

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Dear Superintendent Lawsky and General Counsel Syracuse:

Like many technologists and like the Electronic Frontier Foundation, I am concerned about the BitLicense proposal. I am a PhD student in Computer Science at Columbia University, and while I am not an expert in bitcoins, I have done some research in the area. I'd like to offer some additional thoughts:

1. Most people that use bitcoin at this point do not do so because they want a regulated virtual currency. They want to experiment with "digital cash". So why is this currency getting regulated? I find myself drawing parallels with the net neutrality debate, where it seems that the Federal Communications Commission is regulating the biggest communications infrastructure today (the internet) because that is their mandate. Are we regulating bitcoin because Mt Gox collapsed, and the American people should be guarded against such tragedy, or because exchanges look like banks and for the last few hundred years, this is how we've regulated banks? Who exactly stands to gain from bitcoin regulation? The answer doesn't seem to be the users, to me.

Yes, bitcoin is a wild west and caveat emptor and if you lose your wallet to a used car salesman, that's it, but that's what we built. If there was to be some accountability in the system, it would have been built into the system, and trying to bolt it in afterwards with BitLicense is like trying to make software secure after you've written it insecurely. (It never works.)

2. There are smarter ways to regulate bitcoin if you truly wish to do so. Bitcoin itself is evolving and developing these techniques. Of course, "evolving" is a nebulous word, so let me give you an example.

People used to store their own bitcoin wallets, which was extremely vulnerable to theft; then online wallets with two-factor authentication started appearing; now multi-signature wallets (e.g. <https://greenaddress.it/>) allow multiple parties to veto or allow a transaction before it goes through.

This is the perfect way to add some regulation to bitcoin. Instead of requiring companies to record names, addresses, etc of customers -- which is an antiquated idea, vulnerable to a decade of hackers, and inflames privacy advocates to no end -- you could have a server which can veto or approve transactions. If the store requires identification, and the user has none (is using an anonymous address), then the transaction is vetoed; otherwise, it is logged without the business having to do anything. I think trying to use twentieth-century techniques like forcing name/address lists is going to end in disaster. You should try asking the bitcoin community (<http://bitcointalk.org>) what bitcoin regulation should look like.

3. You do not have to force regulation upon bitcoin. Instead, you can provide a way for bitcoin "banks" to be certified. Basically, they would comply with all the BitLicense requirements (or something similar as I discussed in 3) and provide some transparency into their business. This gives users the option of using an accredited institution instead of the next Mt Gox. This approach would be seen much more positively by most technologists and (due to its voluntary nature) will not "stifle" bitcoin in any way.

I hope some of these comments will be helpful. Please send me follow-up email if you have any questions. Sincerely,

David Williams-King, B.Sc. First Class Honours, M.Sc.
PhD student in Computer Science at Columbia University