

[REDACTED]

[REDACTED]

[REDACTED]

Dear Ms. Syracuse:

I am an attorney and Certified Public Accountant with a Master's Degree in Accounting.

For nearly twenty years I have also been licensed life and health insurance agent, a registered representative of a broker-dealer, and an investment advisor representative of an investment advisory firm. Consequently, I am very familiar with both the purposes of, and need for, financial services regulations.

However, I am also an early Bitcoin adopter, and I have a strong understanding of the practicalities and implications of blockchain technologies.

My legal, accounting, securities, insurance, and investment advisory backgrounds, combined with my familiarity with Bitcoin, make me uniquely qualified to offer feedback and commentary on New York's proposed virtual currency regulations. I hope you find these comments helpful.

Before getting into the details of your proposed regulations, and suggesting edits to them, it is important to first elaborate on what blockchain technologies are, and more importantly what they are not. I shall use Bitcoin as an example of blockchain technologies throughout this commentary since Bitcoin (that is, the world's first blockchain ledger), and the related bitcoins (the unit of account or measurement for transactions taking place on the blockchain ledger), are the first and best-known examples of the technology. I fear that, without this bigger understanding of blockchain technology, New York runs the risk of promulgating regulations that will, embarrassingly for all involved, at best be moot and ineffective as a practical matter and, at worst, cost New York dearly.

Blockchains Are Distributed Ledgers

The Bitcoin blockchain is simply a synchronized ledger that is stored on participating computers throughout the world, including the Macbook Pro on which I am typing this comment. Blockchains are systems of accounting--that is, of keeping track of things. They represent a new and superior way of recording and memorializing transactions or of registering things publicly. There are three primary factors that distinguish the Bitcoin blockchain ledger from an "ordinary" accounting ledger or registration tool:

1. The Bitcoin ledger, the blockchain, is "open", meaning that any person in the world with the necessary credentials (that is, who controls bitcoins) is free to make entries in the ledger,
2. The Bitcoin blockchain ledger is "distributed" and maintained by the public, rather than centralized and maintained by a "trusted third party" (such as a bank or registrar), meaning that anyone who may wish to do so can store a copy of the ledger on their computer or, theoretically, even print it out and read it.
3. The Bitcoin blockchain ledger is secure, meaning that, subject to exceptions that are irrelevant for purposes of this comment, all transactions entered into the ledger are effectively permanent, incorruptible, and irreversible.

Thus, blockchain technologies represent the world's first, and perhaps only, solution to the Byzantine Generals Problem ("BGP"). Because this age old problem of computer science has now been solved, it is possible for the first time in human history to maintain a ledger or register that is both open to the general public and provably secure.

Individual bitcoins or fractions thereof (hereafter just "bitcoins" with a lowercase "b") are both the technological means by which this distributed ledger is secured and the unit of account used to track entries on the ledger. To make an entry into the ledger, one must possess, or rather control via a private cryptographic key, at least the smallest available fraction of a bitcoin, and very importantly, one must transfer said bitcoin (or fraction thereof) to another account as part of making the entry in the ledger or register. Said another way, every single entry in the bitcoin ledger requires the transfer of bitcoin from one account (called an "address") on the ledger to another address on the ledger.

This requirement that every entry in the Bitcoin blockchain ledger involve the transfer of bitcoin from one address to another is an integral part of the solution to the Byzantine Generals Problem. Without this requirement, the ledger would be insecure and would quickly fill with spam. Furthermore, for a variety of reasons, it would no longer be possible to keep all distributed copies of the ledger in sync or to incentivize unrelated parties for administering and maintaining the ledger on their computers.

Blockchains are Not Inherently Financial in Nature

It is important to note that this public ledger technology, the blockchain, has innumerable potential uses, only some of which are financial in nature. For instance, blockchains can serve:

- a) as a mechanism for voting (https://www.google.com/?gws_rd=ssl#q=bitcoin+can+be+used+for+voting&safe=active)
- b) as an alternative domain name system or DNS (https://www.google.com/?gws_rd=ssl#q=namecoin&safe=active)
- c) as a secure and distributed messaging system (https://www.google.com/?gws_rd=ssl#q=bitmessage&safe=active)
- d) as a notary service useful in proving the existence of most any digital file (a picture or an electronic Will, for instance) on a given date and time (<http://www.proofofexistence.com/about>)
- e) as the backbone for an entirely new and distributed version of the Internet (<https://duckduckgo.com/?q=maidsafe>)
- f) as the backbone for future "distributed autonomous corporations" (<https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>)
- h) as a way to rid the world of spam (<https://www.google.com/#q=can+bitcoin+eliminate+spam&safe=active>)
- i) and much, much, much more.

Thus, in a very real sense, blockchain technology is nothing but an extension of the Internet. Most everything that can be done on the Internet can (eventually) be done better, more securely and more robustly using a blockchain overlay. This fact has been recognized by a wide number of knowledgeable commentators, some of whom participated in making the Internet widely accessible (https://www.google.com/?gws_rd=ssl#q=bitcoin+is+like+the+internet&safe=active).

Consider this quote by Marc Andreessen, founder of Netscape, for example:

"A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers.

Political idealists project visions of liberation and revolution onto it; establishment elites heap contempt and scorn on it.

On the other hand, technologists—nerds—are transfixed by it. They see within it enormous potential and spend their nights and weekends tinkering with it.

Eventually mainstream products, companies and industries emerge to commercialize it; its effects become profound; and later, many people wonder why its powerful promise wasn't more obvious from the start.

What technology am I taking about? Personal computers in 1975, Internet in 1993, and—I believe—Bitcoin in 2014."

The full article is a must read for any regulator, and it can be found here: http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_php=true&_type=blogs&_r=0.

So many people have recognized that blockchain technology like the Internet because it is simply an improvement upon it. It is, in fact, part of the Internet itself. This critical for regulators to understand for a number of reasons, the most important of which is that legal precedents regarding the Internet very obviously apply to blockchain technologies.

Blockchains are Protocols

Blockchain technology is so much like the Internet because, like the Internet, it is simply a protocol. Blockchains are simply strings of computer code, and nothing else. They have no physical existence. And, most all of them are open source protocols at that. In information science, protocols are agreed upon rules that permit end points in a given electronic network—the Bitcoin network, for example—to communicate with and understand each other. Protocols are therefore, in a very real and meaningful sense, a language. Anyone can download Bitcoin's open source protocol and run it on their personal computer, and thousands if not millions have.

Protocols are language, and language is undeniably speech. Both the Ninth Circuit Court of Appeals (*Bernstein v. United States*) and the Sixth Circuit Court of Appeals (*Junger v. Daley*) have explicitly ruled that computer source code is free speech that is protected by the First Amendment. We have no reason to believe that courts would likely conclude otherwise with regard to Bitcoin's open source protocols, which is nothing more than computer source code.

Blockchains are a Secure Record of Public Speech

Not only is the blockchain source code itself a very important form of speech, but the transactional record created by the blockchain is itself a secure and practically incorruptible record of public speech. Bitcoin's pseudonymous creator, Satoshi Nakamoto, very clearly understood the blockchain's usefulness and importance as a uncensorable record of speech when he appended a message to the very first bitcoin transaction.

That message said: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". This is, by all accounts, a reference to the January 3rd edition of the Times of London newspaper that contained on its front page the headline "Chancellor on brink of second bailout for banks". Given Satoshi's known libertarian political leanings, Satoshi's reference to the headline is widely understood as a form of political protest speech. In Satoshi's mind, the public distributed ledger offered by Bitcoin represented a way of potentially minimizing the importance of private, "trusted" third party ledgers which, in his mind, had proven less than trustworthy.

Thus, Blockchain technologies permit anyone, anywhere, to speak in uncensorable ways, and ways that can be used to validate the truth of the matter asserted. Imagine, for example, if someone familiar with blockchain technology had managed to snap important and incriminating photos of the recently downed Malaysian Airlines plane destroyed over the Ukraine. The photographer, fearing for his or her safety, might need to take his or her time leaving the country (and may not feel safe publishing the photos from within). With blockchain-based notary tools like "Proof of Existence" (link provided above), the photographer could, if he/she had acted quickly enough while still in Ukraine, demonstrate at anytime after-the-fact, unequivocally and for all eternity, that the exact photos later posted online days or weeks later were, in fact the very ones taken on the day of the crash. That is, the photographer could use the blockchain to prove mathematically that the photos had not been subsequently altered or tampered with in any way since a hash of those photos was stored in the blockchain (presumably on the day of the crash if he/she were careful and acted quickly enough). Imagine the usefulness of this free speech technology to a dissident in Iran or North Korea, or even a whistleblower here in the United States.

For instance, had blockchain technology existed prior to President Obama's birth, and had a hash of his birth certificate been recorded in the blockchain on the day of his birth or shortly thereafter, he would be able to prove with certainty to anyone today that the birth certificate he produced just a few years ago was in fact the exact same one originally used to create the hash stored in the blockchain just days after his birth. There would be no such thing as a "birther".

That bitcoin, like the Internet, facilitates free speech is critical for regulators to understand. In the United States, attempts by governments to regulate speech and tools of free speech are subject to either intermediate or strict court scrutiny, depending upon whether or not the regulation is content neutral or not. Bitcoin facilitates free speech in previously unavailable ways. Since the current bitlicense regulation makes no distinction between using a bitcoin to engage in a commercial for financial transaction and using one to make a public political or personal statement, or to send an email

that is provably not spam, and imposes the same burdens on each, it very likely represents an overly broad infringement upon free speech.

Imagine if New York tried to regulate the exchange of packets of information on the Internet in general instead of just on blockchains. Actually, New York actually did try that, and as we will see, things didn't turn out that well for New York in court.

Individual Bitcoins Are Not Money and Are Not Inherently Financial

Like the Internet, blockchain technology is "financial" in nature only because it can be used to facilitate financial transactions, among a great many other things. Bitcoin has an additional advantage in the sense that the individual units of "virtual currency" that make blockchain technology possible ("bitcoins", which are comparable to individual packets of information in the underlying Internet TCP/IP protocol) have market value (because they are scarce and useful) and are easily transferable.

For instance, bitcoins have value not because they are financial instruments per se, or are inherently financial in nature, but rather because the public reasonably believes that the ability to make an entry into the world's largest and most secure public ledger/register, the Bitcoin blockchain, is valuable, or at least may someday be so. And, as previously noted, making an entry in this ledger/register is impossible unless one controls bitcoins, just like making an entry on the Internet would be impossible without controlling packets of information in the TCP/IP protocol. However, unlike packets in the TCP/IP protocol, bitcoins are scarce (they must be so to secure the public ledger and network, thus solving the Byzantine Generals Problem). Since they are scarce, and since the use cases for this technology are as vast as the Internet (blockchains can theoretically replace the need for most any centralized recordkeeper, recorder, vote counter, or registrar, and can serve as the backbone for an entirely new Internet), the public's assignment of value to this ability to make an entry is not unreasonable or unfounded.

Even so, it's important to note that bitcoins did not always have value and even today are not commonly accepted as payment for goods and services in very many places, especially not (yet) in the "bricks and mortar" economy. In fact, for the first many months of their lives, bitcoins were essentially worthless. The first known commercial transaction with bitcoins took place on May 23rd, 2010, nearly seventeen months after the first bitcoin was "mined" in the "Genesis Block". At that time (May, 2010), 10,000 bitcoins (worth about \$6 million today) were used to purchase two large pepperoni pizzas from a Papa Johns restaurant in Florida. Thus, at that time, 10,000 bitcoins were only worth about \$20, making each bitcoin worth \$.002 USD per coin. Just a few months prior to that, they were, for all practical purpose, not worth a penny.

Thus, bitcoins (or whatever the unit of account on a given blockchain may be called) are not money. They are not even inherently financial in nature and their non-financial uses potentially outnumber, and are potentially more significant than, their financial ones.

Whatever value they have is a result of market forces. They have no issuer or backer guaranteeing them. They are not legal tender. They are not denominated in dollars. They do not inherently represent the debt of any other party. They do not inherently represent a claim on any other asset, financial or real. They cannot be possessed, though they can be controlled and transferred (via a private cryptographic key). They live only and forever on the blockchain, the secure public register/ledger.

Blockchains Undoubtedly Implicate Interstate Commerce

Computers that cooperate to operate the Bitcoin network and maintain the synchronized, public, secure ledger are located in most every jurisdiction on earth, certainly in most, if not every, US state. Additionally, the blockchain had undeniable commercial applications that are at least as broad as the Internet as a whole. In fact, bitcoins allow for revolutionary new commercial transactions, only a small portion of which are likely to be financial in nature.

Consequently, any regulation of the blockchain is unquestionably a regulation of interstate commerce. Given the obvious analogies between blockchain technologies and the Internet (decentralized, multipurpose and multifaceted, multi jurisdictional, etc.), an analysis of precedents in Internet regulation should inform the proposed bitlicense regulations.

In this respect, I would draw your attention to the 1997 case *American Library Association v. Pataki*. In this case, New York attempted to protect minors from the harms of Internet pornography by making it a crime to assist in the transmission of such over the Internet, at least in some cases. Importantly, the statute in question provided for several defenses to

liability, which are not unlike some of the requirements that the New York Department of Financial Services (“NYDFS”) seeks to impose upon those seeking to engage in Virtual Currency Business Activities. For example, Defendants would not be held liable under the New York pornography act if they had made “reasonable efforts” to identify the true age of the minors or the defendant had taken reasonable steps to restrict access of minors to pornographic material (via electronic blocking, requiring credit cards, etc.).

This case is very enlightening. Just substitute “New York Resident” for “minors” and “Virtual Currency Business Activity” for pornography, and the parallels between the ALA v. Pataki case and the proposed “bitlicense” regulations are glaringly obvious.

After pondering various legal analogies to apply to the “new” Internet (is it most like a telephone network, or the US Mail, or a television network, or...what?), US District Judge Preska concluded:

“I find, as described more fully below, that the Internet is analogous to a highway or railroad. This determination means that the phrase ‘information superhighway’ is more than a mere buzzword; it has legal significance, because the similarity between the Internet and more traditional instruments of interstate commerce leads to analysis under the Commerce Clause.”

The exact same thing can, and should, be said of blockchain technologies. After all, blockchain technology is nothing more than a solution to the Byzantine General’s Problem, an age-old problem describing the difficulty of achieving consensus in distributed computer networks like the Internet. As a solution to the BGP, blockchain technology is a means of securing the Internet, a way of making it safe for certain types of transactions and communications that were previously impossible.

Judge Preska observed the following with regards to the Internet (all of which obviously applies equally to blockchain technologies):

“The Internet is a decentralized, global communications medium linking people, institutions, corporations, and governments all across the world. [T]he Internet is a network of networks—a decentralized, self-maintaining series of redundant links among computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control. No organization or entity controls the Internet; in fact the chaotic, random structure of the Internet precludes any exercise of such control....Regardless of the aspect of the Internet they are using, Internet users have no way to determine the characteristics of their audience that are salient under the New York Act—age and geographic location. In fact, in online communications through newsgroups, mailing lists, chat rooms, and the Web, the user has no way to determine with certainty that any particular person has accessed the user’s speech. ‘Once a provider posts content on the Internet, it is available to all other Internet users worldwide’. A speaker this has no way of knowing the location of the recipient of his or her communication. As the poet said, ‘I shot an arrow into the air, it fell to the earth I know not where.’

This highly simplified description of the Internet is not intended to minimize its marvels. While no one should lose sight of the inventiveness that has made this complex of resources available to just about anyone, the innovativeness of the technology does not reclude the application of traditional legal principles—provided that those principles are adaptable to cyberspace. In the present case, as discussed more fully below, the Internet fits easily within the parameters of interests traditionally protected by the Commerce Clause.

The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulations by states that the actor never intended to reach and possibly was unaware were being accessed. Typically states’ jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet. The menace of inconstant state regulation invites analysis under the Commerce Clause of the Constitution, because that clause represents the framer’s reaction to overreaching by the individual states that might jeopardize the growth of the nation—and in particular, the national infrastructure of communications and trade—as a whole.

The Commerce Clause is more than an affirmative grant of power to Congress. As long ago as 1824, Justice Johnson in his concurring pinion in *Gibbons v. Ogden*...recognized that the Commerce Clause has a negative sweep as well. In what commentators have come to term its ‘dormant’ aspect, the Commerce Clause restricts the individual states’ interference with the flow of interstate commerce in two ways. The Clause prohibits discrimination aimed directly at interstate commerce...and bars state regulations that, although facially nondiscriminatory, unduly burden interstate commerce.... Moreover, courts have long held that state regulations of those aspects of commerce that by their unique nature demand cohesive national treatment is offensive to the Commerce Clause.”

Applying the above logic, and after extensive analysis, Judge Preska concluded:

"[T]he New York [Pornography] Act is concerned with interstate commerce and contravenes the Commerce Clause for three reasons. First, the act represents an unconstitutional projection of New York law into conduct that occurs wholly outside of New York. Second, the Act is invalid because although protecting children from indecent material is a legitimate and indisputably worthy subject of state legislation, the burdens on interstate commerce resulting from the Act exceed any local benefit derived from it. Finally, the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether."

Respectfully, if something like Internet pornography lends itself so readily to Commerce Clause analysis, it's difficult to conceive how blockchain technologies, with the obvious potential of revolutionizing Internet commerce, does not. And, if simply requiring the verification of a viewer of pornography's date of birth and geographic location, as the New York pornography act required, is an unconstitutional imposition by New York that violates the Commerce Clause, it's hard to see how some of the far more draconian bitlicense requirements don't do the same, as we shall see.

For these reasons, regulators in general, and state regulators in particular, would do well to remember that Bitcoin is an Internet phenomenon, and prior case law concerning regulation of the Internet by states almost certainly applies. At a minimum, a New York regulator should be very familiar with *ALA v. Pataki* and similar cases, and should be prepared to explain in detail how and why their logic doesn't apply to the bitlicense regulations.

Now, About Those Regs...

Given the extraordinary number of very important non-financial uses of blockchain technology, and given its inherent nature as speech and its potential impact upon interstate commerce, it's important to consider the extent to which the New York State Department of Financial Services can or should regulate so-called "virtual currencies" directly.

Applying financial services industry style regulations to an invention as diverse and useful as blockchain technology, without carve-outs for its non-financial uses and consideration of its impact on interstate commerce in general (especially if multiple states pass irreconcilable regulations) and free speech in particular, represents a fundamental misunderstanding of the extensiveness and significance of the blockchain innovation. Attempting to apply narrow rules of the financial services industry to something as expansive and broadly useful as blockchains is like attempting to apply regulatory rules relevant to pre-1990's telecommunications companies to the Internet as a whole, something that Judge Preska, and many others, have declined to do.

The regs presume wrongly that Bitcoin is only or primarily a financial service, and that financial services regulations are the best legal analogy to apply to the new innovation that is Bitcoin. Like the Internet itself, Bitcoin has financial aspects, but it is much, much more important than that. Regulating Bitcoin merely as a financial service is therefore not only unconstitutional, it is practically impossible and will have numerous inadvertent consequences. Proceeding without due consideration of these facts just won't work, and attempting to do so will:

1. Force innovation to more understanding and technologically sophisticated jurisdictions
2. Turn legitimate innovators into criminals, and legitimate innovations into crimes
3. Restrict the development of non financial uses for blockchain technologies
4. Impose unnecessary restrictions upon interstate commerce
5. Restrict free speech
6. Likely lead to embarrassing court losses for regulators

The best analogy for regulating blockchain technologies is thus the same one employed by Judge Preska in the New York pornography case--that if an interstate highway or railroad, and "information superhighway".

That is not to say that Blockchain technologies don't involve financial considerations. They do. And, to the extent that they link to the already-regulated financial system, they should be regulated. Just like a bank can't escape financial regulation by operating on the Internet only, blockchain technologies can't completely escape regulation either simply because they are Internet-based. But, any such regulation, especially at the state level, must be narrow, targeted, apply intrastate only, extend only as far as the current financial system extends, and not unduly burden free speech (which includes the right to anonymous or pseudonymous speech).

Analysis of the Regs

Applying the above principles to the bitlense regulations leads quickly to the conclusion that, in their current form, they are unconstitutional, unworkable, and will have a great many unintended consequences. Fortunately, most of these defects can be resolved, while still accomplishing the major purposes of the regs, by taking a more modest and humble approach. In the remainder of this comment, I will point out just a few areas where the current regs “go to far” and how that overreach may be corrected.

First is the regulation’s definition of “Virtual Currency”. The regs insist that its definition be interpreted “broadly” to include “any type of digital unit” that is used as a “medium of exchange” or comprises “digital units of exchange”, seemingly regardless of where they originate or how they are obtained. Respectfully, this definition is so broad as to be meaningless. The phrases “medium of exchange” and “units of exchange” are not defined in the regs.

Recognizing that, via the Internet, discrete units of digital information are “exchanged” among computers everyday in “packets”, the regulation goes too far. Such exchange of digital packets is the very basis of the TCP/IP protocols that permit communication over the Internet. Such packets are, in fact, quite clearly the “medium of exchange” of the Internet. Thus, interpreted “broadly”, as the regulation insists must be done, most any Internet communications protocol falls under the purview of these regulations. The exclusions for “gaming” and “affinity or rewards program” are simply not broad enough to save the day.

Second is the definition of “Transmission”. As written, and combined with the definition of “Virtual Currency”, anyone transmitting “units” of digital information “from one Person to another Person” via “third party” servers and/or routers falls under the scope of the regulations. And yet, without doing exactly that, without transmitting discrete units of information from one person to another via third party services and equipment, the Internet would not exist.

I can think of no principled way of defining “virtual currency” so that it includes things like “bitcoins” that are used for financial purposes but excludes more “ordinary” Internet transactions or transmissions. The reason is that both simply represent speech—that is, the transfer of discrete units of information that serve as the medium of exchange for basis of communication for a given language or protocol. Additionally, because blockchain technologies are widely expected to one day serve as the backbone for a whole new generation of decentralized but otherwise “ordinary” Internet applications (like a distributed version of Facebook, or email, or Dropbox, for example), any distinction that is meaningful today would quickly become irrelevant tomorrow.

What is more, bitcoins are not fungible. Individual bitcoins can be “tagged” or “colored” to represent nearly any digital or physical asset or good, or even other currencies. For New York to assert regulatory authority over the transmission of bitcoins in general is for it to thus assert authority regulatory over of the transfer of, potentially, anything and everything. The regs currently make no distinction between bitcoins tagged to represent ownership rights to, say, my car or my Babe Ruth baseball card, or simply transmitted as a means of political speech (such as the Times of London reference) or for the purposes of eliminating email spam, versus those tagged to represent one US dollar, an ounce of gold, or something else more “financial”. Under any reasonable Commerce Clause and free speech analysis, New York does not have the unfettered power to regulate the transfer of everything, or the means of such transfer, even among its own residents and inside the State of New York, but especially when doing so impacts residents of other states, like me in Tennessee.

Third is the definition of “Virtual Currency Business Activity”. The regs purport to apply to any transfer of any bitcoin, regardless of what it may represent (a car, a baseball card, political speech, an email message, etc.) to any resident of New York, regardless of whether the sender has any ties to New York and regardless of whether the New York resident is even in New York at the time of the transmission. I remind you once again of Judge Preska’s comments regarding the Internet (which I paraphrase as follows which my edits in brackets):

“[Bitcoin] is a decentralized, global communications medium linking people, institutions, corporations, and governments all across the world. [Bitcoin] is a network of networks—a decentralized, self-maintaining series of redundant links among computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control. No organization or entity controls [Bitcoin]; in fact the chaotic, random structure of the [Bitcoin] precludes any exercise of such control...Regardless of the aspect of [Bitcoin] they are using, [Bitcoin] users have no way to determine the characteristics of their audience that are salient under the New York [regulations]—[identity], age, [residency], and geographic location, [etc.]. In fact, in online communications through [Bitcoin and related applications], the user has no way to determine with certainty that any particular person has accessed the user’s speech. ‘Once a [sender] posts content on the [Bitcoin network by entering a transaction], it is available to all other [Bitcoin] users worldwide’. A [sender] thus has no way of knowing the location of the recipient of his or her communication. As the poet said, ‘I shot an arrow into the air, it fell to the earth I know not where.’”

Same goes for “receivers” of bitcoins. There is no way to determine from whence they originated or who their actual sender may be without imposing severe restrictions on interstate commerce, certainly far more draconian than the relatively modest ones New York tried to impose when seeking to root out minors’ access to online pornography.

Thus, even if the regulations contained a workable definition of “Virtual Currency” and “Transmission”, and they don’t, the record keeping and licensing requirements imposed per the bitlicense regs on anyone “receiving Virtual Currency for transmission or transmitting the same” are a major imposition on interstate commerce and free speech. Since literally anything (not just money)—even messages or statements, financial records, hashes of legal documents, etc.—can theoretically be recorded for all eternity in the Bitcoin blockchain and transmitted to others by transferring nominal amounts of bitcoins from one place to another (and only via such a transfer, if the Bitcoin network is to be used), New York positions itself via these regulations as regulator of...everything. The regulations literally could not be more broach and overreaching.

Limiting the regulations only to transactions involving New York residents, as it purports to do, is no cure. In *Healy v. The Beer Institute*, 491 U.S. 336 (1989), the court found that the “Commerce Clause...precludes the application of a statute to commerce that takes place wholly outside the State’s borders, whether or not the commerce has effects within the state.” The court continued by saying “a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State’s authority and is invalid regardless of whether the statute’s extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulations is to control conduct beyond the boundaries of the State.”

Thus, a New York regulation requiring me, a resident of Tennessee who (hypothetically) never visits New York, to maintain a list of every New York resident with whom I communicate over the Internet would clearly be unconstitutional and unenforceable. As would a similar regulation that purports to require an online casino operating solely on servers out of China, or New Mexico, to do the same. As would a New York law that required banks operating in Indiana to obtain a New York license before serving New York residents at their Indiana branch location.

And yet, regulating out of state actors is exactly what the bitlicense regulations purport to do with respect to Bitcoin businesses. If I operate a bitcoin trading exchange in Tennessee, in full compliance with Tennessee laws, and I receive bitcoins from a resident of New York (assuming I could even determine his or her location and identity) for purposes of transmitting those bitcoins to others, or for purposes of storing them, or for purposes of converting them to fiat currency, the New York regulations would clearly require that I obtain a license from New York and comply with New York’s rules even if I have never set foot in New York, all of my servers are located outside of New York, I am already subject to regulation in Tennessee, and I have no contacts at all with the State of New York (other than the fact that one of its residents chose to send me a packet of digital information, a bitcoin, over the Internet). Respectfully, under the Commerce Clause, New York has no authority to require a Tennessee resident to obtain a license to transact business with New Yorkers when that business occurs wholly outside of New York, and this is true even if the New York residents are physically in New York at the time the business is transacted over the Internet. And yet, the bitlicense regulations explicitly apply even if the New York resident is visiting me in Tennessee at the time! Again, this would be like New York requiring a bank in Indiana to have a New York license before it can open an account for any New York resident who visits its Indiana location. Any Virtual Currency regulator should spend some time studying the Healy and ALA cases.

Another relevant case is *CTS Corp v. Dynamics Corn of America*. In it, the court stated that “the practical effect of the statute must be evaluated not only by considering the consequences of that statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation.” Therefore, imagine if every single state adopted similar but slightly differing rules from those New York has proposed? How would New York feel about Tennessee trying to regulate transactions between its residents and businesses physically located in New York that take place only over the Internet? I imagine that New York would not like it, and regardless, the result would be chaos and a clear impediment to commerce and free speech. As was said in *Southern Pacific Co. v. Arizona*, “If one state may regulate train lengths, so may all others, and they need not prescribe the same maximum limitation. The practical effect of [a law limiting train lengths] is to control train operations beyond the boundaries of the state exacting it...”.

And the practical effect of a New York regulations purported to dictate how Internet transactions with New York residents must occur is likewise “to control..operations beyond the boundaries of the state...”. And, all blockchain transactions are Internet transactions.

An additional problem with the definition of “Virtual Currency Business Activity” is that it purports to apply to the act of “controlling, administering, or issuing a Virtual Currency.” This is problematic for multiple reasons.

First, when it comes to decentralized ledgers like Bitcoin, any user of the core open source software, such as myself at this moment (it is running in the background on the computer on which I'm typing this comment) participates in "administering" the distributed ledger and the bitcoins thereon by assisting in processing certain transactions, maintaining redundant copies of the ledger, reconciling my copy with that of other users to reach consensus (via Bitcoin's unique solution to the Byzantine Generals Problem) as to the status of the network and ledger at any given moment, and providing computational resources that contribute to the security of the overall network. Thus, my computer, and thousands or millions of others like it, is an "administrator" of bitcoins.

And, because my computer in Tennessee contains an exact and complete replica of the blockchain ledger that it helps administer, and because some of the bitcoins on that ledger are undoubtedly controlled by residents of New York (or...are they, how could I know for sure?), I, a resident of Tennessee with no contacts to New York, would explicitly be required to obtain a license from New York, and comply with all of its rules, simply because I participate in the Bitcoin network. Every single other person running the Bitcoin client on their computer (and participating in the Bitcoin network), regardless of where they live in the world, would seemingly be required to do the same. Clearly, this is unacceptable. It would be like New York passing a law that required anyone using the Internet to obtain a license before communicating with a New York resident.

A final issue is that it is unclear when a controller, administrator or issuer of virtual currencies would need to obtain a license from New York. As written, this would occur when the particular blockchain unit of account becomes a "medium of exchange". Since the term "medium of exchange" is not defined, it's impossible to know when licensing is required. With bitcoins, for example, would it have been within "x" days of when the first pizza was purchased with them in 2010? Assuming so, how would bitcoin's anonymous creator, or the creator of some future digital currency, know when some persons somewhere first began using the unit of account for a given blockchain as a medium of exchange?

Notice that the same problem applies if we set the threshold higher. For example, maybe we require that there be a hundred or a thousand or a million commercial transactions before a given blockchain unit of account is deemed to be in sufficient use to constitute a "medium of exchange". Regardless, it's still impossible for the "currency's" founder or issuer or controller to make the determination about whether the threshold has been met. To this day, it's impossible to know how many of bitcoin's transactions are commercial or financial in nature and how many are not.

Furthermore, just like a wide variety of unrelated developers have contributed to the Internet over the years, a wide variety of unrelated developers contribute to any given blockchain's construction over a great many years as well, at least if it is open source, as most are. Do these developers constitute "controllers" or "administrators" of the virtual currency by virtue of their development? Seemingly so. Would they all be required to register? Seemingly so. Again, this is like New York insisting that anyone developing an Internet application that impacts a New York resident obtain a license to do so. Clearly, that is not permissible.

Conclusion and Recommendations

The proposed bitlicense regulations are fatally flawed because they seek to regulate all blockchain technologies (and actually, as currently written, the entire Internet) from the limited perspective of a regulator of financial services in New York. As the saying goes, "when all you have is a hammer, everything looks like a nail." And, to a financial services regulator like the NYDFS, it's understandable that blockchain technologies appear to be only or primarily a financial service.

But they are not, and regulating Bitcoin as merely or primarily a financial service would be like regulating the Internet as merely or primarily a financial service. The Internet is much, much bigger than financial services, and blockchain technologies are as well. Just like the Internet involves free speech and Commerce Clause implications, blockchain technologies do too. Perhaps even more so.

For these reasons, the regulations must be withdrawn or completely reworked. If the latter course is chosen, there must be a recognition, via carve-outs, of the fact that bitcoin can be used to transfer and register anything (including free speech), not just money or financial services. This will help insure that regulating the financial aspects of blockchain technologies doesn't limit their potential or usefulness in equally important non-financial ways. And, the regulations must be crafted to clearly apply only within New York.

The easiest way of achieving the goal of regulation without risking embarrassingly obvious constitutional attacks and without creating unintended consequences is for the NYDFS to promulgate rules regulating only the relationship of financial institutions and persons already clearly under NYDFS's authority to virtual currencies. This would presumably include and perhaps be limited to those who are already required to obtain licenses to provide financial services in New

York . Clearly New York has authority to direct the interaction of its existing licensees with virtual currencies in reasonable ways.

However, should the NYDFS feel the need to go beyond regulating only its existing licensees, then New York could also clearly regulate blockchain businesses that do business from and within New York. For example, virtual currency exchanges organized and operating out of New York, such as Coinsetter, would clearly fall within the NYDFS's regulatory purview. To the extent that New York might want require that these New York based businesses maintain certain solvency requirements, retain their reserves in fiat, obtain licenses, etc., then it would certainly be free to do so. Doing so would inspire confidence in New York virtual currency businesses, making it an appealing destination for those who seek to increase Bitcoin's credibility and usefulness via regulation. But to the extent that New York seeks to impose its preferred ways on businesses located wholly outside of New York, and communicating with New York residents only via the Internet over blockchains, it clearly exceeds its authority. Proceeding in this manner will have numerous adverse and embarrassing consequences, as previously noted.

Sean G. King, JD, CPA, MAcc