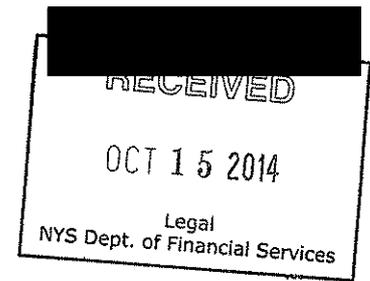


Jonathan Harms



October 8, 2014, 2014

dana.syracuse@dfs.ny.gov

DFS Office of General Counsel – Dana V. Syracuse
New York State Department of Financial Services
One State Street, New York, NY 10004

Re: Comments on Proposed Rulemaking Regarding Regulation of the Conduct of Virtual Currency Businesses - DFS-29-14-00015-P

Dear Mr. Syracuse,

I have authored or co-authored four U.S. patents, and thirteen scientific publications. My employment is in the field of spintronic research which aims to create electronic devices that utilize the angular momentum of electrons to store data. I work at a world renowned research lab in NY. I am also a bitcoin adopter, advocate, speculator, and investor. Thank you for soliciting feedback from the Bitcoin community regarding the regulation of virtual currencies and virtual currency businesses. Please carefully consider my feedback below.

I. Introduction

It is impossible to categorize bitcoin using any available legacy concept, because *we have never had anything like Bitcoin before*. What we can say with certainty is that it is *not a financial product or service*. Bitcoin (capital “B”) is a network of computers that maintain a synchronized, secure, open-access book (a blockchain) of publications, and bitcoin (small “b”) is the ink with which the blockchain is written. Because the nature of bitcoin is a publication tool, the nomenclature could be forked to call the components the “notebook” (blockchain), “ink” (bitcoin), “inkwell” (wallets), and “publishers” (miners) without any of these terms being misnomers.

Although I describe bitcoin as a series of technologies and pieces, the reality is that these are a homogeneous system. Unlike *both ink and money*, bitcoin is intrinsically linked with the blockchain. Just as the surface of paper cannot be separated from the paper itself, so Bitcoin’s publication database (the blockchain) is indivisible from the ink that creates the publications (bitcoin), which is indivisible from the publication network (Bitcoin).

Bitcoin warrants its own definition. When encountering any new idea that does not fit existing constructs, it is necessary to incorporate all perspectives into that definition. Peer-to-peer publishing, a truth-machine, digital ink, a method of coordinating parties, internet infrastructure, and commoditized speech all coherently describe different facets of Bitcoin. Bitcoin is sufficiently different that it will eventually become its own definition. The BitLicense superficially treats bitcoin as a financial instrument, which simply does not reflect bitcoin’s complex nature and in fact misses the whole point of what bitcoin is.

The BitLicense proposal attempts to classify technologies like bitcoin as financial product or service. bitcoin cannot be redeemed. bitcoin has no issuer, no backer, and no counterparty. It represents no debt and no promise of any party. bitcoin cannot be owned, possessed, or held; it can only be controlled. They exist nowhere but in a

distributed database. There are no balances of bitcoin, only calculations of bitcoin. Bitcoin fails to meet the basic definitions of money, currency, or financial instruments. Bitcoin's technology must be evaluated by its nature, not nomenclature. The network's nature is that of a secure peer-to-peer publication platform, and bitcoin's nature is similar to that of digital ink. Its utility comes from the ability to access and create cryptographically provable speech in a worldwide, indelible, and immutable database of publications.

As you will see, Bitcoin combines three technologies, none of which are financial in nature. The *combined* application of these technologies is incredibly valuable, but not inherently financial in nature and does not fall under the jurisdiction of the NYDFS. The first component is cryptographically provable statements, such as permissions, notarizations, instructions, and contracts. The second component is an immutable database of publications created via a peer-to-peer publishing process. The third technology is a method for coordinating distributed peers in a trustless fashion to secure and protect the immutability of this database.

Careful inspection will reveal that Bitcoin's combination of these technologies created a new paradigm that commoditizes truthful speech. Now that Bitcoin has been invented, it seems inevitable that all peer-to-peer publishing platforms that are universally accessible and immutable will digress into Bitcoin. These two properties of any publication platform make possible the evaluation of a cornucopia of statements, permissions, events, identities, and even actions such that their truthfulness can be mathematically and definitively proven. Bitcoin cannot be un-invented; it forever commoditizes access to truth that *inevitably* develops a market.

I will propose a hypothetical peer-to-peer publishing network designed not to be financial in nature, and reason why it must develop a market if it becomes useful. Attempts to divorce secure peer-to-peer publishing from a market is analogous to abolishing the price of ink – it cannot be done. Because blockchains are a publication tool with enormous non-exchange utility, any regulation of them is in essence a dragnet regulation of all peer-to-peer speech. Because publication networks increase in utility and security with more participants, all peer-to-peer publishing is likely to tend towards the largest network, which is currently Bitcoin. Therefore, if the NYDFS does not withdraw the BitLicense proposal, it must exempt bitcoin from regulation as a "virtual currency." Classification as a "virtual currency" would represent a gross misunderstanding of the nature of bitcoin and attempts to do so would ultimately prove unsuccessful.

II. Technical Description of Bitcoin

*"Writing a description for (bitcoin) for general audiences is bloody hard.
There's nothing to relate it to." - Satoshi Nakamoto*

Because Bitcoin is unlike anything that has existed, it is necessary to understand its nature, and not simply rely on nomenclature to understand it. The following three subsections describe perhaps the three most critical components of the Bitcoin technology.

1. *Consensus amongst peers and the consequences of such*

At the core of the Bitcoin protocol is a consensus algorithm. This protocol solves the age old¹ Byzantines' Generals Problem^{2 3} (BGP), which describes the difficulty in coordinating distributed parties. This protocol creates a new database structure which is self-validating⁴, and proves consensus as to what the network has witnessed. This feature is perhaps the single greatest innovation of the Bitcoin publishing platform, and it is what enables the security that ultimately leads to value being created. Cooperation between peers is something that is very difficult to achieve, let alone prove⁵, and was thought impossible without a trusted coordinator.

The solution that Bitcoin invokes is surprisingly simple and eloquent. It is an elaborate number guessing game. Peers in the network take the publications and run them through a cryptographic hash function. The output depends on the input (the publications), but not in any predictable way, and the output space is comparable in size to the number of atoms in the Universe. The participants in the network agree to keep on guessing until they find a certain subset of outputs. Finding these outputs is *incredibly* hard. It is currently about 100 times more difficult than rolling 13 consecutive Yahtzees—an entire game. For an individual computer to find the output, it might take decades, but if millions of computers work together, they could find the correct number in a few minutes. Any computer that strays from the group will be unable to find the correct number in a reasonable amount of time. The meaning, therefore, of the *rate* at which the numbers are found is *cooperation*. You do not need to ask any coordinator if everyone is cooperating, because the rate itself is *proof-of-cooperation*.

The consequences of this ability to cooperate without an organizer are potentially enormous. For example, it would be more economical if all of the users of the internet contributed a small portion of their computer to help run the internet. Before Bitcoin, the trustless coordination between peers was thought impossible. Businesses such

¹ While the BGP started to formalize in academic literature in 1980, it's formulation as a Byzantine Generals trying to communicate on a battlefield reveals that Bitcoin solves a problem as old as humans' attempt to come to consensus while geographically distributed.

² http://en.wikipedia.org/wiki/Two_Generals%27_Problem

³ <http://research.microsoft.com/en-us/um/people/lamport/pubs/reaching.pdf>

⁴ Self-validating means it bears witness to its own authenticity. It does not need to appeal to any outside source (for example, a cryptographic hash stored by a trusted third party) to prove it has not been damaged, tampered with, or changed. All copies but one could be destroyed, and we could still know with confidence that the one remaining is the true and unadulterated record. This data structure type was a necessary component to solving the BGP, for the Byzantine Generals cannot know the authenticity of the message unless the message itself contains its own validation.

⁵ It is highly recommended that as background you read about the two-generals-problem.

as Facebook, Amazon, and Wikipedia spend billions of dollars^{6 7} on datacenters. The coordinating power of Bitcoin enables alternative systems to the server-client model to be built.

Businesses can benefit because the multi-billion dollar infrastructure (potentially every computer on the internet) is already built, cutting their costs. The infrastructure is open and free to innovate upon, so a newly hatched startup can compete with the same resources and network as incumbent technologies. Consensus amongst peers transforms the internet into a truly public good rather than a conglomerate of networks of privately held infrastructure. Prototypes of decentralized consensus infrastructure are already here^{8 9 10 11 12}. Consensus cannot be regulated as a financial service, and as discussed in the introduction, Bitcoin's system is homogeneous and indivisible; therefore any regulation of bitcoin as money is dragnet regulation on consensus applications. This would inevitably lead to the BitLicense being endlessly challenged or evaded.

2. *An immutable peer-to-peer publication platform and the consequences of such*

Bitcoin's coordination is used to create an immutable database of publications called the blockchain. Each of the hard-to-guess numbers in the number guessing game are strung together to form a chain. The chain is linked by making each hard-to-guess number depend on the previously guessed number. The chain is welded to the blockchain via cryptographic hashing ("special number mashing") with the publications such that each number acts as a chain of signatures on a rolling database of publications. The database creates a record of publications, and each page (block) of this publication database is signed by a hard-to-guess number in a way that cannot be forged by individuals. Only the entire network is powerful enough to create these signatures. This database now becomes self-validating, meaning it bears witness to its own authenticity. It does not need to appeal to any coordinator to prove it has not been damaged, tampered with, or changed. All copies but one could be destroyed, and we could still know with confidence that the one remaining is the true and unadulterated record. The Bitcoin blockchain is the most secure publication platform ever created by humans. Anything written in it is absolutely indelible and immutable.

At its core, a simplistic description of Facebook is a collection of data and permissions for that data. A user uploads data to Facebook, and sets permissions for that data ("shares" that data) with certain people. In order to replace Facebook, a secure database would be required to publish permissions for the data and track where the data is stored. Bitcoin is capable of doing this. Already, the storage component has been demonstrated¹³, and the identity component has been created¹⁴. It seems like only a matter of time before the pieces are assembled together.

Of course, not every use for a peer-to-peer publication platform needs to be as ambitious as replacing Fortune 500 companies. I used bitcoin to publish "bitcoin is not money"¹⁵, just to illustrate the unfettered publishing utility of

⁶ http://www.datacenterknowledge.com/archives/2014/08/26/amazon-data-center-project/?utm_source=smschange&utm_medium=widget&utm_campaign=trending_articles

⁷ <http://www.businessweek.com/articles/2013-10-03/facebooks-new-data-center-in-sweden-puts-the-heat-on-hardware-makers>

⁸ Decentralized storage applications <http://stori.io/>

⁹ Decentralized DNS <http://namecoin.info/>

¹⁰ distributed identity <https://onename.io/>

¹¹ distributed PGP repository and identity https://keybase.io/docs/server_security/merkle_root_in_bitcoin_blockchain

¹² <http://www.proofofexistence.com/about>

¹³ <http://stori.io/>

¹⁴ <https://onename.io/>

¹⁵ "bitcoin is not money" is recorded into the blockchain here:

<https://blockchain.info/tx/d3cd45a993345f6e03858b9eef9e9e061dcc8a02e2d0081c867882fb1e1243d5>

bitcoin. I have also included a hash of this letter in Bitcoin's blockchain, so that historians hundreds of years from now will know that their copy is authentic. The blockchain can be used for religious speech¹⁶, political speech¹⁷, commercial speech; anything that can be written on paper can be published to Bitcoin's blockchain¹⁸. Since Bitcoin is an open peer-to-peer publishing platform, anyone is free to download and print the blockchain. General purpose publication cannot be regulated as a financial service and because Bitcoin's system is homogeneous and indivisible, any attempt to regulate bitcoin as money would represent censorship of non-financial peer-to-peer speech.

3. *Cryptographically provable statements and the consequences of such*

The third technological component of bitcoin is cryptography. Anything that can be represented digitally can be assigned a cryptographic key-pair. Using these cryptographic keys, a whole plethora of *provable* statements can be made. Let's say for a moment that we wanted to write an escrow contract without a lawyer or escrow agent. This would be impossible before peer-to-peer publishing, but there is no such limitation when you have Bitcoin. Even for the simplest of trades we could write previously inaccessible contracts such as a two-party double-deposit trustless escrow¹⁹, and because the statements of a contract are provable, and because the publication of the contract was secure, all of the peers in the peer-to-peer network can evaluate for themselves the outcome of the contract. No enforcement is needed because each peer enforces the contract for themselves. Bitcoin has the potential to make contracts *ubiquitously* inexpensive and self-enforcing (i.e. "smart contracts").

The previous paragraph is where all of the magic of Bitcoin comes together. Cryptography and provable statements have existed for quite some time (they are the backbone of internet security). But provable statements cannot develop value without an immutable and universally accessible place to publish them, and until Bitcoin solved the BGP, there was no *trustless* place to publish them. Bitcoin did not invent cryptography or provable statements, *but invented a peer-to-peer publication platform that allows for cryptographic statements to develop value*. The combination of an indelible record and provable statements creates a *truth-machine* that allows provable statements to develop value.

Consider how cryptography combined with peer-to-peer publishing could be used to create a Bitcoin alternative to Ticketmaster²⁰. A venue that doesn't need the marketing services of Ticketmaster could cut costs by publishing event tickets using Bitcoin's peer-to-peer publishing network. These pieces of digital property (the property being a contract for the use of a seat at a particular event), could be recorded, traced, and verified all using cryptographic statements. The terms and conditions of the asset could be defined within the property, such as allowing the ticket to be transferred only once and allowing a refund for 90% of the purchase price if desired. In fact, since purchasers can also publish statements about transfer of ownership which are 100% provable, there would no longer be a need for StubHub.

Furthermore, bitcoin's usefulness is not limited to the electronic world. Because anything can be recorded in the blockchain, and because anything can read what has been published in the blockchain, physical keys could be replaced with bitcoin. My cell phone could publish permission for my son to use my automobile for the afternoon,

¹⁶ <https://blockchain.info/tx/49b0f451df2c17b2d7426f49473a602e1c06e790d7ff63e1318fc40fca7f47e2>

¹⁷ <https://blockchain.info/tx/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdada33b>

¹⁸ Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software <http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html#ref5>

¹⁹ http://blackhalo.info/wp-content/uploads/2014/06/whitepaper_twosided.pdf

²⁰ <http://www.vennd.io/> is an opensource example of such an application.

and my car could read the blockchain and evaluate for itself whether the statement is true. The automobile could trust Bitcoin, because my permission statement is provable, and Bitcoin's database provides proof-of-lack-of-publication that I have not revoked this permission statement (the immutability of the blockchain gives rise to an equally important proof that something has *not* been said). Access to any physical property could be tied to permissions written in bitcoin. Physical keys function as a record of permission, but bitcoin are also capable of writing a verifiable record of permission.

As long as the ability to discern truth is valuable, any access to such a *truth-machine* will inevitably develop value. bitcoin is a commoditized ability to publish to this peer-to-peer publication network, similar to a digital *truth-telling-ink*. Value cannot be separated from the ability to publish on this network as long as people find it useful, but value does not make technology financial in nature nor automatically make it fall under the jurisdiction of the NYDFS.

III. A Hypothetical Non-Financial Peer-to-Peer Publication Platform

Now that Bitcoin has been invented, it seems inevitable that all forms of *secure* peer-to-peer publishing will tend to digress towards Bitcoin. The mere knowledge of bitcoin makes *all secure peer-to-peer speech* permanently valuable to produce. Bitcoin has commoditized truthful speech, and this cannot be undone. Imagine a hypothetical publishing network created under the following framework.

P2Publisher

Abstract. P2Publisher is a peer-to-peer publishing network that records and timestamps any publication to an open source database (called the openbook) that is globally accessible. This openbook can be downloaded by any participant in the network, and because the openbook is universally accessible, anyone can publish to it. Individual peers use a proof-of-work chain to maintain a synchronized, public, and immutable database of publications.

All this system does is timestamp publications and distribute a database of all publications to the global network. *There is nothing financial about this.* There is no integrated token to exchange. This simple publishing platform might be used to publish proof-of-authorship before sending a novel to a potential publisher. It might be useful as a notary service. Others might find use in publishing coupons, loyalty points, advertisements, product reviews, news alerts, microblogs, or nearly anything that paper and ink are used for.

Since the openbook is open to anyone to write whatever they want, it would only be a matter of time before users start employing cryptographic signatures to create a whole plethora of provable statements (or lack of statements) on the openbook. If knowledge of cryptographic signatures is openly published (which it is), then there is no way this simple publication system could not evolve into a *truth-machine*. As long as people find utility in discerning truth, they will employ methods of doing so, and if required will pay money to procure the ability.

Of course, because this system has no integrated token, an attacker might perform the internet equivalent of dumping ink all over the database and making it useless for other participants. Honest users would inevitably employ cryptography to block such abusers. They could start ignoring all publications except for those published with a particular token. This does not even require the other publications to stop. Just as 3D movies employ red and blue stereogram glasses to filter messages to each eye, these tokens simply need to act as filters to block out abusers. These tokens could be distributed in any fashion, with or without a price, but would need to be limited to prevent vandalism to the publication network. Though the publication platform would be technically functional

without a rationed ink, users would naturally migrate towards a rationed platform for usability reasons, even if that platform is only a subset of larger, un-rationed P2Publisher-like network.

Eventually, this secure portion of the platform could become so popular that some people might want more ink than they have access too. If demand was high enough, markets might develop to trade the *truth ink*. In fact, it seems difficult to conceive of a way that such a peer-to-peer publishing system could simultaneously achieve widespread usefulness, maintain security, and *not* develop a market. Market forces will always create a price for something useful and scarce.

This maturation of all secure peer-to-peer publishing platforms into something of value is present even in Bitcoin's own birth. Exchange value is not intrinsic to peer-to-peer publishing systems like Bitcoin. The Bitcoin network functioned for months as a peer-to-peer publishing network while the price of bitcoin was exactly *zero*. As the network began to prove itself, it started to develop a price.

P2Publisher was simply a *secure* publication tool that anyone could access. Even though it was not purposed to be financial in nature, without the censorship of cryptography (which would be technically very challenging) its use inevitably evolved into a tool for discerning the truthfulness of statements, but this was no fault of its own. In light of Bitcoin's invention, it is hard not to see this progression as inevitable for *all secure forms* of peer-to-peer publication. However, because the utility of peer-to-peer networks grows with the number of participants, it seems almost certain that the reciprocal effect will occur—that *all secure peer-to-peer publishing will migrate towards Bitcoin*.

IV. Seven Important Points Regarding Bitcoin

1. The first bitcoin created lack the ability to be transferred, therefore cannot be classified as money.

The first bitcoin ever created was clearly *not money*. It is well known that the coinbase transaction²¹ in the Genesis Block²² indelibly declares "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." By Satoshi Nakamoto's design, the first bitcoin ever created *lack a critical* component of money – the ability to be transferred. The Genesis Block bitcoin can never be mistaken for money because they can never be used as a medium of *exchange*.

2. All other bitcoin are capable of arbitrary speech, and therefore should be considered publication tools.

All ink can be used for speech, and all bitcoin is ink. Money *cannot* declare "bitcoin is not money"; bitcoin *can*²³. Religious speech *cannot* be published in money, while it can in bitcoin²⁴. Anything that can be written on paper can be written with bitcoin on the blockchain²⁵. Anyone can print and read the blockchain just like a book.

3. bitcoin is a commoditized resource that allows publication to the blockchain.

²¹ Coinbase transactions are the transactions which perform the coinbasing, i.e. they create new coins. This is not a form of computer manufacturing or effort, but a consensus mechanism. For example, orphaned blocks are identical in workmanship to non-orphaned blocks, but have no consensus, and therefore no value.

²² The Genesis is the first block, or page, in the Bitcoin ledger.

²³ "bitcoin is not money" is recorded into the blockchain here:

<https://blockchain.info/tx/d3cd45a993345f6e03858b9eef9e9e061dcc8a02e2d0081c867882fb1e1243d5>

²⁴ "Healthy Church 9marks.org," a religious statement about a healthy church, is recorded into the blockchain here:

<https://blockchain.info/tx/49b0f451df2c17b2d7426f49473a602e1c06e790d7ff63e1318fc40fca7f47e2>

²⁵ Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software

<http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html#ref5>

bitcoin is more like ink than money because the ability to control bitcoin allows publication. Ink is perhaps the most appropriate analogy one can imagine. Money cannot publish to the blockchain. *No amount* of money can publish to the blockchain.

4. Bitcoin is economical as a publication platform.

Receiving SMS text messages via Verizon Wireless is currently greater than 15 times more expensive than publishing to the bitcoin blockchain. Bitcoin's blockchain is more secure, universally accessible, and more economical than SMS text messaging. If SMS text messaging is considered a communication tool, then bitcoin should also be considered a tool for communication, similar to ink.

5. The ability to be exchanged does not imply that bitcoin is money.

Because it can be easily transferred, bitcoin *can be* used in exchange, and perhaps it is highly useful as such. However, only a small fraction of its potential use is as a medium of exchange. Just as *some* ink is used in exchange, not *all* ink is used in exchange. Regulating bitcoin as a financial instrument would be like regulating all green ink as dollars.

6. After exchange, bitcoin retains all of its speech ability.

Once ink has been used for to print money, other utility for that ink ceases. In contrast, after exchange, bitcoin remains useful as a publication tool, and can be reused endlessly for anything Bitcoin's peer-to-peer publishing network is capable of. It is impossible to separate the speech utility, for example, from the exchange utility of bitcoin. Therefore any regulation of Bitcoin or bitcoin or blockchains necessarily regulates all functions of bitcoin, regardless of any attempt (that I can conceive) to constrain regulation to the exchange utility of bitcoin only.

7. Bitcoin replaces infrastructure, not products.

Any asset can be written to the blockchain where it can be verified and transferred at near zero cost. bitcoin is not the financial asset, but the pen that drafted it. Bitcoin's publication network could be thought of as a globally distributed alternative to the buildings, computers, and people of the NYSE. To mistake bitcoin as the financial instrument is like confusing the computer used to trade a stock with the stock itself. Bitcoin's blockchain is general purpose, just as computers are general purpose.

V. Recommendations for the BitLicense

After reviewing the BitLicense proposal I am hereby recommending the NYDFS withdraw their BitLicense proposal. It is likely that current laws already provide the consumer protection the NYDFS is seeking. The NYDFS can add no trust to bitcoin. It was invented because of a history of breach of trust, and is a system to eliminate the need for trust. If criminals use tools to commit crimes, they should be punished for committing the crime, not using a specific tool. Existing laws seem sufficient to accomplish this. In contrast, the BitLicense proposal is a dragnet attempt to regulate a publication platform, and is likely to be immediately contested.

If the NYDFS feels it necessary not to withdraw the BitLicense proposal, it is recommended that the NYDFS further extend the public comment period. *The definition of virtual currencies 200.2(n) is too broad for the bitcoin community to adequately provide feedback.* Oranges are held in centralized repositories with integrated payment

systems. This technology is called a supermarket. They exchange oranges in digital²⁶ units for fiat currencies. Oranges store value because they are limited in quantity and useful. Will supermarkets require a BitLicense? Obviously such a broad definition was not intended to regulate oranges, however it is genuinely difficult to draw the line at what exactly is regulated. For instance, if I forked a wallet software and replaced all references of “coin” and “transaction” to “ink” and “publish” respectively, would this exempt the use of these particular units from the regulation? If not, what are the specific attributes that the NYDFS intends to regulate? The current definition is *unworkably* broad, and the final definition needs to be available for community feedback.

Finally, the BitLicense proposal prohibits the obfuscation of identity and requires the storage of identifying information. [200.15 (d), (f)]. This is an extremely dangerous combination with bitcoin, and is completely incompatible with protecting NY State citizens. Bitcoin is the most transparent system ever created. Literally anyone can inspect the blockchain. I am not aware of any *more* transparent system. Yet section 200.15 (f) seems to concede that consumer privacy is important. Because bitcoin is a general purpose publication platform that enables a plethora of technology, any data breach will have impacts far beyond financial.

Recent news reports have highlighted the inability of corporations to store identities, with recent data breaches at Target²⁷, Home Depot²⁸, and Jimmy Johns²⁹, and even the NSA. It is estimated that as many as 43% of companies suffered from a data breach in the past year³⁰. There is no possible way that the NYDFS can guarantee the security of identities, nor would the NYDFS provide reparations for damages done by the BitLicense regulation. It is a plain matter of fact that these records will eventually be leaked. With Bitcoin, the record is public and immutable, therefore the time of the data breaches is irrelevant. If they *ever* occur, they have serious negative consequences, even if separated by long periods of time. Three data breaches could occur over three decades, and the final data breach could provide the missing links that publicly expose an entire lifetime of personal activity, only a small portion of which might be financial in nature. When a data breach happens at Target, the only personal information exposed is that a person shopped at Target. When a data breach eventually happens with a bitcoin business, entire lifetimes of personal information linked to the blockchain will be suddenly exposed, unless mixing was employed to break this chain.

Instead, if the NYDFS is interested in protecting NY State citizens (as implied in 200.15 (f)), it should encourage obfuscation and mixing at every opportunity to limit damage of data leaks to consumers. Even with obfuscation techniques, bitcoin is an incredibly transparent system, and the prohibition of consumer privacy measures proposed in the BitLicense proposal are borderline Orwellian. The level of transparency requested by the BitLicense proposal is reckless and overreaching.

²⁶ Whole oranges are discrete and discontinuous, as opposed to continuous, and therefore fit the proper definition of “digital units”

²⁷ <https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ>

²⁸ https://corporate.homedepot.com/MediaCenter/Pages/Statement1.aspx?cm_mmc=SEM|THD|Test&mid=syNdpcEtb|dc_mtid_8903qmu25195_pcrld_46105304283_pkw_%2Bhome%20%2Bdepot%20data%20breach_pmt_b&gclid=CjwKEAjwwJmhBRC56KOelNOXhxUSJAB_w2uNF8n_tZ9hkGxrOuwhNrrKV8s1mSTg8f9ljfGCzehvthoCBXTw_wcB

²⁹ <https://www.jimmyjohns.com/datasecurityincident/>

³⁰ <http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/>

VI. Conclusions

Thank you for taking the time to carefully review feedback from the bitcoin community. While I do not believe that the BitLicense proposal is neither necessary nor appropriate, I do not want bitcoin to be a lawless technology. Thankfully, it is not. Courts are already prosecuting those who would use tools to harm others, most recently being a judgment against Mr. Trendon Shavers for operating the Bitcoin Savings & Trust Ponzi scheme³¹.

I believe bitcoin could become the most valuable application of the internet, because in the context of humanity, truth is scarce. Already we have seen significant portions of the bitcoin ecosystem abandon NY. It is in NY's best interest to get this regulation right, lest they further push development outside of NY.

Respectfully,



Jonathan Harms

³¹ <http://www.forbes.com/sites/javadkisson/2014/09/25/bitcoin-savings-trust-comes-up-40-million-short-on-the-trust-part/>