WHY BITCOIN SHOULD BE REGULATED BY THE SEC

Avnish K. Mangal[*]

[*] The author is a second-year law student at Cornell Law School, expected J.D. in 2015. The author would like to thank Professor Charles K. Whitehead for his helpful feedback and guidance in writing this paper.

INTRODUCTION

Bitcoin is a revolutionary digital currency that has in recent years taken the media by storm. Most people analogize the technology to currency because it can be used to conduct transactions. One might trade Bitcoin, just as one might the U.S. dollar, in exchange for goods and services. However, as will be discussed throughout this paper, comparing Bitcoin to fiat currencies serves only as a superficial analogy, and nothing more.[1]

Bitcoin was first introduced as a concept in 2008, by the mysterious pseudonymous author, "Satoshi Nakamoto."[2] At that time, the technology was prohibitively complex for regular PC users; computer programmers and financial mathematicians were its only constituents. But as the underlying software underwent continual updates, more people began to participate. Over the following years, bitcoins slowly gained in popularity and price, in turn causing more people to pay attention. Finally by 2013, nearly four years after its creation, Bitcoin successfully entered the mainstream.[3]

Even today, the technology remains highly complex and many of its greatest innovations revel in the obscurities of cryptography, mathematical formulae, and distributed networking. However due to the consumerization of many Bitcoin software components, regular users are able to participate in Bitcoin without understanding any aspect of it. Furthermore, those that do

---

[1] Though this paper will continue to refer to Bitcoin as a "digital currency" or "cryptocurrency," it is nonetheless important to remember that Bitcoin is *not* a fiat currency. It is fundamentally different from ordinary currency in many important ways, all of which will be explored throughout the paper.

[2] Satoshi Nakamoto, *Bitcoin P2P e-cash paper*, MAIL-ARCHIVE (Nov. 01, 2008), http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html.

[3] Neils Christensen, *2013: Year Of The Bitcoin*, FORBES (Dec. 10, 2013, 2:34 PM), http://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/.

choose to research the topic will inevitably face overwhelming numbers of articles that do more harm than good for understanding how Bitcoin works. To present Bitcoin to the general public necessarily requires watering down its intricacies, and news sources have done so with remarkable carelessness. Between unsophisticated news outlets and uneducated technology bloggers, common investors are presented with an endless supply of misinformation about Bitcoin. And it is precisely through society's perpetual misunderstanding of what the technology is, and more importantly what it is not, that investors worldwide keep getting scammed.

I. BITCOIN: A REVOLUTIONARY CRYPTOCURRENCY

A. What is Bitcoin?

1. Bitcoin is a Digital Unit of Exchange

Simply put, Bitcoin is nothing more than a digital unit of exchange. It is not a currency, it is not affiliated with a government, and it is not backed by goods of intrinsic value. However, anyone in the world can access Bitcoin, assuming they have an Internet connection. In fact, this notion alone creates a value proposition for many people, particularly because the *only* requirement of Bitcoin is an Internet connection. For example, if someone in a third world country does not have access to a bank, he is otherwise precluded from Internet commerce entirely. It does not matter whether he has Internet access; the fact is that to conduct any legitimate transaction, he would either need a bank account or a credit card. Both would require him to interface with some sort of financial institution, and depending on where he lives, this may be an impossibility. However, Bitcoin is designed such that all transactions occur directly between buyer and seller. Thus, access to financial intermediaries is no longer a consideration for

anyone wishing to buy or sell goods online.

Fundamentally, this is perhaps the greatest selling point of Bitcoin—financial intermediaries are removed from transactions. However, most people dramatically misunderstand the implications of such a system. Bitcoin is typically promoted as a "decentralized peer-to-peer payment network,"[4] and that is true to some extent. However, such phrasing also perpetuates a devastating oversimplification of how Bitcoin works.

Bitcoin is only decentralized to the extent that government agencies cannot regulate it. Because of the way it is built, bitcoins are distributed based on an algorithm as opposed to government monetary policy. In that sense it is true that institutions like the Federal Reserve do not control Bitcoin. However, that does not preclude other parties from having de facto control over the network. In other words, the absence of government does not conclusively prove that Bitcoin is completely decentralized. At best, it is only decentralized from governments.

The peer-to-peer aspect of Bitcoin also lends itself to confusion. Historically, peer-to-peer networks have been used across the world to distribute illegal data such as stolen documents, movies, music, or video games. Generally one of the advantages of such networks, as opposed industry standard client-server networks, is that they provide some heightened level of anonymity. As opposed to conducting all of your file transfers through a single party, peer-to-peer networks allow computers to connect directly with one another. Therefore, where the single party might require users' identifications, peer-to-peer networks typically cannot incorporate such requirements. However, that is not to say that all peer-to-peer networks preserve the anonymity of their users. Bitcoin again plays on people's assumptions when it advertises its

[4] BITCOIN, https://bitcoin.org/en/faq#what-is-bitcoin (last visited May 12, 2014).

peer-to-peer nature. While it is true that Bitcoin transactions take place between public addresses, which theoretically do not contain personal information, it is still very possible, and indeed somewhat easy, to ascertain the identity of Bitcoin users.

2. Bitcoin is Not a Real Currency

Though Bitcoin is often referred to as a currency, it not recognized by any government as legal tender. In fact, on March 25, 2014, the Internal Revenue Service issued a notice deeming Bitcoin as *property*, not currency.[5] Though some of Bitcoin's advocates vehemently argue that Bitcoin is a currency, for the purposes of U.S. securities regulation, the IRS's statement is particularly important. Whether or not Bitcoin is a de facto currency is immaterial; so long as it remains unrecognized as legal tender in the United States,[6] Bitcoin is at best a speculative investment. The implications of such a distinction will be discussed later in this paper.

B. Why is Bitcoin Unique?

1. Online Commerce Can Be Problematic

Cash transactions may seem obsolete in the face of modern Internet commerce, but they do possess interesting advantages for both buyers and sellers. For one, cash transactions are effectively irreversible. When the buyer exchanges cash for the seller's goods or services, in the event of a defect, the buyer's only recourse is to work with the seller directly. Though this disadvantages the buyer by limiting his recovery options, it also implicitly reduces the

[5] IRS NOTICE 2014-21 (2014), *available at http://www.irs.gov/pub/*.

[6] BITCOIN, https://bitcoin.org/en/faq#what-about-bitcoin-and-taxes (last visited May 12, 2014).

transaction cost of the exchange. Therefore, to the extent the buyer feels safe in dealing with the seller, the buyer might in fact have access to lower purchase prices when using cash because the seller does not have to pay intermediaries to facilitate the exchange. Another advantage of cash is its intrinsic anonymity. Parties may buy and sell at will, without having to worry about extensive paper trails of their conduct.

In online commerce however, both of these advantages disappear. Financial institutions are relied upon to process electronic payments, and therefore serve as permanent third parties to all transactions. When disputes arise, financial institutions inevitably involve themselves in mediation, which in turn means that transactions are never truly non-reversible. One problem with third parties being able to reverse transactions is increased transaction cost. Nakamoto, the author of the original Bitcoin white paper, argues "[t]he cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services."[7] While cash exchanges allow parties to avoid transaction costs, there is no digital equivalent for similarly "lightweight" transactions, which means if parties wish to participate in Internet commerce, they must necessarily accept transaction costs.

Another problem with potential transaction reversibility is that sellers generally bear the burden of fraudulent activity. For large, institutional sellers this is generally not a problem. However for small time sellers, particularly those in third world countries, such costs are prohibitively expensive. Thus, in a system where financial institutions generally prioritize the

[7] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN (2008), https://bitcoin.org/bitcoin.pdf.

protection of buyers over sellers, small business owners must choose between either bearing fraudulent buyer activity, i.e. buyer disputes transaction without cause, or not conducting business altogether. Therefore, while large, corporate sellers can easily bear the aggregate transaction cost of involving intermediaries, small-time sellers are left to their own devices.

2. Bitcoin Removes Third Parties

As explained earlier, perhaps Bitcoin's greatest value proposition is its ability to facilitate exchange without involving such intermediaries. Thus, Bitcoin's removal of third parties actually serves two functions: (1) bringing online commerce to markets that would otherwise be inaccessible, and (2) empowering small-time sellers to open online businesses without bearing the transaction costs of mediating third parties. By using a peer-to-peer, distributed network for managing all payments, Bitcoin is able to avoid financial institutions processing users' transactions. Instead, Bitcoin uses its entire distributed network for processing *all* transactions for *all* parties in the world. Consequently, Bitcoin relies on one global, public ledger, used for tracking every payment made across the entire world.

C. How Does Bitcoin Work?

As a starting point, though Bitcoin resembles cash in some ways, it is fundamentally different in that Bitcoin has no physical manifestation like cash. Unlike legal currency, Bitcoin is entirely composed of digital, cryptographic signatures all stored within single digital files. Simply put, these files are nothing more than lists of accounts and transactions, much like a

traditional ledger.[8] When a transaction takes place, the sender of funds broadcasts a signal on the network indicating the amount the receiver's account should go up, and the amount the sender's account should go down. A copy of this file is maintained on every PC in the Bitcoin network, and with each transaction, each computer ("node") applies the transaction to its own copy of the ledger. Using math-based security, this distributed group of PC's (peer-to-peer network) is able to maintain a single global, synchronized copy of a ledger, reflecting each and every transaction that takes place.

1. Acquiring Bitcoins

One can acquire bitcoins in two fundamentally distinct ways: through "mining," i.e. creating new bitcoins, or through trading, e.g. exchanging cash for existing bitcoins.[9] The former method, mining, literally involves users *generating* Bitcoins via special software. Though they are not purchasing bitcoins outright, users still end up paying other operational costs (e.g. electricity) that ultimately cut against any profits they might earn via mining. The latter method, purchasing bitcoins via exchange, is of particular importance to this paper as it presents the starkest case for why Bitcoin is a security.

a. What is Bitcoin "Mining"?

Conceptually speaking, at some point every currency must be distributed into circulation.

[8] Scott Discoll, *How Bitcoin Works Under the Hood*, IMPONDERABLE THINGS (SCOTT DRISCOLL'S BLOG) (Jul. 14, 2013), http://www.imponderablethings.com/.

[9] BITCOIN, https://bitcoin.org/en/faq#how-does-one-acquire-bitcoins (last visited May 12, 2014).

Fiat currencies generally accomplish such tasks by appointing government agencies. For example in the case of the U.S. Dollar, the Federal Reserve controls the money supply.[10] However, in the case of Bitcoin, there is no "central" authority. Therefore, distribution is handled in a somewhat unique manner.

Simply put, Bitcoin mining serves to both verify pending transactions on the Bitcoin network, *and* to release new bitcoins. By installing mining software on their PCs, users can automatically generate bitcoins by dedicating their computers to solving computationally difficult puzzles.[11] These puzzles serve as a self-regulating mechanism for the Bitcoin network in two ways. First, the puzzles are gradually scaled in difficulty so that only set amounts of bitcoins are released every 10 minutes. This ensures a steady release of bitcoins into the market, and avoids excess supply of bitcoins. Second, the puzzles themselves serve a greater purpose beyond creating money—they are used to check the legitimacy of pending transactions on the entire network. Thus, users are incentivized to mine not only for personal benefit, but to also sustain the network itself.

b. How Can Someone Trade for Bitcoins?

Besides mining their own coins, users can also trade for bitcoins in one of three ways:

[10] THE FEDERAL RESERVE, http://www.federalreserve.gov/paymentsystems/coin_about.htm (last visited May 12, 2014) (The Federal Reserve has authority to determine money supply levels on its own. The Federal Reserve's website states: "As the nation's central bank, the Federal Reserve issues and processes Federal Reserve notes. The Federal Reserve also distributes coin through depository institutions. . . . The amount of currency in circulation depends on the public's demand for currency." Therefore, as opposed to a mathematically distributed algorithm like Bitcoin, the U.S. Dollar can be over or under inflated by a single institution at will).

[11] John Kelleher, *What Is Bitcoin Mining?*, FORBES (May 08, 2014, 3:08 PM), http://www.forbes.com/sites/investopedia/2014/05/08/what-is-bitcoin-mining/.

(1) trade cash for bitcoins via an online exchange; (2) trade cash for bitcoins via a local person; or (3) sell goods or services for bitcoins, either online or in person.[12] These methods are relatively easy to understand, as they closely resemble how one might acquire traditional fiat currency. For example, through some basic research, one can find hundreds of companies willing to trade bitcoins in exchange for currency. The main issue with these methods, particularly with the exchanges, is that in an unregulated state, these markets are highly unstable and remarkably vulnerable to fraudulent activity. This will be discussed further below.

2. Using Bitcoins

Bitcoin functions on public and private key cryptography. As opposed to traditional currency, where transactions occur between legally identifiable individuals, Bitcoin transactions instead take place between "public addresses." This is a crucial component to how the Bitcoin network achieves its decentralized nature.

For example, suppose Adam wants to send a payment to Baker. In a traditional currency model, Adam has two options: (1) he can physically hand cash to Baker, or (2) he can set up an online transaction where a bank handles the transfer of funds between Adam and Baker. In the former, Adam is responsible for identifying Baker. When he hands cash to Baker, he is reasonably assured that Baker is in fact receiving the payment because Adam can visually verify Baker is the recipient. In the latter scenario, the banks themselves must verify the true identities of the parties, ensuring that the payment is being sent from Adam to Baker, and not from Adam

[12] BITCOIN, https://bitcoin.org/en/faq#how-does-one-acquire-bitcoins (last visited May 12, 2014).

to a different party.

The Bitcoin protocol, however, functions differently. It uses a global ledger, which without further clarification would imply zero anonymity in transactions. Instead of using people's real identities however, Bitcoin instead conducts transactions between public addresses. For example, instead of the global leger showing that Adam sent a payment to Baker, the Bitcoin network would instead show that "13mw3EK4jw6aF4umThagnhw82Kgkojt3Kk" sent a payment to "1LLaMxyCm58C57GnMsHP83TeM6KFcoyEf8." Therefore, anonymity in the Bitcoin network is achieved only to the extent that public addresses remain disassociated from parties' identities.

For example, suppose again that Adam wants to send Baker a payment, but this time he wants to use Bitcoin. Using the Bitcoin protocol, Adam broadcasts a signal across the global network: "Send 1.0 Bitcoin from Adam's public address to Baker's public address." Because each node on the network has its own copy of the global ledger, each node must independently update its own ledger to reflect the payment. Therefore each node would adjust its ledger so that Adam's public address now contains 1.0 Bitcoin less than before, and Baker's public address contains 1.0 Bitcoin more than before. But this still begs the question: how can the nodes be sure that the request is authentic? How do they know that Adam himself is broadcasting the message to send payment from Adam's address, and not some other third party that is fraudulently trying to steal Adam's money? That is where Bitcoin's cryptographic mechanisms come in.

3. Cryptographic Security

To prevent fraudulent transactions, Bitcoin requires parties to use highly specific

passwords, which "unlock" the ability to conduct transactions from given addresses. Recall that transactions take place between public addresses, not individuals. Therefore as far as the Bitcoin protocol is concerned, it is the public address itself that is associated with a given balance, not the individual. For example, suppose Adam believes his total Bitcoin balance is 10.0 Bitcoin. Adam can access those Bitcoin only to the extent that he has the specific passwords, which authorize him to actually use the balances. If Adam were to lose his password, though "his" accounts might still reflect 10.0 Bitcoin, he would lose the ability to transact with those Bitcoin. This raises a very critical drawback of Bitcoin: if an account holder ever loses his password, though his Bitcoin balance will remain associated with the public address, for all intents and purposes those bitcoins will be lost forever. The mathematical complexity of cryptographic security ensures almost to certainty that those funds will never be accessible again.

In a cryptographic context, what we have referred to as "public addresses" are more accurately referred to as "public keys." Similarly, the "highly specific passwords" that we have referred to are in fact called "private keys." To transact with Bitcoin, Adam must create a Digital Signature that proves he has authority to send money out of his public key. To create the Digital Signature, Adam must have the appropriate private key associated with his public key address.

4. Vulnerabilities

Bitcoin possesses a number of intrinsic vulnerabilities, many of which have been exploited by hackers around the world. The most obvious vulnerability is that a user's Bitcoin wallet is only as secure as their private key. In other words, if a hacker manages to steal a private key that is associated with a Bitcoin wallet, the hacker now has access to all of its funds,

including the ability to conduct *authorized* transactions. This is important because in removing third parties from the equation, many people do not quite realize what they are giving up. Financial institutions provide an insurance policy of sorts on people's everyday transactions. Such institutions are designed to handle certain levels of fraudulent activity, and they can reimburse nonguilty parties accordingly. However in the case of Bitcoin, the only parties in a transaction are the buyer and seller, and while many people celebrate such a relationship because of lower transaction costs, they forget to consider the dramatically increased risk of identity theft. Bitcoin's only mechanism for identity verification is a private key. Therefore once a private key has been compromised, it is impossible to distinguish between fraudulent and legitimate activity for a given Bitcoin wallet.

II. MARKET ACTIVITY

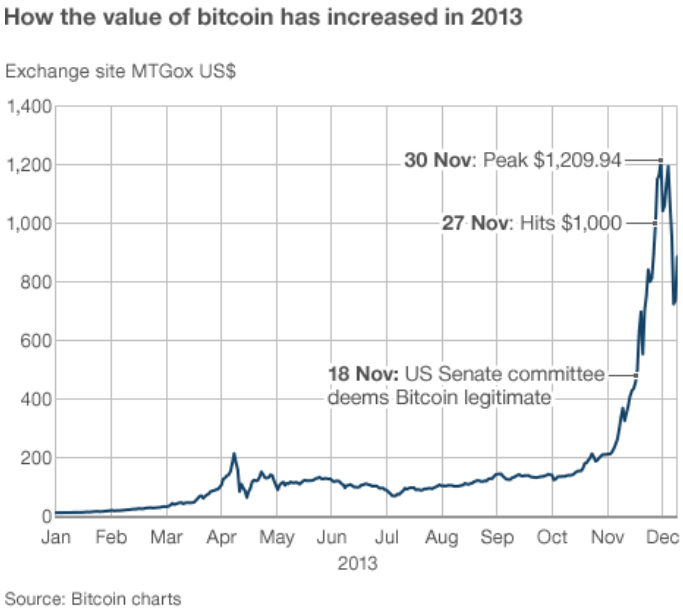
A. Overview

Though the Bitcoin white paper was published in 2008, it took several months before the technology was sufficiently developed to allow real transactions. At first, transactions involved bitcoins only, i.e. people were not yet trading bitcoins for fiat currency. However that all changed when on October 5, 2009, New Liberty Standard published an exchange rate for bitcoins, establishing the value at $1 U.S. Dollar per 1,309.03 bitcoins.[13] From that point forward, online Bitcoin exchanges started emerging from all corners of the world at an increasingly rapid rate.

The New Liberty Standard's exchange rate did not last very long. Fast forward to the

[13] HISTORY OF BITCOIN, http://historyofbitcoin.org/ (last visited May 12, 2014).

beginning of 2013, when bitcoins were trading at $14 per bitcoin ($/BTC).[14] That year, by December of 2013, prices had moved to $1,150/BTC.[15] Thus in a single year, Bitcoin's value increased by over 10,250%.[16] Investors, entrepreneurs, and more importantly, hackers, were now [17]paying very close attention to Bitcoin, and every one of them was focused on making money.



BBC News - Bitcoin: Price v hype (See footnote below).

B. The Key Players

There are hundreds of companies worldwide that participate in the Bitcoin market. Their role can be classified into two broad categories: (1) facilitators of Bitcoin exchange, and (2) producers of Bitcoin-related hardware. The primary focus of this paper is on the facilitators of exchange, i.e. the online currency exchanges that trade Bitcoins for fiat currency.

As explained before, Bitcoin is highly susceptible to hacking. Unfortunately, publicizing

---

[14] Bitcoin Market Price, BLOCKCHAIN.INFO, https://blockchain.info/charts (scroll down; then click on "Market Price (USD)" hyperlink).

[15] *Id.*

[16] Neils Christensen, *2013: Year Of The Bitcoin*, FORBES (Dec. 10, 2013, 2:34 PM), http://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/.

[17] Vanessa Barford, *Bitcoin: Price v hype*, BBC NEWS MAGAZINE (Dec. 13, 2013, 6:40 AM), http://www.bbc.com/news/magazine-25332746.

this fact has done little to dissuade investors from entering the Bitcoin world. In fact, all it has done is create some level of acceptance among Bitcoin users that their bitcoins might come under attack one day. This is actually an interesting psychological tactic because where investors are led to expect unavoidable failures in the Bitcoin protocol, they are susceptible to artificial fluctuations in the price. In other words, if a Bitcoin exchange were to claim that hackers stole investors' money, there is no empirical way to determine whether the exchanges were actually attacked, or whether they actually stole the money themselves. This idea represents the drastic informational asymmetry between those who control Bitcoin exchanges, and those that simply use them.

As a starting point, it is important to understand that in the absence of disclosure rules, users' rely exclusively on trust and faith when transacting with Bitcoin exchanges. The unfortunate problem is that historically speaking, the exchanges have betrayed users' trust over and over again. Usually the companies claim they were hacked, but again, there is no way to know for sure. For example, consider Mt. Gox, a once legendary company in the Bitcoin world. They were at one point viewed as the world's largest online digital currency exchange,[18] and Bitcoin users from all corners of the world used Mt. Gox to conduct lightning fast trades between their fiat currencies (e.g. U.S. Dollar, Chinese Yen, etc.) and their bitcoins. However, as the service gained increasing popularity, it became a regular target for hackers. In its initial years, Mt. Gox was able to address these hacks in one way or another. However after a massive "attack" toward the end of 2013, Mt. Gox was finally forced to file for bankruptcy on February

[18] Michael J. Casey, *Mt. Gox Creditors, Investors Agree to Try to Revive Bitcoin Exchange*, THE WALL STREET JOURNAL (Dec. 13, 2013, 6:40 AM), https://online.wsj.com/news/articles/.

28, 2014.[19] The company lost nearly half a billion dollars after hackers exploited a vulnerability in their system known as "transaction malleability."[20] What is even more interesting however is that after the company claimed such massive losses, they somehow "recovered" about $120 million worth of bitcoins, with no explanation of how the recovery came about. In fact, their statements only raised new questions about whether the half-a-billion dollars in bitcoins were *actually* stolen.[21]

Unfortunately other companies besides Mt. Gox have had similar issues, and all of them are privy to the same informational asymmetry. For example, take Coinbase or even BitPay. Both companies are Bitcoin exchanges and further, purport to be legitimate analogues to companies such as Mt. Gox. With clean and intuitive web interfaces, these companies have managed to convince investors that they are somehow different than Mt. Gox. However, the same fundamental problems associated with nondisclosure plague them just they plagued Mt. Gox. The fact is these companies simply possess an overwhelming incentive to defraud investors.

III. THE SEC AND BITCOIN

A. Securities Regulation in the United States: An Overview

The Securities and Exchange Commission (SEC) is the federal agency tasked with

---

[19] Yoshifumi Takemoto & Sophie Knight, *Mt. Gox files for bankruptcy, hit with lawsuit*, REUTERS (Feb. 28, 2014, 2:30 PM), http://www.reuters.com.

[20] *Id.*

[21] Takashi Mochizuki & Eleanor Warnock, *Mt. Gox Finds 200,000 Missing Bitcoins*, THE WALL STREET JOURNAL (Mar. 20, 2014, 10:51 PM), https://online.wsj.com/news/articles/.

enforcing and regulating federal securities laws.[22] Its mission is "to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation."[23] In the context of securities regulation, the agency is "concerned primarily with promoting the disclosure of important market-related information, maintaining fair dealing, and protecting against fraud."[24]

Thus, investors often look to the SEC for protection from fraudulent companies or investment schemes. However, there are legal criteria to determining whether the SEC actually has regulating authority. In the case of securities regulation, the SEC can only regulate a company or scheme once it is legally established that the company is actually dealing "securities," as defined by the Securities Act of 1933 and the Securities Exchange Act of 1934.

B. Definition of "Security"

The definition of "security" in Section 2(a)(1) of the Securities Act of 1933 and Section 3(a)(10) of the Securities Exchange Act of 1934 covers a broad range of financial instruments. The term includes common instruments and unconventional instruments alike.[25] Common instruments such as stocks, notes, and bonds are explicitly listed in the definition and are

---

[22] John C. Coffee, Jr. & Hillary A. Sale, SECURITIES REGULATION CASES AND MATERIALS 56-7, (Foundation Press, 12th ed. 2012) (The SEC administers six statutes: (1) The Securities Act of 1933; (2) The Securities Act of 1934; (3) Public Utility Holding Act of 1935; (4) Trust Indenture Act of 1939; (5) Investment Company Act of 1940; and (5) Investment Advisers Act of 1940).

[23] THE SECURITIES AND EXCHANGE COMMISSION, http://www.sec.gov/about/whatwedo.shtml (last visited May 12, 2014).

[24] *Id.*

[25] 15 U.S.C. § 77b(a)(1).

presumptively considered to be securities.[26] Unconventional and irregular instruments on the other hand are covered by a single, catchall financial instrument: "investment contract."[27]

In deciding whether the SEC has authority to regulate a given financial instrument, courts first perform a facial comparison between the instrument and the definition of security. They begin with a simple question: Is the instrument explicitly listed in the statute? If yes, they presume the instrument to be a security and place the burden on defendant to prove otherwise. However if the instrument is not explicitly listed, as in the case of Bitcoin, courts then consider whether it might qualify as an "investment contract."

In *SEC v. W.J. Howey Co.*, the Supreme Court further explored the meaning and applicability of the term "investment contract."[28] After noting that Congress's intent was to include "investment contract" as a mechanism to over include financial instruments in the definition of "security,"[29] the court outlined a four part test for gauging whether a given financial instrument would qualify as such under Section 2(a)(1) of the Securities Act of 1933. Thus a

---

[26] The presumption can be defeated however. In *United Housing Foundation v. Forman*, the Supreme Court stressed that the "economic realities" of financial instruments are more important than their names. Thus even if an instrument is technically listed in § 2(a)(1) as a "security," courts may override such a classification if the economic reality necessitates otherwise.

[27] 15 U.S.C. § 77b(a)(1) (By including "investment contract" in the definition of "security," Congress meant to expand the SEC's regulatory authority over new and innovative financial instruments. Doing so meant that new instruments could not escape the SEC's authority just because they were not technically classified as an enumerated financial instrument such as stocks or bonds).

[28] SEC v. W. J. Howey Co., 328 U.S. 293, 298-299 (1946) (The Court explained that though Congress left the term undefined, "investment contract" was actually a relic of many state "blue sky" laws. Incidentally, the term was also left undefined by state statutes. It was through state *judicial* interpretation that "investment contract" became a catch-all for § 2(a)(1) of the Securities Act of 1933); *See* id. (The Court also said "Such a definition . . . has been enunciated and applied many times by lower federal courts").

[29] *Id.* (The Court explained that "such a definition is consistent with the statutory aims [of Congress]").

security is any "contract, transaction or scheme," where an investor makes (1) an investment, (2) in "a common enterprise," (3) where the investor is "led to expect profits," (4) "solely from the efforts of . . . a third party."[30] Though the Court's definition is expansive, it intentionally "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."[31] Furthermore, it is important to note that the mere offering of a security is sufficient to enable SEC regulation. Therefore in the case of Bitcoin, so long as Bitcoin can be established as a security in any possible way, it will come under the purview of the SEC. That does not, however, mean that the SEC will regulate Bitcoin itself. Rather, it implies that the SEC will regulate any companies that are *offering* the security known as Bitcoin. Regardless, for any regulation to take place, one must first establish Bitcoin as a security.

C. Bitcoin Is A Security

1. Bitcoin Requires an Investment of Money

The first component of the Supreme Court's test for a security requires an investment of money. Bitcoin satisfies this requirement. Regardless of whether Bitcoin is viewed as currency or property, an investment of capital is inevitable to realistically participate in Bitcoin. Let us

[30] "[A]n investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party, 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." *Id.*

[31] *Id.* (The Court also stressed the immateriality of whether investors' shares in a security were evidenced by formal certificates or nominal interests).

assume that to participate in Bitcoin, one must actually possess bitcoins.[32] As explained earlier, newcomers to Bitcoin have one of four options for obtaining the cryptocurrency: (1) trade cash for bitcoins via an online exchange; (2) trade cash for bitcoins via a local person; (3) sell goods or services for bitcoins, either online or in person (e.g. person owns lemonade stand and sells beverages in exchange for bitcoins as payment); or (4) mine bitcoins on a personal computer or server.[33] All four likely qualify as an "investment" under the *Howey* test.

The Supreme Court of the United States has explained that to satisfy the first prong of the *Howey* test, i.e. an investment to occur, a person must "give up specific consideration in return for a separable financial interest . . ."[34] The Court continued suggesting that in previous cases where investment contracts were found, " . . . the purchaser gave up some tangible and definable consideration in return for an interest that had substantially the characteristics of a security."[35]

---

[32] Note: at this point we are only discussing whether Bitcoin itself, as a financial instrument, qualifies as a security. We are not yet considering the implications of Bitcoin-backed securities.

[33] BITCOIN, https://bitcoin.org/en/faq#how-does-one-acquire-bitcoins (last visited May 12, 2014).

[34] Int'l Bhd. of Teamsters v. Daniel, 439 U.S. 551, 559 (1979).

[35] *Id.* (lower Federal courts provide better explanations of the criteria for determining what constitutes an investment). In 1976, the 9th Circuit Court of Appeals provided a test for an "investment" in *Hector v. Wiens*: "[A]n 'investment of money' means only that the investor must commit his assets to the enterprise in such a manner as to subject himself to financial loss" (emphasis added); *See* Hector v. Wiens, 533 F.2d 429, 432 (9th Cir. Mont. 1976); Subsequent cases in Federal courts below the Supreme Court have in fact repeatedly used the same test for the "investment" component of *Howey*. In *Warfield v. Alaniz*, after the 9th Circuit quoted the Hector test for "investment of money," it followed up by noting "In *Rubera*, we found this prong satisfied where investors 'turned over substantial amounts of money . . . with the hope that [the investment managers' efforts] would yield financial gains. . . . Furthermore, . . . the investors [in *Rubera*] risked financial loss . . .'" *See Warfield*, at 1021 (quoting *SEC v. Rubera*, 350 F.3d 1084, 1090 (9th Cir. Or. 2003)); Thus between Hector and Warfield, the criteria for "investment of money" hinges on an investment of assets where financial losses are possible. Interestingly, such an interpretation is also consistent with *Int'l Bhd. of Teamsters* to the extent that the plaintiff in *Int'l Bhd. of Teamsters* did not face a risk of financial loss.

We therefore begin by considering whether Bitcoin users give up specific, tangible, and definable consideration in return for a financial interest. [36]

Where prospective Bitcoin participants use cash, goods, or services to purchase bitcoins, they are giving up specific consideration. Further, to the extent that bitcoins can be used in a variety of markets to transact, they possess characteristics of financial interests. However, where prospective participants choose to "mine" in exchange for their bitcoins, a more complicated analysis is required.

Keep in mind that even if Bitcoin mining were to not constitute an "investment," Bitcoin as a whole could still be considered a security. Again, the SEC will regulate companies offering Bitcoins to the extent that securities are being offered at all. Thus even if users that participate in Bitcoin via mining are said to have not "invested" in Bitcoin, the other methods of acquiring Bitcoin, if they in fact constitute an "investment," will still suffice for establishing the first prong of *Howey*.

Nevertheless, it is likely the case that even Bitcoin mining can satisfy the first prong in its own right. As explained earlier, Bitcoin mining is a process where persons either use personal computers or servers to *generate* bitcoins. By running the Bitcoin client on their machine, they can dedicate computer-processing power to "adding transaction records to Bitcoin's public ledger of past transactions."[37] Thus miners are rewarded with bitcoins in exchange for sustaining

[36] Note that in applying the *Howey* test, courts will often use the phrase "investment of *money*." However based on the aforementioned analysis, it seems that "investments" do not necessarily require an expenditure of cash. So long as the consideration is tangible and definable, it will likely qualify as an "investment."

[37] *Mining*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Mining (last visited May 12, 2014).

the integrity of Bitcoin's blockchain, or rather, Bitcoin's public ledger.[38] It is therefore clear that miners receive bitcoins (i.e. "financial interests") in exchange for their mining efforts. But it is also clear that their mining efforts are simultaneously self-serving[39] and thus may be motivated by a desire to preserve the network, not earn bitcoins.

Because an "investment" has two components, specific consideration and a separable financial interest, we begin with assessing whether mining efforts qualify as consideration. Satoshi Nakamoto explains in the original Bitcoin whitepaper "[t]he steady addition of a constant of [sic] amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended." Therefore, whether an investment has been made hinges, at least in part, on whether CPU time and electricity are viewed as consideration.

It may seem obvious on a superficial level that CPU time and electricity would qualify as consideration. After all, it is not difficult to conceive of assigning a market value to expended CPU time and electricity. Coupling such an observation with the idea that consideration need only be specific, tangible, and definable, might lead one to assume the analysis is finished. However, such an assumption is tricky for two reasons: First, in the earliest stages of the Bitcoin network, it was possible to mine hundreds of bitcoins a day with absolutely no additional investment in hardware. Whether you used a decade old PC, your personal laptop, or any other reasonably functional computer, you could mine astronomically large amounts of bitcoins with

---

[38] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin (2008), https://bitcoin.org/bitcoin.pdf.; *see also Mining*, BITCOIN WIKI, *supra* note 37.

[39] It is in every Bitcoin user's best interest to maintain the integrity of the network. To the extent that the network starts facing transaction vulnerabilities, Bitcoin holders are at risk of their investment collapsing overnight.

little or no additional electric output. In such circumstances, one would be hard pressed to conjure any definable consideration that was offered for the bitcoins. The second reason why CPU time and electricity cannot be automatically assumed to be consideration is that mining is self-serving by nature. Beyond being rewarded in bitcoins, miners possess an incentive to continue their activity even if only for ensuring the legitimacy of their own payment network. In an abstract sense therefore, Bitcoin mining can be compared with a separate Supreme Court case, *Int'l Bhd. of Teamsters v. Daniel*.

In *Int'l Bhd. of Teamsters v. Daniel*, the Supreme Court faced a case where the main issue was whether the plaintiff's noncontributory, compulsory pension plan constituted an "investment contract" under securities laws.[40] The outcome ultimately depended on whether the plaintiff's contributions to the pension plan qualified as "investment[s]" under the *Howey* test. The plaintiff argued that a portion of his labor was being "invested" into the pension plan, and thus the first prong of *Howey* was satisfied. However, given the compulsory nature of the pension plan, the Court refused to accept the premise that a "portion" of his labor was being invested into the pension plan.[41] The Court explained that

> Only in the most abstract sense may it be said that an employee "exchanges" some portion of his labor in return for these possible benefits. He surrenders his labor as a whole, and in return receives a compensation package that is substantially devoid of aspects resembling a security. His decision to accept and retain covered employment may have only an attenuated relationship, if any, to perceived

[40] Int'l Bhd. of Teamsters v. Daniel, 439 U.S. 551, 553 (1979).
[41] *Id.*

> investment possibilities of a future pension. Looking at the economic realities, it seems clear that an employee is selling his labor primarily to obtain a livelihood, not making an investment.[42]

In other words, because his labor was primarily exchanged for his livelihood and not an investment, his labor did not qualify as specific, tangible, and definable consideration.

Therein lies the wrinkle in assuming that CPU time and electricity used in Bitcoin mining automatically suffice as consideration. While it is true that one can assign a market value to such expenditures, it is still possible to argue that those expenses are undertaken primarily to enjoy one's own personal computer—not to earn bitcoins. Presumably if mining bitcoins had a negligible impact on one's electric bill because the computer used for mining was always on and consistently used for other purposes anyway, one might argue that *Int'l Bhd. of Teamsters* applies. In that case, while miners might receive separable financial interests, they would not be giving up specific consideration.

Similar reasoning could also be applied to the argument that miners only mine to sustain the integrity of Bitcoin's network—not to actually receive bitcoins themselves. In that case, regardless of whether miners expend specific consideration, opponents would be arguing that the generated bitcoins from mining are simply too attenuated to the real value of mining, and therefore there is no separable financial interest.

Nevertheless, both wrinkles can be ironed out. As the Bitcoin network currently stands, mining is *extremely* costly and resource intensive. While that was not the case from 2008 until mid-2013, today mining for the purposes of acquiring bitcoins requires thousands of dollars'

---

[42] *Id.*

worth of equipment. Even then it is a poor investment. The professional server farms dedicated exclusively to competitive mining ensure anything but a fruitless endeavor for the average consumer. Therefore while it may have been possible to rely on *Int'l Bhd. of Teamsters* in the past, today it is obvious that competitive mining requires a dramatic investment of specific, tangible, and definable capital in exchange for bitcoins as a financial interest. Finally any remaining concerns regarding those users who do not mine for bitcoins but rather for maintaining the network, are addressed by the Supreme Court in *Howey* when the Court explains that the finding of an investment contract is

> Unaffected by the fact that some purchasers choose not to accept the full offer of an investment contract by declining to enter into a service contract with the respondents. The Securities Act prohibits the offer as well as the sale of unregistered, non-exempt securities. Hence it is enough that the respondents merely offer the essential ingredients of an investment contract.[43]

2. Bitcoin Investors Are in a Common Enterprise

Whereas the first prong of the *Howey* test focuses on what is being invested, the second prong of the test focuses on where the investment is going. After establishing that participating in Bitcoin necessarily requires an investment, we turn next to show why the investment ultimately places Bitcoin users in a "common enterprise."

The *Howey* Court was brief in its explanation of what a common enterprise means, leaving much room for interpretation amongst lower Federal courts. Indeed there is a split

[43] SEC v. W. J. Howey Co., 328 U.S. 293, 300-301 (1946).

amongst lower courts as to what constitutes a common enterprise.[44] Thus far lower courts have established two broad categories of commonality amongst investors: horizontal commonality and vertical commonality.[45] Further, some circuits split vertical commonality into two subcategories that are best referred to as "narrow vertical commonality" and "broad vertical commonality." Needless to say, there is no uniform standard as of yet.[46]

Before delving into the requirements of each commonality, it is important to recall the context in which these terms apply. As discussed before, securities laws are thematically based on the idea of disclosure. The idea is that when sophisticated parties (herein referred to as "third parties") seek funding from common investors, they must adhere to certain disclosure rules so as to prevent fraudulent activity, as well as provide investors with information to make sensible investment decisions. Thus the various types of commonality are best understood when framed as different levels of risk allocation between those third parties that seek funding, and those common investors that in turn invest.

With that in mind, let us briefly explore the requirements for each.[47] Horizontal commonality requires a pooling of assets amongst all investors and third parties so that all share in the profits and risks of the investment.[48] In effect, horizontal commonality requires third parties to be investors themselves. Therefore if the investment were to perform poorly, the third

---

[44] "Thus far, neither the Supreme Court nor this court has authoritatively determined what type of commonality must be present to satisfy the common enterprise element." SEC v. Sg Ltd., 265 F.3d 42, 50 (1st Cir. Mass. 2001).

[45] Mordaunt v. Incomco, 469 U.S. 1115, 1115-1116 (1985)

[46] *Sg Ltd.*, 265 F.3d at 49-50.

[47] For the purposes of explaining these commonalities, we will momentarily refrain from adding Bitcoin to the analysis.

[48] *Sg Ltd.*, 265 F.3d at 49.

parties would face the same losses as their investors.

Vertical commonality on the other hand allows two further permutations. Whether narrow or broad, vertical commonality removes the requirement for third parties to be traditional investors alongside their common investors. Narrow vertical commonality, the stricter of the two, requires that investors' fortunes be dependent on the efforts and *success* of the third parties.[49] Imagine a scenario where a third party manages investors' assets and in turn is paid exclusively through a percentage of *profits* from those assets. Though the third party does not share the same overall level of risk as the investors, they are still only paid when the investors succeed, i.e. when the investors' assets succeed. In contrast, broad vertical commonality simply requires all investors to be dependent upon the third parties' expertise—nothing more.[50] In such a scenario, if the third party were to charge static fees for its asset management services, it would receive payment regardless of the performance of the underlying assets.

Bitcoin again complicates the analysis because as a starting matter, it is difficult to identify a centralized third party. This of course is by design as a central theme of Bitcoin is its own decentralized nature. However, of the three aforementioned types of commonality, one renders third parties and investors indistinguishable: horizontal commonality. And in fact, Bitcoin fits quite well into a horizontal commonality paradigm.

Recall that the Supreme Court has never addressed horizontal commonality and its application under the *Howey* test.[51] Thus we must turn to interpretations of Federal circuit courts

[49] *See generally* SEC v. Glenn W. Turner Enterprises, Inc., 474 F.2d 476, 482 (9th Cir. Or. 1973).

[50] *See generally* SEC v. Koscot Interplanetary, Inc., 497 F.2d 473, 478 (5th Cir. Ga. 1974).

[51] That being said, a careful analysis of *Howey* shows that investors in *Howey* likely shared

to understand why Bitcoin users share horizontal commonality. In 1994, the Second Circuit explained "A common enterprise within the meaning of *Howey* can be established by a showing of 'horizontal commonality': the tying of each individual investor's fortunes to the fortunes of the other investors by the pooling of assets, usually combined with the pro-rata distribution of profits."[52]

Bitcoin by definition ties all investors' fortunes to each other. It is very much the case that Bitcoin market value affects *all* Bitcoin holders. Thus as the value of Bitcoin increases, each Bitcoin holder is proportionally better off. And as the value decreases, each Bitcoin holder is proportionally worse off. For the purposes of "investing" into Bitcoin itself (and not Bitcoin based derivatives), this kind of a relationship amongst investors is inevitable.

Knowing that investors are tied to one another, the only remaining piece of the common enterprise prong of *Howey* is establishing the "enterprise" component. That too, is easy to identify in the context of Bitcoin: the online exchanges. Regardless of how savvy a Bitcoin investor might be, he is still at the mercy of the online exchanges. Because Bitcoin ultimately requires conversion to fiat currency, exchanges single handedly comprise the common enterprise that investors are tied to. Investors' fortunes are only as valuable as the extent to which the exchange can conduct transactions. If investors keep their holdings with the exchange, they are effectively holding shares in the exchange's performance. If the exchange is hacked, whether genuinely or artificially, all the investors' bitcoins are subject to being permanently

---

horizontal commonality. The fact that Bitcoin fits best into horizontal commonality (and not vertical commonality) is perhaps the strongest position it could be in to satisfy the second prong of the *Howey* test.

[52] Revak v. SEC Realty Corp., 18 F.3d 81, 87 (2d Cir. N.Y. 1994).

unrecoverable.

3. Bitcoin Investors Are Led to Expect Profits

The third prong of *Howey* requires that investors be led to expect profits from investing their money in Bitcoin. In fact, there are many aspects of Bitcoin that lead investors to expect profits. Perhaps the most identifiable aspect is Bitcoin's programmed hard cap. As discussed earlier, the Bitcoin protocol is designed so there can only be 21 million bitcoins in total. Many investors who lack sophisticated economics backgrounds immediately take this to mean Bitcoin is deflationary. This generally leads them to two conclusions: First that Bitcoin will inevitably fail as a currency. This mindset generally stems from neoclassical economics, which suggests all currencies must have inflationary components lest the economy grind to a halt. The second conclusion, however, is more important. After investors realize that Bitcoin is doomed to fail, many start betting on a Bitcoin bubble that would precede the failure. With a hard cap of 21 million bitcoins, it is easy to understand why one might believe Bitcoin prices will consistently move upward, at least until the bubble collapses. Therefore, they believe that investing into Bitcoin, assuming the protocol survives long enough, is a sure fire way to earn a return on their investment because at some point, demand will outweigh supply and therefore drive market prices up. Accordingly, it is very much the case that many Bitcoin users invest their own capital specifically because they are led to expect profits.

Furthermore, the currency discussion is once again implicated in this prong too. It does not matter what the proffered motive is of investors. The unequivocal fact is that to the extent bitcoins are not considered legal tender, there necessarily exists a group of investors will need to

convert their holdings to a currency such as USD before being able to use it. At that point, it is clear that the only motivation for involving oneself in Bitcoin to begin with is to capitalize on arbitrage opportunities.

4. Bitcoin Profits Are Derived From the Efforts of Others

The final prong of *Howey* tests whether those profits "come solely from the efforts of others."[53] Thus we are to show why Bitcoin users, after having "invested" into a "common enterprise" from which they "expect profits," must rely on the "efforts of others" to generate those profits.

On the onset of this analysis, one might rightly point out that *Howey* technically requires profits to come "solely" from the efforts of others. Why then does this paper reduce the standard to "efforts of others"? Must not others' efforts be the *sole* factor in generating profits?

Indeed defining the phrase "efforts of others" is necessary to the analysis yet difficult to perform. In *Howey*, whether the investors had to rely solely on the efforts of others was not at issue; investors were purely passive and performed no duties whatsoever. Consequently, *Howey* provides little guidance on situations where investors perform any duties at all, even if only minimal.[54]

The Ninth Circuit was consequently forced to explore this very issue in *SEC v. Koscot*

---

[53] SEC v. W. J. Howey Co., 328 U.S. 293, 301 (1946).

[54] *Koscot Interplanetary, Inc.*, 497 F.2d at 480 (The Ninth Circuit explained that "[n]owhere in [*Howey*] does the Supreme Court characterize the nature of the 'efforts' that would render a promotional scheme beyond the pale of the definition of an investment contract. Clearly the facts presented no issue of how to assess a scheme in which an investor performed mere perfunctory tasks").

Interplanetary, Inc., a case that hinged on whether profits were required to be *solely* generated from the efforts of others.[55] The case dealt with a pyramid scheme where investors had to perform the minimal duty of bringing new investors to Koscot sales meetings. Though existing investors did in fact bring prospective investors to meetings, their duties stopped there. Once at the meeting, prospects were lured into the Koscot pyramid scheme by Koscot employees, not Koscot investors.[56] Nevertheless had the court applied a literal interpretation of *Howey*, the existing investors' simple acts of bringing prospective investors to Koscot meetings might have entirely precluded Koscot's investment scheme from SEC regulation.

Thus in adopting a functional interpretation of "efforts of others," the Ninth Circuit noted that

> [a] literal application of the *Howey* test would frustrate the remedial purposes of the Act . . . . 'it would be easy to evade [the *Howey* test] by adding a requirement that the buyer contribute [only] a modicum of effort.' . . . Moreover, a close reading of the language employed in *Howey* and the authority upon which the Court relied suggests that . . . we need not feel compelled to follow the 'solely from the efforts of others' test literally.[57]

Finally a year after the Ninth Circuit's decision in *Koscot*, the Supreme Court briefly readdressed the "efforts of others" prong in *United Housing Found., Inc. v. Forman*, specifically noting that "[an] essential attribute[] [of a security] . . . is a reasonable expectation of profits to

---

[55] *Id.* at 479 ("[T]he critical issue in this case is whether a literal or functional approach to the 'solely from the efforts of others' test should be adopted, i.e., whether the exertion of some effort by an investor is inimical to the holding that a promotional scheme falls within the definition of an investment contract").

[56] *Koscot Interplanetary, Inc.*, 497 F.2d at 485.

[57] *Id.* at 480 (quoting *SEC v. Turner Enterprises, Inc.*).

be derived from the *entrepreneurial or managerial* efforts of others" (emphasis added).[58] Thus between *Koscot* and *United Housing*, investors' expectations of profits from Bitcoin need only come from the "entrepreneurial or managerial efforts of others,"[59] not necessarily "*solely* from the efforts of others."

In light of such an interpretation, establishing that Bitcoin investors rely on the managerial efforts of others is not very difficult. For one, we have already established that Bitcoin's online exchanges comprise the required "enterprise" under the *Howey* analysis. Thus to satisfy this final prong of *Howey*, we must demonstrate why Bitcoin investors are necessarily reliant on the managerial efforts of the exchanges personnel.

---

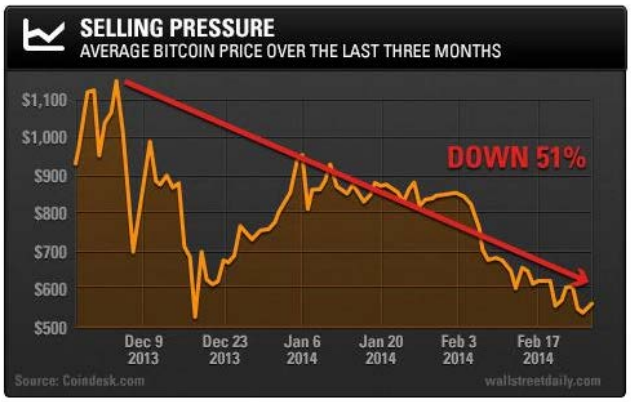
[58] United Housing Found., Inc. v. Forman, 421 U.S. 837, 852 (1975).

[59] In fact the *Koscot* court also added a requirement that "others' efforts" *at minimum* involve "managerial" duties:

> We confine our holding to those schemes in which promoters retain immediate control over the essential managerial conduct of an enterprise and where the investor's realization of profits is inextricably tied to the success of the promotional scheme. Thus, we acknowledge that a conventional franchise arrangement, wherein the promoter exercises merely remote control over an enterprise and the investor operates largely unfettered by promoter mandates presents a different question than the one posed herein. But the Koscot scheme does not qualify as a conventional franchising arrangement.

SEC v. Koscot Interplanetary, Inc., 497 F.2d 473, 485 (5th Cir. Ga. 1974).

To the extent that Bitcoin exchanges are not required to disclose their financials, all users of such services are necessarily reliant on the efforts of the exchanges to ensure the value preservation of their investments, i.e. bitcoins. Mt. Gox is a perfect example of such reliance. Users stored their coins with the online exchange expecting, at the very least, that they would have access to their own bitcoins should something happen. But instead, the service claimed they were hacked, reported a loss of nearly half-a-billion dollars, and offered no explanation for how the attack occurred or how they plan on remedying the situation. In fact, the effects of their shutdown were felt across the entire Bitcoin market.[60] Bitcoins tumbled in value as people began to realize the gravity of Mt. Gox's fraud.



Wall St. Daily – The Exact Date for Bitcoin's Final Crash

Further, for the purposes of establishing an alternative, less obvious way in which Bitcoin users are dependent on the efforts of others, one can also think of the Bitcoin *network's* core programmers as the enterprise. It turns out, Bitcoin users are reliant on their efforts as well. According to Bitcoin's main website, seven programmers comprise Bitcoin's "core development" team.[61] Though the Bitcoin protocol is open source, meaning that its internal programming code is freely available to everyone around the world, it is still developed by a core group of people. While it is true that anyone can view or even edit the code, the reality is that

[60] Louis Basenese, *The Exact Date for Bitcoin's Final Crash to $0.00*, WALL ST. DAILY (Feb. 27, 2014), http://www.wallstreetdaily.com/2014/02/27/bitcoin-2/.

[61] BITCOIN, https://bitcoin.org/en/development (last visited May 12, 2014).

these core programmers exercise an unmatchable level of control over the entire Bitcoin network. To fully appreciate the extent of their control, one need only look at instances where hackers have attacked Bitcoin. For example in 2010, a hacker managed to exploit a flaw in the Bitcoin protocol and managed to fraudulently assign himself 184 *billion* bitcoins.[62] Within hours after the flaw was discovered, Bitcoin's core development not only patched the flaw, but also managed to effectively "*roll back*" the entire public ledger to remove all traces of the 184 billion-bitcoin transfer. The significance of such a maneuver cannot be overstated: a group of five to seven programmers, single handedly, reversed a transaction worth *billions* of bitcoins. Of course it may seem obvious that the transaction needed to be reversed. After all, the Bitcoin protocol is only supposed to allow a maximum of twenty one *million* bitcoins—so when the hacker generated bitcoins in the order of *billions*, clearly something had to be done. However in our context this illustration is not meant to highlight the efficacy of distributed problem solving, rather it is meant to highlight the extreme level of control that Bitcoin's core development team can exercise. Though in that instance the transaction was fraudulent, it is entirely possible that a similar course of action could be undertaken for future legitimate transactions.

Despite Bitcoin's facially distributed, decentralized, and open source nature, the de facto reality is that a core group of people still control the fate of the Bitcoin protocol. This is not to say that they are (or have) acted maliciously in any way. However it does demonstrate why the previously mentioned "enterprise" of programmers does in fact exercise managerial control over Bitcoin users' investments.

---

[62] Reuben Grinberg, Comment to *Why Bitcoin Isn't a Security Under Federal Securities Law*, LEX TECHNOLOGIAE (Jun. 26, 2011, 11:49 PM), http://www.lextechnologiae.com (user comment made on June 27, 2011).

CONCLUSION

Bitcoin is a security and should accordingly be regulated by the Securities and Exchange Commission. It fully meets the four-part test outlined in *SEC v. W.J. Howey Co.*, and further, thousands of investors have already been defrauded by investing into Bitcoin. The SEC stresses disclosure as a mechanism to facilitate fair markets for investors. Those policies must be implemented into Bitcoin companies such as online exchanges with the utmost speed lest more investors be defrauded.

Luckily, On May 7, 2014, the Securities and Exchange Commission issued its second ever warning on Bitcoin investments.[63] Its first warning came in July of 2013, after the agency successfully prosecuted a Ponzi scheme that used Bitcoin to scam investors.[64] But this time, the agency focused on Bitcoin itself, as opposed to Ponzi schemes in general.[65] This is a big step forward for investors as it signals that the SEC is aware of the potential for fraud in Bitcoin investments. However, for investors to be fully secured, the SEC must officially recognize Bitcoin as a security.

As a final note, Bitcoin truly is innovative, and to that extent, should not be frowned upon. It incorporates cryptographic principles in a novel way to facilitate the decentralized peer-

---

[63] THE SECURITIES AND EXCHANGE COMMISSION, http://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html (last visited May 12, 2014).

[64] *Supra* note 63 at http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf.

[65] *Supra* note 62 (The agency warned that "[t]he rise of Bitcoin . . . creates new concerns for investors. . . . Bitcoin [] has the potential to give rise both to frauds and high-risk investment opportunities. Potential investors can be easily enticed with the promise of high returns in a new investment space and also may be less skeptical when assessing something novel, new and cutting-edge").

to-peer payment network that it is, and thus, Bitcoin's creators and programmers are to be applauded on some level. However, the ingenuity of its implementation does not affect whether it can be used to defraud investors on a mass scale. Though it has taken years of fraudulent activity for regulatory institutions to pay attention to Bitcoin, it is still not too late for them to protect investors. The SEC should immediately classify Bitcoin as a security, and begin regulating those institutions that use fraudulent arbitrage to take advantage of unassuming investors.