The Era of Cryptocurrencies: Current and Future Regulations

~ Ekakshra Mahajan Mandhar

I. INTRODUCTION:

An average person doesn't possess much knowledge about cryptocurrencies.[1] A recent study noted that 65% of the public are unfamiliar with Bitcoin and of those who were aware, 84% have never used it.[2] Merriam-Webster Online Dictionary defines money as something generally accepted as a medium of exchange, a measure of value, or a means of payment.[3] Traditionally, society has been aware of and used physical money. However, less familiar is the concept of "money of account", defined by Merriam-Webster as "a denominator of value or basis of exchange which is used in keeping accounts and for which there may or may not be an equivalent coin or denomination of paper money."[4] Digital currencies fall within this definition of money.[5] Additionally, Oxford Online Dictionaries defines Cryptocurrency as: "a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank."[6] Many people invested in Bitcoin to make money by buying low and selling high.[7] Others invested in Bitcoin because they saw its potential for rivaling other established currencies.[8] Both schools of thought are being employed for either the benefit of an individual or for society as a whole. Regulation of digital currency will usher in a new wave of investment, but it may be curtailed by the uncertainty that looms over the volatile nature of Bitcoin's value.[9] This Article works on the premise that even if Bitcoin falters, there is still great promise in the Blockchain technology due to its versatility. Section II seeks to explore Blockchain and the technology underlying it. Section III weighs the potential benefits of the technology along with the risks associated with it. Section IV analyzes Smart

Contracts which are programs controlling digital assets, and the concept of Initial Coin Offerings discussing the problems prevalent in the ICO market. Section V highlights how cryptocurrencies have been classified by various courts and agencies and the regulations adopted by various states and countries to govern the usage of cryptocurrencies. It also succinctly discusses the cognizance taken by the SEC. Section VI highlights the existing standards for reviewing the users of cryptocurrencies and the potential of creating a new subpoena power to deal with the identity of anonymous users. Section VII proposes what regulations should potentially look like and finally, it concludes by arguing for a minimalist approach to Bitcoin regulation.

II. BLOCKCHAIN TECHNOLOGY:

A cryptocurrency is a "digital or virtual currency that uses cryptography for security."[10] The technology underlying cryptocurrencies is blockchain.[11] It is a distributed public ledger system that records all transactions in a particular cryptocurrency.[12] Each cryptocurrency has its own blockchain with its individualized security measures which include public-key encryption.[13] Bitcoin, a cryptocurrency[14] that is best known as a peer-to-peer electronic cash system, is touted as being as revolutionary as the Internet.[15] The potential of Bitcoin[16] and other cryptocurrencies extends beyond their applications as units of account or mediums of exchange. The unique technological innovation common to most cryptocurrencies is a public ledger that functions as a decentralized system for recording ownership and value transfers. While the technical operation of the ledger is complex[17], the core idea is rather simple. When an owner of a cryptocurrency transfers the cryptocurrency to a recipient, the transaction is verified in a process called "mining."[18] A crowd of "miners" consults the ledger, verifies the owner's claim of ownership, and documents the transfer to the recipient, who from now

on is logged on the ledger as the owner of the cryptocurrency.[19] The verification process is a competitive one. The miners do not simply verify the transaction; they compete to solve a complex cryptographic problem.[20] The first miner to succeed wins the competition, logs the transaction on the ledger, and is awarded a new batch of cryptocurrencies.[21] The new batch of cryptocurrencies is automatically generated by the software and functions both as an incentive to participate in the mining process[22] and as a decentralized mechanism for the issuance of new cryptocurrencies. Anyone can become a miner by downloading the necessary software. Cryptocurrency software is open-source and generally not controlled by a central entity.[23]

To summarize, cryptocurrencies are essentially protocols that allow for the validation of transactions without the need for a trusted third party such as a bank, credit card company, escrow agent, or recording agency. As such, cryptocurrencies hold great innovative potential. They have been described as a "generative" technology on which powerful applications can be built.[24] They allow for the creation of self-enforcing smart contracts that do not rely on financial institutions, lawyers, or accountants for their execution.[25]

III. BENEFITS AND ASSOCIATED RISKS:

BENEFITS:

1. Transaction costs and time:

Bitcoin transactions drastically reduce transaction costs.[26] Whether domestic or international, they have the ability to close in a few minutes *vis a vis* international wire transfers which take several days.[27] It also reduces transaction costs and can cut a significant amount of cost out of the process of post-trade financial manufacturing.[28] There are two primary transaction costs that merchants pay when making internet

purchases.[29] The first is the fee paid to a trusted third party, such as a bank or credit card company, which serves as an intermediary in order to validate the transaction.[30] These fees occur each time a purchase is made and become expensive in the aggregate.[31] By contrast, Bitcoins allow individuals to transact amongst themselves without a third-party intermediary and avoid this expense.[32] The second significant transaction cost comes from the uncertainty associated with transaction reversibility or, in other words, the ability to return or cancel a transaction.[33] Chargebacks make reversibility more expensive in traditional transactions than in Bitcoin transactions.[34]

2. **Anonymity of users:**

Individuals are plagued with credit card fraud on a regular basis.[35] Blockchain mitigates the risk of identity theft because the identity of all the parties is anonymous.[36] There is no central currency storage location, akin to a financial institution that can be robbed or hacked.[37] Bitcoin, is a string of computer data stored in a wallet either on a user's computer, webserver or in printed form.[38] The Blockchain is also reliable.[39] It is guaranteed to be safe and secure and everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer.[40] The only way to access and transfer a coin is with the private key.[41] The Blockchain checks the legitimacy of each coin before allowing it to be transferred to another individual.[42] Again, the amount of computer power required to fraudulently alter the Blockchain is too high to pragmatically occur.[43] Bitcoin transactions are protected by the underlying computing power of the Blockchain, rather than the security of a single financial institution.[44]

3. **Inflation concerns:**

Bitcoin is not backed by any central government monetary policy so any effects on inflation will not cause a decrease in their purchasing power.[45] There is an artificial cap on the number of bitcoins in circulation which helps curb inflation concerns.[46] This cap

was incorporated to ensure a stable money supply since Bitcoin is valued by market forces rather than government intervention.[47] The stability of the supply of bitcoins along with the safety and reduced transaction speeds and Bitcoin transaction costs should be supported by minimal government regulation and intervention.[48]

4. **Avoidance of double-spending dilemma:**

Before the creation and dissemination of virtual currencies, online transactions required the direct intervention of a third party who acted as an intermediary in transactions given that virtual goods could be reproduced infinitely.[49] In such a situation, the same virtual money could be presented to two different persons and perform two valid payments.[50] Given that each Bitcoin and fraction of Bitcoin has their own identification and that the systems check its use since the moment in which the Bitcoin was created, it is impossible to copy a Bitcoin a perform multiple payments with the same instrument.[51]

ASSOCIATED RISKS:

1. **Exchange management:**

Prima facie, Blockchain technology is relatively secure but can pose security risks to users.[52] Poorly managed Bitcoin exchanges have had a checkered history.[53] The Mt. Gox failure stands testimony to how critical Bitcoin exchanges are to the Bitcoin marketplace.[54] Mt. Gox, the largest bitcoin exchange at the time of its headline-grabbing demise, declared bankruptcy after the theft or disappearance of 850,000 bitcoins valued at $450 million in February 2014, along with $27 million in cash.[55] Although 200,000 were eventually found, the location of the remaining 650,000 remained unknown and the subject of much speculation over the last few years.[56] After Mt. Gox filed for bankruptcy it became clear that over $400 million worth of Bitcoins

were lost and stolen.[57] As of May 2016, 650 thousand Bitcoins, worth $292 million, were still unaccounted for.[58]

2. <u>Perverse uses of technology:</u>

The advent of Bitcoin technology might be relatively nascent but it has already been sued to facilitate illegal transactions.[59] The Silk Road case demonstrates how the technology can be misused.[60] Between January 2011 and arrest of its entrepreneur during October 2013, Silk Road operated as an intermediary, much like eBay or CraigsList, by providing buyers and sellers with a transaction infrastructure platform.[61] However, unlike eBay or CraigsList, Silk Road is dedicated to providing a high level of anonymity between buyers, sellers and third parties who might desire to learn the details of these transactions.[62] Silk Road is just one of several anonymous networks that have recently become possible with the advent of relatively easy-to-use browser interfaces.[63] Sites dealing primarily in illicit goods and services such as Black Market Reloaded and The Silk Road "use Bitcoins because they can be exchanged and accumulated like cash without any third party recording these transactions unlike PayPal or other ways of sending money online, Bitcoins are untraceable since they do not require a particular identity to be attached to them."[64] The indictment announced on February 4, 2014 in Manhattan Federal Court of Ross William Ulbricht states that Ulbricht sought to anonymize transactions on Silk Road in two principal ways.[65] First, Ulbricht operated Silk Road on what is known as "The Onion Router," or "Tor" network, a special network of computers on the Internet, distributed around the world, designed to conceal the true IP addresses of the computers on the network and thereby the identities of the networks' users.[66] Second, Ulbricht designed Silk Road to include a Bitcoin-based payment system that served to facilitate the illegal commerce conducted on the site, including by concealing the identities and locations of the users

transmitting and receiving funds through the site.[67] Although the original Silk Road was shut down, a continuous cycle of new anonymous marketplaces has emerged.[68] However perverse uses of Bitcoin do not result from an inherent flaw with the technology itself and should not dictate the technology's regulation as a whole since the Blockchain itself enables law enforcement to deal with such cases.[69]

3. Inherent Problems:

Bitcoin suffers from a few inherent problems which have majorly limited its broad acceptance and use. It is new and confusing since it's difficult to understand the underlying technology.[70] It suffers from liquidity concerns because only a small subset of the population uses the technology.[71] Without a robust Bitcoin market, it can be cumbersome to exchange traditional currency, goods or services for Bitcoin causing price volatility.[72] Finally, the price of Bitcoins varies drastically which can make it difficult to use as currency.[73] The price pattern probably explains that speculative investors rather than active users increasing the number of Bitcoin transactions are driving the market.[74] Logically this variance discourages potential users from using Bitcoin out of fear of a vast devaluation.[75]

4. Anonymity:

Cryptocurrencies are also uniquely suited to facilitate harmful behaviors.[76] The only truly public feature of the ledger is the documentation of ownership and transfers. The owners themselves are not identified by name on the ledger, but rather by a set of letters and numbers representing their public cryptocurrency address.[77] Anyone can freely create as many wallets as he or she desires, at practically zero cost, without providing any identifying information.[78] This relatively high level of anonymity makes it difficult for regulators to identify individuals who use the protocol for illicit value transfers. our financial-regulation system heavily relies on regulating intermediaries that are uniquely

positioned to disrupt misconduct.[79] For example, we subject financial institutions to "know-your-customer rules" in order to prevent money laundering, use banks as tax-withholding agents to prevent tax evasion[80], and regulate securities exchanges to protect investors. Some commentators argue that the public ledger has the potential to "eliminate intermediaries without eliminating the underlying conduct."[81] If that is the case, then regulators would lose the ability to use intermediaries as regulatory agents.[82]

However, Blockchain can be used to create a contract that is automatically enforced, between two people, in a decentralized fashion also referred to as a Smart Contract. Rather than relying on trust or a legal framework to ensure that each party that enters into a contract will adhere to its terms, Blockchain can be used to create such contracts.

IV. SMART CONTRACTS:

A smart contract is a computer program that controls a digital asset.[83] Smart contracts help exchange data money, property, shares or anything of value without the need of a third-party intermediary.[84] As the technology continues to grow, a great array of smart contract transactions will likely become available.[85] Initial Coin Offering or ICO is an example of its growing pervasiveness.

Initial Coin Offering (ICO):

"An ICO is a fundraising event, effected using distributed ledger technology, in which a 'token' or 'coin' is offered to a participant in return for either cash (fiat currency) or cryptocurrency, such as Ether or Bitcoin. A token entitles its holders to various rights, which typically include the right to use a service to be developed and offered by the issuer. The proceeds of the token sale are used to fund a venture or a project undertaken by the ICO sponsors. Similar to equity securities, however, tokens sold in ICOs may

also confer profit rights, may appreciate in value, and can be traded. ICO tokens do not represent an ownership interest in a venture."[86] (emphasis added).

The following are the most pressing and prevalent problems in the ICO market:

1. Pump and Dump:

One way fraudsters seek to profit is by engaging in market manipulation, such as by spreading false and misleading information about a company (typically microcap stocks) to affect the stock's share price.[87] They may spread stock rumors in different ways, including on company websites, press releases, email spam, and posts on social media, online bulletin boards, and chat rooms.[88] The false or misleading rumors may be positive or negative. For example, pump-and-dump schemes often occur on the Internet where it is common to see messages posted that urge readers to buy a stock quickly or to sell before the price goes down, or a promoter will call using the same sort of pitch.[89] In reality, the author of the messages may be a company insider or paid promoter who stands to gain by selling their shares after the stock price is 'pumped' up by the buying frenzy they create.[90] With more money pouring into Coins with lower market caps and lesser track records, market manipulation for fraudsters, promoters, and company insiders has become substantially easier.[91] When trading in coins of lower market capitalizations, the influx of capital necessary to manipulate the price of a coin can be substantially lower than for a coin of a much higher market capitalization.[92]

2. Exposure of highly sensitive information:

Many of the exchanges require sensitive information in order to permit higher trading limits. Most higher limit exchanges require a submission of a passport, often times forcing investors to send this sensitive information overseas.[93] Without making any allegations or pointing to a specific exchange, this appears to be information that is unnecessary to the transaction, yet could easily be distributed to other parties relatively

anonymously if exchanged for some form of cryptocurrency, since many of the currencies themselves are anonymous or pseudo-anonymous.[94]

3. Widely speculative token pricing:

Not all tokens are inappropriately valued and not all ICOs are initiated to take advantage of securities laws or to rapidly accumulate capital for an idea that otherwise, through more traditional forms of fundraising, could not acquire such capital so quickly. Nevertheless, many newly formed ICOs have sprung up in response to investor demand, rather than the merit of tokenizing some process.[95] With investors struggling to differentiate use-cases, and hoping for lottery-like returns, wildly speculative pricing has crept into the token space, particularly for newly created tokens. many investors are playing a very risky game by gambling in a highly inflated space without truly understanding their investments.[96]

V. CLASSIFICIATION AND REGULATION:

A. OBJECTIVES:

It is essential to note that Bitcoin remains inexpensive and efficient.[97] Any regulation that increases costs or slows down transactions is critically flawed because it would inadvertently affect the benefits of Bitcoin.[98] The free market should dictate the competitive advantages over other forms of currency.[99] Bitcoin regulation must satisfy two critical components. First, Bitcoin regulation must ensure that the unique benefits of Bitcoin remain.[100] Second, Bitcoin regulation must be tailored to the specific risks faced by consumers.[101] Strict regulation or an outright ban of Bitcoin will eliminate the efficiency benefits of the technology, worsen liquidity and acceptance problems, and increase the risks of illegal activity associated with Bitcoin or Bitcoin-like technologies.[102]

B. CLASSIFICATION OF CRYPTOCURRENCIES:

In order to regulate Bitcoin, courts and agencies have deployed different methods to classify Bitcoins as investment contracts, money, property and commodities.

1. Security:

In 2014, a Texas court ruled that a Bitcoin investment opportunity was a security.[103] *S.E.C. v. Shavers* arose out of Bitcoin Savings and Trust, an "online investment scheme in which its founder and operator, Shavers solicited and accepted all investments, and paid all purported returns," in Bitcoin.[104] Shavers solicited individuals online to invest in his business, falsely promising "investors up to 1% interest daily to be paid every three days at first, or 7% interest weekly, purportedly based on Shavers' trading of bitcoin against the U.S. dollar."[105] However, Shavers was not actually trading Bitcoins against[106] the U.S. dollar; rather, he was paying off withdrawals and interest with new deposits while appropriating funds for personal use.[107] Final judgment was entered against Shavers for operating a Ponzi scheme and defrauding investors out of over 700 thousand Bitcoins."[108] In 2013, the court ruled on the preliminary issue of whether it had subject matter jurisdiction over the case pursuant to the Securities Act of 1933 and the Exchange Act of 1934 (Securities Act).[109] In order for the court to have subject matter jurisdiction, it had to find that the Bitcoin scheme was a security.[110] But, it first needed to find whether there was an investment contract in the Bitcoin investments.[111] If so, the investment would be a security.[112] The Court applied the test propounded by the Supreme Court in *S.E.C. v. W.J. Howey Co.* which determined whether an investment contract exists.[113] The *Shavers* court found that all the prongs of the *Howey* test were satisfied and held that Bitcoins were investment contracts and therefore securities.[114]

2. Currency:

In 2014, in the case of *U.S. v. Ulbricht*, which dealt with Silk Road, the Southern District of New York classified Bitcoin as currency.[115] The court found that Bitcoins could be considered money that could be laundered.[116] The most pertinent issue examined in *Ulbricht* is how digital currency should be classified.[117] Reading the language of the money laundering statute broadly, the court found that Bitcoins could be used to launder money if they fit within the definition of financial transactions.[118] The opinion stated that financial transactions capture movement of all "funds,"[119] which should be read in a "colloquial sense" to mean something that "can be used to pay for things."[120] "Sellers using Silk Road were not alleged to have given their narcotics and malicious software away for free, they were alleged to have sold them."[121] As such, the court held that Bitcoins are "funds," and therefore apart of financial transactions.[122] By extension Bitcoins are included within financial transactions and can be used to launder money.[123] Although Bitcoin shares many of money's attributes, state statutes that deal with Bitcoin should be specifically tailored to virtual currency.[124] A Florida State Court found that its state anti-money laundering statute did not cover Bitcoin transactions because the statute was drafted too vaguely to include virtual currency.[125] The defendant was not convicted for laundering Bitcoins.[126] Accordingly, in order to prevent nefarious uses of Bitcoins and bring them within existing currency regulations, state regulations should explicitly include digital currency.[127]

3. Property:

Bitcoins can be traded for goods and services and exchanged for cash, and thus the act of acquiring Bitcoins has tax implications. In 2014, the Internal Revenue Service (IRS) issued guidelines in treating Bitcoin for federal tax purposes.[128] The guidelines treat Bitcoin as convertible property.[129] The IRS stated that general tax principles applicable

to property transactions apply to transactions using virtual currency.[130] For instance, if a taxpayer successfully 'mines' virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income.[131] In sum, if an individual uses his computer to support the Blockchain and mine for Bitcoins, and the individual is awarded coins successfully verifying a transaction, he or she must pay income tax on those coins.[132]

C. STATE REGULATIONS:

1. CSBS Model framework:

In September 2015, the Conference of State Bank Supervisors (CSBS), a non-profit organization that seeks to develop consistent banking regulatory policy amongst the states,[133] published a model regulatory framework for Bitcoin and other virtual currency.[134] The objective of the model framework is to assist states' regulation of virtual currency and, more importantly, to promote consistent regulation amongst the states.[135] However, the framework is not binding on any jurisdiction.[136] The model framework applies to activities that involve a third party, such as an exchange or wallet, maintaining control over an individual's virtual currency.[137] The framework does not apply to individuals or businesses that use virtual currency simply to transact for goods or services.[138] The model framework suggests that states should use a "licensing system that enables states to share licensing and enforcement data in real time."[139] There should be a "uniform application" amongst the states in order to enhance efficiency and communication between regulators.[140] Moreover, licensees would be required to maintain strict capital requirements and investment reserves.[141] Licensees would also be required to maintain strong consumer protection standards, possess a robust cyber security program, and implement a compliance program.[142] Further, they would be required comply with the Bank Secrecy Act[143] and Anti-Money Laundering statutes,[144]

maintain adequate books and records, and comply with state and federal regulations.[145] Particularly beneficial for small companies, the framework does not require companies acquire costly cyber risk insurance.[146]

2. New York:

In mid-2015, New York regulators published the final version of their BitLicense regulations, which regulate the use of Bitcoin.[147] New York's BitLicense allows New York "persons"[148] to engage in certain virtual currency business activities,[149] such as operating an exchange or wallet, or issuing virtual currency.[150] Merchants who simply want to accept virtual currency in exchange for goods or services, however, do not need a BitLicense.[151] Among other rules and requirements, companies holding a Bit License are required to: (1) Have a Bit License compliance officer and policy,[152] (2) maintain strict capital levels,[153] (3) keep financial books and records for seven years,[154] (4) face compliance examinations no less than 2 years.[155]

3. California:

California has tried to implement Bitcoin regulations but has been unsuccessful in its implementation.[156] California tried introducing a Bill to regulate Bitcoins but faced immediate resistance since companies believed that virtual currency should not be regulated until the technology matures else it would chill innovation.[157] It was also believed that inconsistencies between state regulatory schemes would create confusion for users.[158]

D. SEC REGULATIONS:

Prior to mid-2017, the SEC had been largely silent with respect to directly regulating the purchase or sale of cryptocurrencies. Most of its regulation in this area had, instead, solely attempted to protect the public from issuers or exchanges which operate cryptocurrency-related businesses and offer conventional securities. The SEC regulated

online exchanges that use cryptocurrencies to trade in securities[159], redemptions of shares in a trust that held cryptocurrencies as its sole assets[160] issuers selling shares in themselves in exchange for cryptocurrencies[161], and issuers holding cryptocurrency assets or operating cryptocurrency-related businesses that did not disclose sufficient information about such assets[162] or made fraudulent representations (including operation of Ponzi schemes).[163] However, this changed with an investigation report released on July 25, 2017 (the "DAO Report"), where the SEC found for the first time, that cryptocurrencies issued for the purpose of raising funds are securities and thus subject to securities laws.[164] Notably, the SEC refused to create a one-size-fits-all solution and instead chose to regulate cryptocurrencies based on the particular functionality of each cryptocurrencies stating that "securities law may apply to various activities, including distributed ledger technology, depending on the particular facts and circumstances, without regard to the form of the organization or technology used to effectuate a particular offer or sale."[165] Thus, the standard for determining whether a financial instrument, including a cryptocurrency, constitutes a security remains a functional one. The SEC disregards the underlying technology, including the blockchain, on which the cryptocurrency is based. The SEC then applied the Howey test to specifically determine that the DAO Token it was investigating was an "investment contract," a type of security, and, as a result, the DAO Token's ICO violated federal securities laws.[166]

E. OVERSEAS REGULATIONS:

Regulation in the international community is varied. For example, Japan's cabinet has officially recognized virtual currencies, including Bitcoin, as real money.[167] Digital currencies will also be recognized as "asset-like-values" that can be used in the place of money.[168] In India, the technology is starting to be implemented, but very slowly.

The founder of BTCXIndia, a Bitcoin wallet, Mupparaju Siva Kameswara Rao, mentions that while Bitcoin can solve some of the economic issues in India, the struggles of implementing regulatory practices and the lack of guidance may be a barrier to the wide-spread adoption of the currency.[169] However, the needs of the population that do not own a bank account or debit card may be catered to when the technology is implemented.[170] The Bank of India endorsed the use of Blockchain technology: *"With its potential to fight counterfeiting, the "blockchain" is likely to bring about a major transformation in the functioning of financial markets, collateral identification (land records for instance) and payments system. As against this, the "blockchain" technology is based on a shared, secured and public ledger system, which is not controlled by any single ("central") user and is maintained collectively by all the participants in the system based on a set of generally agreed and strictly applied rules."*[171] Although China does not have any regulation related to the cryptocurrency, the government has imposed restrictions on investment by its citizens.[172] Unfortunately, the restriction limits Chinese investors from accessing international markets and exchanges.[173] In fact, the Chinese government's manipulation of its currency has recently led to large Bitcoin trading as the alternative investment.[174] Additionally, because of the large population, the mining pools in China are significantly larger than those of other areas and countries in the world, attributing to the fact that it is the largest volume producer of Bitcoins in the world.[175] In Australia, the concern by the Australian Digital Currency and Commerce Association is to protect the customer in this highly unregulated market.[176]

VI. EXISTING STANDARDS AND PROPOSED MODIFICATIONS:

Existing standards:

In civil litigation, the new 'e-discovery' standards encompass information that exists in an intangible medium and can only be read on a computing device.[177] This broad category includes files saved on a computer as well as those located on the Internet.[178] The sheer volume of available electronic data on a computer, tablet, or smartphone expands the wealth of information that parties can access through discovery.[179] Discovery has become much more expensive and onerous because of the expansion of discoverable materials from paper files to e-discovery.[180] Due to the sheer volume of available electronic information, companies could spend millions of dollars to remove privileged information or work product documents.[181] Rule 26(b)(2)(B) of the *Federal Rules of Civil Procedure* sets forth limitations upon discovery of electronically stored information.[182] In order to address cost concerns with potentially unreasonable e-discovery requests, Rule 26(b)(2)(B) emphasizes proportionality.[183] When considering these requests, courts tend to weigh cost, relevance, and efficiency; specific determinations are left to the discretion of the judge.[184] In addition to traditional discovery, litigants can use subpoena powers to obtain information in a civil lawsuit.[185] In contrast to the updated Federal Rules of Civil Procedure, which have clear-cut procedures on how to deal with electronically stored data, the Federal Rules of Criminal Procedure have not been updated to specifically address these technological developments.[186] For now, since the standard remains unchanged, the government can often easily obtain a grand jury subpoena for electronic material.[187] Rule 17 of the *Federal Rules of Criminal Procedure* sets forth the standard subpoena process.[188] The government does face some restrictions on its use of subpoenas duces tecum.[189] A court can deem the subpoena terms to be unreasonable or oppressive and require modification

of its terms or quash it entirely.[190] Since the government can subpoena a recipient for documents they do not own, both the recipient and the owner of the requested materials can file a motion to quash the subpoena.[191] It is difficult, however, to quash a subpoena because the recipient bears the burden of proving the government's request is unreasonable.[192] Another restriction disallows the subpoena power to "violate a valid privilege," which includes infringements upon constitutional rights.[193] If the recipient of the subpoena makes a legitimate constitutional claim, the government must overcome the level of scrutiny protecting such a claim.[194]

The First Amendment, which provides a constitutional right to free speech, likely covers anonymous online speech.[195] In 1995, in *McIntyre v. Ohio Elections Commission*, the U.S. Supreme Court reaffirmed that the First Amendment protects anonymous speakers.[196] Although the Court in *McIntyre* considered political speech contained in a printed pamphlet, lower courts have extended this protection to anonymous online speech.[197] The First Amendment may protect online data regarding monetary transactions as well.[198] In 2010, in *Citizens United v. Federal Election Commission*, the U.S. Supreme Court held that in certain situations, money could be a proxy for speech.[199] The plaintiffs were challenging campaign finance legislation that limited a corporation's ability to make political expenditures.[200] The Court held that these restrictions violated the First Amendment because they quelled a corporate entity's political speech.[201] In reaching this conclusion, once again the Court acknowledged there is speech value in monetary transactions.[202] Therefore, some believe that *Citizens United* opened the door to a First Amendment speech right in virtual currency transactions.[203]

The Digital Millennium Copyright Act provides a civil option for plaintiffs to access the identities of anonymous Internet speakers.[204] The DMCA allows plaintiffs to sue

anonymous individuals who have violated copyright law on the Internet.[205] Using § 512(h) of the DMCA, copyright holders can subpoena third-party Internet service providers to unmask infringing users.[206] Over time, courts have interpreted the DMCA's subpoena power to apply only when an Internet service provider has stored the infringing material on its servers.[207] Thus, the ability to subpoena an individual's identity does not apply to providers that act only as conduits and nothing more.[208] Courts balance a series of criteria in determining whether to quash a subpoena under § 512(h) Due to First Amendment issues that arise when unmasking anonymous speakers on the Internet, many courts are adamant that a factual basis for the request exists before allowing the subpoena.[209] The standard is strict: there must be a legitimate reason to justify the issuing of a subpoena.[210] Courts have even compared subpoenas in a civil context to warrants in a criminal case.[211]

Necessity of a new standard:

The absence of criminal subpoena standards for electronically stored information and the continual misuse of Bitcoin highlights the importance of updating government regulations to address this gap. No current statute exists that provides a targeted criminal subpoena standard.[212] Due to Bitcoin's open source nature, it is difficult to identify perpetrators who use the virtual currency to facilitate their criminal acts.[213] There is no single company behind Bitcoin that the government can subpoena or raid; Bitcoin exists only on a network of computers.[214] The standard subpoena process set forth in Rule 17 of the *Federal Rules of Criminal Procedure* is lacking in several ways.[215] Without amending the standard to adapt to e-discovery, the current interpretation of the rule makes it difficult for the government to obtain desired electronic information.[216] To get a third party subpoena, the government has to show that the information sought is relevant, that it is admissible, and that the subpoena

specifically identifies the materials sought.[217] It is doubtful that the federal government will be able to successfully and in a timely manner use its current criminal subpoena power to unmask the individuals committing illegal Bitcoin transactions.[218] The government likely cannot meet the specificity requirement because it would have to go through millions of transactions and hundreds of thousands of user accounts in order to pinpoint specific targets.[219] The government might be able to overcome this by using a grand jury subpoena to expedite the process or by targeting websites where the transactions are largely illegal in nature.[220] At the same time, if the government uses a grand jury subpoena to sidestep the difficulty of showing specificity, the framework becomes too lenient and open to abuse.[221] Once the Bitcoin marketplace reaches the point where most individuals are engaging in legal transactions, lax subpoena standards become a problem. The U.S. Supreme Court and Congress must be careful when developing a criminal subpoena standard for Bitcoin because it will primarily affect anonymous speech, a crucial First Amendment right that has been highly valued throughout U.S. history.[222] If the government can easily issue subpoenas duces tecum and force marketplace sites to unmask individuals, it might infringe upon Bitcoin users' First Amendment rights to maintain anonymity on the Internet.[223] This creates a far-reaching effect that would not apply to traditional subpoena duces tecum or grand jury subpoenas because they generally deal with witness production of relevant documents in a criminal case and not identifying anonymous defendants.[224]

Creation of a special Subpoena Power:

Virtual currencies like Bitcoin are likely to proliferate over the Internet.[225] As the government moves toward regulating various aspects of Bitcoin, it must establish new e-discovery rules targeting users who have taken advantage of Bitcoin's anonymity to commit illegal acts.[226] At the same time, potential solutions need to ensure that the

government will not be able to overreach and infringe upon the rights of legitimate Bitcoin users who wish to maintain their anonymity.[227] The U.S. Supreme Court and Congress should amend Rule 17 of the Federal Rules of Criminal Procedure to reflect e-discovery, but with respect to Bitcoin, it needs to go one step further and specifically address the issues that would arise with revealing the identities of anonymous users.[228] In addition, before issuing a subpoena to unmask a Bitcoin user, courts and grand juries should consider the same two concerns that courts contemplate when determining whether to quash a subpoena under the Digital Millennium Copyright Act.[229] First, in order for a court or grand jury to approve the subpoena, the government should be required to show some evidence of illegal activity.[230] Second, the government should be required to show that the subpoena is relevant to the claim.[231] When it comes to criminal subpoenas, specificity and relevancy are important to ensure that the government is narrowly tailoring its actions to prevent treading upon First Amendment rights.[232] The other factors that courts consider when deciding to quash a DMCA subpoena should not explicitly apply to the initial approval of a criminal subpoena request because they would be too restrictive.[233] Although these factors should not apply to the initial decision to grant a subpoena, it should be left to the court's discretion to determine whether to consider these other issues when reviewing a recipient's motion to quash a subpoena.[234]

VII. PROPOSAL:

As investors continue to seek unfathomable returns, it is yet to be determined if the concerns surrounding cryptocurrencies are legitimate by ascribing value to something which might have no value or a new revolution playing an integral role in facilitating trust-based processes across many industries. Irrespective, as history has been privy, State omission cannot be tolerated where people have large stakes involved. It is

essential that the State undertakes regulatory oversight but without infringing upon the basic objectives of the technology.

A. Register businesses with State Regulatory Authority:

Bitcoin is still a nascent technology with only a small subset of the population utilizing it. This has led to a surge in intermediaries which unilaterally have the power to execute or prevent a transaction on behalf of a user.[235] There is a risk to consumers when a business has the ability to lose, misspend, permanently immobilize or fail to protect aa customer's funds entrusted to them.[236] The effects of these regulations could have been seen on Mt. Gox.[237] The users used the services of Mt. Gox which had the power to unilaterally transfer the Bitcoins because it had both public and private keys.[238] Had regulations been implemented, and Mt. Gox registered with an appropriate State Authority, it could have greatly reduced the risk to effected customers.[239] Thus, businesses which facilitate transactions involving cryptocurrencies must be registered with their states.

B. Regulation of miners:

Miners should not be regulated. They do not have the ability to unilaterally transfer or prevent transfers.[240] Bitcoin miners have the ability to validate Bitcoin transactions. However, even if one miner wants to fraudulently carry out a particular transaction, it would not pose to be a risk to individual transactions or to the marketplace, since it would be invalidated by the other miners.[241] Since mining does not pose to be a risk to consumers, it meets the objective envisaged, that regulations should be tailor made to the issues faced.

C. Regulation of users and merchants:

Users and merchants who are simply transacting in goods and services should not be regulated.[242] Such regulations would unnecessarily levy burdensome obligations on

users, increase transaction costs and chill innovation.[243] Mere transmission poses no risks and thus regulation would serve no purpose since Bitcoin provides adequate security.[244] Blockchain ensures that only valid transactions occur, the true identity of the user's personal information is anonymous which reduces the possibility of identity theft and it removed the potential for double spending.[245]

D. <u>Start-up exemptions:</u>

Startups and small businesses should be exempt from the full scope of Bitcoin regulations to encourage innovation.[246] The uncertainty of whether an exemption will be granted (or even revoked) makes it difficult for a startup to plan ahead.[247] Instead, states should implement specific carve-outs for startups to reduce uncertainty.[248] These provisions should be clearly written to enable entrepreneurs to know whether their business is exempt.[249]

E. <u>Self-regulation:</u>

Self-regulation plays an important role in scenarios where the State has not yet manifested itself or is struggling with the same.[250] Internationally, this is how cryptocurrencies have been perceived.[251] Self-regulation has been defined as *"Regulation promoted by the economic agents themselves to which the rule is intended. The agents themselves are most interested in having clear and quality rules, as this depends on the existence of a business-friendly environment. It is also assumed that they possess the technical know-how characteristic of their branches of action, and therefore, may be even better than the style regulator in the elaboration of rules and in the identification of problems."*

Self-regulation has a major impact on the cryptocurrency market as national regulatory bodies have not yet issued relevant decisions on the subject. Thus, in order to generate greater credibility to the market, the participants themselves issued rules to regulate the

activity, uniformizing the applicable standards. Virtual Currency users are spread around the world and therefore their impact should also be analyzed globally, what increases the role of international institutions when it comes to verifying which procedures must be incorporated in these kinds of transactions and which standards must be taken into account.[252] Such standards are necessary so that the use of crypto-currency becomes accepted and widespread.[253] As the cryptocurrencies, despite their great advantages, do not have good reputation before national and international bodies, companies and people.[254] As soon as the market for cryptocurrencies generates a series of difficulties for the State they shall start to regulate their use.[255] In the meantime, private institutions have much more freedom and much more responsibility in their performance.[256] They must idealize and implement measures that make the use of crypto-coins accepted by the market as a whole and popular opinion, presenting its advantages and minimizing its risks.[257] Such measures, above all, have to aim to promote cooperation between the market agents, have to help build a scenario in which the use of cryptocurrencies is endowed with its own procedures and easy assimilation by all users of the system (consumers and companies) , showing important aspects of its operation.[258]

VIII. CONCLUSION:

Virtual currencies have quickly become a reality, gaining significant traction in a very short period of time, and are evolving rapidly. Innovation in the pace of development of new currencies and technologies continues to create ongoing challenges for responsible users of technology and regulators alike. Cryptocurrencies and the block chain have the potential to effectuate a meaningful change to the world's underfinanced, overcharged and overlooked. Yet the failure of large exchanges like Mt.

Gox, the idea that almost 600 billion dollars of the world economy is floating around in a virtually regulation-free environment coupled with price volatility of these cryptocurrencies can be rather unsettling for the layman looking for viable alternatives from the risky stock market or the low interest bank deposits. There is an urgent need to help incubate this nascent technology to ensure all the benefits can be utilized without any of its drawbacks pulling the entire industry down. The only way this can be achieved is by maintaining a delicate approach towards legislations while taking a no-tolerance policy towards perpetration of crimes.

ENDNOTES:

[1] David Fialkow et al., *Cryptocurrency 2018: When the law catches up with game-changing technology*, 23 N0. 21 WESTLAW JOURNAL BANK AND LENDER LIABILITY (2018)
[2] Daniel Roberts, *The Bitcoin Book Boom*, FORTUNE (Mar. 6, 2018, 10:04 AM), *http://fortune.com/2015/03/06/bitcoin-book-boom/*.
[3] *Money*, MERRIAM-WEBSTER ONLINE, (last visited April 1, 2018, 10:30 PM *http://www.merriam-webster.com/dictionary/money*).
[4] *Money of Account*, MERRIAM-WEBSTER ONLINE, (last visited April 1, 2018), *http://www.merriam-webster.com/dictionary/money+of+account*
[5] Sean McLeod, *Bitcoin: The Utopia or Nightmare of Regulation*, 9 Elon L. Rev. 553 (2017)
[6] Cryptocurrency, OXFORD DICTIONARIES, (last visited April 1, 2018, 10:45 AM), *http://www.oxforddictionaries.com/us/definition/american_english/cryptocurrency*
[7] *How to Profit from Bitcoin*, FLIPPING INCOME (Mar. 2, 2018, 10:50 AM), *http://flipping-income.com/how-to-profit-from-bitcoin/*.
[8] Cade Metz, *Everyone Says Bitcoin is Back. But it Never Really Left*, WIRED (Mar. 11, 2018 11:30 PM), *http://www.wired.com/2015/11/bitcoin-is-back-but-it-never-really-left/*.
[9] McLeod, supra note 5 at 2.
[10] *Cryptocurrency*, Investopedia, *asp* (last visited Mar. 28, 2018 9:45 AM), *http://www.investopedia.com/terms/c/cryptocurrency*.
[11] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG (Mar. 24, 2018 2:45 PM), https://Bitcoin.org/ Bitcoin.pdf [hereinafter *Bitcoin White Paper*].
[12] Derek A. Dion, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash*, 2013 U. ILL. J.L. TECH & POL'Y 165, 167 (2013) ("Bitcoin is an example of a virtual currency, and, as such, it is not regulated by a central bank or any other form of governmental authority; instead, the supply of bitcoins is based on an algorithm which structures a decentralized peer-to-peer transaction system.").
[13] *See id.*
[14] 'Cryptography' for the purposes of this Article is being referred to as a digital currency that relies on peer-to-peer cryptography for the validation of value transfer.
[15] See, e.g., Saumya Vaishampayan, *Bitcoin Is Like the Early Internet, Minus the VC Money*, Market Extra (Market Watch Apr 28, 2014 7:30 PM), online at http:// www.marketwatch.com/story/bitcoin-venture-capital-money-hasnt-kept-up-with-buzz-2014-04-28 (visited Mar. 16, 2018 5:45 PM).
[16] See Kate Cox, *Bitcoin: What the Heck Is It, and How Does It Work?*, Consumerist (Mar 4, 2018 7:30 PM), online at http://consumerist.com/2014/03/04/bitcoin-what-the-heck-is- it-and-how-does-it-work (visited Mar. 16, 2018).
[17] For a thorough explanation of the verification process, see Ritchie S. King, Sam Williams, and David Yanofsky, *By Reading This Article, You're Mining Bitcoins*, Quartz (Mar. 17, 2018 5:30 PM), online at http://qz.com/154877/by-reading-this-page-you-are- mining-bitcoins (visited Apr. 16, 2018 4:45 PM).
[18] James Gatto et al. *Bitcoin and Beyond: Current and Future Regulation of Virtual Currencies*, 9 OHIO ST. ENTREPRENEURIAL BUSINESS LAW JOURNAL (2015)
[19] *See id.*
[20] *See id.*
[21] *See id.*
[22] Alternatively, Miners could also charge a fee for verifying the transaction.
[23] McLeod, supra note 5 at 22.
[24] The term "generative" is used here in the sense suggested by Jonathan Zittrain, who describes generativity as "a function of a technology's capacity for leverage across a range of tasks, adaptability to a range of different tasks, ease of mastery, and accessibility." Jonathan L. Zittrain, *The Generative Internet*, 119 HARV L REV 1975, 1981 (2006). For a reference to Bitcoin as a "generative" technology, see, for example, Timothy B. Lee, *Here's What Critics Miss about Bitcoin's Long-Term Potential*, The Switch (Wash Post Feb 3, 2013 8:30 PM), online at http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/03/heres-what- critics-miss-about-bitcoins-long-term-potential (visited Apr 18, 2018 6:30 PM).
[25] Vitalik Buterin, *DAOs Are Not Scary, Part 1: Self-Enforcing Contracts and Factum Law*, Bitcoin Magazine (Feb 24, 2014 4:30 PM), online at http:// bitcoinmagazine.com/10468/daos-scary-part-1-self-enforcing- contracts-factum-law (visited Nov 16, 2014 3:30 PM).
[26] Michael Abramowicz, *Cryptocurrency-Based Law*, 59 ARIZ. L. REV. 359 (2016)

[27] *See id.*
[28] *See* Kimberly Johnson & Blythe Masters, *What Blockchain Is and What It Can Do*, WALL ST. J. (Mar 19, 2018), http://www.wsj.com/articles/whatblockchainis-and-what-it-can-do-1466388185 [https://perma.cc/DYM5-4B89] (stating that the technology underpinning Bitcoin can "cut a significant amount of cost out of the process of post-trade financial manufacturing and actually reduce risk because it reduces the time it takes to complete a financial transaction once it has been agreed in the marketplace").
[29] Edward V. Murphy ET AL., CONG. RESEARCH SERV., R43339, BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 1 (2015).
[30] *See id.*
[31] *See, e.g.*, Ben Dwyer, *Credit Card Processing Fees & Rates*, CARDFELLOW, https://www.cardfellow.com/credit-card- processing-fees/ (April 22, 2018 5:30 PM) ("Visa, MasterCard and Discover make money by charging assessments on every transaction involving one of their credit cards .... In January 2015, Visa raised its assessment on credit volume from 0.11% to 0.13%.").
[32] Nakamoto, supra note 11, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN 1 (Mar. 23, 2018), http://bitcoin.org/ bitcoin.pdf [https://perma.cc/8DGC-THBR] ("A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.")
[33] MURPHY ET AL., supra note 29, (stating that reversibility concerns are costly for merchants)
[34] *See id.*
[35] Press Release, Bureau of Justice Statistics, 17.6 Million U.S. Residents Experienced Identity Theft In 2014 (Mar. 27, 2018), http://www.bjs.gov/content/pub/press/vit14pr.cfm [https://perma.cc/QPF4-TY2J].
[36] Nakamoto, supra note 11, ("The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone."). *But see* MURPHY ET AL., supra note 29, at 3 ("Because of the public ledger, researchers have found that, using sophisticated computer analysis, transactions involving large quantities of Bitcoin can be tracked ....").
[37] Timothy Bierer, *Hashing it out: Problems and Solutions concerning Cryptocurrency used as Article 9 Collateral*, 7 CASE W. RESERVE J.L. TECH & INTERNET 79 (2016)
[38] *See, e.g.*, Nakamoto, *supra* note 11, at 6.
[39] *See* Michael Jackson, *Bitcoin's Big Challenge in 2016: Reaching 100 Million Users*, COINDESK (Jan. 1, 2018, 4:34 PM), http:// www.coindesk.com/2016-bitcoin-challenge-100-million-users/ [https://perma.cc/87FE-9BHJ].
[40] *See id.*
[41] *See* Nakamato, supra note 11 and accompanying text (analyzing the key system in maintaining privacy).
[42] Each node checks the authenticity of a Bitcoin before recording the transaction.
[43] *See id.*
[44] The only way to fraudulently modify the Blockchain would be with more computing than the summation of all honest computers in the Blockchain.
[45] *See* MURPHY ET AL., supra note 29, at 6 ("Most often governments (or their central bank) regulate the supply of money and credit and most often some degree of mismanagement of this government function is at the root of a persistent high inflation problem.").
[46] *See id.*
[47] *See id.* ("Despite being a currency with no intrinsic value, the Bitcoin system's operation is similar to the growth of money under a gold standard ....").
[48] *See id.*
[49] HAYEK, Friedrich. Denationalization of Money: The Argument Refined. 5. ED. LONDRES: THE INSTITUTE OF ECONOMIC AFFAIRS, 1990. 146 p. Available at: <https://mises.org/system/tdf/DenationalisationofMoneyTheArgumentRefined_5.pdf?file=1&type=document>. Accessed on: 24 Jan. 2018
[50] *See id.*
[51] Alexander B. Lindgren, *Blockchain Regulation: Growing Pains of a Financial Revolution*, 59-OCT ORANGE COUNTY LAW. 38 (2017)
[52] Anthony F. Fata, *Inside this Issue: Marketplace Overview and Regulatory Developments: The Blockchain Bandwagon: Cryptocurrency on the Move*, 32 CBA RECORD 26 (2018)
[53] *See id.*
[54] https://www.reuters.com/investigates/special-report/bitcoin-gox/ (Last visited April 22, 2018)
[55] https://www.coindesk.com/mt-gox-the-history-of-a-failed-bitcoin-exchange/ (Last visited April 22, 2018)

[56] *See generally* Robin Sidel, Michael J. Casey & Eleanor Warnock, *Shutdown of Mt. Gox Rattles Bitcoin Market*, WALL ST. J. (Feb. 26, 2018, 1:21 PM), http://online.wsj.com/news/articles/SB10001424052702304834704579404101502619 (discussing the shutdown of Mt. Gox).
[57] *See id.*
[58] *See id.*
[59] Stephen T. Middlebrook et al., *Regulating Cryptocurrencies in the United States: Current issues and future directions*, 40 WM. MITCHELL L. REV. 813 (2014)
[60] *See id.*
[61] https://www.forbes.com/data/silk_road_trial/ (Last visited April 18, 2018 4:30 PM)
[62] *See id.*
[63] Nicholas Christin, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace* 2 (In Proceedings of the 22nd International World Wide Web Conference (WWW'13), 213 Rio de Janeiro, Brazil (May 2013), Working Paper No. CMU-CyLab-12-018), *available at* http:// www.cylab.cmu.edu/files/pdfs/tech_reports/ CMUCyLab12018.pdf (internal quotations omitted).
[64] *See generally* Mina Rady, *Anonymity Networks: New Platforms for Conflict and Contention* 22 (MIT Political Science Department, Research Paper No. 2013-5), *available at* http://ssrn.com/abstract=2241536 (discussing the various consequences of anonymity network).
[65] http://nation.time.com/2013/10/04/a-simple-guide-to-silk-road-the-online-black-market-raided-by-the-fbi/ (Last visited April 18, 2018 2:30 PM)
[66] *See id.*
[67] Press Release, United States Attorney's Office for the Southern District of New York, Manhattan U.S. Attorney Announces The Indictment of Ross Ulbricht, The Creator and Owner of The "Silk Road" Website (Feb. 4, 2018 6:45 PM) (*available at* http:// www.justice.gov/usao/nys/pressreleases/February14/RossUlbrichtIndictmentPR.php).
[68] Kyle Soska & Nicolas Christin, *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*, 24 USENIC SEC. SYMP. 33 (2015), https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska- updated.pdf [https://perma.cc/GKX4-UX9A].
[69] Omri Marian, *A Conceptual Framework for the Regulation of Cryptocurrencies*, 82 U. CHI. L. REV. DIALOGUE 53 (2015)
[70] *See* Sydney Ember, *Data Security Is Becoming the Sparkle in Bitcoin*, N. Y. TIMES (Mar. 1, 2018 6:45 PM), http://www.nytimes.com/2015/03/02/business/dealbook/data-security-is-becoming-the-sparkle-in-bitcoin.html [https:// perma.cc/HZ33-6LCA] ("Explaining how the block chain [sic] works can tangle the tongues of even those who are most enthusiastic about Bitcoin.").
[71] Tom Zanki, *SEC Approval of Digital Shares Could Spur Experimentation*, LAW360 (Mar. 18, 2018, 9:27 PM), http://www.law360.com/articles/739837/sec-approval-of-digital-shares-could-spur-experimentation [https://perma.cc/ TFS9-CBYC].
[72] *See id.*
[73] *See* MURPHY ET AL., supra note 29 at 32.
[74] *See id.*
[75] *See id.*
[76] A recent report by the Europol, for example, suggests that cryptocurrencies "are heavily abused by criminals." Europol, *The Internet Organised Crime Threat Assessment (iOCTA)* (2014), online at https:// www.europol.europa.eu/sites/default/files/ publications/europol_iocta_web.pdf (visited Apr 16, 2018 6:30 PM).
[77] See Bitcoin, *Some Bitcoin Words You Might Hear*, online at https:// bitcoin.org/en/vocabulary#private-key (visited Mar. 20, 2018 6:30 PM).
[78] See Omri Marian, *Are Cryptocurrencies* Super *Tax Havens?*, 112 MICH L REV FIRST IMPRESSIONS 38, 42 (2013).
[79] Stephen T. Middlebrook et al., *Regulating Crytocurrencies in the United States: Current issues and future directions*, 40 WM. MITCHELL L. REV. 813 (2014)
[80] See Europol, *iOCTA* at (cited in note 76); IRS, *Withholding Agent*, (Apr 14, 2018 4:30 PM), online at http://www.irs.gov/ Individuals/International-Taxpayers/Withholding-Agent (visited Apr 14, 2018).
[81] See generally, for example, Stephen T. Middlebrook and Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM MITCHELL L REV 813 (2014); Jerry Brito, Houman B. Shadab, and Andrea Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and*

Gambling, 16 COLUM SCI & TECH L Rev (forthcoming 2014), online at http://papers.ssrn.com/sol3/papers.cfm?abstract_ id=2423461 (visited Nov 26, 2014); Nicholas A. Plassaras, *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*, 14 CHI J INTL L 377 (2013). For two recent exceptions to the field-tailored approach that advocate a broader view of the problem, see Andy Yee, *Internet Architecture and the Layers Principle: A Conceptual Framework for Regulating Bitcoin*, 3 INTERNET POL REV 1, 6-7 (2014); Kevin V. Tu and Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 Wash L Rev (forthcoming 2015), online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2485550 (visited Mar 16, 2018 7:30 PM).

[82] *See id.*

[83] TechCrunch, *Decentralizing Everything with Ethereum's Vitalik Buterin,* YOUTUBE,_(Sept._18_2017),_www.youtube.com/watch?v=WSN5BaCzsbo&t=467s

[84] Isaac Pflaum et al., *A Bit of a Problem: National and Extraterritorial Regulation of Virtual Currency in the age of financial disintermediation,* 45 GEO. J. INT'L L. 1169 (2014)

[85] *See id.*

[86] Steve Gatti, Megan Gordon & Daniel Silver, *SEC Enforcement Against Initial Coin Offering,* CLIFFORD CHANCE LLP (Oct. 2017)

[87] Juliya Ziskina, *The Other Side of the Coin: The FEC's Move to approve Cryptocurrency's Use and Deny its Viability,* 10 WASH. J. L. TECH. & ARTS 305 (2015)

[88] *See id.*

[89] *See id.*

[90] *Investor Alert: Public Companies Making ICO-related Claims,* U.S., SEC. & EXCH. COMM'N (2017), *https://www.sec.gov/oiea/investor-alerts-andbulletins/ia_icorelatedclaims* (last visited Jan. 29, 2018 6:30 PM).

[91] Joshua S. Morgan, *What I learned trading cryptocurrencies while studying the law,* 25 U. MIAMI INT'L & COMP. L. REV. 159 (2017)

[92] *See id.*

[93] Jonathan Lane, *Bitcoin, Silk Road, and the need for a new approach to virtual currency regulation,* 8 CHARLESTON L. REV. 511 (2014)

[94] *See id.*

[95] *See generally* Nathan Reiff, *Ethereum Founder on ICOs: "We Are in a Bubble, A Lot of Projects Will Fail*," INVESTOPEDIA (Mar. 12, 2018 6:30 PM), *https://www.investopedia.com/news/ethereum-founder-cautions-icobubble-vitalek-buterin/.*

[96] *See id.*

[97] Jerry Brito et al., *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144, 151 (2014).

[98] See *id. (explaining that BitCoin transactions are also resistant to censorship, as there is no financial intermediary that controls who a user may transact with or donate to).*

[99] Nikolei M. Kaplanov, Comment, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 171-72 (2012) ("By letting the market determine whether or not bitcoin should survive is preferable to federal policy seeking to shut it down.").

[100] Eric Engle, *Is Bitcoin Rat Poison? Cryptocurrency, Crime and Counterfeiting,* 16 J. HIGH TECH. L. 340 (2016)

[101] *See id.*

[102] Yilu Zhang, *The Incompatibility of Bitcoin's Strong Decentralization and its Growth as a scalable Currency,* 11 NYU J.L. & LIBERTY 556 (2017)

[103] S.E.C. v. Shavers, No. 4:13-CV-416, 2014 WL 4028182, at (E.D. Tex. 2014).

[104] *See id.*

[105] *See id.*

[106] *See id.*

[107] Litigation Release No. 23090, U.S. Securities & Exch. Comm'n, Final Judgment Entered Against Trendon T. Shavers, A/K/ A/ "Pirateat40" - Operator of Bitcoin Ponzi Scheme Ordered to Pay More Than $40 Million in Disgorgement and Penalties (Apr. 22, 2018 7:45 PM), https://www.sec.gov/litigation/litreleases/2014/lr23090.htm [https://perma.cc/85X2-VGN9].

[108] *See id.*

[109] S.E.C. v. Shavers, 2013 WL 4028182, No. 4:13-CV-416, (E.D. Tex. Aug. 6, 2013).

[110] *See id.*

[111] *See id.*

[112] *See id.*

[113] S.E.C. v. W.J. Howey Co., 328 U.S. 293, 298-99 (1946) ("An 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.").
[114] Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & T ECH. L. J. 159, 197 (2011), http://ssrn.com/abstract=1817857 [https://perma.cc/M3LV-WSDY].

[115] United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014).

[116] *See id.* at 570.
[117] *See id* at 571.
[118] *See id.* ("Congress intended to prevent criminals from finding ways to wash the proceeds of criminal activity by transferring proceeds to other similar or different items that store significant value.").
[119] 18 U.S.C. § 1956(c)(4) (2010) ("The term 'financial transaction' means a transaction which in any way or degree affects interstate or foreign commerce involving the movement of funds by wire or other mean.").
[120] *Ulbricht*, 31 F. Supp. 3d at 570.
[121] *See id.*
[122] *See id.*
[123] *See id.*
[124] Florida v. Espinoza, CR-F14-2923 (11th Cir. Jul. 22, 2016). In *Espinoza*, the defendant was involved in an undercover operation wherein an undercover detective traded cash to the defendant in exchange for Bitcoins. After a few transactions, the undercover detective told the defendant that he was involved in the buying and selling of stolen credit cards for profit. One issue for the court to consider was whether the defendant's sale of Bitcoins to the detective in exchange for "dirty" money constituted money laundering under the state money laundering statute. In order to launder money, an individual must have "the intent to promote carrying on of the illegal activity." The court ultimately found that the defendant could not have laundered because the statute was too vaguely drafted to include virtual currency.
[125] *See id.* at 7.
[126] *See id.*
[127] I.R.S. Notice 2014-21 (Apr. 14, 2014), https://www.irs.gov/pub/irsdrop/n-14-21.pdf [https://perma.cc/Y4K9-B8DH].
[128] I.R.S. Notice 2014-21 (Apr. 14, 2014), https://www.irs.gov/pub/irsdrop/n-14-21.pdf [https://perma.cc/Y4K9-B8DH].
[129] *Ulbricht*, supra note 120; Interestingly, the *Ulbricht* court seems to simply disregard this position. *Ulbricht*, 31 F. Supp. 3d at 569 ("In any event, neither the IRS nor FinCEN has addressed the question of whether a 'financial transaction' can occur with Bitcoins.").
[130] I.R.S. Notice 2014-21 (Apr. 14, 2018), https://www.irs.gov/pub/irsdrop/n-14-21.pdf [https://perma.cc/Y4K9-B8DH].

[131] *See id.* at 4 (However, if the gain is less than $200, it is not taxable.).

[132] *See id.*
[133] *See About the Conference of State Bank Supervisors*, CONF. ST. BANK SUPERVISORS, https://www.csbs.org/about/what/ Pages/default.aspx [https://perma.cc/QR7K-BJ3R] ("The Conference of State Bank Supervisors (CSBS) is the nationwide organization of banking regulators from all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands .... For more than a century, CSBS has given state supervisors a national forum to coordinate supervision of their regulated entities and to develop regulatory policy.").
[134] CONF. ST. BANK SUPERVISORS, STATE REGULATORY REQUIREMENTS FOR VIRTUAL CURRENCY ACTIVITIES CSBS MODEL REGULATORY FRAMEWORK, (2015), https://www.csbs.org/regulatory/ep/Documents/ CSBS-Model-Regulatory-Framework(September%2015%202015).pdf [https://perma.cc/Y326-UJE8] [hereinafter CSBS Model].
[135] Press Release, Conference of State Bank Supervisors, State Regulators Issue Model Regulatory Framework for Virtual Currency Activities (Mar. 15, 2018), https://www.csbs.org/news/press-releases/pr2015/Pages/PR091515.aspx [https:// perma.cc/NAA3-KBD7].
[136] Charles M. Horn et al., *The Conference of State Bank Supervisors Adopts Model Regulatory Framework for Virtual- Currency Businesses*, MORGAN LEWIS (Feb. 14, 2015), https://www.morganlewis.com/pubs/csbs-adopts-modelregulatory- framework-for-virtual-currency-businesses [ttps://perma.cc/4532-G99X].
[137] CSBS Model at 11.

[138] *See id.*
[139] *See id.* at 12.
[140] *See id.* at 4.
[141] *See id.* at 12.
[142] *See id. at 13.*
[143] Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114-4 (1970) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., and 31 U.S.C.) ("Amending the Federal Deposit Insurance Act to require insured banks to maintain certain records, to require that certain transactions in United States currency be reported to the Department of the Treasury, and for other purposes.").
[144] *E.g.*, 31 U.S.C. § 5318(h) (2014) (requiring financial institutions to "establish anti-money laundering programs").
[145] CSBS Model at 13-14
[146] *See id.* at 7.
[147] *See* Michael Bobelian, *NY's BitLicense Reveals The Difficult Tradeoffs Of Regulating Bitcoin*, FORBES (Mar 8, 2018 7:30 PM), http://www.forbes.com/sites/michaelbobelian/2015/06/08/nys-bitlicense-reveals-the-difficulttrade-offs-of-regulating- bitcoin/2/#1ca0c4c9b0e8 [https://perma.cc/A4AS-DLHN].
[148] 23 N.Y. LAW § 200.2(i) (defining person as "an individual, partnership, corporation, association, joint stock association, trust, or other entity, however organized").
[149] 23 N.Y. LAW § 200.3(a) ("No Person shall, without a license obtained from the superintendent as provided in this Part, engage in any Virtual Currency Business Activity."). For the full definition of virtual currency business activities, see § 200.2(q).
[150] 23 N.Y. LAW § 200.2(q).
[151] 23 N.Y. LAW § 200.3(c)(2).
[152] 23 N.Y. LAW § 200.7. The regulations require that a "[e]ach licensee shall maintain and enforce written compliance policies, including policies with respect to antifraud, anti-money laundering, cyber security, privacy and information security, and any other policy required under this Part, which must be reviewed and approved by the Licensee's board of directors or an equivalent governing body." § 200.7(c).
[153] 23 N.Y. LAW § 200.8 ("Each licensee shall maintain at all times such capital in an amount and form as the superintendent determines is sufficient to ensure the financial integrity of the Licensee and its ongoing operations based on an assessment of the specific risks applicable to each Licensee."). The superintendent will consider many factors including composition of assets and liabilities, the leverage and liquidity of the licensee, and the financial protection the licensee implements to protect its customers. § 200.8(a).
[154] 23 N.Y. LAW § 200.12 ("Each Licensee shall, in connection with its Virtual Currency Business Activity, make, keep, and preserve all of its books and records in their original form or native file format for a period of at least seven years ... in a condition that will allow the superintendent to determine whether the Licensee is complying with all applicable laws, rules, and regulations").
[155] 23 N.Y. LAW § 200.13 ("Each Licensee shall permit and assist the superintendent to examine the Licensee whenever in the superintendent's judgment such examination is necessary or advisable, but not less than once every two calendar years ....").
[156] *See* Press Release, Assemb. Matthew Dababneh, Assembly Member Dababneh Issues Statement on the Regulation of Virtual Currency (Aug. 15, 2016), https://a45.asmdc.org/press-release/assemblymember-dababneh-issuesstatement- regulation-virtual-currency [https://perma.cc/LFJ3-XQKF].
[157] *See* Rainey Reitman, *A License to Kill Innovation: Why A.B. 1326-California's Bitcoin License-is Bad for Business, Innovation, and Privacy*, ELECTRONIC FRONTIER FOUND. (Aug. 7, 2015), https://www.eff.org/deeplinks/2015/08/licensekill- innovation-why-ab-1326-californias-bitcoin-license-bad-business [https://perma.cc/UKU2-E2EE].
[158] *See id.*
[159] BTC Trading, Corp., Exchange Act Release No. 73783, 110 SEC Docket 8 (Dec. 8, 2014).
[160] Bitcoin Investment Trust, Exchange Act Release No. 34-78282, 114 SEC Docket 11 (July 11, 2016).
[161] In re Erik T. Voorhees, Securities Act Release No. 9592, 109 SEC Docket 1 (June 3, 2014).
[162] In re Sunshine Capital, Inc., Exchange Act Release No. 80435, 116 SEC Docket 10 (Apr. 11, 2017).
[163] SEC v. Homero Joshua Garza, Civil Action No. 3:15-CV-01760 (D. Conn. filed Dec. 1, 2015); SEC v. Trendon T. Shavers, Civil Action No. 4:13-CV-416 (E.D. Tex. filed July 23, 2013).
[164] The Dao, Exchange Act Release No. 81207, 117 SEC Docket 5 (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf) [hereinafter "The DAO Report"] (distinguishing between cryptocurrencies that qualify as securities and those that qualify as virtual currencies).
[165] *See id.*

[166] *See id.*
[167] Shivdeep Dhaliwal, *Japan Officially Recognizes Bitcoin and Digital Currencies as Money*, COINTELEGRAPH (Mar 2, 2018 7:30 PM), *https://cointelegraph.com/news/japan-officially-recognizes-bitcoin-and-digital-currencies-as-money*.
[168] James Moreau, *Japan's Cabinet Passes Bills to Officially Recognize Digital Currencies as Real Money*, CRYPTOCOINS NEWS (Apr. 3, 2018), *https://www.cryptocoinsnews.com/japans-cabinet-passes-bills-offiically-recognize-digital-currencies-real- money/*.
[169] *India's Bitcoin Use Set to Surge in 2016*, RED HERRING (Apr. 11, 2018), *http://www.redherring.com/finance/indias-bitcoin- use-set-surge-2016/*.
[170] *See id.*
[171] JP Buntinx, *Reserve Bank of India Publicly Endorses Blockchain Technology*, BITCOINIST (Mar. 28, 2018, 3:27 PM), *http://bitcoinist.net/reserve-bank-of-india-publicly-endorses-blockchain-technology/*.
[172] Gautham, *China, Driving the Bitcoin Wagon with BitMex and Others*, NEWSBTC (Mar. 5, 2018, 11:30 PM), *http://www.newsbtc.com/2015/12/05/china-driving-bitcoin-wagon-with-bitmex/*.
[173] *See id.*
[174] *See id.*
[175] *See id.*
[176] Georgia Wilkins, *Bitcoin Faces Calls for Tougher Regulation Amid Igot Scandal*, THE SYDNEY MORNING HERALD (Apr. 12, 2016), *http://www.smh.com.au/business/banking-and-finance/bitcoin-faces-calls-for-tougher-regulation-amid-igot-scandal- 20160412-go44xo.html*.
[177] Alice Huang, *Reaching within Silk Road: The need for a new Subpoena Power that targets illegal bitcoin transactions*, 56 B.C. L. REV. 2093 (2015)
[178] *See* FED. R. CIV. P. 34 (describing the scope of e-discovery to include "writing, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations" that are "stored in any medium in which information can be obtained directly or, if necessary, after translation by the responding party into a reasonably useable form");
[179] Huang, supra note 177 at 32, (stating that human review is improbable for cases dealing with massive amounts of electronic data);
[180] *See id.* (describing the expenses associated with e-discovery as potentially "outcome determinative").
[181] *See id.* (citing a study on costs associated with the review of data in the electronic discovery process that revealed "manual review of 30 gigabytes of data would cost up to $ 3.3 million");
[182] *See* FED. R. CIV. P. 26(b)(2)(B*)*; (detailing how the 2006 amendment modified Rule 26 to include e-discovery).
[183] *See* Steven C. Bennett, *E-Discovery: Reasonable Search, Proportionality, Cooperation, and Advancing Technology*, 30 J. INFO. TECH. & PRIVACY L. 433 (2014) (stating that the Federal Rules require proportionality);
[184] Michael J. Martin, Note, *The Discoverability of E-Mails: The Smoking Gun of the Modern Era*, 7 U. MASS. L. REV. 182, 196 (2012) (discussing the use of Rule 45 in discovery to obtain emails from third parties); *see* also United States v. Crosland, 821 F. Supp. 1123, 1129 (E.D. Va. 1993) (The term 'subpoena,' most often encountered in the civil practice or grand jury context, carries with it a strong connotation of 'discovery').
[185] United States v. Crosland, 821 F. Supp. 1123, 1129 (E.D. Va. 1993) (The term 'subpoena', most often encountered in the civil practice or grand jury context, carries with it a strong connotation of discovery.).
[186] Joshua Gruenspecht, *Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J.L. & TECH. 543, 552 (2011) (asserting that unlike the civil rules, criminal rules and cases do not provide much guidance for electronically stored information). In the criminal context, the traditional discovery rule focuses on the defendant's ability to gain access to the material documents that the government has gathered.
[187] *See* FED. R. CRIM. P. 17 (detailing the current criminal subpoena standards);
[188] *See id.*
[189] *See* Nixon, 418 U.S. at 698 (addressing limitations on subpoenas duces tecum set forth in the Federal Rules of Criminal Procedure Rule 17); In re Zuniga, 714 F.2d at 636 (citing United States v. Calandra, 414 U.S. 338, 346 (1974)) (discussing the limits on grand jury subpoenas); *see also* Margoles v. United States, 402 F.2d 450, 451 (7th Cir. 1968) (providing courts the discretion to reject subpoenas duces tecum).
[190] FED. R. CRIM. P. 17(c)(2) ("On motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive."); *see* Nixon, 418 U.S. at 698 (reiterating that Rule 17(c) does not allow for oppressive or unreasonable subpoena requests).
[191] *See id.*

[192] *See* R. Enters., Inc., 498 U.S. at 301 (discussing the standard of proof in a motion to quash a subpoena); *see also* In re Grand Jury Proceedings, 616 F.3d 1186, 1201 (10th Cir. 2010) (applying the *R. Enterprises, Inc.* standard when considering a request to quash); In re Grand Jury, 111 F.3d 1066, 1075 (3d Cir. 1997*)* (citing and applying *R. Enterprises, Inc.*). In 1991, in United States v. R. Enterprises, Inc., the U.S. Supreme Court interpreted Rule 17(c) to give the government the presumption that the grand jury subpoena was reasonable. 498 U.S. at 301. The Court emphasized the language of the rule, which only allows a subpoena to be quashed if compliance is unreasonable.
[193] *Calandra*, 414 U.S. at 346. The Court pointed to cases where a criminal subpoena would have violated defendants' Fourth and Fifth Amendment rights. *Id.* (citing Hale v. Henkel, 201 U.S. 43, 76 (1906); Boyd v. United States, 116 U.S. 616, 631 (1886)).
[194] *See In re* Grand Jury 87-3 Subpoena Duces Tecum (*In re Grand Jury), 955 F.2d 229, 231 (4th Cir. 1992)* (citing Branzburg v. Hayes, 408 U.S. 665 (1972)) (deciding that when a defendant has established a prima facie case, the burden of proof moves to the government); *In re* Subpoenas Served upon Wood (*In re Wood), 430 F. Supp. 41, 45 (S.D.N.Y. 1977)* (citing *Branzburg, 408 U.S. 665)* (stating that the burden shifts onto the government when a valid First Amendment claim has been made). *See Id.* Huang at 137.
[195] *See generally* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995*)* (finding a constitutional right to anonymous speech); *Cahill, 884 A.2d at 454* (providing some constitutional protection for anonymous online speech); Lyrissa Barnett Lidksy, *Anonymity in Cyberspace: What Can We Learn from John Doe*?, 50 B.C. L. REV. 1373, 1376 (2009) (arguing that libel suits intent on unmasking anonymous online speakers threatened the First Amendment right to speak anonymously, but also recognizing the limits of such a right).
[196] *See* McIntyre, 514 U.S. at 342 (holding that the First Amendment protects a speaker's right to anonymity).
[197] *See* id. at 344; *see also* Cahill, 884 A.2d at 454 (addressing the standard that should be used in assessing an online speaker's First Amendment right to anonymous speech); Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377, 380 n.4 (Va. 2001) (referencing the lower court's consideration of the First Amendment rights of anonymous online speakers).
[198] *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 314 (2010) (holding that the First Amendment protects some monetary transactions that are used to fund speech); Sara Jeong, *Is Bitcoin Free Speech*?, SLATE (Feb. 7, 2018, 8:48 AM), *http://www.slate.com/articles/technology/future_tense/2014/02/bitcoin_as_free_speech_regulating_cryptocurrency_has_ramifications_for_democracy.2.html [http://perma.cc/947J-DZFQ] (hypothesizing that Bitcoin transactions could be protected by the First Amendment);see also Press Release, Electronic Frontier Foundation, EFF, Internet Archive, and Reddit Oppose New York's BitLicense Proposal (Oct. 21, 2014), https://www.eff.org/press/releases/eff-internet-archive-and-reddit-oppose-new-yorks- bitlicense-proposal [http://perma.cc/AQN2-4235] (protesting New York's BitLicense program, which regulates digital currencies, by pointing to a violation of speech rights).*
[199] *See* Citizens United, 558 U.S. at 310; *see also* Buckley v. Valeo, 424 U.S. 1, 143 (1976) (holding that limits on an individual's campaign finance expenditures violated First Amendment rights).
[200] Citizens United, 558 U.S. at 319-21 (detailing the events that led to plaintiff's challenge of the Bipartisan Campaign Reform Act of 2002's restrictions on political expenditures).
[201] *See id. at 365.*
[202] *See id*. at 351 (noting that speakers "use money . . . to fund their speech . . . [and] the First Amendment protects the resulting speech"); *see also Buckley, 424 U.S. at 16* (analyzing the use of money as not purely conduct but involving primarily speech, primarily conduct, or a mix of the two).
[203] *See* Huang, supra note 177 (referring to *Citizens United* as placing speech value in monetary transactions and arguing that this creates a possible free speech argument for Bitcoin use);
[204] *See* Digital Millennium Copyright Act, 17 U.S.C. § 512 (2012); BELLIA ET AL., *supra* note 18, at 340-42 (providing an overview of the DMCA).
[205] 17 U.S.C. § 512(h) ("A copyright owner . . . may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.").
[206] Jeannie Roebuck, *BitTorrent Sharing: The Case Against John Does*, 18 INTELL. PROP. L. BULL. 35, 40 (2013) (noting that Congress is worried about chilling innovation by placing liability on intermediary services); *see also* Laura Rogal, *Anonymity in Social Media*, 7 PHOENIX L. REV. 61, 72 (2013) (discussing the scope of the DMCA's subpoena powers); Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 339-40 (2008) (pointing to the DMCA as a method of obtaining a "John Doe subpoena").
[207] *See* Huang, supra note 177 at 152.
[208] *See id.*
[209] *See* Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 578-79 (N.D. Cal. 1999) (providing important considerations when evaluating a motion to quash); *see also* 17 U.S.C. § 512. These factors include: (1) whether

there is prima facie evidence of unprotected speech in the claim; (2) whether the claim can survive a motion to dismiss or summary judgment; (3) whether the subpoena is relevant to the claim; (4) weighing the interests of both parties; and (5) whether plaintiff has exhausted all means available to identify the defendant.

[210] *See* Matthew Mazzotta, Note, *Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers*, 51 B.C. L. REV. 833, 850 (2010) (noting that courts place a high burden of proof on plaintiffs before unmasking an Internet speaker's identity);

[211] *See* Huang, supra note 177 at 159.

[212] *See* FED. R. CRIM. P. 17 (describing current criminal subpoena standards);

[213] Daniel B. Garrie et al., *"Criminal Cases Gone Paperless": Hanging with the Wrong Crowd*, 47 SAN DIEGO L. REV. 521, 527 (2010*). See* generally McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (discussing a First Amendment right to anonymity). This Note does not address how the government should regulate the Bitcoin market to overcome its anonymity features.

[214] *See* Danton Bryans, Note, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L.J. 441, 442-43 (2014) (detailing how virtual currencies function);

[215] *See* FED. R. CRIM. P. 17;

[216] *See* Cheney v. U.S. Dist. Court for D.C., 542 U.S. 367, 387 (2004) (providing a narrow interpretation of the specificity prong); United States v. Nixon, 418 U.S. 683, 700 (1974) (explaining the standard that the government would have to overcome in order to issue a subpoena duces tecum);

[217] *See* Nixon, 418 U.S. at 700; see also Cheney, 542 U.S. at 387 (discussing the precision required to meet specificity); United States v. Binday, 908 F. Supp. 2d 485, 492 (S.D.N.Y. 2012*)* (reiterating that the *Nixon* standard places these three limitations on subpoenas). But see Kerr v. U.S. Dist. Court for N. Dist. of Cal., 426 U.S. 394, 399 (1976) (allowing a broad interpretation of relevancy in pretrial contexts).

[218] *See id.*

[219] *See Cheney*, 542 U.S. at 387 (setting a narrow scope on specificity); Nixon, 418 U.S. at 700 (explaining the limitations placed upon traditional criminal subpoenas); *see also Binday, 908 F. Supp. 2d at 492.*

[220] *See id.*

[221] *See* Bourjaily v. United States, 483 U.S. 171, 172 (1987) (concluding that *Nixon* does not apply to subpoena requests arising during a grand jury proceeding);

[222] *See id.*

[223] *See McIntyre*, 514 U.S. at 341-42 (striking down an Ohio statute that prohibited anonymous leafleting of campaign literature); The First Amendment likely provides Bitcoin users some protection in maintaining anonymity but thus far, Fourth Amendment claims regarding electronic content have been less successful. Although in specific situations courts have allowed a limited expectation of privacy in electronic material such as email messages, in general they have not been open to the idea that Fourth Amendment protections apply to electronic data shared with third parties.

[224] *See* Doe v. Cahill, 884 A.2d 451, 454 (Del. 2005*)* (acknowledging a First Amendment interest in anonymous online speech);

[225] Cameron Graham, *Out of the Spotlight, Bitcoin Gains Legitimacy*, WIRED (Mar. 15, 2018, 2:34 PM), *http://www.wired.com/insights/2014/09/bitcoin-gains-legitimacy/* [*http://perma.cc/PC8H-2GKF*] (analyzing the ebb and flow of interest in Bitcoin as the virtual currency's novelty value wears off).

[226] Once Bitcoin exchange and wallet sites are regulated, the government will have a source to subpoena for user information. *See* Graham, *supra* note 225, at 9 (describing the resulting decrease in anonymity once Bitcoin intermediaries have to comply with financial regulations).

[227] *See Cahill, 884 A.2d at 546* (finding limited First Amendment rights in anonymous online speech);

[228] *See* FED. R. CRIM. P. 17; Graham, *supra* note 225, at 73 (addressing why courts hesitate to unmask online speakers);

[229] *See* Citizens United, 558 U.S. at 314 (providing First Amendment protection for certain monetary transactions).

[230] *See* Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 578-79 (N.D. Cal. 1999) (describing the factors a court will consider when assessing a DMCA subpoena);

[231] *See* 17 U.S.C. § 512(h); This requirement prevents the government from randomly gathering a group of transactions or all the transactions on a general Bitcoin website and issuing a subpoena to identify those users.

[232] See Packwood v. Senate Select Comm. on Ethics, 510 U.S. 1319, 1320-21 (1994) (discussing standards for evaluating a pretrial subpoena duces tecum); Kerr, 426 U.S. at 399 (providing a broad scope for pretrial relevancy determinations); Nixon, 418 U.S. at 700 (requiring "relevancy" as a necessary element in issuing a criminal subpoena duces tecum). This is a relatively low hurdle for the government to pass and is also one of the elements the U.S. Supreme Court established for Rule 17 of the Federal Rules of Criminal Procedure.

[233] Courts have generally required specificity when evaluating a DMCA subpoena because it prevents bad faith and frivolous claims. *See* Michael Sherlock, *Bitcoin: The Case against strict regulation,* 36 REV. BANKING & FIN. L. 975 (2017)
[234] If the grand jury considered the existence of prima facie evidence of the crime, it would be too high a standard for simply obtaining a subpoena. *See* Graham, *supra* note 225. This is especially true due to the higher burden of proof in criminal cases. *See id.*
[235] *See generally* Jerry Brito & Peter Van Valkenburgh, State Digital Currency Principles and Framework (2015), https://coincenter.org/wpcontent/uploads/2015/04/StatePrinciplesandFrameworkV1-0.pdf [https:// perma.cc/ZP9E-X3VE].
[236] *See id.*
[237] *See, e.g.*, Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster,* WIRED (Mar. 3, 2018 7:30 PM), http://www.wired.com/2014/03/bitcoin-exchange/ [https://perma.cc/SHF3-BYPZ].
[238] Nicholas Galunic, *The (Private) Key To Unlocking Bitcoin Legal Issues*, LAW360 (Feb. 19, 2018, 10:38 AM), https:// www.law360.com/articles/622698/the-private-key-to-unlocking-bitcoin-legal-issues [https://perma.cc/3MN5-7879].
[239] *See id.*
[240] Lawrence Trautman, *Virtual Currencies; Bitcoin & What now after liberty reserve, silk road, and Mt. Gox?,* 20 RICH. J.L. & TECH. 13 (2014)
[241] *See id.*
[242] *See* Van Valkenburgh, supra note 235, at 32 ("[B]itcoin'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.").
[243] *See id.*
[244] *See id.*
[245] Van Valkenburgh, supra note 235, at 33.
[246] *See id.* at 20-21
[247] *See id.* at 21 ("Small startups can be shielded from the costs of regulation by explicitly exempting them from regulation up until the point at which they pose serious consumer protective risks.").
[248] *See id.* at 22.
[249] *See id.* at 21-22 ("The $5 million per year transaction level is an appropriate threshold among companies that can pose serious, systemic risks to consumers (e.g. Mt. Gox), and those where risk-level is tolerable given the benefits that unfettered start-up innovation could bring.").
[250] United Nations, UNCITRAL, "Cryptocurrencies: International Regulation and Uniformization of Practices, available from https://www.uncitral.org/pdf/english/congress/Papers_for_Congress/29-DOLES_SILVA-Cryptocurrencies_and_International_Regulation.pdf
[251] *See id.*
[252] Jonathan Lane, *Bitcoin, Silk Road, and the need for a new approach to virtual currency regulation,* 8 CHARLESTON L. REV. 511 (2014)
[253] Kyle Torpey, *Four Key Disagreements Between Bitcoin Classic and Bitcoin Core,* BITCOIN MAGAZINE (Mar. 4, 2016, 10:52 AM), *https://bitcoinmagazine.com/articles/four-key-disagreements-between-bitcoin-classic-and-bitcoin-core-four-key- disagreements-between-bitcoin-classic-and-bitcoin-core-four-key-disagreements-between-bitcoin-classic-and-bitcoin-core- 1457106744*.
[254] *See id.*
[255] Paul Levy, *Finally, Interesting Uses for Blockchain that goes Beyond Bitcoin*, PHYS.ORG (Dec. 7, 2015), *http://phys.org/news/2015-12-blockchain-bitcoin.html*.
[256] *See id.*
[257] *See id.*
[258] Jeanne Schroeder, *Bitcoin and the Uniform Commercial Code,* 24 U. MIAMI BUS. L. REV. 1 (2016)