

Crypto-Economy Working Group  
c/o Institute for the Future  
201 Hamilton Avenue  
Palo Alto, CA 94301  
<http://cewg.iff.org/>  
[REDACTED]

10/21/2014

Office of General Counsel  
New York State Department of Financial Services  
One State Street, New York, NY 10004  
[REDACTED]

Email: [dana.syracuse@dfs.ny.gov](mailto:dana.syracuse@dfs.ny.gov)

**Re: Regulation of the Conduct of Virtual Currency Businesses – Addition of Part 200 to Title 23 NYCRR**

To NYDFS Office of General Counsel:

This Bitlicense comment is a result of input from several of the cryptocurrency non-profit research, self-regulatory, and advocacy groups, as well as many entrepreneurs, engineers, and legal and financial experts working in the industry.

In it we hope to begin a dialogue on the potential for technological solutions to policy mandates and regulatory objectives of virtual currencies. We believe these technologies can enable the cryptofinancial industry to ultimately supersede the security, compliance, and transparency of modern institutional finance.

Some of these technologies are online now, some are in commercial development, while others are still in the research labs and are years or more away from deployment. However, we hope to impart a sense of what is in the pipeline, and to impress upon you the value of regulatory safe havens and/or testing environments to enable the continued development, iteration, and maturing of these technologies.

Following is a high-level review of some of these emerging technologies. Further, we recognize Superintendent Lawsky's observation of the current theoretical nature of technological solutions to policy mandates and his call for actual implementation examples. A few are already deployed in the industry and discussed here, and we hope to be able to add to that list in a subsequent letter for the second Bitlicense comment period.

Finally, there is some debate about whether virtual currency firms should be regulated under new, technology-specific regimes like Bitlicense, or under pre-existing technology-neutral regimes like state Money Transmitter laws. CEWG takes no stance on this question, and this letter should not be construed as support for or opposition to either position. We simply hope to provide a view into how technological alternatives may effectively address existing policy mandates and regulatory objectives, regardless what form they take.

Thank you for your consideration of our efforts.

Sincerely,  
Crypto-Economy Working Group  
<http://cewg.iff.org/>

---

## Contents

Contents	2
Introduction	3
Policy Mandates	4
Technology Solutions: In Production	4
Technology Solutions: Near-Term Pipeline	5
Technology Solutions: Long-term Pipeline	7
Industry Topology: Segregation of Duties	8
Conclusion	9
Appendix A: Unique Characteristics of Virtual Currency Organizations	10
Appendix B: References	10

---

## Introduction

This is not a comment addressing the Bitlicense draft proposal directly, as many others have already provided comprehensive analysis and commentary on the proposal. Rather, here we attempt to respond to NYDFS's request for dialogue on technological solutions to policy mandates and regulatory objectives for virtual currencies.

Emerging blockchain-based cryptographic tools and techniques promise not only to alter the financial ecosystem, but governance and regulatory systems as well. However, this shift is still very early stage and the technologies are just beginning to be developed and deployed. Initial blueprints are promising but maturity of a comprehensive ecosystem of technologies for self-governance will take time.

The challenge for the entire community - technologists, entrepreneurs, investors, lawyers, lawmakers, and regulators - is that some new technologies may provide a dual use of facilitating and enabling some types of crime, such as money-laundering, while others will enable the mitigation or elimination of other types of crime, for instance, internal corporate fraud and embezzlement.

Hence, the policy and regulatory goal posts are moving, and will require us to learn how best to adjust. Many of us in the virtual currency industry hope a response will be, that lawmakers and regulators provide safe harbors necessary for the development, deployment, and maturity of technological solutions to these difficult problems, such that we do not find ourselves burdened years down the road with hard-coded regulatory requirements made obsolete by innovative new technological solutions to the underlying policy mandates.

This process will be ongoing and require continuous reconsideration as new technologies come online that can satisfy policy mandates as well or better than prior methods. Hence we hope for some form of adaptable, multi-tiered regulatory approach, for example:

1. Tier 1: Blockchain and/or cryptography-based technological self-regulation and self-governance
2. Tier 2: Where #1 is not possible or effective, fall back to traditional financial/banking/certificate authority industry self-regulation and governance best practices — segregation of duties, auditing, certification, cryptographic key management, SRO oversight, etc.
3. Tier 3: Where #2 is not possible or effective, fall back to traditional governmental regulatory requirements and regimes.

Over the coming years and decades we hope to find increasingly advanced and powerful technology-driven means of satisfying the policy mandates for virtual currencies, continually increasing the weight of Tier 1 in this approach.

Additionally, it behooves the virtual currency industry to learn from the hundreds of years of evolution of the modern banking and securities industries, and to adapt their best practices wherever technological means are insufficient, especially but not limited to, segregation of duties and rigorous independent third party auditing regimes.

However, a more difficult problem to solve will be developing technologies that satisfy the policy mandates around AML/KYC and prevention of organized crime and terror financing, while simultaneously finding effective ways of safeguarding customers' personally identifiable information (PII) from increasingly sophisticated international data thieves, as there is an inherent tension between the two objectives. We are not unaware of this problem and some in the industry are working on it as well, but solutions will take longer to discover and prove.

Finally, this letter provides a high-level overview only, as attempts at compiling all known technological means of addressing policy mandates have only just begun. We hope and intend to be able to submit additional implementation examples and details in a subsequent comment for the second Bitlicense comment period.

---

## Policy Mandates

Several policy mandates drive virtual currency regulation and it is useful to enumerate them in order for the industry, lawmakers, and regulators to begin to think about and communicate about how new technologies may address these mandates:

1. Safety and soundness
2. Consumer protection
3. Money laundering, terrorist financing, or other criminal activity
4. Financial transparency and accountability

Unsafe and unsound practices consist of practices or conducts which create the likelihood of material loss, insolvency, or dissipation of the licensee's assets, or otherwise materially prejudices the interests of a firm's customers.

Consumer protection focuses on whether consumers have sufficient information to make informed decisions about their purchase of goods and services, including financial services, and that the entity selling the product or service is not engaging in unfair, deceptive, or abusive practices.

The use or abuse of a virtual currency product or service for money laundering, terrorist financing and other criminal activity also covers a nonexclusive list of other activities such as child pornography, human smuggling, human trafficking, narcotics trafficking, health care fraud, other types of fraud and online gambling as well as money laundering and terrorist activity and many other activities.

Greater financial transparency and accountability are critical to promoting sustained, long term investment from investors, venture capital firms, and institutional finance, which is necessary for growing the industry beyond the small niche it currently occupies.

---

## Technology Solutions: In Production

Several technologies which can be used for self-governance are already in production, namely Multi-Signature Governance and Escrow, Proof of Reserves/Solvency, and Keyless Wallets. These can help satisfy the policy mandates for Safety & Soundness, Consumer Protection, and Financial Transparency.

### **Multi-Signature Governance and Escrow**

Modern corporations are run under segregation of duties regimes. For example, large purchases, cash transactions, or movement of funds can only be effected the signature of both the CEO and CFO, and the custodial bank is responsible for verifying both signatures. This helps prevent the risk of loss due to mistakes, internal fraud, or compromise of the credentials of one or the other party.

Bitcoin's multi-signature capability can enable similar segregation of duties, requiring "M of N" signatures to release and move funds, be it 2 of 3, 5 of 8, or other arbitrary permutation. The process is cryptographically assured and the blockchain serves as the third party signature verifier instead of a bank.

"M of N" multi-sig authorization can also enable business continuity in the case of death or incapacitation of some subset of signatories, by assuring there are backup signatories capable of releasing funds if a primary is unable to, while still enabling segregation of duties.

This capability is one of the easiest to deploy and is already in widespread use across the industry in most firms that custody either their customers' Bitcoin or their own. For example, BitGo Inc. provides an enterprise multi-sig service with spending limits, corporate treasury policies, and approvals required for large transactions. Pamela Morgan of Empowered Law provides an excellent reference implementation [11].

### **Proof of Reserves/Solvency**

Proof of Reserves [10] is a technique by which a cryptocurrency firm that custodies customer private keys may prove that its assets are greater than its liabilities, but without publicly divulging any concrete information on customer account holdings.

It is useful for enabling cryptocurrency-only firms to comply with Consumer Protection mandates, partially useful for firms that custody both cryptocurrency and fiat, and a component of Continuous Real-Time Auditing discussed below.

### **Keyless Wallets**

One of the oldest online Bitcoin services is [Blockchain.info](https://blockchain.info), and the digital currency wallet service they provide remains a model for how a virtual currency financial intermediary can provide financial services while enabling customers to serve as their own asset custodians.

In cryptocurrency, control of the private keys equates to control of the corresponding ledger entries, or funds, but it is not technologically necessary for the financial intermediary providing the service to also control the customer's private keys - the two functions of provision of the service and custodianship of the keys can be segregated.

If the financial intermediary fails, customer assets are protected. It is cryptographically impossible for the wallet service to steal, filch, defraud, or embezzle their customers' assets, contributing to improved safety & soundness and better satisfaction of consumer protection mandates.

Several other virtual currency companies offer this service as well, and we imagine it will become increasingly popular as the public becomes accustomed to this new way of handling digital assets and interacting with digital asset services.

---

## Technology Solutions: Near-Term Pipeline

Two of the most interesting technologies under development are Continuous Real-Time Auditing and Keyless Trading. CRTA will enable current and prospective customers to evaluate the up-to-the-minute soundness of any participating cryptofinancial intermediary at any given time. Keyless Trading will enable customers of exchanges to serve as their own asset/private key custodians, while exchanges retain the power to enforce settlement of gains/losses at any arbitrary pre-determined interval (hourly, semi-daily, daily, etc).

## Continuous Real-Time Auditing

CRTA requires a combination of emerging blockchain technology (Proof of Reserves/Solvency, hierarchical deterministic watch-only wallets, multi-signature corporate governance), bank APIs (ex: Standard Treasury [19], Epiphyte [20]), Accounting-As-A-Service (ex: Subledger [21]), and also a possible opportunity for auditors to develop new software that consumes the data from the AaaS and provides real-time audit results based on that data.

To summarize, CRTA consists of:

- Continuous real-time accounting as made possible by companies such as Subledger.com,
- Continuous reconciliation with the blockchain as a running representation of the state of the "cash drawer" if you will,
- And continuous reconciliation with escrow bank accounts that can provide data using an API such as that provided by Standard Treasury or Epiphyte
- Much of this can happen outside of the control of the entity being continuously audited itself, reducing the risk that compromising the entity can compromise the internal ledger in a way that takes time to be noticed and flagged.

All the pieces already exist to make this possible, but to date we only have a high-level conception of how it should work, and are just starting on the implementation details. But Continuous Real-Time Auditing could be quite an improvement over the current status quo of discrete, approximately quarterly auditing.

Our ultimate objective is to specify a reference implementation which we can then open source and disseminate to the virtual currency industry via our various non-profits - Bitcoin Foundation [4], DATA [5], CDC [6] - for industry-wide implementation, and communication to lawmakers and regulators. That would represent a big step toward bringing the operational integrity of the industry as a whole up to institutional finance standards, while maintaining a long-term goal of objectively exceeding existing standards in every way.

## Keyless Trading and Exchange

As mentioned before, there are several web wallets-as-a-service like Blockchain.info that provide wallet services to customers without custodial customers' private keys. It is also conceivable that cryptocurrency exchanges will be able to extend this model to facilitating market making and exchange among traders using a similar model in which traders serve as their own asset custodians (for crypto assets at least, not fiat). This is theoretically possible but the technology is still in R&D phases.

If it can be accomplished, then the crypto equivalents of both banks and of exchanges will likely evolve to this model over time, since it removes the current risk mis-pricing in which exchanges take on the risk of custodial customer private keys for free. It will also help move the industry toward a stronger, more cryptographically assured state of safety and soundness.

## Blockchain Data Analytics

Many startups are being created to provide a healthy ecosystem of virtual currency technology. This ecosystem includes technological solutions related to problems in the regulatory and policy mandate space. Many of the technologies are provided free to the community. Reference implementations, demonstrations, and production-capacity support are available in some cases.

To address the AML challenge put in place by FinCEN director J.S. Calvey, here we review briefly some of the technologies available both for AML and general forensic investigation. For example, one start-up in this

space, Coinalytcs [14], provides technologies for fast transaction scoring, entity identification and currency flow visualization for AML and forensic investigation.

### **Fast Transaction Scoring**

Fast transaction scoring, initially created to facilitate evaluation of inbound transactions during the sub-confirmation threshold period, can also provide real-time evaluation associated with AML and anti-terror concerns in the network. Scoring analysis takes into account anonymization techniques such as mixing. During the real-time scoring procedure a transaction will be scored lower for factors including utilization of anonymization techniques.

### **Entity Identification**

Entity identification is performed based on the heuristics outlined in Spagnuolo 2014 [15]. Entity identification makes address-entity evaluation - where an address is associated with an entity - possible. Address-entity evaluation is used to simplify analysis and visualization of network activity and relationships. Entity identification is a technique to identify addresses that belong to a single entity based solely on the history of network activity. Entity identification is an AML technique and should not be confused with the KYC association of an entity with PII.

### **Currency Flow Visualization**

Currency flow visualization is a forensic technique for understanding the flow of currency among accounts and entities over time. Coinalytcs has created several currency flow visualization interfaces - built on multiple underlying technologies - which are used 'in-house' only and available for private demonstration. These interfaces are being prepared for production-grade consumption in the final quarter of 2014 and the first quarter of 2015. Currency flow visualization takes what is already public and makes it understandable.

---

## Technology Solutions: Long-term Pipeline

### **Hard Problem: AML/KYC vs PII Security**

Perhaps the most difficult problem to solve technologically is enabling the real-time identification and reporting of suspicious activity, while securing customers' personally identifiable information (PII) against increasingly sophisticated international data thieves. The former requires making PII more available and accessible, the latter requires making it less so, hence there is a fundamental tension between these two objectives.

Financial intermediaries are obligated by law to track customers' 1) source of funds, 2) destination of funds, and 3) purpose of transactions. This obligation is commonly referred to as Know Your Customer and transaction monitoring. However, KYC is not simply knowing the identity of your customer, but truly "knowing" your customers: who they are, their habits, intentions, where they derive their income, how they spend their wealth, and with whom they do business. Currently this requires PII to be relatively easily accessible in real-time.

Yet, as Superintendent Lawskey observed recently, such detailed data monitoring and recording raises significant identity theft concerns. Even our most well-resourced, strictly audited and governed, major US multinationals can't seem to guarantee the security of US citizens' identity data, and some recent breaches have even involved elaborate strategies of physical infiltration, for example via HVAC subcontractor at Target.

As a result, potentially the majority of US citizens' personal data is now for sale in data black markets, and classified military and national security information is in the hands of foreign powers. Forward thinkers in the security industry now believe that our modern data security architecture is fundamentally insufficient to the task.

Reconciling these two needs is, in the scientific sense, a hard problem. It is foreseeable that a solution exists which will enable both stronger end-to-end encryption of PII and simultaneously the reliable detection of suspicious activity, using advanced cryptographic tools and machine learning techniques. For example, oblivious transfer, fully homomorphic encryption, continuous real-time cryptographic signature comparisons with OFAC watchlists, and machine learning algorithmic blockchain analysis for suspicious activity comprise a few avenues for further research.

However, some of those technologies are still in their infancy and are years or more away from commercial deployment. While this is a longer term effort, we believe enough of the parts are at least mathematically and computationally proven for us to be hopeful about future prospects for solving even this seemingly intractable problem. Again, we hope that regulation can be structured in such a way as to account for the emergence of increasingly sophisticated and powerful technological solutions in the short, medium, and long term and provide enough flexibility for their adoption when ready.

---

## Industry Topology: Segregation of Duties

### *Pattern: Separation of Duties*

1. *Start with a function that (a) is too valuable to dispense with, and (b) to be performed, requires power that can be abused.*
2. *Divide the function into separate steps, each necessary for the function to work or for the power that enables that function to be abused. A function so divided can be called a cycle, and corresponds to a formal mathematical model called a state machine. (You do not need to know this mathematics to follow this discussion; just follow the cycle step by step).*
3. *Assign each step to a different person or organization. The different entities perform their particular roles in the cycle, and monitor and constrain each other, using inter-party integrity constraints, to perform just their respective roles. [1]*

It is crucial to observe that modern professional financial institutions segregate duties across multiple organizations. For example, professional trading is typically segregated across four different kinds of organizations:

1. Broker - takes trade instructions from a trader
2. Exchange - consolidates orders from various brokers and executes them
3. Clearinghouse - ensures that the orders are settled (i.e. that the assets that have been traded actually end up being properly transferred)
4. Custodians - hold the title of record for the asset(s) being traded.

Each of these organizations keeps independent records of each transaction -- each organization operating under a different CEO and each computer system's root being controlled by a different systems administrator.

Most early Bitcoin financial intermediaries, by contrast, are comparatively centralized, non-segregated organizations that combine most or all of these functions into a single entity and hence lack all the safeguards

of the modern securities industry. Their centralized server security and non-segregation of duties makes it prohibitively difficult to implement proper financial controls and business continuation processes.

However, industry entrepreneurs recognize this problem and are honing in on a topology for how financial controls and segregation of duties should work at both the firm level and industry level, adapting the modern institutional finance model to the cryptofinancial industry, while upgrading some of the traditional backoffice components with equivalent or stronger cryptographic tools and techniques.

At a high level, the industry topology consists of the following components, each housed in wholly independent organizations:

1. Custodian (fiat): Registered escrow bank accounts managed by registered escrow agent/attorney, such that customer fiat is protected in the event of exchange/brokerage failure.
2. Custodian (virtual currency): Multi-signature escrow services, such that customer bitcoins are protected in the event of exchange/brokerage failure. In the future, we anticipate exchanges will offer “keyless trading”, enabling customers to serve as their own asset custodians, while exchanges maintain the ability to enforce settlement of gains/losses at pre-determined intervals.
3. Exchanges: Sells/rents seats to brokerages, market makers, does not interface directly with traders.
4. Brokerages: Sells exchange interface to traders.
5. Clearing House: Blockchain.

Again, our various non-profit SRO and advocacy organizations - DATA [5], CDC [6], Bitcoin Foundation [4] - as well as virtual currency-oriented startup accelerators, investors, and entrepreneurs, will be instrumental in driving the implementation of this model industry-wide, as well as communicating it to lawmakers and regulators.

---

## Conclusion

Above we have presented an incomplete view of technological solutions available to address policy mandate and regulatory concerns in the virtual currency domain. Some of these technologies are online now, some are in commercial development, while others are still in the research labs and are years or more away from deployment. Here we have presented a sense of what is in the pipeline to demonstrate the value of regulatory safe havens and/or testing environments that enable the continued development, iteration and maturing of these technologies.

We intend to have started a productive dialogue on the potential for technological solutions in the virtual currency space. We anticipate the dialogue to reveal the potential for the cryptofinancial industry to ultimately supersede the security, compliance and transparency of modern institutional finance. Again, thank you for your consideration of our efforts.

---

## Appendix A: Unique Characteristics of Virtual Currency Organizations

It is also worth enumerating the unique characteristics and different permutations of types of virtual currency firms in order to better evaluate how and where policy mandates and regulatory objectives should apply:

1. Non-profit (Bitcoin Foundation) vs. for-profit (exchanges, some wallets, etc)
2. Free and Open Source Software (FOSS) [2] (most desktop wallet software) vs. proprietary (most web wallet services)
3. Is a cryptolegder system (Bitcoin) vs. is not a cryptolegder system, but provides services on top of cryptolegder systems
4. Serves customers (online wallets, exchanges, etc) vs. does not serve customers (non-pooled miners)
5. Custodies customers' private keys vs. does not custody customers' private keys
6. Custodies customers' fiat money vs. does not custody customers' fiat money
7. Currency and finance applications (shares, bonds, derivatives, and currencies) vs. non-financial applications (Namecoin, Filecoin, etc that use currency only in support of the actual application of the particular blockchain)

Question: Do new certification or audit regimes need to be developed to enable organizations to prove to lawmakers and regulators to which category they belong?

Financial intermediaries meeting the criteria of both “do not custody customers' private keys” and “do not custody customers' fiat money” probably should not be regulated in the same way as other services that do control the private keys and/or fiat money of their customer deposits, yet how are regulators to be assured of the difference? This may require a new industry-standard certification/audit regime legitimate in the eyes of institutional finance, regulators, and government.

These unique characteristics and permutations are quickly leading to novel kinds of businesses models and practices, which may be vulnerable to new types of problems and challenges, but completely immune to older ones.

---

## Appendix B: References

[1]: <http://szabo.best.vwh.net/separationofduties.html>

[2]: [https://en.wikipedia.org/wiki/Free\\_and\\_open-source\\_software/](https://en.wikipedia.org/wiki/Free_and_open-source_software/)

[3]: <http://cewg.iftf.org/>

The Crypto-Economy Working Group at IFTF explores the many ways to proactively anticipate the technology, decision-making architectures and regulatory frameworks associated with crypto-currencies over the coming decades.

### DISCLAIMER:

Institute for the Future (IFTF) is a 46-year-old non-profit, independent research institute dedicated to convening diverse voices and perspectives to understand and anticipate the most urgent futures that confront society today. We do not advocate for specific political, policy, or technological solutions but rather serve as a platform for thinking systematically about complex future issues. IFTF has not funded, nor has it received funding for the work of the Crypto-Economy Working Group on this Bitlicense comment; rather it has simply provided an online platform and monthly meeting space for the group to consider the various issues and arguments.

The opinions expressed in this comment are those of the individual signatories and are not representative of IFTF or its directors.

[4]: <https://bitcoinfoundation.org/>

The Bitcoin Foundation exists to standardize, protect, and promote the Bitcoin digital currency and protocol. It organizes funding of core development efforts; maintains, improves, and legally protects the integrity of the protocol; and promotes understanding and clarity among the public as to the nature of this new technology.

[5]: <http://dataauthority.org/>

DATA objective: Develop and standardize self-regulatory best practices that signal to government and regulatory agencies that we the industry understand their regulatory mandates and are governing our industry accordingly.

[6]: <http://digitalchamber.org/>

The mission of the Chamber of Digital Commerce is to promote the acceptance and use of digital assets and digital currencies.

[7]: <http://nakamotoinstitute.org/>

[8]: <http://coincenter.org/>

[9]: <http://www.ffiiec.gov/>

[10]: <https://iwilcox.me.uk/2014/proving-bitcoin-reserves>

[11]: <https://empoweredlaw.wordpress.com/2014/06/27/bitcoin-multi-signature-account-operating-manual/>

[12]: [https://en.bitcoin.it/wiki/Bitcoin\\_Escrow\\_Service/](https://en.bitcoin.it/wiki/Bitcoin_Escrow_Service/)

[13]: <https://github.com/ethereum/wiki/wiki/Problems/>

[14]: <http://coinalytics.co/>

[15]: [http://maggi.cc/library/My%20Publications/Conference%20Papers/Bitlodine\\_Spagnuolo\\_et\\_al\\_2014.pdf](http://maggi.cc/library/My%20Publications/Conference%20Papers/Bitlodine_Spagnuolo_et_al_2014.pdf)

[16]: <https://www.bitgo.com/>

[17]: <http://startbitcoin.org/>

[18]: <http://coinometrics.com/>

[19]: <http://standardtreasury.com/>

[20]: <http://epiphyte.com/>

[21]: <http://subledger.com/>