?topic=78403.msg874553#msg874553> (“If a 51% attacker stopped including all broadcast transactions in blocks “we” would quickly figure out a rule or rules to reject their blocks.”).

⁷⁴ A paper released in 2013 by Cornell University-based cryptographers Ittay Eyal and Emin Gun Sirer describes and names a variant attack strategy, the *selfish miner attack*. The paper explains why rational miners may have an incentive to solve blocks but withhold them from the network (effectively, choosing not to broadcast the solution they’ve obtained). After finding a secret solution, the miner attempts to solve another block on top of their secret block. If, during this time, another, honest miner finds a valid block, then the *selfish* miner will forego the reward they could have had if they would have made their own solution public. However, if the miner can mine two blocks faster than all other miners together can create one, then the selfish miner can release both and the network will ignore the honest miner’s single block. Described so far this is not so much an attack on the network, as it is a way to cheat the system and find larger rewards as compared to the rest of the network. The strategy is worrisome, however, in that it creates an incentive amongst honest miners, to join (pool their hashing power) with the selfish miner in order to split the outsized rewards and avoid situations where your honest block is skipped over

This focus on computing effort as the measure and gateway for legitimate participation is referred to in computer science terminology as **proof-of-work**.⁷⁵ There are, however, other possible consensus mechanisms for ensuring or incentivising honest participation within a cryptocurrency network. Two mechanisms warrant brief description here: **proof-of-stake** and **permissioned distributed ledgers**.

Proof-of-stake systems do not require the mathematical calculations and costly hardware investments of proof-of-work systems.⁷⁶ In these cryptocurrencies the network semi-randomly selects participants for the privilege of writing the next block. To be eligible for selection, a participant must have an address on the network and some “stake” in the cryptocurrency. The details of what that stake must be can vary (and would be set in the cryptocurrency’s consensus rules), but, generally, those with more of the cryptocurrency will be more often eligible to write new blocks to the blockchain.

Permissioned distributed ledgers utilize merely the digital signatures of certain enumerated participants to determine who may write new blocks.⁷⁷ For example, rather than having an *open* or *permissionless* distributed ledger wherein anyone may submit proofs of work, or anyone with a positive cryptocurrency balance on the network may submit proofs of stake, a *permissioned* distributed ledger could be set up so that only certain network participants, identified and authenticated by use of a public-private keypair, are empowered to write new blocks either at random, in alternating turns, or according to some voting rule. The advantage of this system is that no costly proof is needed to ensure honest and committed participation (because participation is limited, *ex ante*, to a set of entities deemed trustworthy).⁷⁸ The disadvantage of

when a selfish miner reveals their longer, secret chain. This increases the risk that a coalition of self-miners could grow to have over 50% of the network’s hashing power and the attendant ability to block transactions or double spend. Ittay Eyal, Emin Gun Sirer, “Majority is not Enough: Bitcoin Mining is Vulnerable” *arXiv:1311.0243v5 [cs.CR]* (Nov. 2013) <http://arxiv.org/pdf/1311.0243v5.pdf>.

⁷⁵ Proof-of-work systems were initially proposed and developed by computer scientists as a means of limiting spam email. Under a proof-of-work email system, the sender of an email would have to perform some amount of costly computing in order for her message to reach the recipient. For a typical user (e.g. no more than 20 emails per day) the cost of sending email would be vanishingly small—a bit of extra electricity and a barely noticeable delay before the message sends—but for someone sending thousands of spam emails robotically, the costs would be prohibitive. The concept was first proposed by Cynthia Dwork and Moni Naor. See Cynthia Dwork, Moni Naor. “Pricing via Processing or Combatting Junk Mail” *CRYPTO ’92 Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology* 139-147 (Aug. 1992). Later, it was independently invented and developed by Adam Back. See Adam Back. “hash cash postage implementation” *Cypherpunks Mailing List* (Mar. 1997) <http://www.hashcash.org/papers/announce.txt>. Back’s formulation was later the basis for the proof-of-work system utilized within the Bitcoin protocol. See *infra* Appendix 1. The Bitcoin Mining Mechanism: Proof of Work Consensus.

⁷⁶ For a technical analysis of proof-of-stake systems see Andrew Poelstra, “A Treatise on tokens” 14 (Mar. 2015) <https://download.wpsoftware.net/bitcoin/alts.pdf>.

⁷⁷ See generally Tim Swanson, “Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems” *R3 CEV* (Apr. 2015) available at <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>

⁷⁸ Cf. Tim Swanson, “Watermarked tokens and pseudonymity on public blockchains” *R3 CEV* (Nov. 2015) <http://r3cev.com/s/Watermarked-tokens-and-pseudonymity-on-public-blockchains-Swanson.pdf> (“For better and for worse, Bitcoin and Bitcoin-like systems must be energy intensive [as compared with

this system is that dishonest participation must be punished outside of the protocol in the real world of politics, business negotiation, or law: fraudulent blocks or transaction validations must be removed from the ledger by the coordinated actions of the other, honest participants, and the dishonest participant must be excluded from future participation through a readjustment of the protocol and/or external legal action.⁷⁹

Finally there is the possibility for hybrid consensus models. a token may begin as a proof-of-work system in order to create an initial distribution of tokens and later it may switch to a proof-of-stake system,⁸⁰ or it may employ both simultaneously. So long as this shift or co-specification is widely discussed and development decisions are made in a decentralized manner, this should not raise concerns. More troubling, perhaps, are hybrid systems that combine elements of the permissionless models (work and stake) with elements from permissioned distributed ledgers.

As previously described, Peercoin, an early proof-of-stake token, suffered a series of attacks that led developers to switch to a model where only certain identified non-attacker participants were allowed to submit proofs of stake.⁸¹ This model is a form of permissioned distributed ledger—only certain identified participants may participate in the consensus process. Even more worrying is the example set by a questionable fork of Peercoin called Paycoin. Paycoin was developed by Homero Joshua Garza, formerly of two other ventures, GAW Miners and Great Auk Wireless, both of which have been the subject of investigations for fraud.⁸²

Paycoin was nominally a proof-of-stake consensus system, like its progenitor Peercoin. However, changes were made to the software that created a hybrid consensus mechanism wherein certain enumerated addresses, presumably in the control of Garza or someone else its developers saw fit to benefit, were capable of providing stake and generating new tokens at an annual rate of 3,000% above a normal address.⁸³ The result is a privileged class of participants

permissioned ledgers], otherwise attackers could easily rewrite history. Miners compete through wealth destruction, as “real economic goods (time in fabs, electricity, engineering efforts) are being removed from the economy for the sake of proof-of-work mining.”)

⁷⁹ See Swanson *supra* note 77 at 43 (“all participants are already authenticated and entities like validators and transmitters require legal identities.”).

⁸⁰ Ethereum’s developers, for example, are working on developing a robust proof-of-stake mechanism, called Casper, that could one day supplant the existing proof-of-work system. See Vlad Zamfir, “Bringing Ethereum Towards Proof-Of-Stake With Casper” *Epicenter Bitcoin* (Nov. 2015) <https://epicenterbitcoin.com/podcast/105/>.

⁸¹ See Poelstra *supra* note 76 at 14.

⁸² See Cyrus Farivar, “Over 10,000 people were duped by Bitcoin mining startup, feds say” *ars technica* (Dec. 2015)

<http://arstechnica.com/tech-policy/2015/12/feds-sue-yet-another-cryptocurrency-startup-alleging-19m-ponzi-scheme/> and Erin Mansfield, “Great Auk Wireless founder under SEC investigation” *Battleboro Reformer* (Jul. 2015)

http://www.reformer.com/latestnews/ci_28451349/great-auk-wireless-founder-under-sec-investigation.

⁸³ See suchmoon, “GAW / Josh Garza discussion Paycoin XPY xpy.io BTCLend LNC. ALWAYS MAKE MONEY :)” *BitcoinTalk* (Aug. 2015) <https://bitcointalk.org/index.php?topic=857670.0> (“Removal of the “floor” puts into doubt another widely promoted advantage of Paycoin over other crypto currencies - price stability. In addition to that it has been revealed that Paycoin source code contains special

who earn outsized rewards for participation despite the coin's branding as an equitable proof-of-stake consensus model.⁸⁴ There may be legitimate reasons to combine elements of permissioned and permissionless models, but key to any such effort will be transparency from the developers regarding how the system is set up, why it is necessary, and who is benefitting from being enumerated as a special participant (*i.e.* an address on the network identified as receiving some added powers or functionality within the consensus model).

With all of these consensus mechanisms outlined, what can be said for their relative risk to users or investors? One clear distinction can be made between the two permissionless systems (proof-of-work and proof-of-stake) and the permissioned distributed ledger. In a permissionless system there is a going market rate for participation and an open competitive industry seeking to provide updates to the blockchain. In a permissioned system there is a closed group of individuals or institutions who have ultimate authority over the blockchain, and should these entities collude in order to block the transactions of particular users, little could be done to stop them. Additionally, if—as would likely be the case—these permissioned users are also the developers of the software, then effectively any change to the protocol (*e.g.* decisions to enlarge the total supply of tokens, or reverse certain previous transactions, or freeze all transactions) could be effectuated without the agreement of outside individuals or the platform's users.

Such collusion is also, in theory, possible in a proof-of-work or proof-of-stake system. Several powerful miners (proof-of-work) or currency-rich individuals (proof-of-stake) could join forces to obtain 51% of the mining or staking power and then refuse to add transactions from blacklisted users into the blockchain. However, given that any particular participant's power is contestable by new entrants, such a cartel would be inherently unstable. This is particularly true if the user or group of users targeted for censorship offered large fees to a miner or stakeholder willing to break ranks and process the transaction or a new miner or stakeholder who enters the market and refuses to join the blocking cartel.

Additionally, a miner with 51% of the computing power on the network would not be able to change the scarcity of the cryptocurrency, reverse transactions that were recorded in the blockchain previous to her majority control, or make any other changes to the consensus rules, because the remaining 49% of the network would not recognize blocks with such changes as valid. She will have forked the network by mining these non-compatible blocks. She'd be, effectively, mining her own coin that is no longer, for example, Bitcoin.

The natural differences between commodities and securities may be instructive here. A group of individuals issuing a security have full control over the fundamentals of that investment vehicle: they can organize production within the firm, they can choose to offer more shares and dilute existing ownership interests, they have full control over the accounting internal to the organization, and the only external limits to these activities are legal—either through contract or regulation. A group of individuals producing some commodity, say gold, could attempt to

exceptions for certain wallets that can stake - or generate new tokens - at rates in excess of 3000% annually, which would create hyperinflation.”).

⁸⁴ *Id.*

withhold large amounts of gold from the market, flood the gold market with supply, create rumors about gold production, or choose to only sell gold to certain favored counterparties, but at the end of the day they can't stop other producers or resellers from offsetting these manipulative activities with their own buying, selling, or rumor-mongering.

Another takeaway from this discussion of consensus is that within a proof-of-work or proof-of-stake cryptocurrency, there is only true resilience against fraud or manipulation when there is a large and competitive market for providing these proofs. To take Bitcoin, for example, the cost of gaining a 51% share of the mining power is constantly changing (and generally increasing as more people become involved and the technology becomes increasingly specialized) but one recent estimate puts that number at \$120 million dollars in initial hardware investment, \$8,000 per hour in electricity costs just to run the mining hardware, and as much as \$5,000 per hour in electricity costs to cool the facility (because ASIC mining chips generate a considerable amount of heat).⁸⁵

Additionally, for permissionless systems, the cost of these attacks scale monotonically with the value of the underlying currency. In proof-of-stake currencies this is intuitive, if the value of the currency rises, so too do the costs of having a given required stake for selection as a transaction validator. In proof-of-work, so long as we assume rational miners, a similar proportional increase in the cost-to-validate will hold. If the value of the underlying currency rises, the reward for mining a new block similarly increases. Rational miners will increase their capacity to mine new blocks until their marginal costs equal their marginal revenue. As miners compete to find the new, more lucrative blocks fastest, the difficulty required to attack the network scales with the value of the currency it secures.⁸⁶

A new permissionless cryptocurrency or one with fairly little adoption, by comparison, may have a sparse market for proofs, and, therefore, a few large entities may exercise outsized control over its maintenance. This may be particularly true of proof-of-stake systems where a large portion of the currency is held by the initial creators of the protocol, and buying these units can only be accomplished via an exchange platform also controlled by the creators. In this scenario the creators can, in theory, reorganize the blockchain, block transactions, or change the underlying fundamentals (e.g. scarcity of the token) with impunity until sufficient tokens to qualify for proof-of-stake are purchased from the creators by unaffiliated users. In proof-of-work systems, at least, the ability to take part in consensus is predicated on dedication of fairly uniform and ubiquitously available computing power and not on possession some exotic digital asset sold only by those already invested in the network. Because of this weakness, many in the community perceive proof-of-stake as a consensus method that can only

⁸⁵ See Nate Eldredge, "How much would it cost to do a 51% attack" *Bitcoin Beta StackExchange* (Sep. 2015) <http://bitcoin.stackexchange.com/questions/40577/how-much-would-it-cost-to-do-a-51-attack>.

⁸⁶ The protocol automatically adjusts mining difficulty based on the cumulative amount of effort expended by miners over the previous 2016 blocks (roughly two weeks). See "Target" *Bitcoin Wiki* (last accessed Jan. 2015) <https://en.bitcoin.it/wiki/Target>.

be built on top of an existing proof-of-work currency: switching the consensus mechanism from work to stake once the currency is already distributed across the network.⁸⁷

Finally, hybrid systems present special challenges to a risk analysis. If certain addresses are enumerated as possessing special powers within the consensus mechanism (e.g. the ability to earn outsized rewards in the Paycoin example⁸⁸) the technology should be viewed with healthy skepticism. Particularly worrisome are hybrid systems marketed as normal proof-of-work or proof-of-stake systems. In these cases, users will presume that rewards come in some fixed proportion to participation, that no special participants exist. If this presumption is untrue, the user has, in effect, been scammed. She was led to believe that participation would grant her a pro-rata stake in the token, when in truth some other stakeholders may have the playing field tilted in their favor.

Scarcity

The core software powering the Bitcoin protocol sets a maximum total bitcoin supply; accordingly, there should at most only ever be 21 million bitcoins in circulation.⁸⁹ The rate at which new bitcoins enter the economy is also fixed in the software. New bitcoins are regularly created and awarded to the miner who dutifully works and finds each new block. On average, new blocks are calculated every ten minutes and the reward amount has been set, from the start in 2009 at 50 new bitcoins per block, to halve every 210,000 blocks (roughly four years). As of today, the reward is at 12.5 bitcoins per block and is predicted to halve to 6.25 sometime in May 2020.⁹⁰ The final bitcoin block reward should be mined at some point in the year 2140.⁹¹

Various tokens may have a different total supply, or a different schedule for the creation of new tokens.⁹² Some may, instead, have no capped supply (*i.e.* they will always be inflationary). The nature of supply is an important variable in assessing investor or user risk because the scarcity of any given cryptocurrency is the central mechanism that establishes commonality between participants: I know that my bitcoin is 1/21 millionth of the total bitcoins that will ever be available; I know that the same is true of yours. If my understanding of the scarcity of some token is untrue (e.g. the software-specified cap is not correctly disclosed) my understanding of my position as it relates to other users is distorted (*i.e.* I may own more or less of the total supply than I'd suspected).

⁸⁷ This is currently the plan for Ethereum. See Zamfir *supra* note 80.

⁸⁸ See *infra* at p. 23.

⁸⁹ See *infra* at note 4.

⁹⁰ "Bitcoin Block Reward Halving Countdown", *bitcoinblockhalf.com*, <https://www.bitcoinblockhalf.com/> (Aug. 2018).

⁹¹ These predictions lack precision not because of uncertainty in the way the protocol is specified, but rather because the time between blocks can only be estimated probabilistically: each block requires an answer to a math problem solvable only by random guess-and-check, six answers will, on average, be found within any hour-long period, but some blocks will be longer to calculate and some will be quicker. See Joseph Bonneau, "How long does it take for a Bitcoin transaction to be confirmed?" Coin Center (Nov 2015) <https://coincenter.org/2015/11/what-does-it-mean-for-a-bitcoin-transaction-to-be-confirmed/>.

⁹² Litecoin, for example, will have a total supply of 84 Million tokens. See Hanna Halaburda, Miklos Sarvary, *Beyond Bitcoin: The Economics of Digital Currencies* (Dec. 2015).

Software is, of course, merely a collection of ones and zeros, therefore changing any cryptocurrency's scarcity (even Bitcoin's scarcity) is potentially as easy as changing a few variables in code. However, the actual implementation of a change will necessarily require acceptance of the new software code by the network of Internet-connected peers that allow the cryptocurrency to function—miners, message relayers, users, businesses etc. That network, built as it will be of thousands of already-invested incumbents, would likely prove resistant to any change that ultimately dilutes the value of its holdings. The reverse, changes that decrease the ultimate total supply, may be less repugnant to incumbents. However, the mere fact that a known fixed supply has suddenly become flexible may be sufficiently unsettling as to make such adjustments unpalatable.

The Bitcoin community generally perceives changes to the underlying scarcity of bitcoins as verboten.⁹³ Other token communities have been less reticent. For example, the underlying scarcity of the token Dogecoin was originally specified as 100 billion total tokens. Later analysis of the software indicated that a variable in the code, `MAX_MONEY`, did not, in fact, limit the total supply (it merely limited the maximum size of any one transaction). The community, after some discussion (and perhaps owing to the meme-based currency community's whimsical and easy-going attitude), decided to carry-on as if this mistake had been deliberate. Dogecoin, once believed capped at 100 billion, became a perpetually inflationary cryptocurrency. Wow!⁹⁴

Regulators should not be primarily concerned with *whether* a given cryptocurrency is inflationary or deflationary, but, rather, how transparent the community is with regard to disclosing these relevant economic fundamentals and discussing any potential changes. These concerns will be revisited in the next section on transparency.

Transparency

Strong transparency is the hallmark of all legitimate cryptocurrency or token projects. Three questions help a regulator to gauge the relative transparency of a given project:

1. Is the software code that powers the network open source licensed and is it widely available for review and analysis?

⁹³ See, e.g., "Prohibited changes" *Bitcoin Wiki* (last accessed Dec. 2015)

https://en.bitcoin.it/wiki/Prohibited_changes ("These changes are considered to be against the spirit of Bitcoin. Even if all Bitcoin users decide to adopt any of these changes, the resulting cryptocurrency can no longer be considered 'Bitcoin' because it has diverged too much from the original design. . . . Increasing the total number of issued bitcoins beyond 21 million. Precision may be increased, but proportions must be unchanged.").

⁹⁴ See dogecoin, "Not actually capped at 100 billion? #23" *Github Dogecoin: Issues*. (Dec. 2013)

<https://github.com/dogecoin/dogecoin/issues/23> ("Hm, I think you are right. It seems that many altcoin algorithms assume `MAX_MONEY` will cap the coin, while a closer inspection of the code seems to reveal that it only caps transaction size and not total coin supply. If this assumption is correct, the way it is will cause something like 5% inflation / year (rather insignificant) after the random blocks have all been mined. More testing is needed.").

2. When changes to that software are contemplated, are the proposed changes made public, and are discussions over the acceptance of those changes public?
3. Is the blockchain created by the network publicly auditable?

Bitcoin provides a good model of transparency. Bitcoin’s software is developed under an MIT open source license.⁹⁵ That means that anyone is free to “use, copy, modify, merge, publish, distribute, sublicense, and/or sell”⁹⁶ copies of the Bitcoin core reference client. As discussed earlier, this reference client need not be copied exactly in order to ensure compatibility with the network. Individuals can change some aspects of this reference software, sometimes referred to as policy rules. For example, a user can alter the core software that she chooses to run on her hardware, in order to avoid relaying transactions below a certain size—perhaps because the user believes these tiny transactions are spam. Additionally, the bitcoin core software can be integrated into a larger software program that provides, for example, an alternative user-experience for a wallet,⁹⁷ versions compatible with smartphone operating systems like iOS⁹⁸ or Android,⁹⁹ more robust key management for highly secure systems,¹⁰⁰ scalability for use in a data-center,¹⁰¹ and any number of other tweaks, changes, or derivative products. As of this report there are: at least 15 versions of the bitcoin client, all with various design goals or device compatibility;¹⁰² at least 12 different software tools for integrating bitcoin payments into online shopping cart systems,¹⁰³ libraries of bitcoin-related software functions and objects in no fewer than 7 different computing languages;¹⁰⁴ and effectively too many mobile apps, browser plug-ins, and web-based wallets to count.

Much of this software is publicly shared and distributed using the online service GitHub.¹⁰⁵ GitHub provides cloud-hosted distributed revision control and source code management for a

⁹⁵ See “Copying” *Bitcoin Core*, *Github* (Jan. 2016) <https://github.com/bitcoin/bitcoin/blob/master/COPYING>.

⁹⁶ *Id.*

⁹⁷ See e.g., Greenaddress, <https://greenaddress.it/en/> (last accessed Jan. 2016) (providing extra security for user hosted bitcoin wallets via multi-signature and n-lock transactions).

⁹⁸ See e.g., Breadwallet, <http://breadwallet.com/> (last accessed Jan. 2016) (“Unlike other iPhone wallets, breadwallet is a real standalone bitcoin client. There is no server to get hacked or go down, so you can always access your money. Using SPV mode, breadwallet connects directly to the bitcoin network with the fast performance you need on a mobile device.”).

⁹⁹ See e.g., Bitcoin Wallet, <https://github.com/schildbach/bitcoin-wallet> (last accessed Jan. 2016) (“Bitcoin Wallet app for your Android device. Standalone Bitcoin node, no centralized backend required.”).

¹⁰⁰ See e.g., Armory, <https://bitcoinarmory.com/> (last accessed Jan. 2016) (“Armory pioneered easily managing offline Bitcoin wallets using a computer that never touches the Internet. Everything needed to create transactions can be managed from an online computer with a watching only wallet. All secret private key data is available only on the offline computer. This greatly reduces the attack surface for an attacker attempting to steal bitcoins.”).

¹⁰¹ See e.g., BlockCypher, <http://dev.blockcypher.com/> (last accessed Jan. 2016) (“BlockCypher is a simple, mostly RESTful JSON API for interacting with blockchains, accessed over HTTP or HTTPS from the api.blockcypher.com domain.”).

¹⁰² See “Clients” *Bitcoin Wiki*, <https://en.bitcoin.it/wiki/Clients> (last accessed Jan. 2016).

¹⁰³ See “Software” *Bitcoin Wiki* <https://en.bitcoin.it/wiki/Software> (last accessed Jan. 2016).

¹⁰⁴ *Id.*

¹⁰⁵ “Explore GitHub” *GitHub*, <https://github.com/explore> (last accessed Jan. 2016).

variety of user-uploaded software projects (most are unrelated to bitcoin).¹⁰⁶ One can think of GitHub as an online track-changes tool (as found in Microsoft Word or Google Docs) for software. Anyone can set up their own personal GitHub account,¹⁰⁷ create a new software repository (like creating a new word document), and/or begin suggesting edits to any other public repository (like using the comment tool on someone else's document). After edits are suggested by contributors, certain specified users can choose to incorporate those edits into the current version in the repository, these special users have what is called "commit access" to the repository.¹⁰⁸ Github also stores a complete history of all changes made to the software since the repository was first created.¹⁰⁹

The most notable Bitcoin software repository on GitHub is Bitcoin Core.¹¹⁰ This is the repository where a group of volunteer developers keep and maintain the current version of the Bitcoin reference client. By looking through the Bitcoin Core repository on GitHub, an observer or security analyst can see the entirety of the current source code, as well as every change to and past version of that code going back to August 2009. As of this report, a look at the GitHub repository shows that there have been nearly 18,000 accepted modifications to the code from over 550 different contributors since the repository was first created in 2009.¹¹¹

GitHub also allows users to "fork" public repositories.¹¹² Forking means that a new identical copy of the software is made available for tinkering, modifying, or incorporating into a larger project. Changes to this fork will not change the software in the original; effectively, it's a tool for building derivative works or for making experimental changes without starting from scratch. As of this report, the Bitcoin Core repository has been forked over 20,000 times.¹¹³ Some of those forks remain compatible with the Bitcoin network as wallets, mining software, or other tools, other forks broke compatibility and went on to become functioning token projects such as litecoin.¹¹⁴ Some of those forks are forked themselves to create a derivative of a derivative of Bitcoin, as is the case with Dogecoin.¹¹⁵

¹⁰⁶ See e.g., the repository for the Linux (open source computer operating system) kernel, <https://github.com/torvalds/linux> (last accessed Jan. 2016).

¹⁰⁷ "Join Github" *GitHub* <https://github.com/join> (last accessed Jan. 2016).

¹⁰⁸ "Permission levels for a user account repository" *GitHub* <https://help.github.com/articles/permission-levels-for-a-user-account-repository/> (last accessed Jan. 2016).

¹⁰⁹ Here, for example, is a history of all changes made to the Bitcoin Core repository: <https://github.com/bitcoin/bitcoin/commits/master> (last accessed Jan. 2016).

¹¹⁰ "Bitcoin Core" *GitHub* <https://github.com/bitcoin/bitcoin> (last accessed Jan. 2016).

¹¹¹ "Bitcoin Core Contributors" *GitHub* <https://github.com/bitcoin/bitcoin/graphs/contributors> (last accessed Aug. 2018).

¹¹² "Fork a repo" *GitHub Help*, <https://help.github.com/articles/fork-a-repo/> (last accessed Jan. 2016).

¹¹³ "Bitcoin Core" *GitHub* <https://github.com/bitcoin/bitcoin> (last accessed Aug. 2018) (Notice the fork counter in the upper right hand corner of the page. By clicking "fork" you too can make your own copy!).

¹¹⁴ "Litecoin" *GitHub* <https://github.com/litecoin-project/litecoin> (last accessed Jan. 2016) (Notice the subtitle under the repository name in the upper left corner of the page: "forked from bitcoin/bitcoin").

¹¹⁵ "Dogecoin" *GitHub* <https://github.com/dogecoin/dogecoin> (last accessed Jan. 2016) ("Dogecoin is a cryptocurrency like Bitcoin, although it does not use SHA256 as its proof of work (POW). Taking

Because of open source licensing and the use of public software repositories like GitHub, Bitcoin's software has been scrutinized by a large, though ultimately unknowable, number of security analysts, critics, hackers, and academics. This means that it is unlikely that any backdoor or severe vulnerability exists in the protocol.¹¹⁶ This also means that it is extremely clear and widely known what the fundamental features of Bitcoin are: it is clear that the protocol puts a limit on the total number of bitcoins that will ever be in circulation, it is clear that the protocol demands that transactions be signed by the private key corresponding to the source address, it is clear that chains with the same bitcoins spent twice will not be recognized as authoritative by the network. These are the technical specifications upon which a user relies when she decides to trade real world valuables for bitcoins; it is important that they be public knowledge and publicly specified in the network's software and documentation.

Additionally, the authoritative record of all Bitcoin transactions, the blockchain, is entirely public.¹¹⁷ This aspect of Bitcoin's transparency adds additional certainty over the question of scarcity. While it is the software that ultimately describes which mining rewards are and are not permissible, it is the blockchain that records the full history of mining rewards, *i.e.* the full history of new money creation in the Bitcoin economy.¹¹⁸ Similarly, while it is the software on the network that would reject attempts to double-spend bitcoin transaction outputs, it is the blockchain that authoritatively records past transactions for the purposes of detecting such counterfeiting attempts.¹¹⁹

The blockchain also records the difficulty, *i.e.* the amount of computing power leveraged to solve the block's proof-of-work calculation, of each newly mined block as well as the Bitcoin public address of the miner who solved that proof-of-work.¹²⁰ This enables the public to view the competitiveness of the market for providing these proofs. To make another comparison to commodities and securities: just as a gold miner must, generally, reveal information about her highly successful operations in order to profit (through the act of selling the commodity), a Bitcoin miner cannot be rewarded for proofs without leaving a publicly auditable record of her windfall. This can be contrasted to a manager within a publicly traded corporation who must be

development cues from Tenebrix and Litecoin, Dogecoin currently employs a simplified variant of script.”).

¹¹⁶ The idea of security by way of massive public auditing and transparency has come to be called “Linus’ Law” and it is commonly expressed as “Many Eyes Make All Bugs Shallow.” See Jeff Jones, “Linus’s Law aka “Many Eyes Make All Bugs Shallow”” *Microsoft Cyber Trust Blog* (Jun. 2006) <https://blogs.microsoft.com/cybertrust/2006/06/07/linuss-law-aka-many-eyes-make-all-bugs-shallow/>.

¹¹⁷ If you are running the free and open software that powers bitcoin you can query any transaction on the network's blockchain. You can also go to a website where blockchain data can be easily searched and viewed *e.g.* *Blockchain.info* <https://blockchain.info/> (last accessed Jan. 2016) (At the top are the most recent blocks accepted by the network; scrolling at the bottom left are the most recent transaction messages sent by users).

¹¹⁸ This transaction, which was included into a block on January 22, 2016, is a coinbase transaction, *i.e.* a transaction that created new bitcoins as a reward for the miner who created this block: <https://blockchain.info/tx/68d7644ae9c6b19924408fe2d5cb56bc1f1d28072e809eda2be56f750401714b>.

¹¹⁹ See *infra* Appendix 2. Digital Signatures and Bitcoin Transactions.

¹²⁰ See *e.g.*, information within Block #394471 as displayed via *Blockchain.info*: <https://blockchain.info/block/0000000000000000056018ef1620bebbc7c817c178e684e5f268ffc9d0b2c83f>

trusted not to “cook-the-books,” and may be capable of profiting at the expense of others in the firm, or even shareholders, without leaving much trace, let alone proof of the value of her contributions to the firm or the legitimacy or fairness of her profits. To be clear, the difference is how controls are placed on would-be bad actors: in a public blockchain, the only way to become wealthier is to leave a public record. In a corporate setting, there may be similar records, but the fidelity of those records is based on legal compliance and honest accounting under the threat of regulatory sanction or shareholder prosecution should past malfeasance be revealed (rather than a verifiable, public, and real time proof of rewards given for proven efforts made).

Aside from the relative transparency of the software utilized within the network and the transparency of the records generated by that software, there is a final area for analysis: the relative transparency of discussions and processes undertaken to update that software. Bitcoin, again, provides a useful baseline.

Within the Bitcoin community, proposals to change the core software are always public. Bitcoin Core is widely regarded as the authoritative version of the software, it is the reference client. However, any software that upholds the consensus rules is, by definition, compatible with the Bitcoin network. One can think of Bitcoin Core as a rallying point around which the community discusses and ultimately chooses how to modify the software on the larger network.

Small changes to the reference client, *i.e.* fixes for small bugs or typos in the software, can be made by forking the public repository (creating an identical copy), making changes to that forked version, and then submitting a “pull request” to the core developers maintaining the core repository.¹²¹ A pull request is simply a formal request that changes made in a fork be incorporated into the original code.¹²² A small group of unaffiliated volunteer developers, referred to as the Core Devs, have permission on the GitHub repository to “commit” these changes to the core software, thus incorporating them into the reference client.¹²³

More fundamental changes to Bitcoin Core, *e.g.* code that creates new features or changes the consensus rules, must be described in a formal specification document, called a Bitcoin Improvement Proposal or BIP.¹²⁴ BIPs are shared amongst developer mailing lists and ultimately publicly displayed in the Bitcoin Core GitHub repository, the Bitcoin Wiki, and elsewhere

¹²¹ “Contributing to Bitcoin Core” *Bitcoin Core GitHub*

<https://github.com/bitcoin/bitcoin/blob/master/CONTRIBUTING.md> (last accessed Jan. 2016) (“The Bitcoin Core project operates an open contributor model where anyone is welcome to contribute towards development in the form of peer review, testing and patches. This document explains the practical process and guidelines for contributing.”).

¹²² *Id.*

¹²³ See Alec Liu “Who’s Building Bitcoin? An Inside Look at Bitcoin’s Open Source Development” *Motherboard* (May 2013).

<http://motherboard.vice.com/blog/whos-building-bitcoin-an-inside-look-at-bitcoins-open-source-development>.

¹²⁴ See “Bitcoin Improvement Proposals” *Bitcoin Core GitHub* <https://github.com/bitcoin/bips> (last accessed Jan. 2016).

online.¹²⁵ The pros and cons of incorporating any BIP into the reference client are hotly debated in online fora as well as in person at publicly accessible conventions and conferences.¹²⁶ Ultimately, these larger changes too, if eventually agreed upon, built-out and tested in forks, could be incorporated into the core software repository through a commit from one of the core developers.

While this description may appear to introduce a central point of control in our understanding of how Bitcoin is developed and maintained, it's important to reiterate that Bitcoin "is" effectively whatever software the unaffiliated network participants choose to run.¹²⁷ The reference client, Bitcoin Core, is just that; it's for reference or exemplary purposes. It is a guide and baseline from which compatible software for the network can be made. So, for example, if the core developers were to lose their minds or be tempted by some dark cause, their malicious changes to that core repository would have no effect on the network or Bitcoin's continued value, unless network participants writ large (miners, users, merchants, exchanges), sometimes referred to as the economic majority¹²⁸ on the network, decided to run the new software on their machines. Additionally, any new software that breaks the consensus rules (the most important rules that prevent fraud) would fork the blockchain, and, unless merchants and exchanges

¹²⁵ *Id.*

¹²⁶ See e.g., "Scaling Bitcoin" <https://scalingbitcoin.org/hongkong2015/#workshop> (last accessed Jan. 2016) ("In recent months the Bitcoin development community has faced difficult discussions of how to safely improve the scalability and decentralized nature of the Bitcoin network. To aid the technical consensus building process we are organizing a pair of workshops to collect technical criteria, present proposals and evaluate technical materials and data with academic discipline and analysis that fully considers the complex tradeoffs between decentralization, utility, security and operational realities. This may be considered as similar in intent and process to the NIST-SHA3 design process where performance and security were in a tradeoff for a security critical application. Since Bitcoin is a P2P currency with many stakeholders, it is important to collect requirements as broadly as possible, and through the process enhance everyone's understanding of the technical properties of Bitcoin to help foster an inclusive, transparent, and informed process.").

¹²⁷ As lead core developer Gavin Andresen remarked in a question and answer session at MIT:

"Q: Thanks for being here. So, early on in your presentation you made mention of how you made some changes in order to keep the gambling site from .. so, the company I am representing, we're working with a central bank in a country in the world to get a license to use Bitcoin in that country. One of their concerns is who controls Bitcoin. What you just said is a fundamental, I don't know what the word is, but you're basically saying that you're in control.

A: I said we were in control.

Q: You and the 5 developers. I'm not against anything, there's no bad stuff going on here, but they want to know who is in control. And when you say things like "we made that change", who's in control.

A: The answer is that everybody. It's the miners. It's the developers. It's the exchanges. It's anyone who decides to run a new version of the software. We made the change. I may have actually implemented the code. I submitted it. It got reviewed. It got pulled into the tree. We spun a release. That didn't change anything at that point. It took people downloading and running the new code for that to change. The entire Bitcoin community decided that this was the right thing."

<http://diyhl.us/wiki/transcripts/mit-bitcoin-expo-2015/keynote-gavin-andresen/> (last accessed Jan. 2016).

¹²⁸ Not to be confused with the majority hashing power across miners on the network.

accept transactions listed on the new fork, the new version will produce nothing of value and be abandoned in favor of the fork with the original consensus rules.

To round up this discussion of transparency, there are several key aspects of Bitcoin that are public and easily auditable. The software is open source. Key versions of that software, the reference client in particular, are publicly displayed in an open, online software repository—GitHub—along with comments, proposed changes, and all accepted changes to that software. The blockchain that the network generates is also, itself, public, and keeps records of all transactions as well as all new money entering the system as rewards for miners. Finally, discussions over major changes to the software are also had in multiple public fora both online and off.

The transparency exhibited by Bitcoin should be the model for all token projects. Several notable tokens follow this model.¹²⁹ Within a token community that has already released a publicly available token, *any* deviation from these transparent practices may be cause for concern. Proprietary software, private blockchains, or closed development communities who announce changes without public debate, engender greater risks to investors and users, because such practices conceal from the participants the very economic and technological fundamentals upon which the digital asset is built. The resultant informational asymmetries are conducive to short-term scams and fraudulent marketing schemes. In such a new and rapidly evolving field, the norm will often be *caveat emptor* (buyer beware); buyers, or—at least—sophisticated proxies for their interests (critics, security analysts, regulators), must have visibility into the community and the code it produces in order to form a clear picture of risks and rewards.

Abundance and Diversity of Developers and Validators

As previously discussed, a token’s consensus rules are enforced by the individuals or groups who have authority to write new blocks to the blockchain. In a proof-of-work system, that set of individuals is open—the ledger is “permissionless”—it includes anyone willing and able to provide energy-intensive calculations to the network, and we call these participants miners. In a proof-of-stake system that set includes users holding sufficient amounts of the cryptocurrency, and in a permissioned distributed ledger, that set will be a group of participants specified *ex ante* in the protocol software, and identified according to a private-public keypair—these ledgers are “permissioned.” Any resulting class of validators can be characterized by how dispersed and diverse they are, and that dispersion or diversity will have implications for the soundness of the token network.

Additionally, the non-mining or non-validating participants on the network may or may not be a diverse group. Long-established cryptocurrencies or cryptocurrencies with strong, user-based development communities will generally have more diverse users. These platforms have multiple use cases and design goals in mind. These various use cases may conflict: for example a community of users who are primarily interested in censorship resistant payment technology (e.g. to make sure that political organizations can take donations even if the credit card

¹²⁹ See e.g., “Litecoin” GitHub <https://github.com/litecoin-project/litecoin> (last accessed Jan. 2016).

networks refuse to process their payments) will often clash with a community of users who want to lower the compliance costs of running a token exchange (e.g. by putting more customer identification tools into the protocol).

When the class of validators and users is large and widespread, there is inherent inertia in the decision-making process. This inertia prevents malicious or questionable changes to the consensus rules from being easily enacted. In a proof-of-work system this inertia is especially pronounced, because changes to the consensus rules could affect the return on investment of miners. Miners on the Bitcoin network must, for example, invest heavily in application-specific integrated circuits, or ASIC chips for short, in order to remain competitive. These ASICs are not multi-purpose computing systems; they can do only one thing well: provide proof-of-work calculations to the Bitcoin network. Miners are, therefore, heavily invested in preserving the status quo of Bitcoin; any change that jeopardizes their future returns is often viewed with hostility.

This inertia would not be present in nascent cryptocurrencies with a small or centralized mining or stake-based community. In these communities, miners may also be the primary developers of the code as well its most ardent promoters and users. Without a competitive market of various stakeholders, monolithic changes to the protocol are more attainable—potentially even changes that benefit some core group at the expense of follow-on investors.

This inertia would also not be present in a permissioned distributed ledger. In such systems a core group of enumerated individuals or groups is empanelled by the developers to enforce the consensus rules. This group, acting together, can block any user on the network from transacting, double spend transactions, change the history of the ledger, and create new money from nothing.¹³⁰

The best evidence of a healthy and decentralized community may be visible examples of disagreement, stalemate, and compromise between various stakeholders regarding proposed changes to consensus rules. The long running debate between Bitcoin stakeholders over changes to the block size cap (the maximum size, in megabytes, that a valid block to be added to the blockchain may be) provides a useful example.¹³¹

The size of a block corresponds to the number of transactions included in that block; so a block size limit is also a *de facto* limit on the number of transactions that can take place per block (i.e. per ~10 minute period).¹³² Additionally, if block space is limited, users hoping to get their transactions validated quickly may compete for inclusion by appending larger mining fees to

¹³⁰ But they can, in theory be identified and punished for this behavior outside of the network using legal sanctions or government regulation.

¹³¹ See Timothy B. Lee, “Bitcoin is on the verge of a constitutional crisis” *Vox* (Aug. 2016) <http://www.vox.com/2015/8/18/9168977/bitcoin-constitutional-crisis>.

¹³² *Id.*

their transactions; miners would sooner include transactions with substantial fees within a finite block than they would a feeless transaction.

The block size limit affects various stakeholders differently. Those focused on consumer adoption—exchanges and merchant processors—tend to want a larger maximum limit, because they do not want their users to suffer either delayed transaction validation or the larger fees that could be necessary to expedite validation if block space was scarce. Those focused on mining or the stability of the network write large, tend to want smaller blocks because (A) there may be bigger rewards to miners if block space is scarce and users compete for inclusion with fees, and (B) smaller blocks travel across communications networks faster and prevent potential problems associated with network latency (like brief forks in the blockchain when two sides of the network disagree over which new block arrived first and is therefore authoritative).

The debate has generated some compromises. Rather than scale the blockchain by increasing block sizes many (if not most) in the Bitcoin community ultimately came to support a scaling solution called SegWit that compresses and truncates the transaction data such that more transactions can fit in the same size block. Ultimately, however, some big block partisans insisted that this was not a suitable way to address the scaling problem, and in mid-2017 some developers decided to fork the network by altering the block size consensus rule in a new version of the Bitcoin software that they developed and released. This fork has persisted and the new resultant token has been named Bitcoin Cash by its partisans.

The block size debate provides a useful example of decentralization because no single viewpoint or stakeholder has been able to easily and successfully advocate for the precise change they want. Instead, a variety of compromises and amicable separations have emerged. The diversity of stakeholders is a naturally conservative force in the evolution of the network. This can be frustrating from the narrow point of view of a partisan in the debate, however it is a boon to the network at large and through the long term—rash changes, fraudulent amendments, and inequitable revisions stand little chance of survival in a highly decentralized community of stakeholders.

Profit-Development Linkage

The final question central to an inquiry into the decentralization of a token is: *Are developers also holding and selling a large share of the scarce tokens, and are they substantially profiting from that activity in the short term?* The question is meant to determine to what degree the developers of a cryptocurrency are motivated by profit, and additionally, what the timescale of that profit-taking can look like.

With a long enough time horizon, anyone could be characterized as motivated primarily by the prospect of future profits. We often cultivate hobbies and skills primarily because of an enjoyment of the work, a desire to participate in a community, or to solve some personal problem in our own lives. If, however, as a result of our efforts we eventually make something of notable commercial value (say, a work of art, an innovative design for a boat hull, a patentable invention for irrigating crops) it would be unusual not to seek and take some profit from that

work. Should we be particularly successful in monetizing our past passion, hindsight may make our otherwise tinker-like motivations appear to be driven more by greed than they really ever were.

Take, for example, the work of Satoshi Nakamoto, the pseudonymous inventor of Bitcoin. He, she, or they, certainly did not harbor the then outlandish belief that a new, toy-like Internet protocol for creating electronic cash amongst a small circle of curious developers would—with any certainty—go on to become a \$100 billion prototype for stateless currency. As stories from the first two years of Bitcoin’s use indicate, the technology was largely prized by enthusiasts, hobbyists, and ideologically motivated individuals. Bitcoins were frequently lost in buried hard drives, at the bottom of landfills, in laptops ruined by spilled beverages, or in thumb-drives misplaced and never found again. Bitcoins were traded more for fun than profit (and often at a great loss if we look at the future price), as in the case of alpaca farmers accepting bitcoins on websites in exchange for woven socks,¹³³ or the case of a million-dollar pizza purchase through a friend across an ocean.¹³⁴

And still to this day several blockchain-based projects are developed by a community of dedicated volunteers; individuals motivated more by the desire to see some cooperative process or service (cloud storage, domain name registries, single sign-in identification, music production, and more) automated and decentralized, rather than any expectation of huge future profits.¹³⁵

Others, however, plainly have less benign motives. Desiring quick profits, they hype their future technology, market it to trusting buyers online, promise future integrations and applications, all without developing much beyond a simple fork of Bitcoin or some other pre-existing open source token software.¹³⁶

But motives and intent can be a difficult metric for regulators or law enforcement to uncover and rely upon in prosecutions. Both the truly radical innovations as well as the scams will often be pitched with similar rhetoric and bravado, or have similar delays in development. Rather than look at the promises or claims surrounding a token, it may be better to look at how the development process is financed, and how the technology is structured to reward (or not reward) the developers.

Earlier, in the section on distribution,¹³⁷ we discussed pre-mining as well as promises of a future minimum price floor. These are notable indications of a strong link between development and profit. Developers creating a pre-mined currency will often retain large amounts of the scarce

¹³³ See Ariella Brown, “Alpacas: the unofficial mascot of bitcoin?” *CoinDesk* (May 2013) <http://www.coindesk.com/alpacas-the-unofficial-mascot-of-bitcoin/>.

¹³⁴ See Brian Merchant “This Pizza Cost \$750,000” (Mar. 2013) <http://motherboard.vice.com/blog/this-pizza-is-worth-750000>.

¹³⁵ See Storj and Madsafe *supra* note 143.

¹³⁶ See Stan Higgins “GAW Miners Altcoin Launch Sparks Speculative Frenzy” *CoinDesk* (Dec. 2014) <http://www.coindesk.com/gaw-miners-altcoin-launch-sparks-speculative-frenzy/>.

¹³⁷ See *infra* at p. 11.

coin. These developers will often be the prime generators of hype surrounding the future promise of the network; the extreme example being a guarantee of a future price-floor for the token (a promise to buy back tokens at a set rate).¹³⁸ If, in response to this hype, the price on exchanges surges once the currency becomes publicly available, the developers may have a strong incentive to sell their large holdings for Bitcoin or some other more reliably valuable asset. At this point the developers can walk away with large windfalls even if the underlying technology has yet to meet the expectations or promises of its marketing. It may simply be a forked version of Bitcoin with different branding, produced and released at almost no cost. When the promised innovations fail to materialize the price of the token on third-party exchanges may plummet, leaving follow-on investors who bought at the height of the craze with nothing.¹³⁹

The clearest indication of an unhealthy link between network profits and development comes from the Paycoin example described in the previous subsection on consensus. In that example, Paycoin was marketed as a standard proof-of-stake based token. Paycoin was, in reality a hybrid consensus system utilizing concepts from both proof-of-stake and permissioned distributed ledger systems. Developers had enumerated certain network addresses within the code, identified with a public-private key pair, in order to grant those users disproportionately large rewards. It is not unreasonable to assume that these addresses were, in fact, in the control of Paycoin developers and promoters. In this example, developers have a very strong profit motive, while Paycoin grows they are benefited by these oversized rewards at the expense of normal users who presumed they were equal participants. The software, in a case such as this, is effectively a bargain that has been fraudulently and materially misrepresented.

These worst-case scenarios can be contrasted with a developer or group of developers who choose to distribute their new tokens only through open, competitive mining, or through an airdrop or proof-of-burn¹⁴⁰ system where bitcoins are sacrificed—not exchanged—by interested users wishing to obtain some of the token. Similarly benign would be development utilizing a sidechain,¹⁴¹ where interested users will simply move bitcoins into the new project, retaining full ownership and control over those digital assets and offering nothing to the developer in exchange.

¹³⁸ See, e.g., suchmoon, “GAW / Josh Garza discussion Paycoin XPY xpy.io BTCLend LNC. ALWAYS MAKE MONEY :)” BitcoinTalk (Aug. 2015) <https://bitcointalk.org/index.php?topic=857670.0> (“A major selling point for Paycoin since its introduction was a \$20 “floor”, i.e. GAW maintaining a USD reserve fund and using it to buy XPY at \$20 each on Paybase. The “floor” has now been rescinded and XPY is trading at market prices.”).

¹³⁹ See David Morris, “Beyond bitcoin: Inside the cryptocurrency ecosystem” *Fortune* (Dec 2013) <http://fortune.com/2013/12/24/beyond-bitcoin-inside-the-cryptocurrency-ecosystem/> (“ Then, when the hyped, bogus coin is released, adoption by cryptocoin enthusiasts can give its value a brief bump, and unscrupulous founders can unload their pre-mined loot. ‘In excess of 80% of altcoins are pump-and-dump schemes in the most traditional sense of the term,’ says Antonopoulos.”).

¹⁴⁰ See *infra* at pp. 13-14.

¹⁴¹ See *infra* at p. 15.

In all of these benign examples, the developers have no means of taking quick profits from their network. Developers working on a token network that openly offers tokens, from the start, to competitive miners get no pecuniary benefit from each marginal miner that joins the network. Developers working on a token that can be obtained by proof-of-burn, do not gain bitcoins from each new user—those bitcoins are simply destroyed in the process. And developers working on a sidechain do not gain control over the bitcoins pegged by users in order to obtain sidechain tokens. The tokens may be branded as something new, but they are perfectly fungible with bitcoins. As the developers of Rootstock, a sidechain that seeks to replicate the smart contracting capabilities of Ethereum, explain,

The sidechain is a two-way mechanism, so when the miners receive the rootcoins in payment for contract execution, they can turn them back into bitcoin right away. So you have a one to one conversion rate. It's actually bitcoins - we call them rootcoins in order to explain that those bitcoins are living in the Rootstock blockchain and not in the Bitcoin blockchain. It's more a conceptual thing.¹⁴²

All this is not to say that sidechain or proof-of-burn utilizing developers stand no chance of profit. Instead, such developers stand the chance to profit—fairly—in the long term from their actions, rather like early pioneers of a new and profitable industry. If successful, they will have helped build a system that generates strong network effects, making it indispensable to a large community of users. Their intimate knowledge of and long-running participation in that system will make them attractive employees or collaborators in business circles. Their own personal investment in the system may also prove lucrative, but they will be risking only their own capital and not that of any prospective user. And, they will—no doubt—profit from their own use of a successfully developed tool; much as any open source software developer is often motivated primarily to create and release a tool to solve some personal annoyance, like having to retype the same code over and over, or build a subroutine from scratch for each new client.¹⁴³

C. Functionality

Our final question differentiating token risk is *what functionality or powers does possession of a token grant the user*. This may be analogized to the legal rights that attend possession of a bearer instrument, however, this should be understood merely as an instructive metaphor. “Possession” of some cryptocurrency or token is most accurately described as exclusive knowledge of some cryptographic secret (similar to a password) that is technologically necessary to record a token transaction (or perhaps record some other data) on the network’s blockchain. Mere knowledge of a secret string of numbers does not, in and of itself, generate

¹⁴² Ian Allison, “Rootstock merges Bitcoin and Ethereum to help the World Bank drive financial inclusion” *International Business Times* (Nov. 2015) <http://www.ibtimes.co.uk/rootstock-merges-bitcoin-ethereum-help-world-bank-drive-financial-inclusion-1528902>.

¹⁴³ Within management science, the concept of user-driven innovation is often referred to as “lead user innovation.” The concept was first developed and explained by MIT Professor Eric von Hippel. See Eric von Hippel, “Lead users: a source of novel product concepts” *Management Science* 791–805 (1986).

any particular legal rights, liabilities, or relationships. For such legal rights to exist, either in contract or property, certain legal circumstances must obtain (e.g. I discovered and brought under my control bitcoins that had been abandoned or as of yet unclaimed, I manufactured bitcoins using my labor, I was gifted these tokens or received them in a bargained-for exchange.) What we refer to herein as “functionality” is the non-legal question of what capabilities will the user have on the network when she has knowledge of the private key(s) that correspond to funded address(es) on the token network’s blockchain.

Functionality across tokens varies from non-functional—a hypothetical future token being promised to buyers in a fundraiser or a token whose only value is contingent on an issuer honoring some promise—to functional because it is probably scarce and transferrable—e.g. Bitcoin—to functional because it grants access to a decentralized computing service—e.g. Ether, a token that allows users to write and run smart contracts on the Ethereum network—to functional because it allows users to vote amongst possible investments and claim profits—e.g. The DAO token that was launched and subsequently failed in 2016.

This section begins by explaining the most basic functionality that a token or cryptocurrency can have: the ability to send a provably scarce asset over the internet without the need to trust any intermediary. Then we will discuss more complex functionality that may adhere to a token. Finally we will briefly discuss what we’ll term non-functional tokens, wherein any usefulness or value inherent in the token is derived not from a decentralized network but rather from promises or guarantees made by the issuer or some other legally responsible third party.

Functionality Contingent on Scarcity and Decentralization

The basic case of functionality is Bitcoin. As François Velde of the Federal Reserve Bank of Chicago has remarked, “Bitcoin is a system for securely and verifiably transferring bitcoins.” Having bitcoins means you can send bitcoins; that’s about it. The nature of the bitcoin network, however, means that this seemingly simple fact is rather revolutionary.

Before Bitcoin there was no such thing as a scarce digital asset that could be sent person-to-person without relying on a trusted intermediary. Computer files like Word documents or images that we might attach to an email or send in a text message can, of course, be sent over the Internet. But when an image or document file is sent, it is not actually transferred *from* one person *to* another. Instead, a copy is made and both sender and recipient have the file. This inherent “copy-ability” of digital things makes electronic peer-to-peer value transfer much more difficult than in-person value transfer, where two people can meet and physically hand over something of value.

Before Bitcoin, if someone wanted to provably send another person money or value electronically, they would have to rely upon a mutually trusted third party to keep track of a ledger that described who gave up the asset and who obtained it. For example, when one uses PayPal to send dollars to a friend, she and the recipient must trust the company, PayPal, to deduct from the sender’s balance and credit the recipients. The same is true with online stock

trading or any other online financial transaction; before Bitcoin, there was always a trusted institution in the middle.

Bitcoin replaces that once-essential trusted intermediary with a blockchain. Now, one Bitcoin user can send bitcoin to another and both can check the public blockchain to confirm that the sender has given up the asset and the recipient has obtained it. Every transaction is included in that ledger and so too, therefore, is a record of the total supply of bitcoins. This means that bitcoins are provably scarce and transferrable despite being non-physical assets.

But Bitcoin's blockchain is not a magical autonomous authority on the internet; it is merely a record of transactions kept by a decentralized network rather than a record kept by a bank or other single trusted intermediary. It is this decentralization, as described in the previous section, that makes Bitcoin truly special. Bitcoin's blockchain and its consensus mechanism allows a person holding a bitcoin to send that bitcoin to someone else irrespective of any person's attempts to censor or prevent the transaction. That isn't a *promise* from some person or company upon which that the holder relies; it is a *consequence* derived from the network's rules and the protocol's ability to incentivize continued, free, fair, and open participation in that network.

Thus the scarcity and decentralization afforded by the Bitcoin network is the fundamental functionality that a person obtains whenever they obtain a bitcoin. It's rather like obtaining some amount of gold. Gold is functional for its holder because it is a reliably scarce commodity that is capable of being transferred and traded (quite literally handed from one person to another). As such it can be a store of value, hedge against other assets, and means of payment. Bitcoin is, in fact, a bit more useful than that, because, unlike gold, it can be sent over the Internet; in essence, gold but with a teleporter.

Functionality Beyond Scarcity and Decentralization

Bitcoin's digital scarcity is revolutionary on its own, but more complicated and flexible token functionality feasible. The proof-of-stake consensus system described in the previous subsection on consensus¹⁴⁴ provides a simple example of further functionality. As with Bitcoin, a proof-of-stake token network gives users the ability to prove control over tokens, and it allows the user to send those tokens to other users, but it also provides a further functionality: provable control over some amount of tokens (*i.e.* the stake) also enrolls the user in a lottery whose prize is permission to write a new block to the blockchain and receive any block rewards or fees that are generated from that new block.

Some developers, utilizing combinations of the technologies described thus far, have begun work on so-called *app-coins*, *decentralized computing platforms*, or *decentralized autonomous organizations*. These developers seek to create a digital platform that generates some kind of cooperative result but does so without utilizing any form of hierarchical or top-down control. The design goal is broad: complex cooperative organization with a network protocol supplanting all or most traditional legal or business structures. Examples are necessary to

¹⁴⁴ See *infra* at p. 18.

avoid unhelpful abstraction in the description of these new platforms. The easiest example is Bitcoin itself. Bitcoin is a system without top-down control that achieves complex cooperation: the transmission and storage of value.

A more extensive example, however, can suggest what the future may hold. To start, consider YouTube, the video sharing website owned by Google.¹⁴⁵ Some aspects of YouTube are run via an open, user-driven market: for example, the choice of which ads to display generally comes down to a bidding process, the choice of which videos to watch comes down to a given user's willingness to expend time and opportunity cost on a given video, and the choice of what videos will be on the platform comes down to whether individual content creators decide to upload their content to YouTube. Much of YouTube is already built from the interactions of users with other users—peer-to-peer interactions mediated through the technology—as compared with the interactions of employees, contractors, or subscribers with the corporation—hierarchical interactions mediated through law or corporate structures.

Ultimately, however, many—perhaps the majority of—decisions critical to YouTube's success are made by the employees, managers, directors, owners and shareholders of YouTube and Google. These decisions include: designing the user interface, choosing whether to censor or remove user-uploaded content, choosing whether to display ads and how often to show them, choosing whether to offer a premium ad-free version, deciding how to design the server warehouses that host all these uploaded videos, figuring out who to pay to build and maintain that infrastructure, and who to hire or fire to develop the platform itself, deciding how to raise capital for future improvements or services. These are decisions made within firms rather than within markets; what Ronald Coase called the islands of socialism within a market economy.¹⁴⁶

Now, imagine a fully user-owned and controlled YouTube. As with today's YouTube, videos are uploaded by users and individual viewers choose their own programming. Unlike today's YouTube however, the myriad other decisions that YouTube, the firm, would make are now made, also, by users. This sort of cooperative control could be achieved by use of a decentralized cryptocurrency specific to the platform—an app-coin.

Users buy or obtain these app-coins (we'll call them YouCoins) and possession of the tokens grants the user certain non-legal rights (technical functionality on the distributed network). Most fundamental may be the right to vote on key decisions regarding how the platform is built and maintained going forward. Rather than having a centralized server warehouse, the platform uses the spare system resources of its users' computers to host, store, and route content (not unlike how the BitTorrent file-sharing protocol allows for the distribution of large files without a centralized server¹⁴⁷), and all of this shared infrastructure is knit together with software. Decisions over how to write and rewrite that software can be made through *ex-ante* specified voting rules (so-called on-chain governance). These rules can be as basic as *simple majority and one token one vote*, or as complicated as needed (with quorums, sequential voting rounds, veto

¹⁴⁵ <https://www.youtube.com>.

¹⁴⁶ Coase, Ronald, "The Nature of the Firm" 4 *Economica* 386–405 (1937).

¹⁴⁷ <http://www.bittorrent.com>.

powers attached to some YouCoins, etc.). If Condorcet, Kenneth Arrow, or the Framers of the Constitution can imagine it, it can be coded in software.

The platform could be ad-supported or it may be fee-based. For example, some number of YouCoins may be required for a user to upload a video, or to view a video. Users who uploaded videos may be paid in YouCoins each time someone views their content. Perhaps they can set their own prices. Other users who sell their spare disk space, network connectivity, or other distributed infrastructure can be rewarded with YouCoins based on the prices they set. The network can be set up to automatically use the cheapest reliable infrastructure first, but as the network becomes more heavily trafficked, infrastructure providers with higher marginal costs and higher prices may find that they too will be paid in YouCoins. This going-rate for use of the infrastructure can be utilized to automatically increase or decrease the prices set for video uploads or views.

Developers who suggest new code that improves the user interface or the underlying network infrastructure could be rewarded with YouCoins when a sufficient number of users vote to include their changes into the new version of the software. Curators who make particularly entertaining playlists of videos could be rewarded with YouCoins when enough users vote to post the curated playlist to the platform's homepage. All of these user interactions (whether voting, uploading, viewing, curating, providing infrastructure, developing the software) are recorded (perhaps by pseudonym for privacy) and the identities of contributors are validated using a shared ledger and scarce tokens to make spam, sabotage, or other counterproductive participation prohibitively costly.

In this hypothetical example, the token is more than a currency; it is a system resource within a distributed computing platform. The coin is used not only as a means of exchange or payment but also as a means to account for, judge, and verify valuable community participation through provable viewership and payment statistics as well as votes cast in decisions over changes to the platform. It is also used to give would-be users a credible commitment that valuable participation will always be rewarded in the future through self-executing contracts and publicly auditable voting rules and records. The distributed computing platform, its transparent design, reliable recordkeeping, and scarce tokens, assure a prospective user: If you help the network by providing extra space for video storage, then you will be rewarded immediately and by the byte. If you generate popular content, then you will be rewarded immediately and by the view.

Under such a system, the token (our hypothetical YouCoin) is the native fuel that facilitates interactions within the cooperative. It also, however, would be a reliable metric for the platform's success writ large. If the platform sees increased demand from new users and if the supply of the token is limited, then its value may increase against dollars or bitcoins. In some ways this increase is rather like the increase in share price for a successful corporation. In some ways, however, it is not. The value of the token comes from the individual actions of all platform participants who are using or holding the token—again rather like the value of a scarce but useful fungible commodity (like oil) within a particular industry. There is no hierarchical

management structure with the ability to raise new capital, create liquidity, and offer or issue equity in this model. Instead, the collective actions of participants determine the relative supply and demand of the token, factors that in aggregate enhance or reduce the value of the whole.

For clarity, we can refer to tokens that are native to some particular consumer-oriented platform, e.g. our distributed YouTube example, as app-coins. A cryptocurrency- and blockchain-based cooperative, however, may have many applications as diverse as the range of centrally hosted web apps we know today (general cloud storage as well as simple video hosting, a network of self-driving cars, an online marketplace like eBay, a review site for local restaurants and businesses), and many of these platforms may share tokens, ledgers, and users. We can refer to these more general systems as distributed computing systems. Some, however, refer to such diverse and multi-purpose blockchain-mediated cooperatives as DAOs, decentralized autonomous organizations, or DACs, decentralized autonomous cooperatives/communities/corporations. While these newer uses of blockchain technology are in large part speculative, a variety of initiatives are, as of this report, actively developing proofs-of-concept.¹⁴⁸

Decentralized tokens may ultimately have many uses beyond value storage or payment. Control over the coin could afford the user with various abilities and capacities on the network. While some tokens may be, primarily, vehicles for speculation, others will be far different. In some cases tokens may be more akin to a system resource (like CPU-cycles, RAM, or disk-space) within a distributed computing system that is built and maintained by a loose community of participants.

Non-Functional Tokens

By non-functional tokens we mean tokens that *don't* or *can't* do anything natively, but, instead, rely on the commitments of an issuer to have efficacy. By way of example, a bitcoin will always allow its holder to write a transaction to the decentralized bitcoin blockchain irrespective of whether any particular person in the world makes good on any promise to Bitcoin users, and its scarcity will be guaranteed by consensus software that rejects attempts to counterfeit or create more than 21 million units. This, as described in detail in the previous section, is what we mean by functional and decentralized. Some tokens however, will only be useful or valuable if certain promises made by issuers or third-parties are kept.

We can imagine a variety of such promises: *The holder of my token will be granted admission to the concert that I'm promoting. The holder of my token will be able to claim a 1/40th share of my business' profits every quarter. The holder of my token will be able to prove to strangers that I have verified their age as over 21. The holder of my token will be able to vote in this state gubernatorial election. The holder of my token will get X number of rewards points to spend in my stores based on*

¹⁴⁸ See e.g., Filecoin <https://filecoin.io/> or Storj <http://storj.io/> (decentralized cloud storage systems), and Blockstack <https://blockstack.org/>, Urbit <https://urbit.org/>, or Maidsafe <http://maidsafe.net/> (decentralized server and identity architecture for web applications).

their past purchasing activity. The holder of my token will be entitled to X dollars, which we have deposited into our bank.

Note that in all these cases there is a real-world good or outcome promised to token holders. Open blockchain networks only have power over the data in their blockchain; they can't reach into the physical world and control real objects. For example, the Bitcoin blockchain can award miners with new bitcoins (which is merely data recorded in the blockchain), but it cannot assign dollars or any physical-world asset to those miners. The interface between a blockchain and the real world will always, at least with present-day technology, rely on some trusted intermediary person or persons. As such, we call tokens with associated issuer-backed promises "non-functional."

It's true that the gold you might redeem from a gold-backed token is functional, but the token itself is just a bearer instrument, a legal document of sorts that ascribes rights and, on its own, nothing more than virtual paper. An analogy to the facts in the paradigmatic securities law case dealing with investment contracts, *SEC v. Howey Co.*,¹⁴⁹ may be helpful. Howey was selling investors a package that included land and a promise to maintain profitable orange groves growing on the land. While it's true that the land and orange groves in the *Howey* case were functional, the promise to grow them and hand over the profits was not; it was merely a bargained-for promise on paper, an investment contract.

Non-functional tokens may still travel "on top of" a decentralized network.¹⁵⁰ For example, several such tokens can be developed on top of Ethereum using the ERC20 token standard,¹⁵¹ and then they can be transferred between ethereum addresses. The decentralized network, however, is only attesting to one question about such non-functional tokens: *who has the token now and who had it before?* The actual usefulness or value of the non-functional token, however, is predicated on the promise made by the centralized issuer and not a decentralized network (as compared with the YouCoin example above, where video hosting and rewards flow from a peer-to-peer protocol rather than the promises of ongoing work made by some scheme organizer).

What we call non-functional tokens could go by various names depending on the underlying promise: security tokens, dollar-tethered tokens, rewards points or loyalty tokens, and more. We will not analyze these non-functional tokens with respect to securities laws except as a contrast to functional decentralized tokens, wherein the value and usefulness of the token is instantly and inherently available to anyone who possesses the associated private keys and wherein no issuer or third-party's promises make that value or functionality contingent. Some of our examples of non-functional tokens are likely securities (*e.g.* anything with rights to shares of profit from the issuer's enterprise) while others likely are not (*e.g.* an identity attestation token, or, probably, a loyalty point). Our concern is the more novel discussion of

¹⁴⁹ 328 U.S. 293 (1946). We discuss this case extensively throughout the final section of this report.

¹⁵⁰ See Peter Van Valkenburgh, "What does it mean to issue a token "on top of" Ethereum?" *Coin Center* (May 2017) <https://coincenter.org/entry/what-does-it-mean-to-issue-a-token-on-top-of-ethereum>.

¹⁵¹ See *Id.*

whether functional and decentralized tokens would or would not benefit from regulation as securities, a discussion we will take up in the next and final section.

III. A Rubric for Securities Regulators

Having outlined a range of variables for tokens, it should begin to be clear how some particular projects may come to resemble traditional securities. This section will systematically undertake that analysis using the Howey test from American securities law as a guide.

The Howey Test

The general applicability of federal securities law to non-standard investments is, in large part, based on the Howey test, taken from the seminal 1946 Supreme Court case of the same name.¹⁵² The test is clearly laid out and can be divided into four prongs alongside a clear statement of facts not relevant to the determination:

An investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person [1] invests his money in [2] a common enterprise and is led to [3] expect profits [4] solely from the efforts of the promoter or a third party, [excluded factors] it being immaterial whether the shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical assets employed in the enterprise.¹⁵³

The Howey test, according to the Court, “embodies a flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits.”¹⁵⁴ It eschews classification based on formalities, such as offering stock certificates, or terminology, such as selling “shares” or “stock,” in favor of a flexible test based on economic circumstances. As a later Supreme Court opinion affirms, “in searching for the meaning and scope of the word ‘security’ . . . form should be disregarded for substance and the emphasis should be on economic reality.”¹⁵⁵

Purchasing tokens utilized on a cryptocurrency network can, arguably, be characterized as taking “nominal interests in the physical assets employed in the enterprise.”¹⁵⁶ Moreover, cryptocurrency technology has, assuredly, been utilized as persuasive window-dressing in the marketing of ponzi schemes, or to use the Court’s terms, “schemes devised by those who seek the use of the money of others on the promise of profits.”¹⁵⁷ Courts and the SEC have only begun to opine on the question of whether any particular purchase of some token is, in fact, an investment contract, and then whether offering those tokens to the public, in general,

¹⁵² Securities and Exchange Commission v. W. J. Howey Co., 328 U.S. 293 (1946).

¹⁵³ *Id.* at 299.

¹⁵⁴ *Id.*

¹⁵⁵ *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967).

¹⁵⁶ *Howey* at 299.

¹⁵⁷ *Id.*

constitutes the sale of a non-exempt, unregistered security.¹⁵⁸ This question should be a fact-specific inquiry dependent on the unique software and community variables exhibited by the cryptocurrency, and utilizing the Howey test as a guide.

Additionally complicating matters, while it is the case that obtaining tokens on a cryptocurrency network is effectively similar to obtaining a nominal interest in physical assets—in internal capital, vaguely defined—if the cryptocurrency or token network is truly decentralized, then this capital is not owned or controlled by a company. It is not on the balance sheet of any corporation or government. Instead, it is capital internal to a peer-to-peer network. The balance sheet is kept by transaction validators (miners, stakeholders, or enumerated users in a permissioned distributed network) and users buy tokens from independent exchanges, miners, or other users. Should a cryptocurrency fit the definition of a security, who—in this complicated arrangement—is the “issuer” or “promoter” under federal securities laws? Is anyone at all? As we go through the subsequent sections, we’ll find that transaction validators and developers may appear to fill this role, but only in certain special circumstances where the cryptocurrency’s software or community variables lead to a situation where the tokens on offer fit into the Howey test. Generally speaking, this will be the case whenever a token is not decentralized and does not provide functionality to users beyond mere expectation of profits.

A fundamental guiding question for regulators should be: is there a person or affiliated group of persons whose honest disclosures are **both sufficient and necessary** to address grave information asymmetries between users of the network and those who are promoting investment in the network? A network powered by open source software and competitive miners or validators working in an open consensus protocol has no such person. Many people may have information about the network’s risks and benefits but no one speaks with authority. It’s more like the gold industry writ-large; many have ideas about the scarcity and usefulness of gold, but no one (save God perhaps) can speak with authority about what gold actually *is* to mankind. A network that lacks this decentralization, however, may very well have persons whose unique knowledge and efforts are essential to understanding the functioning and value of the token. As such, there is little difference between these individuals and the promoters of a security.

The Howey test for an investment contract is, of course, not definitive nor preclusive to a determination that some blockchain innovation is a security; but it presents an excellent rubric for crafting a policy for SEC actions and some clarity for innovators seeking guidance on what factors may present red-flags to the SEC. The following subsections will go through each of the

¹⁵⁸ See, e.g., Peter Van Valkenburgh, “The SEC today has said that some tokens can be securities” *Coin Center* (Jul. 2017)

<https://coincenter.org/link/the-sec-today-has-said-that-some-tokens-can-be-securities>; Neeraj Agrawal, “SEC Chairman Clayton: Bitcoin is not a security.” *Coin Center* (April 2018)

<https://coincenter.org/link/sec-chairman-clayton-bitcoin-is-not-a-security>; and David Benger, “A top SEC official said that Ether is not a security.” *Coin Center* (June 2018)

<https://coincenter.org/link/a-top-sec-official-said-that-ether-is-not-a-security>.

four prongs of the Howey test, looking at how the software and community variables outlined in the previous sections could affect a determination that a particular token sale does or does not satisfy each prong. This should not be viewed merely as an academic legal exercise. Despite the newness of these technologies, the aging Howey test still provides a surprisingly lucid rubric for judging the relative risks of token sales, and determining which sales warrant, from a public policy perspective, some form of oversight. Beyond being, ultimately, the test that a judge might use to determine the statutory authority behind a particular enforcement action, it is also an appropriate standard to determine when buyers of a token are at risk and should therefore be protected by treating that offering as a security, and regulating it as one.

Investment of Money

For this and subsequent sections, the relevant token-project variables described previously will be highlighted in bold followed by a brief description of how these variables correspond to each prong in the Howey test.

Distribution

Variability in the manner that the token is distributed should, from a public policy perspective, be the first factor contemplated in analysis of whether sales of a token are or are not securities (just as the question of investment is in the first factor of the Howey test).

If the primary mode of distributing new tokens is through a sale of those tokens, particularly sales initiated and made directly between users and the developers of the network, then this prong is likely satisfied. A line of cases, generally dealing with memberships in country clubs or private parks, suggests that sales of common assets that are, as of yet, unrealized or undeveloped (e.g. memberships in a country club that will be built once sufficient funds are raised), are more indicative of an investment than sales of common assets already developed (e.g. memberships in a country club already built).¹⁵⁹ In this light, a token that is offered in a **pre-sale**¹⁶⁰ and developed and/or distributed to supporters only after that pre-sale is complete, appears more like an investment of money than mere sales and resales of tokens already mined or distributed on a network that has already been developed. Similarly, **sales of pre-mined tokens**¹⁶¹ by developers, particularly if accompanied by promises of future rewards or a future **minimum price floor**,¹⁶² also appear to fit well within the understanding of this prong.

¹⁵⁹ Compare *Silver Hills Country Club v. Sobieski*, 55 Cal.2d 811, 13 Cal. Rptr. 186, 361 P.2d 906 (1961) (finding that a membership to an as-of-yet unbuilt country club was a security) with *All Seasons Resorts v. Abrams*, 68 NY 2d 81 (1986) (finding that a membership to an extant park was not a security, but rather a right to use). See also *Jet Set Travel Club v. Corporation Commissioner*, 535 P.2d 109 (1975) (“The requirements of the “risk capital” test are not fulfilled because the benefits of the membership have materialized and have been realized by other members prior to any capital raised by the sale of Oregon memberships.”).

¹⁶⁰ See *infra* at p. 12.

¹⁶¹ See *infra* at p. 12.

¹⁶² See *infra* at p. 12.

If, on the other hand, tokens on the network are primarily distributed through **mining**, **proof-of-burn**, a **sidechain**, **airdrop**, or as a **reward for contributing resources** to the network (e.g. in return for providing video hosting capacity in our YouCoin example¹⁶³) there is less evidence of actual investment on the part of users. A line of cases following *Howey* indicates that the risk of losing the value of the contract price is indicative of an investment.¹⁶⁴ In the case of mining or the provision of resources, money is not provided in return for the interest—there is no purchase *per se*; instead, there is participation in the enterprise, effectively labor, in return for rewards. And though we may not always believe we’ve been compensated the fair market value for the work we’ve contributed to an employer or common cause, this disappointed expectation is less calculable than contributing a known sum of money to a formal enterprise with some sort of disclosable risk profile.

The underlying purpose of securities law is to force honest disclosure from issuers who would otherwise be motivated to overstate the value of their company’s shares.¹⁶⁵ We do not have similar laws requiring honest disclosure from more diffuse or abstract common causes to which people give their energies. There is no law, for example, that the scientific community must be honest about the likelihood that cancer treatment breakthroughs will be achievable in the near future, nor do we worry that too many young cancer researchers are contributing to that effort under a false sense of the common endeavor’s likelihood of success.

The analogy to more traditional legal questions may be member-run limited liability corporations, or general partnerships. As participants in the common enterprise, members or partners, like miners, are not characterized as investors.¹⁶⁶

Finally, particularly in the case of airdrops and sidechains, there is no risk of losing the value of the “purchase” because—in the case of airdrops—no value was sacrificed at the outset, and—in the case of sidechains—the token can always be forfeited for the original bitcoin/parent-chain investment at a fixed rate. Therefore, in a sidechained or airdropped token, we would not expect to find an investment of money. Note, however, that if an airdrop is designed to dragoon the recipients into further investing or promoting others to invest in the token, then it may

¹⁶³ See *infra* at pp. 40-43.

¹⁶⁴ See *Majors v. SC SECURITIES COM’N*, 644 SE 2d 710, 373 SC 153 (2007) (“An ‘investment of money’ under *Howey* means the investor must have committed his assets to the enterprise in such a manner as to subject himself to financial loss.”); see also *Jet Set Travel Club v. Corporation Commissioner*, 535 P.2d 109 (1975).

¹⁶⁵ The words of the preamble: ‘An Act To provide full and fair disclosure of the character of securities sold in interstate and foreign commerce and through the mails, and to prevent frauds in the sale thereof, and for other purposes.’ 48 Stat. 77, as amended, 48 Stat. 906, 15 U.S.C. 77d, 15 U.S.C.A. § 77d..

¹⁶⁶ See *Sync Labs LLC v. Fusion Manufacturing*, United States District Court, D. New Jersey, September 4, 2013 (“If the holder of the membership interest participates actively in the LLC (it is “member-managed”), a court is likely to find that he is not relying solely on the efforts of others and the interest is not a security. If the interest holder does not participate actively in the LLC (it is ‘manager-managed’), then a court is likely to find that he is a passive investor and the interest is a security.”).

resemble other stock giveaways that have, in previous enforcement actions, been reasonably construed as unregistered securities issuance.¹⁶⁷

From a pure policy perspective the legal test for investment also elucidates the most important concerns facing users. When new or as-of-yet undeveloped tokens with an uncertain future value are offered by developers in exchange for money, users are at the greatest risk of loss, and unscrupulous developers have the best chance of finding short-term gains (e.g. the windfalls of a pre-sale or the profits from selling a pre-mined token) with little concern over long term obligations (i.e. the developer can easily walk away from the effort, pocketing the funds).

Conversely, if a blockchain token is functional and not a mere idea-to-be-developed by its promoters, then information asymmetries between purchasers and sellers are minimized because of (A) the public blockchain that records all token transfers, (B) the publicly auditable open source software that powers the network, and (C) the contestability of all roles essential to the network's operation. Any and every miner, software developer, or exchange can be replaced and no barrier exists to discourage public and competitive participation in these endeavors. In a token pre-sale, by contrast, there is no blockchain or running open source software as of yet, and most data relevant to the fate of the project as well as the number of tokens sold and the prices of those sales is locked in the minds and plans of a select few individuals. The information asymmetries inherent in a token pre-sale agreement are by-necessity more pronounced than a sale of a token powered by a running decentralized network.

Contrasted with pre-sales, when tokens are distributed to the user in return for valuable participation (e.g. mining or app-coins) or the provable destruction of some other token (i.e. proof-of-burn), even though the user still risks a failure to recoup the value they have contributed or sacrificed, the developer or promoter does not gain any short-term reward from these distribution schemes. Therefore, their interests are better aligned with users—the platform will only benefit them if it survives into the future and grows in real, long term utility rather than mere short term hype and investment.

Finally, when tokens are distributed through an automated exchange with another token at a fixed rate (**sidechains**), provable destruction of another token (**proof-of-burn**) or giveaway (**token airdrops**) then there is very limited risk of loss to the user, and no short term gains available to developers of the sidechain (bitcoins just flow into and out of their network always under the full control of users).

Common Enterprise: Horizontal and Vertical Commonality

The next factor of the Howey test is whether investment is made in a *common enterprise*.¹⁶⁸ Common enterprise has been further refined by the circuit courts into two linked concepts,

¹⁶⁷ Peter Van Valkenburgh, “A token airdrop may not spare you from securities regulation,” *Coin Center* (Sep. 2017) <https://coincenter.org/link/a-token-airdrop-may-not-spare-you-from-securities-regulation>

¹⁶⁸ *Securities and Exchange Commission v. W. J. Howey Co.*, 328 U.S. 293 (1946)

horizontal commonality and vertical commonality.¹⁶⁹ There is currently a circuit split over what sort of commonality is necessary to satisfy *Howey*'s second prong.¹⁷⁰ Briefly, horizontal commonality can be defined as the pooling of investor funds such that the fates of all investors rise or fall together, often—though not always—through a pro-rata sharing of profits.¹⁷¹ Vertical commonality requires that the “fortunes of the investor are interwoven with and dependent upon the efforts and success of those seeking the investment or of third parties.”¹⁷²

Courts and regulators differ on the question of whether mere pro-rata profit-sharing is sufficient to prove horizontal commonality or whether some specific pooling of investor funds by the issuer or promoter must also be shown. If the network is decentralized (powered by open source software and open, competitive mining) and no discernable third party is accepting investments from users in return for their being solely or substantially responsible for the network's future development, then, by definition, no funds are being pooled to build the innovation. If I buy a bitcoin from my friend who mined it (assuming he is one of several miners), then the invested funds are going to my friend and not to the promoter of the network—the funds are not being “pooled” network-wide under the control of the promoter or developer, hence there is no common enterprise. If, on the other hand, a centralized entity has held itself out as substantially responsible for the future efficacy and, thereby, value of the token *and* has accepted investments from users on account of these warranties, then there may be a better case for pooling and horizontal commonality. Thus, younger projects with clear reliance on a discernible number of promise-making developers who have pre-sold their tokens may more likely qualify as securities issuance.

Interestingly, when legal scholars analyze the circuit split between horizontal and vertical commonality, horizontal commonality is uniformly regarded as the more stringent of the two tests (primarily because individual investments in a common enterprise may not always be perfectly fungible as in the case of various tracts of land in an orange grove).

¹⁶⁹ See James D. Gordon III, “Defining a Common Enterprise in Investment Contracts” 72 Ohio State Law Journal 59, 71-76 (2011).

¹⁷⁰ *Id.* at 68-69 (“The Third, Sixth, and Seventh Circuits require horizontal commonality. See, e.g., *Deckebach v. La Vida Charters, Inc.*, 867 F.2d 278, 282 (6th Cir. 1989); *Stenger v. R.H. Love Galleries, Inc.*, 741 F.2d 144 (7th Cir. 1984); *Salcer v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 682 F.2d 459, 460 (3d Cir. 1982). The Fifth, Eighth, Tenth, and Eleventh Circuits use the vertical commonality test. See, e.g., *McGill v. American Land & Exploration Co.*, 776 F.2d 923, 925-26 (10th Cir. 1985); *Villeneuve v. Advanced Business Concepts Corp.*, 698 F.2d 1121, 1124 (11th Cir. 1983) (en banc); *SEC v. Continental Commodities Corp.*, 497 F.2d 516, 521-22 (5th Cir. 1974); *SEC v. Koscot Interplanetary, Inc.*, 497 F.2d 473, 478-79 (5th Cir. 1974); *Miller v. Central Chinchilla Group, Inc.*, 494 F.2d 414, 418 (8th Cir. 1974). The Ninth Circuit now accepts either vertical or horizontal commonality. *Hocking v. Dubois*, 839 F.2d 560, 566 (9th Cir. 1988). The First and Fourth Circuits have declined to decide the issue, leaving their district courts split. See Shawn H. Crook, Comment, What is a Common Enterprise? Horizontal and Vertical Commonality in an Investment Contract Analysis, 19 CUMB. L. REV. 323, 333-40 (1989). Though not yet expressed as a requirement, the Second Circuit appears to favor a horizontal commonality requirement. See *Revak v. SEC Realty Corp.*, 18 F.3d 81, 87-88 (2d Cir. 1994).”).

¹⁷¹ See *Hocking v. Dubois*, 839 F.2d 560, 566 (9th Cir. 1988)

¹⁷² *Id.*

However, when we look at how commonality may or may not exist within a cryptocurrency network, the opposite appears true: horizontal commonality may be easy to establish (my bitcoin is worth exactly what your bitcoin is worth and will rise and fall in value identically) and vertical commonality is difficult to establish. Many companies mine, sell, and/or promote Bitcoin as a network, but their profits and losses will be unique to their individual structure and success within a competitive market for bitcoin-related services. Profits will be tied to internal capital costs (e.g. purchasing new and state-of-the art mining hardware) and internal revenue (e.g. fees earned for facilitating exchanges between buyers and sellers). These profits will generally vary substantially as compared with the simple price of Bitcoin. For example, the price of Bitcoin may plummet but the frequency of trades throughout a panic may generate increased fee revenue for an exchange. Similarly, a developer working on the software of Bitcoin will not find their efforts consistently rewarded in parallel with the going market price. Many volunteer their time to maintain the protocol, sacrificing the opportunity costs of otherwise lucrative programming wages. Others are paid to maintain the protocol by companies or academic institutions in the space.¹⁷³ This will generally be a set salary denominated in dollars rather than a fluctuating rate as percentage of the Bitcoin network's total value.

Moreover, investor risk seems greatest in the token space when vertical commonality *can easily be proved* and horizontal commonality *cannot*. Take, for example, the case of Paycoin. Unlike nearly every other successful cryptocurrency, Paycoin was not a perfectly fungible asset because some stakes in the network paid their holders disproportionate amounts—a weaker case for horizontal commonality.¹⁷⁴ Additionally, the developers of Paycoin, a for-profit corporation called Geniuses at Work, held and sold the vast majority of all paycoins, meaning that their profits tracked well with rise and fall of the Paycoin price itself—a stronger argument for vertical commonality.¹⁷⁵ Paycoin proved to be disastrous for most investors and the creators are under investigation.¹⁷⁶ As a general rule, cryptocurrency networks exhibiting strong vertical commonality between average users and a small class of creators may warrant careful scrutiny from a public policy perspective. Specifically, the following community and software factors are relevant to the two alternative approaches to commonality.

Scarcity

Investment in a token with a known scarcity and fungibility necessarily indicates horizontal commonality. The future of all investors is knitted to the token's value. When some tokens on the network are not, in fact, of equal and fungible value the case for horizontal commonality is

¹⁷³ See e.g., Core developers Gavin Andresen, Cory Fields and Wladimir van der Laan are paid to continue their work on the protocol by MIT, or Greg Maxwell and Pieter Wuille who work for the for-profit company Blockstream. See Pete Rizzo “Bitcoin Core Developers Join MIT Digital Currency Initiative” *CoinDesk* (Apr. 2015) <http://www.coindesk.com/bitcoin-core-developers-join-mit-digital-currency-initiative/>; and “Our Team” *Blockstream* <https://blockstream.com/team/> (last accessed Jan. 2016).

¹⁷⁴ See *infra* at p. 18.

¹⁷⁵ See suchmoon *supra* note 153.

¹⁷⁶ See “Press Release: SEC Charges Bitcoin Mining Companies” *U.S. Securities and Exchange Commission* (Dec. 2015) <http://www.sec.gov/news/pressrelease/2015-271.html>.

weaker. However, particularly if this lack of fungibility is not clearly disclosed (as in the case of Paycoin) such non-fungibility should be a cause for concern as a form of fraud or misrepresentation to users of the network, who often reasonably believe that—as is the norm in tokens—they share equally in a pro-rata distribution of the network’s total value.

Decentralization

Again, horizontal commonality generally requires a pooling of invested funds, usually combined with a pro rata sharing of profits.¹⁷⁷ If the network is decentralized then, by definition, no funds are being pooled to build the innovation. If I buy a bitcoin from my friend who mined it (assuming he is one of several miners), then the invested funds are going to my friend and not to the promoter of the network—the funds are not being “pooled” network-wide under the control of the promoter or developer hence there is no common enterprise (but note that some courts do not require pooling to prove common enterprise).

If there are many unaffiliated miners, transaction validations, and businesses on the network then there is, effectively, no singular promoter with which investors could have vertical commonality. All of these participants will have individuated profits and losses based on their unique business models and decoupled from the price of the token held by typical users. By analogy, if there are many people mining platinum we do not assume a common enterprise with the platinum industry, or any particular platinum miner, simply because we own some of the metal.

If, on the other hand, there is little decentralization in the development and maintenance of a token network (*i.e.* all developers are employed by the same for-profit company and/or there are few and highly centralized transaction validators on the network), then there is a stronger case for horizontal commonality because invested funds are likely pooled among these non-diverse individuals. There would also be a strong case for vertical commonality between an investor class of users on the network, and the small and united group of developers and validators. The network is not made up of diverse participants, it is monolithic and the few individuals or groups with power determine it’s fate; as goes the price of the assets on that network, so goes the profits or losses to the few that actually control it and develop it.

This legal test for vertical commonality and the test for horizontal commonality (*when it includes a pooling requirement*) tracks with public policy goals. Without decentralization, the health and safety of a given cryptocurrency network becomes more reliant on trusting the honest behavior of the few powerful participants or developers. This is against the stated design goal of Bitcoin and many follow-on networks, which is to establish a secure payment mechanism amongst mutually distrustful parties without empowering any sort of trusted third party. The simpler test for horizontal commonality, where pooling is not required and mere pro-rata profit-sharing is sufficient to prove commonality, does not track well with good policy goals. It risks being over-inclusive. Everyone who owns gold shares pro-rata in any profits inherent in the rising price of gold and yet gold, writ-large, is clearly not a common enterprise

¹⁷⁷ Hocking, 839 F.2d at 566

because the totality of money invested in gold is not pooled it is held by diverse and unaffiliated parties. So too would this analysis hold for a highly decentralized cryptocurrency like bitcoin. These themes will be revisited in our analysis of the fourth prong, efforts of a third party.¹⁷⁸

Profit-Development Linkage

If developers hold many tokens and/or distribute pre-mined tokens then there is a stronger case for vertical commonality. As primary holders of the tokens, changes in the price will be a large factor in the profits or losses of the developer, particularly if they choose to liquidate those holdings in a sale of pre-mined tokens.

Here again, the legal test for vertical commonality and the test for horizontal commonality with a pooling requirement tracks with public policy goals. When developers also retain and have the option to sell (or do, in fact sell) a large amount of the network's total tokens, they may be tempted to overstate the value of the network in marketing materials or within online forums. Should the price spike, they may choose to liquidate their holdings and abandon the project.

If, on the other hand, developers do not hold a large share of the total tokens or if they only hold tokens for which they too have sacrificed some value (as would be the case in competitively mined, proof-of-burn, or sidechained tokens) then there is no short term profit-taking motive or incentive to cash-out and abandon the project.

To review commonality in general, vertical rather than horizontal commonality is more indicative of investor risks within cryptocurrency networks. Factors that indicate vertical commonality are presale or pre-mined distribution schemes, a lack of decentralization amongst transaction validators and developers, and developers who also hold a large share of the total tokens on the network—a strong profit-development linkage. The test for horizontal commonality is also indicative of investor risk when it includes a pooling requirement. Without a pooling requirement, the test for horizontal commonality risks being over inclusive, labeling whole industries or ecosystems as common enterprises when they are in fact diverse and competitive landscapes where trust is diffuse and markets combined with generally available public information can best address information asymmetries and investor risk.

Expectation of Profits

In many ways this prong may be the easiest for any token sale to satisfy. These technologies are very new and much of their value is speculative. Accordingly, an expectation of profits is a prime motivator for many who buy or come to hold cryptocurrency. There are only two relevant variables that are worth discussing in greater depth.

Distribution

Tokens pegged to bitcoin via a sidechain indicate that an expectation of profits is unlikely. The value of the sidechain coin will always be pegged to bitcoin, and the only way to obtain sidechain tokens will be to immobilize bitcoins, or—depending on how you choose to think

¹⁷⁸ See *infra* at p. 53.

about it—move bitcoins into the sidechain. Therefore, there is no chance of profits coming from one’s decision to move/peg bitcoins into the sidechain. If the innovations of a sidechain are particularly valuable, then that value should be reflected in the price of bitcoin itself, rather than anything traveling within the sidechain exclusively.

Functionality

If tokens are sought primarily for their use-value because they grant access to some tool or computing platform (e.g. our YouTube appcoin example), then there is a poor case for expectation of profits. This is also relevant for so-called app tokens, and also in the broader case of distributed computing platforms, where tokens are sought by users not to hold or exchange but, instead, as a system resource necessary to build some application that runs on the distributed network.¹⁷⁹

A line of cases stemming from *Howey* supports this analysis. In cases dealing with investments made in housing cooperatives, courts have found no expectation of profits when the investor wishes to live in or rent out the property.¹⁸⁰ Examples from app tokens and distributed computing platforms are not all that different from the real world where purchases of shares in a housing cooperative or communal parkland grant the owner access or a right to use the facility. Some potential examples include tokens that grant the user a right to: store a video in a decentralized cloud, claim a domain name for their website, vote in a contest, or otherwise accomplish some cooperative goal for which the network requires a set type of tokenized “fuel.”¹⁸¹

As we’ve described them, non-functional tokens¹⁸² will, by definition, be sought in part based on an expectation that the issuer will honor a promise to redeem. If that promise is or could become a promise to redeem value that will have increased or been preserved over time thanks to their efforts, then an expectation of profits may be easy to find. We will discuss what type of expected or promised efforts could result in an asset-backed or non-functional token being classified as a security in the next section.

Efforts of a Third Party

This final prong of the *Howey* test revives much of the earlier discussion over vertical commonality.¹⁸³ Where that test focused primarily on correlation—whether the profits of the individual user mirror those of the promoters or issuers—this discussion focuses on the

¹⁷⁹ See e.g., Ethereum, which uses a native token as a necessary “fuel” or “gas” for powering smart contracts. “Gas and transaction costs” *Ethereum Frontier Guide* <https://ethereum.gitbooks.io/frontier-guide/content/costs.html> (last accessed Jan. 2016)

¹⁸⁰ See *Goldberg v. 401 North Wabash Venture LLC*, 755 F. 3d 456 (2014) (finding an investment into condominium units was not a security); *United Housing Foundation, Inc. v. Forman*, 421 US 837 (1975) (holding that a commercial transaction is not a security where the purpose of the transaction is not investment for profit).

¹⁸¹ See *Ethereum supra* note 34.

¹⁸² See *infra* at p. 43.

¹⁸³ See *infra* at p. 45.

question of causation: whether the actions of a particular third party are substantially the cause of increased profits and, more precisely, whether buyers rely on those efforts.

In discussing token projects, it is not uncommon to hear particularly zealous advocates suggest that the technology is “trustless” or that it is guaranteed by “math” alone. These are unfortunate oversimplifications. A user of a token *does* rely on the honest efforts of others on the network. The innovation behind Bitcoin is not the removal of trust, but rather the minimization of trust through decentralization. Bitcoin is arguably the most clearly decentralized of any cryptocurrency and so we will begin this section by looking at why it is unlikely that Bitcoin users rely substantially on the efforts of any discernible third party. Later we will turn to other token projects.

Bitcoin’s decentralization is accomplished using both math (cryptography) and economics (structured incentives built into the protocol). A Bitcoin user, for example, relies on the efforts of miners in order to have her transaction processed and included in the blockchain. However, the protocol ensures that she is never beholden to the honest effort of any particular miner. The protocol is built to accept new blocks from semi-randomly selected miners every 10 minutes on average. If her transaction was deliberately ignored by one miner, the next may still validate it. Math is used to ensure that only serious and invested participants are selected (by requiring a costly calculation to participate) and incentives are built in to the protocol to encourage participation (by rewarding successful miners with the opportunity to create new tokens for themselves, and take any fees attached to the transaction by users). Additionally, if a miner attempts to change the recipient in a transaction, substituting her own address for the address specified by the sender, the network will disregard her fraudulent participation. Math, again, is used to prevent the miner from changing the recipient (because altering the sender’s transaction message would invalidate a cryptographic digital signature from the sender), and incentives, again, ensure that only blocks with valid, signed transactions are included in the chain (other miners will only build on top of blocks that their software says are valid, because building on other blocks would exclude them from the chance to win future mining rewards).

So users do, in an abstract sense, rely on the efforts of third parties to maintain the value of their tokens. Specifically, they rely on miners and the software designers who build software that miners run. However, if a consensus method is well designed, and the developer community is transparent and diverse, that reliance will be, by design, spread across such a large number of participants that the efforts of any single individual or company are, in effect, non-substantial to the value of the whole.

In this best case scenario, saying that a Bitcoin user relies on the efforts of a particular miner or software designer for her profits, is akin to saying that a person who owns land relies on the deed clerk at the county courthouse in order to generate profits. While this is in some ways true, there are innumerable other confounding factors to consider: will the deed clerk act dishonestly? Would the deed clerk get away with it? Can the owner prove title in other ways? did she get title insurance? Is the land in a nice neighborhood? Is the quality of the neighborhood improving? Did she build on or otherwise improve the land? In fact, Bitcoin may

be safer than our land example, because if the clerk forges your deed there may be no record of that fraud—there’s only one record and it lives in the clerk’s office. If a miner tries to reassign your bitcoin it will be checked against every other copy of the blockchain—copies exist on every one of the thousand-plus full peer-to-peer nodes on the network—and the attempt will be immediately discovered and ignored as invalid.

Bitcoin, thanks to its well-functioning consensus mechanism and diverse developer and user ecosystem, is likely the clearest case of non-reliance. However, purchasers of other tokens may clearly be relying on the efforts of a discernible third-party in at least four hypotheticals:

1. Issuer-backed **non-functional tokens**,
2. **Pre-sales** of yet-to-be-developed tokens,
3. Tokens with **poorly designed or permissioned consensus mechanisms**, and
4. Tokens with **small and non-transparent developer communities**.

In these first two hypotheticals there is an obvious third party, either the non-functional token issuers or the fundraiser for the to-be-developed token. We will discuss these hypotheticals with respect to the legal and policy question: *When are the efforts of these third parties sufficiently substantial to satisfy the final prong of Howey?* We’ll briefly turn to that discussion now before analyzing the third and fourth hypotheticals in later subsections.

A line of cases expounds on when the efforts of a promoter are sufficiently substantial. The contrast between two well-known cases, *Gary Plastic*¹⁸⁴ and *Marine Bank*,¹⁸⁵ specifically, merits discussion. In both cases investors were purchasing, at root, a non-security, in the form of bank-issued interest-earning certificates of deposit (CDs) from a non-bank reseller. In *Marine Bank*, the reseller acknowledged it was dealing only in conventional CDs.¹⁸⁶ In *Gary Plastic*, the promoter characterized the investment as wholly different from ordinary bank-issued CDs because purchasers would be able to rely on them for certain benefits. These included: (A) the ability to exit the investment by selling the CD to another interested buyer on a secondary market maintained by the promoter, (B) the ability to sell the investment back to the promoter if interest rates dropped, and (C) the ability to instantly liquidate their CD with the promoter if the original issuing-bank becomes insolvent, and while the promoter pursues a lengthier FDIC-insurance claim against the issuing bank.¹⁸⁷

In the *Marine Bank* case the reseller was not deemed to be issuing securities. In the *Gary Plastic* case, however, the reseller was deemed to be an unregistered issuer because of investor reliance upon these sufficiently substantial additional efforts.

The same should hold true with respect to tokens. If a promoter is selling or reselling tokens, and if they are promising to repurchase them under certain conditions, facilitate the creation of secondary markets where resale will be possible, or make other guarantees about liquidation,

¹⁸⁴ *Gary Plastic Packaging Corporation v. Merrill Lynch*, 756 F.2d 230 (2d Cir. 1985)

¹⁸⁵ *Marine Bank v. Weaver*, 455 U.S. 551 (1982).

¹⁸⁶ 455 U.S. 551 (1982) at 552.

¹⁸⁷ 756 F.2d 230 (2d Cir. 1985).

including redeeming them for valuable real-world assets, then there may be substantial reliance on the efforts of the promoter such that the contract, implicit or explicit, between the investor and the promoter constitutes a security. Within an issuer-backed non-functional token project, the promise to redeem the token for an asset could be a security irrespective of whether the underlying asset is, itself, a security. Similarly, within a pre-sale, the contract to build the future token for investors could be a security irrespective of whether the future token, once delivered, will be a security.

With respect to running tokens that are intended to be decentralized and functional, two factors from our discussion of token project variables, consensus and transparency, and their relationship to the final prong of Howey warrants further discussion.

Consensus

Well functioning **proof-of-work**¹⁸⁸ systems generally indicate that users do not rely on the efforts of any particular miner to provide her profits. In these systems anyone can become a miner simply by submitting costly calculations to the network, miners are semi-randomly empowered to validate new blocks based on their ability to provide calculations, and other miners will ignore attempts at dishonest participation. In this competitive market for creating new tokens and validating the transfers of existing tokens, each would-be miner has strong incentives to behave honestly and is simply incapable of committing certain types of fraud. This is analogous to actual commodities mining: anyone capable of raising capital and developing expertise can become a platinum miner and sell her platinum; anyone can decide to go into the business of transporting platinum or machining it into valuable products. All participants in that market have strong incentives to mine more platinum, find better ways of transporting it, or better ways to make new platinum products. Participants in that market will also reliably fail when attempting certain fraudulent actions; a miner who coats an iron ingot with a thin layer of platinum will not be able to deceive her buyers for long. From a regulatory standpoint, the securities offered within that industry will be private or public investment in the individual platinum firms. No one would think that purchasing platinum itself constitutes a security. And individuals who actually own platinum clearly rely on no one company to guarantee the continued value of platinum as compared to other metals or dollars.

Proof-of-stake¹⁸⁹ systems may be less robust at distributing trust and avoiding an outcome where users rely on a single third party for their profits. A perceived flaw in all known proof-of-stake consensus algorithms is that larger stakeholders on the network may be able to utilize their existing power on the network in order to become even more powerful in the future (*i.e.* use their ability to validate transactions in order to amplify the stake they hold on the network by blocking the participation of other stakeholders).¹⁹⁰ As a core group of highly successful stakeholders solidifies their control over the network, the profits of this group may begin to mirror the price of the token—vertical commonality from our earlier discussion. This is

¹⁸⁸ See *infra* at pp. 18-21.

¹⁸⁹ See *infra* p. 22.

¹⁹⁰ See Poelstra *supra* note 76 at 14.

not only a correlative relationship, the core group is now capable of *causing* profits or losses through their participation. This core group becomes the only group actually receiving the rewards of block validation (whether new tokens or fees from transactions on the network), and can also control all access to the ledger. The value of tokens on this network now mirrors the confidence users have in the controlling stakeholder.

There are, however, many researchers working on improving proof-of-stake systems; if a stake-based consensus mechanism can be designed that avoids this centralization tendency—if stakeholders remained decentralized—then it would be difficult to make an argument that users rely on the efforts of any particular third party.

A **permissioned distributed ledger**¹⁹¹ system will always lead to the reliance of users upon the class of enumerated transaction validations. This group effectively controls the ledger and can issue new tokens at will. All access to the network is mediated by this group, and the total value of the network would therefore be predicated on the faith or trust that users choose to place in that group.

Transparency

Transparency has a twofold importance in this discussion. First, we need transparent software and a transparent blockchain in order to ensure that the network, as it is currently running, is properly decentralized—we need to see how the consensus mechanism is designed and what the network that uses it looks like. Transparency is the only way to guarantee that users are not reliant on the efforts or honesty of any particular parties. Second, a transparent developer community will find it difficult to update (either by mistake or deliberately) existing software in any manner that damages this decentralization.

If the software is developed by multiple unaffiliated individuals with open source distribution, and public discussion of development goals, then no singular individual or organization is primary to the expectation of profits. As per our discussion in the subsection on transparency, Bitcoin provides a useful model for transparent design:

1. Software is published under **open sources licensing agreements**,
2. Software is developed, distributed, and changes are tracked using **public repositories** like GitHub
3. The **blockchain generated by the network is public** and records all transactions on network as well as the proofs submitted by validators/miners.
4. There is an **open system for suggesting bug-fixes or new features** to core software repositories.
5. There are **open discussions over larger changes** to the core software.

If, on the other hand, the software is closed source and not widely distributed or licensed to other participants, then users will necessarily be reliant on the efforts of the copyright holder. If core software is not easily auditable via a public software repository, then users may be reliant

¹⁹¹ See *infra* p. 22.

on the efforts of the private group that maintains and controls access to the software. If the network creates a blockchain visible only to some enumerated group of participants, then users may be reliant on the efforts of that group, or the developers who choose who will be enumerated in the software. If bug-fixes and changes to the core network software can be included secretly and without public discussion or debate, then users may be reliant on the efforts of whoever controls the software development process.

General Policy Goals Based on the Howey Test

The software and community variables explained throughout this paper describe a full range of possible token network designs and developer communities. Based on these variables, it is clear that there are colorable arguments that some token sales can be, in effect, investment contracts. What is, perhaps, more surprising is that the longstanding test for applicability of securities law, the Howey test, happens to also be an effective guide for determining whether a token possess heightened risks to users. The more a given token's software and community variables allow it to fit the definition of a security, the more need there may be to protect its users with regulation.

The reverse may also be true. Tokens (including Bitcoin) that do not have software and community variables indicative of a security under this interpretation of the Howey test, are less likely to pose risks to users. These users are already protected by the decentralization and transparency of their networks. That's not to say that these are riskless assets to hold, but rather that they are more akin to actual commodities—their prices will fluctuate but that is a market phenomenon rather than one controlled by managers or corporate boards.

Chilling Innovation vs. Protecting Investors

Following the analysis outlined throughout this report, securities regulators should take the following approach to these technologies:

1. **Avoid chilling promising innovations that are ill-fitted to the Howey test, presenting less risk to users:**
 - a. **Highly decentralized cryptocurrencies** (e.g. Bitcoin, Litecoin) because of a lack of vertical commonality or a discernible third party or promoter upon whose efforts investors rely.
 - b. **Sidechained** Cryptocurrencies/Blockchains because there is no expectation of profits on the part of participants who hold tokens with a value pegged to their existing bitcoin/parent-chain holdings.
 - c. Cryptocurrencies where initial distribution is made through **open competitive mining or proof-of-burn** because there is no investment of money, *i.e.* no risk capital is provided to an issuer or promoter.

- d. **App-Coins or Distributed Computing Platforms** (e.g. Ethereum) because participants seek access to these tokens for their use-value rather than an expectation of profits.
2. **Take action necessary to protect investors against cryptocurrencies well-fitted to the Howey test, presenting greater risks to users:**
- a. **Closed-source or low-transparency** cryptocurrencies because without visibility into the operation of the technology there is no reason to believe that profits come from anything other than a promoter's hype.
 - b. Open but heavily marketed **pre-sales** or sales of **pre-mined cryptocurrencies** with a **small and non-diverse mining and developer community** when the facts indicate that profits come primarily from the efforts of this discrete and profit-motivated group.
 - c. Cryptocurrencies with **permissioned ledgers** or a **highly centralized community of transaction validators**.

Separate the Analysis for Pre-sale Agreements and Derivative Tokens

Using the above guidelines a regulator or investor can discern different levels of risk inherent in various token projects. A fundamental difference, however, exists between the agreement to buy and sell a future token and the token itself if it has achieved a genuine level of functionality and decentralization. Running the analysis twice, both may turn out to be securities, or neither, or merely the pre-sale agreement, if the token that eventually reached the wild achieved a genuine level of functionality and decentralization making it rather indistinguishable from Bitcoin or some other token that never had a pre-sale.

There is no investor protection argument in favor of a fruit-of-the-poisonous tree approach, wherein the mere incident of a (perhaps non-compliant) historic pre-sale dooms an otherwise decentralized and functional token to perpetual classification as a security. The token should be judged separately to ensure that investors are protected by disclosure and registration when warranted, and only where a discernible third-party exists within the new running token ecosystem whose disclosure would be *both necessary and sufficient* to addressing any information asymmetries that put users of the network and investors at risk. To do otherwise would be akin to deeming the land that was the subject of the sale in *Howey* securities in perpetuity.

There are several reasons why a functional and decentralized token can be distinct from the agreement that may have funded its development:

- **Spreadsheet vs. blockchain:** Pre-sale-rights are generally evidenced by private records kept by the preseller, issuers, or an agent of these parties. Actual token ownership is evidenced by a decentralized blockchain.

- **Profit vs. use:** Pre-sale rights are useful exclusively as a marker of future value owed to the holder. A decentralized token may be useful for peer-to-peer currency-like transactions, for paying for use of a decentralized computing system, and/or as a reward for miners or validators who maintain the system.
- **Reliant on the few vs. the many:** Pre-sale terms, recordkeeping, and promised efforts of the issuer are dependent on a small number of individuals. A running token network's continued vitality may be dependent on hundreds of independent software developers, thousands of independent nodes, and millions of users.

In short, separate and apart from any investment contract that may or may not exist at the birth of a token, the token, once running, may be sufficiently functional and decentralized for it to no longer fit the relevant test for treatment as a security. Conflating the pre-sale and the running network is confused analysis that could be misunderstanding the tech or the law or both.

For a real world analogy, take the facts of the *Howey* case itself, and make a small change. As before, Mr. Howey convinces people to give him money for land in Florida; he says they own the land and he says he'll maintain the orange trees that grow on the land. But, instead of promising to pay investors profits from selling the oranges at market, he promises to give them the oranges. This fact does not change the outcome in *Howey*—the court would still have found that investment contracts for an orange grove in Florida had been sold—but, of course, the oranges themselves would never have been found to be securities. If one of the resultant oranges ends up in a grocery store, you don't need a broker dealer to buy it for you. People know this intuitively with oranges and other scarce physical things (of course this inert object I hold in my hand isn't a security—it's just a thing), but many haven't yet internalized that scarce digital things now exist and the same reasoning applies.

That digital scarcity is, indeed, striking and revolutionary, and while it certainly does not warrant a complete revolution or revision of securities laws, it does warrant extra-careful application of existing flexible standards. Only this cautious and educated approach can ensure that investors are protected without unnecessarily stifling capital formation and a vibrant new technological ecosystem.

Conclusion

Tokens, including cryptocurrencies like Bitcoin, will likely have a profound effect on the future of the Internet, financial technology, and governance systems in general. Perhaps the most exciting aspect of the technology is that it is entirely open for experimentation—there’s no patent or copyright to license, no university or corporation from which to seek a job, no exclusive membership fee to pay. Anyone with a computer and an Internet connection can develop and share her own currency, her own vision of the future. The openness of this system makes it vibrant but it also can make it hazardous. Some new uses of the technology will be nothing more than scams garnished with the sort of techno-babble that inspires, confuses, and beleaguers the caution of naive investors who want to believe. The framework described in this report will hopefully enable regulators to more easily delineate between these inevitable scams and the legitimate innovations that will improve our lives, ensuring that a few bad oranges do not spoil the grove.

Appendix

1. The Bitcoin Mining Mechanism: Proof of Work Consensus

New bitcoins are created by miners who prove to the larger network that they have solved a math problem. Specifically, the network expects competing miners to release new “blocks.” A block consists of various information including: (a) valid transaction data for some period of time on the network, (b) an identifier (a “hash”) for the preceding block (so that the chain or order of blocks can be determined), and (c) a random number or “nonce.” In order to be a valid new block that will be accepted by the other peers on the network, the “hash” of the data in the new block must begin with a certain number of zeros.

A hash function is a mathematical process that consistently generates a short, fixed size output from an input of indeterminate size. Good hash functions are designed to always generate a unique output for any possible input and also designed such that the output appears random. For example, using the SHA256 hash function (the same function used in Bitcoin), the text of the first paragraph of the Declaration of Independence becomes:

0e948931f853d6a087339383663faa8794f8b657c8da85c9f7149effbac7d15b

You can try this yourself by cutting and pasting the text of the Declaration’s first paragraph¹⁹² into a web-based hash calculator.¹⁹³

The bitcoin network will only recognize new blocks as valid when the hash of their contents begins with a certain number of zeros, *e.g.*

¹⁹² As transcribed at http://www.archives.gov/exhibits/charters/declaration_transcript.html

¹⁹³ See *e.g.* <http://www.xorbin.com/tools/sha256-hash-calculator>.

0000000009c5c4a6d5434de87dbd4162f745f32b2a6aedf89c89d31d863b022b

Any hash with that many zeros at the start would be valid, but because hashes are designed such that most inputs generate random-looking outputs, finding an input that would create such a regular output is difficult, like finding a particular grain of sand on the beach.

To create an output hash with sufficient leading zeros, miners need to try multiple different inputs with different random numbers, called nonces, until they stumble upon an output with sufficient leading zeros. Leveraging specialized equipment and the additional electricity necessary to power it, some miners gain an edge in calculating these hashes, increasing the odds that they'll be the first to find each new block.¹⁹⁴

New bitcoins are created by miners who find block hashes with sufficient leading zeros. The new bitcoins are, technically, just a transaction recorded in that new block called a *coinbase transaction*.¹⁹⁵ Coinbase transactions have no sender (the bitcoins are new) and the miner specifies a recipient, herself. The miner can then send these new bitcoins to other users by writing another transaction (which would be recorded in subsequent blocks) referencing the coinbase transaction as the input for the transaction, and specifying another bitcoin user as the recipient. Users are identified using pseudonymous public addresses, and can exercise control over the transactions sent to them by signing transaction messages with corresponding private keys. All bitcoin transactions are incorporated into the data that miners hash in order to create new blocks. The recipient of a transaction can be certain that her public address is now the only user in possession of the bitcoins because she can see all transactions going back to the original creation of the bitcoin on the blockchain, the coinbase transaction from the miner that solved that block.

2. Digital Signatures and Bitcoin Transactions

To make a Bitcoin transaction, a user must write and sign a valid transaction message and send it to the peer-to-peer network, (more accurately the user's software writes, signs, and sends the message at the user's behest).

These messages are signed using an ECDSA keypair. ECDSA stands for *elliptic curve digital signature algorithm*. It is a widely used digital signature algorithm that creates a matching public and a private key. Messages (whether on the bitcoin network or elsewhere, e.g. emails) can be signed using the private key before they are sent to recipients. If, while in transit, the message text is altered by a malicious interloper, the signature will no longer match the sender's previously announced public key. The recipient can therefore check the signature as

¹⁹⁴ For a more detailed description of Bitcoin mining, see Peter Van Valkenburgh, "What is Bitcoin Mining and why is it Necessary?" Coin Center (Dec. 2014) <https://coincenter.org/2014/12/bitcoin-mining/>.

¹⁹⁵ Not to be confused with the company, Coinbase, which runs a third party exchange (bitcoins to and from dollars) service. Coinbase, like several other companies (e.g. itbit, xapo, blockchain.info) builds software that helps people access the bitcoin peer-to-peer network in a user-friendly manner. These companies do not build or maintain the network itself.

compared with the message text and the purported sender's public key in order to verify that it originated from that sender and has not been altered in transit.¹⁹⁶

In order to make any bitcoin transaction, the sender's transaction message must reference "inputs"—generally, past transactions wherein she was the recipient—that will fund the transaction. Transactions typically have specified recipient(s) identified by one or more public addresses. These addresses are generated from an ECDSA public key (described above). In order to fund her new transaction, a user can reference any transaction on the blockchain that she can sign using the private key that matches the prior transaction's specified public key(s). Attempts to reference transactions as inputs without providing valid signatures for those inputs will result in invalid transaction messages that the network will ignore as per the bitcoin consensus rules.

Digital signatures, as described in the previous two paragraphs, accomplish much of the work in setting up an electronic cash scheme like Bitcoin. However, one problem remains. How can the recipient of my transaction be certain that I've never before signed these input (funding) transactions over to someone else? If the same prior transaction can be used to fund endless future transactions, then the scheme fails to maintain the scarcity of the electronic cash. Signing a transaction is effectively costless, and I could sign as many as I'd like, effectively like sending an email over and over to many different recipients. This is known as the double spending problem in computer science. To solve it, Bitcoin and other cryptocurrencies utilize a blockchain, an authoritative list of all past transactions. Transactions are only considered final and may only be spent in future transactions once they are on the blockchain, and a transaction will not be included into the blockchain if it references, as inputs, transactions that have already been spent to fund other, previous transactions (i.e. is begin double spent).

3. Sidechains

A sidechain is effectively a token (i.e. a different blockchain keeping track of the movements of a different batch of scarce tokens), but it has a pegged exchange rate with Bitcoin.¹⁹⁷ To use the sidechain, a user sends her bitcoins to a special address on the Bitcoin blockchain, at which point that bitcoin will be immobilized and a token on the sidechain will be released to a sidechain address that she controls. The same happens in reverse. A user of the sidechain can send the sidechain token to a special address that will immobilize the token and release the corresponding bitcoin on the bitcoin blockchain back into her control. This "conversion" occurs without trusted intermediaries because it relies solely on mathematically provable statements (x bitcoins have been sent to y bitcoin address; x sidechain tokens have been released from y sidechain address), referred to as SPV proofs (Simple Payment Verification proofs)¹⁹⁸ on the two

¹⁹⁶ See e.g. https://www.nsa.gov/ia/_files/ecdsa.pdf

¹⁹⁷ See *id.* at 8 ("Two-way peg refers to the mechanism by which tokens are transferred between sidechains and back at a fixed or otherwise deterministic exchange rate.").

¹⁹⁸ See *id.* ("A simplified payment verification proof (or SPV proof) is a DMMS [dynamic-membership multi-party signature] that an action occurred on a Bitcoin-like proof-of-work blockchain.").

decentralized networks (bitcoin and sidechain).¹⁹⁹ Given the fixed conversion rate, and the automated and deterministic process for conversion, it may be more appropriate to think of sidechains as new blockchains that the user can simply move her bitcoins into and out of at will.

¹⁹⁹ See *id.* at 10 (“To use Bitcoin as the parent chain, an extension to script which can recognise and validate such SPV proofs would be required. At the very least, such proofs would need to be made compact enough to fit in a Bitcoin transaction. However, this is just a soft-forking change, without effect on transactions which do not use the new features.”), and *id.* at 17 (describing a temporary alternative for Bitcoin integration—the Federated Peg) .