STATE OF NEW YORK
COURT OF CLAIMS

THEO CHINO, Claimant, - against - The Department of Financial Services; and Benjamin Lawsky in his official capacity as Superintendent of the New York State Department of Financial Services, Defendant.	AFFIDAVIT IN OPPOSITION Claim No. 124835 Weinstein, J.

Theo Chino, a resident of New York State, being duly sworn, deposes and says:

1. I am the claimant in this matter. I make this affidavit in opposition to the motion by the Attorney General of the State of New York for an order to dismiss the claim.

2. I believe the court should deny the motion because I have suffered damages the day the Department of Financial Services published a Proposed Rule Making in the New York State Register engaging the State of New York to a course of action regarding Blockchain technology (annexed hereto at Exhibit “A” & “B”).

   In Richard A. Hutchens CC, LLC v. State of New York or Waters of Saratoga Springs, Inc. v. State of New York, a prior relationship existed between the parties and this make it irrelevant in this matter since there was a communication path between the entities.

   In my case, my corporation and the State of New York are not engaged in any contract and therefore no relationship exists between my corporation and the State of New York.

   I do not have any recourse to engage the State of New York to discuss how their action are affecting my business and

therefore the damages became ascertainable the moment the Superintendent published the regulation to the New York State Register on July 2014 as shown in Exhibit “A”.

Whether the DFS has the right to engage the State to regulate virtual currency (which is mistakenly referred to “BitCoin” in the motion instead of “Blockchain technology” (Exhibit “C”)) is a case for an Article 78 under CPLR once the regulation goes into effect.

The case in front of this court is whether or not I have suffered actual damages after the publication of the Proposed Rules Making in the New York State Register.

What I seek is not a payday for my small corporation but an avenue to bring it into compliance within the proposed rules of the State of New York.

The regulations as written force me in 90 days to either:

- raise a substantial amount of capital;
- relocate my business outside the State Of New York;
- operate illegally in the State of New York;
- or close my business.

In a speech at Cardoza Law School (Exhibit “D”), Superintendent Lawsky said “We do not, for instance, let someone run a bank out of their garage.”

As illustrated in the blog of a Wall Street Journal journalist (Exhibit “E”) that a multitude of startup “did, in fact, start in a garage.”

This shows the dichotomy between the Department of Financial Service and the small business community regarding the Blockchain technology.

Starting a business in a Garage with limited resources is as American as Apple Pie and should be protected and nurtured.

Exhibit “F” shows that my corporation was incorporated on November 2013 and exhibit “G” show that I canceled my corporation Workers Compensation policy after letting go my employee on July 19, 2014.

The proposed regulation would requires my business to hire a Compliance Officer, a Chief Information Security Officer, various cyber security personnel, new equipment for

business continuity and disaster recovery, new equipment to protect the information produced by the new personnel, new personnel to design a framework to house the new personnel and the new equipment. Bringing my business into compliance with the framework of the State of New York would require an amount of work and capital in order to be compliant by March 2015.

At this time, this court is the only venue I have to engage the State of New York in a genuine conversation about what the Blockchain Technology should be for small business in the State of New York.

If the State of New York and its divisions refuses, then the state should be liable for the upgrades into compliance of my small business.

WHEREFORE, I respectfully request that this motion be denied.

Dated: New York, New York
November 11, 2014

_____
Theo Chino, Pro Se

Sworn to before me this ____ day of _____ 20 ___

_____
Notary Public

Exhibit A

1034

Hi, this is Ben Lawsky at NYDFS. Here are the proposed BitLicense regulations. (self.Bitcoin)

submitted 3 months ago by BenLawsky

Hi Reddit – This is Ben Lawsky, Superintendent of Financial Services at the New York State Department of Financial Services (DFS). As some of you may remember, I stopped by Reddit for an AMA in February while DFS was in the process of developing a regulatory framework for virtual currencies.

Today, DFS is announcing that we're publishing that proposed framework for public comment. A copy is available here on the DFS website.

The regulations will be formally published in the July 23, 2014 edition of the New York State Register – which starts a 45-day public comment period. After that public comment period, the rules are subject to additional review and revision based on that public feedback before DFS finalizes them. For information on how to submit a formal comment for DFS consideration under the NY State Administrative Procedures Act (SAPA) after the proposed regulations are published, please visit the New York State Register's website.

In developing this regulatory framework, we have sought to strike an appropriate balance that helps protect consumers and root out illegal activity – without stifling beneficial innovation. These regulations include provisions to help safeguard customer assets, protect against cyber hacking, and prevent the abuse of virtual currencies for illegal activity, such as money laundering.

We recognize that not everyone in the virtual currency community will be pleased about the prospect of a new regulatory framework. Ultimately, though, we believe that setting up common sense rules of the road is vital to the long-term future of the virtual currency industry, as well as the safety and soundness of customer assets. (We think the situation at Mt. Gox, for example, made that very clear.) Moreover, given that states have specific regulatory responsibilities in this area, we also have a legal obligation to move forward on this framework.

By the same token, we also recognize that – like any part of the financial industry – no regulatory framework can ever completely eliminate the risks customers face when dealing with financial firms. As such, we've included a strong set of consumer disclosures to help make sure customers have the information they need to make the choices that are best for them.

While this is not a formal AMA, I'll try to stop by this thread (and chime in from time to time) during the course of the public comment period. (However, to be clear, if you wish to submit a formal comment under our state regulatory process, you will have to visit the New York State Register.)

As the first state to put forward specially tailored rules for virtual currency firms – continued public feedback will be an important part of finalizing this regulatory framework. We look forward to carefully and thoughtfully reviewing public comments on our proposal.

2171 comments share save hide give gold report

Exhibit B

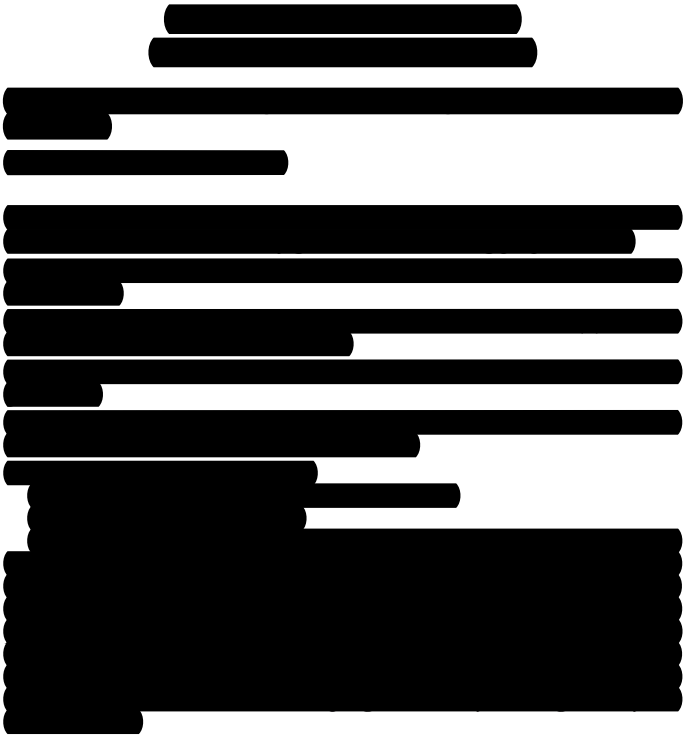
RULE MAKING ACTIVITIES

Each rule making is identified by an I.D. No., which consists of 13 characters. For example, the I.D. No. AAM-01-96-00001-E indicates the following:

AAM -the abbreviation to identify the adopting agency
01 -the *State Register* issue number
96 -the year
00001 -the Department of State number, assigned upon receipt of notice.
E -Emergency Rule Making—permanent action not intended (This character could also be: A for Adoption; P for Proposed Rule Making; RP for Revised Rule Making; EP for a combined Emergency and Proposed Rule Making; EA for an Emergency Rule Making that is permanent and does not expire 90 days after filing.)

Italics contained in text denote new material. Brackets indicate material to be deleted.

Office of Alcoholism and Substance Abuse Services



[...]

PROPOSED RULE MAKING
NO HEARING(S) SCHEDULED

Regulation of the Conduct of Virtual Currency Businesses

I.D. No. DFS-29-14-00015-P

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following proposed rule:

Proposed Action: Addition of Part 200 to Title 23 NYCRR.

Statutory authority: Financial Services Law, sections 102, 104, 201, 206, 301, 302, 309 and 408

Subject: Regulation of the conduct of virtual currency businesses.

Purpose: To regulate retail-facing virtual currency business activity in order to protect New York consumers and users and ensure the safety and soundness of New York licensed providers of virtual currency products and services. This regulation complements the Department of Financial Services' Order of March 11, 2014, which provides for the regulation, pursuant to the Banking Law, of exchanges that interact primarily with institutions.

Substance of proposed rule (Full text is posted at the following State website: www.dfs.ny.gov): The following is a summary of the proposed regulation:

Section 200.1, "Introduction," sets forth the statutory authority for the rule.

Section 200.2, "Definitions," defines terms used throughout the proposed regulation. Most significantly this Section defines "virtual currency" and "virtual currency business activity".

Section 200.3, "License," prohibits any Person from engaging in virtual currency business activity without a license.

Section 200.4, "Application," sets forth the information to be included in a prospective licensee's application.

Section 200.5, "Application fees," requires applicants to pay an application fee to the Department of Financial Services (the "Department") and provides that licensees may need to pay fees for the processing of additional applications related to the license.

Section 200.6, "Action by superintendent," provides for the superintendent to approve or deny an application and, if approved, to suspend or revoke a license on specified grounds after a hearing.

Section 200.7, "Compliance," requires licensees to comply with all applicable federal and state law, designate a compliance officer, and maintain and enforce various written compliance policies.

Section 200.8, "Capital requirements," sets forth minimum capitalization requirements and a list of permissible investments.

Section 200.9, "Custody and protection of customer assets," requires licensees to establish a bond or trust account for the benefit of their customers, requires licensees to hold virtual currency in the same type and amount as any virtual currency owed by the licensee, and prohibits licensees from encumbering customer assets.

Section 200.10, "Material change to business," requires licensees to seek prior approval by written application to introduce a new, or materially change an existing, product or service.

Section 200.11, "Change of control; mergers and acquisitions," requires licensees to seek prior approval by written application before executing a change of control or merger or acquisition.

Section 200.12, "Books and records," requires licensees to maintain certain records pertaining to each transaction and make such records available to the Department upon request.

Section 200.13, "Examinations," requires licensees to permit the superintendent to examine the licensee, including the licensee's books and records, at least once every two years and to make special investigations as deemed necessary by the superintendent.

Section 200.14, "Reports and financial disclosures," requires licensees to file quarterly financial statements and audited annual financial statements, to make special reports upon request, and to notify the Department upon discovery of any breach of law or upon a proposed change to the methodology used to calculate the value of virtual currency in fiat currency.

Section 200.15, "Anti-money laundering program," requires licensees to establish and implement an anti-money laundering program, which includes customer identification and transaction monitoring, to maintain records, and to make reports as required by applicable federal anti-money laundering law.

Section 200.16, "Cyber security program," requires licensees to design a cyber security program and written policy, designate a chief information security officer, make reports, and conduct audits.

Section 200.17, "Business continuity and disaster recovery," requires licensees to establish and maintain a written business continuity and disaster recovery plan to address disruptions to normal business operations.

Section 200.18, "Advertising and marketing," requires licensees to display a legend regarding its licensure by the Department, maintain all advertising and marketing materials, comply with all applicable federal and state disclosure requirements, and not make any false or misleading representations or omissions.

Section 200.19, "Consumer protection," requires licensees to disclose material risks and terms and conditions to customers and to establish an anti-fraud policy.

Section 200.20, "Complaints," requires licensees to disclose the licensee's and the Department's contact information and other information pertaining to the resolution of complaints.

Section 200.21, "Transitional period," requires Persons already engaged in virtual currency business activity to apply for a license with the Department within 45 days of the effective date of the regulation.

Text of proposed rule and any required statements and analyses may be obtained from: Office of General Counsel - Dana V. Syracuse, New York State Department of Financial Services, One State Street, New York, NY 10004, (212) 709-1663, email: dana.syracuse@dfs.ny.gov

Data, views or arguments may be submitted to: Same as above.

Public comment will be received until: 45 days after publication of this notice.

This rule was not under consideration at the time this agency submitted its Regulatory Agenda for publication in the Register.

Regulatory Impact Statement

1. Statutory Authority.

Section 102 of the Financial Services Law (FSL) states the legislature's

intent that the superintendent of Financial Services regulate "new financial services products," and "ensure the continued safety and soundness of New York's banking, insurance and financial services industries, as well as the prudent conduct of the providers of financial products and services, through responsible regulation and supervision." The definition of "financial product or service" in FSL section 104(a)(2) includes "any financial product or service offered or sold to consumers" other than those regulated under the exclusive jurisdiction of a federal or other New York state agency or where such regulation of such financial product or service would be preempted by federal law. Virtual currency meets the definition of "financial product or service," and is therefore subject to regulation by the superintendent.

Moreover, the superintendent has the explicit power under FSL section 301(c) "to protect users of financial products and services," and, under FSL section 302(a)(1), to "prescribe. . . rules and regulations. . . effectuating any power given to the superintendent under the provisions of this chapter." The superintendent therefore has statutory authority to prescribe regulations regarding virtual currency for the purpose of protecting users of virtual currency and virtual currency-related services.

Other statutory authority includes: Financial Services Law, sections 201, 202, 206, 302, 303, 304-a, 305, 306, 309, 404, 408; State Administrative Procedures Act, section 102; Banking Law, sections 10, 14, 36, 37, 39, 40, 44, 44-a, 78, 128, 225-a, 600, 601-a, 601-b; and Executive Law, section 63.

2. Legislative Objectives.

FSL section 201 is entitled "Declaration of policy" and states:

(a) It is the intent of the legislature that the superintendent shall supervise the business of, and the persons providing, financial products and services, including any persons subject to the provisions of the insurance law and the banking law.

(b) The superintendent shall take such actions as the superintendent believes necessary to:

(1) foster the growth of the financial industry in New York and spur state economic development through judicious regulation and vigilant supervision;

(2) ensure the continued solvency, safety, soundness and prudent conduct of the providers of financial products and services;

(3) ensure fair, timely and equitable fulfillment of the financial obligations of such providers;

(4) protect users of financial products and services from financially impaired or insolvent providers of such services;

(5) encourage high standards of honesty, transparency, fair business practices and public responsibility;

(6) eliminate financial fraud, other criminal abuse and unethical conduct in the industry; and

(7) educate and protect users of financial products and services and ensure that users are provided with timely and understandable information to make responsible decisions about financial products and services.

Virtual currency business activity is currently in its infancy and is almost entirely unregulated. The current lack of regulation, along with the dangers associated with virtual currency, may subject consumers and the businesses themselves to undue risk. The proposed regulation is intended to protect members of the public by imposing regulatory standards on virtual currency transactions and services that involve New York or New York residents, ensure the solvency, safety, soundness, and prudent conduct of persons or entities engaged in virtual currency business activity, and to foster the growth of the financial industry in New York by setting forth clear guidelines that will inspire confidence and allow for the establishment of legal virtual currency business activity.

3. Needs and Benefits.

Extensive research and analysis by the Department of Financial Services (the "Department"), including a two-day hearing held in January 2014, has made clear the need for a new and comprehensive set of regulations that address the novel aspects and risks of virtual currency. Existing laws and regulations do not cover proposed or current virtual currency business activity. The proposed regulation is therefore necessary to ensure that: (a) persons or entities engaged in virtual currency business activity operate in a safe and sound manner; (b) New York consumers and other residents are protected from the risks posed by virtual currency business activity; and (c) persons or entities engaged in new virtual currency business activity have a framework within which they can grow.

4. Costs.

Persons licensed under the proposed regulation will be responsible for ensuring that they are in compliance with this regulation, which will impose some costs on their operations. The Department will develop procedures to effectuate the licensing and examination of regulated persons or entities engaged in virtual currency business activity. In addition, the Department's operating expenses will be assessed in accordance with the provisions of FSL section 206. There should be no costs to any local governments as a result of the proposed regulation.

5. Local Government Mandates.

The proposed regulation does not impose any new programs, services, duties, or responsibilities upon any county, city, town, village, school district, fire district or other special district.

6. Paperwork.

Persons licensed under the proposed regulation will be required to keep and maintain books and records, make quarterly financial reports to the superintendent, and provide written applications for the initial license, and to seek approval for changes in control of, or material changes to, their businesses.

7. Duplication.

The proposed regulation does not duplicate, overlap, or conflict with any other regulations.

8. Alternatives.

The Department considered amending existing laws or regulations, particularly under the Banking Law, to include virtual currency. The Department decided not to pursue that alternative because of the widespread and potentially unforeseen ramifications such modification could have on the financial services industry and currently regulated entities. The Department also considered not acting at all, but concluded that failure to regulate virtual currency business activity will place the public at risk.

9. Federal Standards.

There are no applicable federal standards.

10. Compliance Schedule.

Persons or entities engaging in virtual currency business activity as of the effective date of the regulation must file an application for a license within 45 days of the effective date of the regulation.

Regulatory Flexibility Analysis

1. Effect of the rule.

Local governments do not engage in the virtual currency business activity covered by the proposed regulation. This regulation will not impose any adverse economic impact or any reporting, recordkeeping, or other compliance requirements on local governments. To the extent a small business engages in any of the conduct specified in the proposed regulation, it will be required to comply with the requirements of the regulation. At this time, because virtual currency technology is relatively new, there exists no comprehensive estimate of the number of small businesses in New York that would be impacted by the proposed regulation.

2. Compliance requirements.

Small businesses, like all businesses licensed under the proposed regulation, will be required to make quarterly financial reports to the superintendent of Financial Services, keep and maintain accurate books and records, be subject to examinations, and provide written applications for the initial license and to seek approval for changes in control or material changes to their businesses.

3. Professional services.

Small businesses, like all businesses licensed under the proposed regulation, will be required to satisfy an annual audit requirement, which will require the retention of qualified professionals to perform the audit.

4. Compliance costs.

Persons licensed under the proposed rule will be responsible for ensuring that they are in compliance with the regulation, which will impose some costs on their operations. Although the cost of compliance, particularly with regard to anti-money laundering and cyber security, could be significant for small businesses, the overwhelming need for such compliance to protect New York residents outweighs such costs. In addition, very few, if any, small businesses currently engage in the conduct that is subject to regulation under the proposed rule. For small businesses that do not engage in virtual currency business activity, the regulation will impose no adverse impact or increased costs.

5. Economic and technological feasibility.

The Department of Financial Services (the "Department") believes it will be economically and technologically feasible for small businesses to comply with the requirements of the proposed regulation.

6. Minimizing adverse impact.

To minimize any adverse economic impact of the proposed regulation on small businesses, the Department will adjust small businesses' capital requirements to reflect the size of their operations. Small businesses generally will have lower capital requirements than large businesses.

7. Small business participation.

The proposed regulation will be published publicly, including on the Department's website, for notice and comment, which will provide small businesses with the opportunity to participate in the rule making process. Further, prior to drafting this regulation the Department held a two day public hearing and sought input from dozens of virtual currency businesses, venture capital companies, and academics.

Rural Area Flexibility Analysis

1. Types and estimated numbers of rural areas.

Persons subject to the licensing requirements of the proposed regulation could possibly operate anywhere in this state, including rural areas.

2. Reporting, recordkeeping and other compliance requirements; and professional services.

Persons licensed under the proposed regulation will be will be required to make quarterly financial reports to the superintendent of Financial Services, keep and maintain accurate books and records, be subject to examinations, and must provide written applications for the initial license and to seek approval for changes in control or material changes to their businesses.

3. Costs.

Persons licensed under the proposed regulation will be responsible for ensuring that they are in compliance with this regulation, which will impose some costs on their operations. The costs are not expected to be any higher for entities in rural areas than for any other entity in the state.

4. Minimizing adverse impact.

The proposed regulation is not expected to have an adverse impact on public or private sector interests in rural areas. This regulation is specifically tailored to the pressing need to regulate virtual currency business activity involving New York or New York residents and is likely to have a positive impact on interests in rural areas by increasing the financial services available to them.

5. Rural area participation.

The proposed regulation will be published publicly, including on the Department's website, for notice and comment, which will provide public and private interests in rural areas with the opportunity to participate in rule making.

Job Impact Statement

A Job Impact Statement is not being submitted with this proposed regulation because it is evident from the subject matter of the regulation that it will not have an adverse impact on jobs and employment opportunities in New York State. The proposed regulation is intended to protect members of the public by imposing a regulatory framework on persons or entities that wish to engage in virtual currency business activity involving the State of New York or New York residents and to provide the market with guidance and clarity with regard to the use of virtual currency. Based on the feedback the Department of Financial Services (the "Department") has received from virtual currency businesses to date, the Department believes that the proposed regulation will have a positive impact on jobs and employment opportunities in New York by allowing for the establishment and growth of legitimate virtual currency businesses.

Department of Health

[...]

Exhibit C

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. 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. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

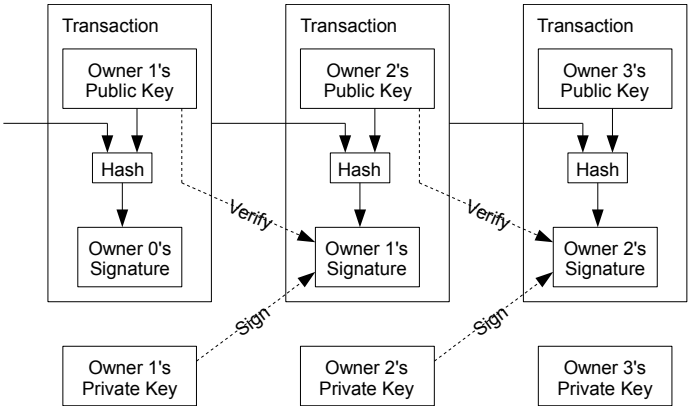
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

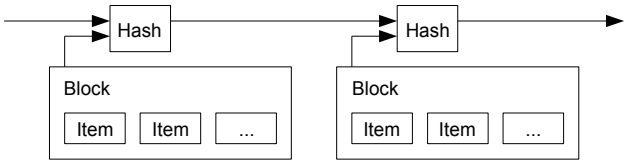


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

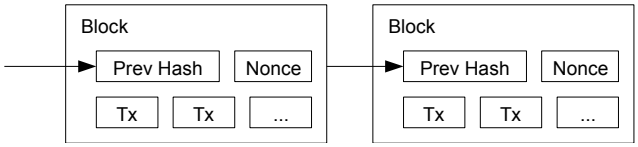
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

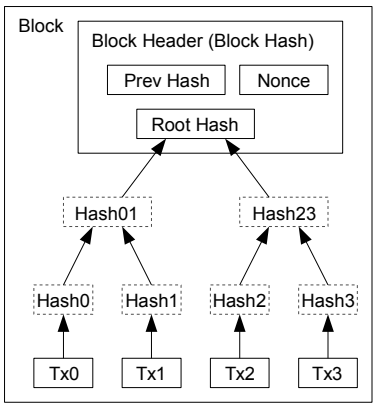
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

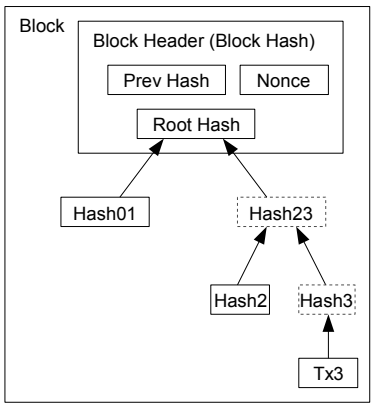
The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



Transactions Hashed in a Merkle Tree

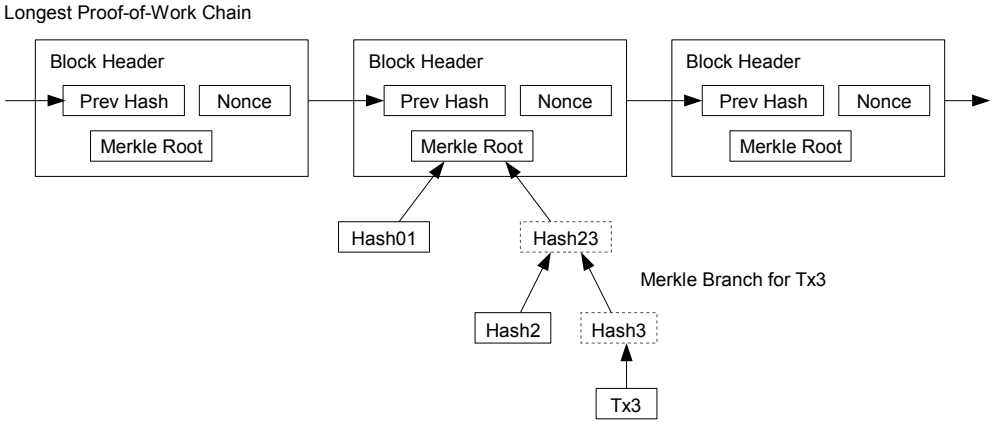


After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

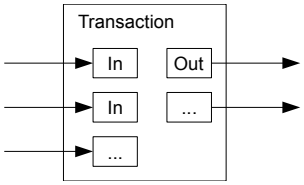
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

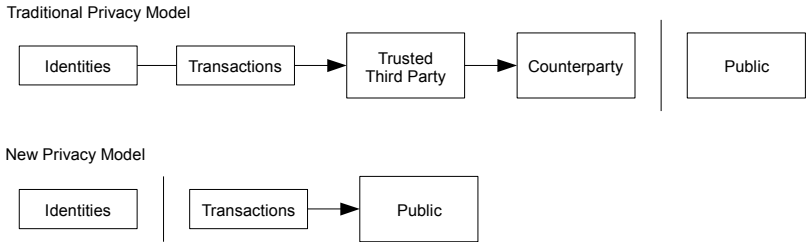
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Exhibit D

EXCERPTS FROM SUPERINTENDENT LAWSKY'S REMARKS ON VIRTUAL CURRENCY AND BITCOIN REGULATION IN NEW YORK CITY

Benjamin M. Lawsky, Superintendent of Financial Services for the State of New York, is delivering remarks today at the Benjamin N. Cardozo School of Law in New York City. The following are excerpts from Superintendent Lawsky's remarks on virtual currency and Bitcoin regulation as prepared for delivery.

***

Excerpts from Superintendent Lawsky's Remarks at the Benjamin N. Cardozo School of Law
New York, NY
October 14, 2014

As Prepared for Delivery

Ultimately, after the Mt. Gox collapse, we redoubled our efforts and put forward our proposal for public comment six months ahead of schedule in July 2014.

That regulatory framework included a number of key provisions to safeguard customer assets; protect consumers from fraud and abuse; root out money laundering and other illicit activity; and put up strong defenses against would-be hackers by emphasizing the need for robust cyber security.

To be clear, our proposal was meant as a beginning – not an end – to a healthy, vigorous public discussion about what the final regulation should look like.

We want to move quickly to put in place rules of the road for virtual currency firms to provide greater clarity and certainty about the regulatory environment. But not move so quickly that we risk mistakes.

To that end, while we put forward our proposal for public discussion ahead of schedule – after some members of the virtual currency community asked for additional time to formulate their feedback, we listened and doubled the length of the initial comment period. Indeed, I think there may have been some who mistakenly assumed our initial regulation was a take-it-or-leave-it, all-or-nothing proposal that would take effect in a matter of days or weeks.

Truth be told, public comment periods generally take a good deal of time in government.

Moreover,we will likely make certain changes to our initial proposal – and clarify other provisions.

And state law provides for an additional comment period when an agency makes material changes to a proposed regulation, which should provide a further opportunity for public feedback.

Suffice it to say, there is and will be a significant amount of time for stakeholders to provide input on the Department's regulatory framework.

***

Now, while we will be making substantive changes to the regulation, and we very much appreciate the time so many people took to formulate and submit comments – I've read many of them myself – we do think that many of the original proposals make sense, are good for consumers, and good for the long-term health of the virtual currency industry.

The rules also generally mirror the types of requirements that other banks, financial institutions, and money transmitters have to live by – with some alterations owing to the unique nature of virtual currencies.

This is a point that is not well understood. In part, perhaps, because virtual currency sits at the crossroads of a more lightly regulated technology sector and more heavily regulated financial sector.

There is a basic bargain that when a financial company is entrusted with safeguarding customer funds and receives a license from the state

to do so – it accepts the need for heightened regulatory scrutiny to help ensure that a consumer's money does not just disappear into a black hole.

And most of what Bitcoin firms are being asked to do – whether it is examinations, anti-money laundering compliance, accounting, or recordkeeping – is similar to what other financial firms must do.

Additionally, we agree with the sentiment that financial regulation should be – to the extent practical – technologically neutral. But we cannot stick our heads in the sand about the fact that – when it comes to consumer disclosures, capital accounting, and other issues – there are real differences between fiat currency and virtual currency.

We should simply endeavor to make sure that where there are technologically specific regulations – they are appropriately tailored, reasonable, and warranted.

Moreover, to the extent that there are some specific areas of the regulation that are somewhat stronger or more robust for virtual currency firms than those for other financial institutions – such as our cyber security rules – that is primarily because we are actually considering using them as models for our regulated banks and insurance companies.

As evidenced by the recent JPMorgan hack, cyber security is one of the most important issues the Department of Financial Services (DFS) will face as a regulator in the months and years ahead across the entire financial system. And you will be hearing a lot more from our agency about this in the near future.

***

As I said, there are some important changes I think we will make to the proposed regulations, many of which I expect will be clarifying in nature. While I cannot address every category of feedback today because our team is still going through all the comments we've received – I can say we are reviewing all of them closely – I would like to go through a few of these areas today.

First, there is some confusion about who will be required to obtain a BitLicense. For example, some believe that our proposed regulation requires all software developers and individual users of virtual currency to obtain licenses.

To clarify, we do not intend to regulate software as software or software development. For example, a software developer who creates and provides wallet software to customers for their own use will not need a license. Those who are innovating and developing the latest platforms for virtual currency will not need a license. We are regulating financial intermediaries. We are not regulating software development.

Individual users are similarly exempt from the license requirement. People who want to use virtual currency to make purchases or want to hold virtual currency solely for investment purposes will not be required to obtain a license.

Second, there appears to be some concern that virtual currency businesses will need to get several different types of licenses, resulting in a cumbersome and duplicative application process.

To the extent an applicant requires both money transmitter and virtual currency licenses, for example – which is possible – the process will be streamlined. Applicants will be able to cross-satisfy the requirements of each license.

Third, we have also received comments claiming banks are completely exempt from complying with the virtual currency regulations and that is not fair.

That, of course, would not be fair. However, it also isn't true.

The banks we regulate cannot start providing virtual currency services without prior approval from DFS, and they will be have to comply with any requirements that are otherwise imposed on virtual currency businesses.

Fourth, there is much speculation about whether we intend to regulate mining. Mining per se will not be regulated. To the extent a miner engages in other virtual currency services, however – for example, hosting wallets or exchanging virtual currency – a license may be required for those activities.

Finally, I know that there is some concern about the compliance costs of regulation on new or fledgling virtual currency enterprises. This is a difficult issue. We certainly get it and are wrestling with it. There has to be a way for start ups to start up and play by the rules without getting crushed by huge compliance costs. This goes back to that original collision between traditional banking and tech innovation. It requires a creative solution and we are working on that issue.

In part, this concern is also why we want to make the revised regulation quite clear that software companies do not need a BitLicense in order to develop new software and innovate. We are not seeking to stifle technological innovation.

But if a software company is also taking on the responsibility of actually safeguarding customer money – it is a much more difficult calculation.

Again, that is the basic bargain of financial services regulation. We do not, for instance, let someone run a bank out of their garage.

And licensure and regulation often helps foster greater trust among consumers.

Companies can, of course, try and run from regulation in a race to the bottom.

To set up shop in dark corners of the globe with little to no oversight.

Or play one regulator off one another to try and water down the rules – a process known as regulatory arbitrage or regulator shopping. We saw this phenomenon a lot during the lead up to the financial crisis.

But our hope is that companies recognize that effective, appropriate regulation will help create a race to the top.

That it will foster greater trust and confidence among both customers and investors – who want to do business with firms committed to consumer protection. And that will spur a virtuous cycle of greater adoption of virtual currencies. A cycle where it is possible to innovate, make a profit, and play by the rules all at the same time.

At a basic level, our guiding principle for virtual currency regulation is similar to our guiding principle for regulation at all financial companies.

We have never been an agency that supports regulation for regulation's sake.

We simply want to make sure that there are appropriate guardrails so that consumers are protected and we help prevent illicit activity.

When it comes to safeguarding customer money at a financial company – an unregulated world of caveat emptor has never been a sufficient answer.

Right now, I think, the virtual currency industry is at a bit of a crossroads regarding whether it will become an important part of the future financial system.

At DFS, we're committed to proceeding thoughtfully since virtual currency could ultimately have a number of benefits for our financial system.

Events and discussions like this one really help as we strive to rightsize and modernize our regulation of new financial technologies like virtual currencies.

So thank you for the opportunity to speak with you today and I look forward to your questions.

Andrew M. Cuomo, Governor

Benjamin M. Lawsky, Superintendent

New York State Department of Financial Services

Exhibit E

MONEYBEAT

MARKETS
Nick Woodman Is Selling Some of His GoPro Shares

Morning MoneyBeat: Doubters, Reconsider

6:01 pm ET
Oct 14, 2014 FOREX

BitBeat: Lawsky Outlines Changes to BitLicense

By PAUL VIGNA and MICHAEL J. CASEY CONNECT

— Megan Miller

Welcome to BitBeat, your daily dose of crypto-current events, written by Paul Vigna and Michael J. Casey.

Bitcoin Latest Price: $405.87, up 4.5% (via CoinDesk)

Crossing Our Desk:

- **The BitLicense is coming, but it won't be the draconian net many** in the bitcoin community fear, according to Benjamin Lawsky's prepared opening remarks for a panel discussion on digital currencies and regulation at Cardozo Law School in New York City Tuesday evening.

In his remarks, Mr. Lawsky, the superintendent of the New York State Department of Financial Services, outlined several changes he'll make to the proposal – a special banking license **introduced by his agency in July** to regulate virtual currencies. The comments appeared to be his first detailed public comments he's made on the proposal.

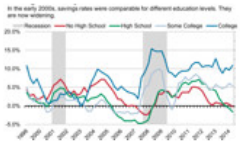
Software developers, bitcoin miners, and individuals (unless they also offer financial services) doing business in New York state won't have to apply for a BitLicense, he said, according to the prepared remarks, but traditional banks looking to get into digital currencies will. The proposal was meant as a starting point, not an ending point, he said, but it was also influenced by the collapse of the Mt. Gox exchange.

Popular Now

What's This?

1 Meet Prime Minister Narendra Modi's Postmen

2 One Lesson People Increasingly Learn in College: Saving



3 Cybercrime Gang Targets Execs Using Hotel Internet

4 Who's Who in Narendra Modi's New Cabinet in India

5 The High Price of Being an Uninformed Patient

"The virtual currency industry is at a bit of a crossroads regarding whether it will become an important part of the future financial system," he said. "At DFS, we're committed to proceeding thoughtfully since virtual currency could ultimately have a number of benefits for our financial system."

He emphasized, however, that if companies want to provide financial services via digital currencies, they are going to have to accept some measure of regulation. "When it comes to safeguarding customer money at a financial company – and unregulated world of caveat emptor has never been a sufficient answer," he said.

The current open-comment period is slated to end this month, and Mr. Lawsky said that the DFS will release an amended version of the proposal that itself will be put out for public comment. "Suffice it to say," he said, "there is and will be a significant amount of time for stakeholders to provide input."

He addressed several concerns and outlined some of the changes he expects to make, including a key complaint that the proposal be "technology neutral." Mr. Lawsky said that the license will not cover software firms, **something he noted in August**, or mining companies, but also said "we cannot stick our heads in the sand about the the fact that – when it comes to consumer disclosures, capital accounting, and other issues – there are real differences between fiat currency and virtual currency."

wants to offer financial services via digital-currencies, mpany, miner, or traditional bank, he said.

re of complaints about the cost of compliance, especially This is a difficult issue," he acknowledged. "It requires a orking on that issue." But these costs, whether for a ultimately a cost of the business of financial services.

in of financial services regulation. We do not, for instance, their garage."

e chose that metaphor, knowing how many Silicon Valley ck to Hewlett and Packard, did, in fact, start in a garage.

ver the $400 level on Tuesday, less than 10 days after way to $300, which right now appears to be the bottom of a me and the hashrate has come off the bloating levels **" trade**, and it seems like the community has finally en back to something that resembles normal.

ill down about 50%, but a rise like this will likely calm some pointed out before, at $400, or even $300, bitcoin prices at any point in its (brief) history before November 2013.

itcoin's value, beyond the currency, is Pantera Capital's nber of factors, like developer interest, the hashrate, user hes on Google, and transaction volume, and produces an sense of bitcoin's growth. The index currently sits around hing forward, despite the price drop. (*Paul Vigna*)

It will cover any company that whether it's a start-up, tech co

He said the department is awa on how it will affect start-ups. " creative solution and we are w start-up or a multinational, are

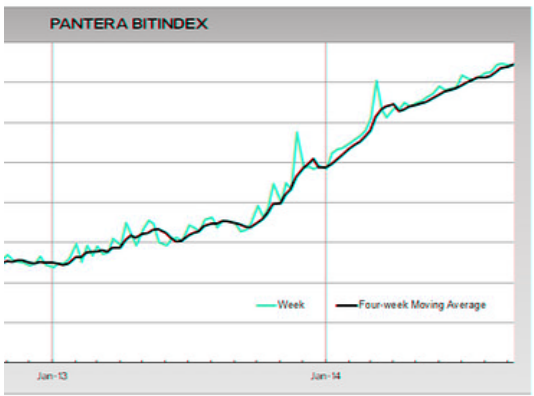
"Again, that is the basic bargai let someone run a bank out of

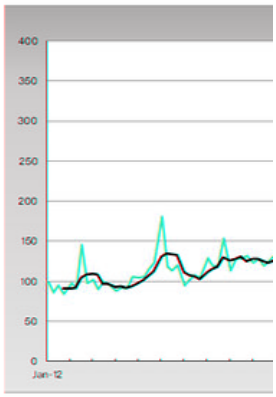
We wonder how consciously h start-ups, going all the way ba (*Paul Vigna*)

- Bitcoin prices rose back o the digital currency fell all the nine-month slide. Trading volu **sparked by the "BearWhale** swallowed that trade, and gott

Year-to-date the currency is st jangled nerves, and as we've are still higher than they were

Another interesting gauge of b "Bitindex," which plugs in a nur and merchant adoption, searc index that captures a broader 370, and has been steadily inc





— Pantera Capital

Contacts: paul.vigna@wsj.com, @paulvigna / michael.casey@wsj.com, @mikejcasey

MONEYBEAT HOME PAGE

Email Print

Exhibit F

State of Delaware
Secretary of State
Division of Corporations
Delivered 12:22 PM 11/19/2013
FILED 11:41 AM 11/19/2013
SRV 131324060 - 5434708 FILE

CERTIFICATE OF INCORPORATION

FIRST: The name of this corporation shall be: CHINO LTD

SECOND: Its registered office in the State of Delaware is to be located at 2711 Centerville Road, Suite 400, Wilmington, County of New Castle, Delaware, 19808. The name of its registered agent at such address is The Company Corporation.

THIRD: The purpose or purposes of the corporation shall be:

To engage in any lawful act or activity for which corporations may be organized under the General Corporation Law of Delaware.

FOURTH: The total number of shares of stock, which this corporation is authorized to issue is One Thousand, Five Hundred (1,500) shares of common stock without a par value

FIFTH: The name and address of the incorporator is as follows:

The Company Corporation
2711 Centerville Road
Suite 400
Wilmington, Delaware 19808

SIXTH: The Board of Directors shall have the power to adopt, amend or repeal the by-laws.

SEVENTH: No director shall be personally liable to the Corporation or its stockholders for monetary damages for any breach of fiduciary duty by such director as a director. Notwithstanding the foregoing sentence, a director shall be liable to the extent provided by applicable law, (i) for breach of the director's duty of loyalty to the Corporation or its stockholders, (ii) for acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of law, (iii) pursuant to Section 174 of the Delaware General Corporation Law or (iv) for any transaction from which the director derived an improper personal benefit. No amendment to or repeal of this Article Seventh shall apply to or have any effect on the liability or alleged liability of any director of the Corporation for or with respect to any acts or omissions of such director occurring prior to such amendment.

IN WITNESS WHEREOF, the undersigned, being the incorporator herein before named, has executed signed and acknowledged this certificate of incorporation this 19th day of November, 2013.

The Company Corporation, Incorporator

By: /s/ William Bartz
Name: William Bartz
Assistant Secretary

N. Y. S. DEPARTMENT OF STATE
DIVISION OF CORPORATIONS AND STATE RECORDS ALBANY, NY 12231-0001

FILING RECEIPT

ENTITY NAME: CHINO LTD

DOCUMENT TYPE: APPLICATION FOR AUTHORITY (FOREIGN BUS) COUNTY: NEWY

FILED:02/24/2014 DURATION:PERPETUAL CASH#:140224000732 FILM #:140224000671
DOS ID:4533808

FILER:	EXIST DATE
THEO CHINO 640 RIVERSIDE DRIVE 10B NEW YORK, NY 10031	02/24/2014

ADDRESS FOR PROCESS:

THEO CHINO
640 RIVERSIDE DRIVE 10B
NEW YORK, NY 10031

REGISTERED AGENT:

The corporation is required to file a Biennial Statement with the Department of State every two years pursuant to Business Corporation Law Section 408. Notification that the biennial statement is due will only be made via email. Please go to www.email.ebiennial.dos.ny.gov to provide an email address to receive an email notification when the Biennial Statement is due.

SERVICE COMPANY: ** NO SERVICE COMPANY ** SERVICE CODE: 00

FEES	225.00	PAYMENTS	225.00
FILING	225.00	CASH	0.00
TAX	0.00	CHECK	225.00
CERT	0.00	CHARGE	0.00
COPIES	0.00	DRAWDOWN	0.00
HANDLING	0.00	OPAL	0.00
		REFUND	0.00

DOS-1025 (04/2007)

Exhibit G

STATEMENT OF PREMIUM ADJUSTMENT
WORKERS COMPENSATION AND EMPLOYERS LIABILITY

INSURER: HARTFORD INSURANCE COMPANY OF THE MIDWEST (G)

POLICY NUMBER:	POLICY PERIOD:	AUDIT PERIOD:
76 WEG GE0960	03/13/14 **To** 03/13/15 CANC PRO-RATA	03/13/14 **To** 07/19/14

HOUSING CODE: 76

Named Insured and Mailing Address:
CHINO LTD

640 RIVERSIDE DR APT 10B

NEW YORK, NY 10031

Producer's Name:
AP INTEGO INSURANCE GROUP LLC

Producer's Code: 250846 SCIC

*01002760E09600114 01297

Insured/State/Location Description	Class Code	Basis of Premium	Rate	Earned Premium
INSURED: 01 CHINO LTD				
STATE: 31 NY				
LOCATION: 01 640 RIVERSIDE DR APT 10B NEW YORK NY 10031				
SALESPERSONS, COLLECTORS *	8742	4,950	.46	23
NEW YORK STATE ASSESSMENT (0932) 13.80 PERCENT				3
EXPENSE CONSTANT				70
TERRORISM (9740)		4,950	.040	2
TERRORISM (9740) PER CAPITA 2.9 PERCENT				0
CATASTROPHE (9741)		4,950	.010	0
CATASTROPHE (9741) PER CAPITA 0.7 PERCENT				0
STATE TOTAL EARNED PREMIUM - NY				98

* SEE POLICY DECLARATIONS/SCHEDULE FOR FULL DESCRIPTION

STATEMENT UPLOAD **Total Earned Premium:** 98

CMM PROG ID: A501

Premiums calculated hereon are subject to revision and approval by the Home Office.