Colin M. Lacina
840 S. Prospect Ave.
Bartlett, Illinois, 60103-5035
(630) 945-8848
LacinaC@DuPage.edu

December 8th, 2016

Illinois Department of Financial & Professional Regulation
100 W. Randolph St., Floor 9
Chicago, Illinois, 60601-3218

To whom it may concern at the IDFPR:

I have read the full text of your proposed “Digital Currency Regulatory Guidance” document that you have requested comments on and would like to provide my input. As someone who has been involved with decentralized digital currencies—cryptocurrencies specifically—in some fashion since approximately late 2013, have been a part of a few cryptocurrency organizations, and have worked on editing cryptocurrency source code, I feel I am qualified to comment as I have a thorough understanding of how decentralized digital currencies work mechanically, the terminology used to describe decentralized digital currencies and their functions, and the various intricacies of the decentralized digital currency economy.

First, I applaud the amount of research and thought you have placed in your proposed draft of the “Digital Currency Regulatory Guidance” document. It is evident that you have put much work into it and command a mastery of the topic far beyond the lay person. I remember seeing another RFC from Europe that clearly lacked your mastery and needed much correction. I only need to ask you to make a few for your document and ask for some legal clarification on your stance.

As far as corrections go, you first should know that not all decentralized digital currencies call the process of earning units of the currency through the consensus (or proofing) algorithm “mining” and those that perform this process “miners.” Some decentralized digital currencies, most commonly those using alternative consensus algorithms (i.e. algorithms other than the original Proof-of-Work algorithm used by Bitcoin). Most decentralized digital currencies that use Proof-of-Stake algorithms refer to the process of earning units of their currency through the consensus algorithm as “Staking” and those who do so as “Stakers.” At least one of these Proof-of-Stake

decentralized digital currencies—NXT in particular—calls the process “Forging” and those performing the process as “Forgers.” Another decentralized digital currency, called NEM (or New Economy Movement), uses what they call a Proof-of-Importance consensus algorithm and call the process of executing this algorithm “Harvesting” and those performing the process “Harvesters.” It is a fallacy to call the process of performing a consensus algorithm to earn units of a decentralized digital currency “mining” as the name for the process varies from consensus algorithm to consensus algorithm and sometimes from decentralized digital currency to decentralized digital currency within currencies using the same consensus algorithm.

Another fallacy is the assumption that “Miners,” “Stakers,” “Forgers,” “Harvesters,” or anyone else performing a consensus process for a decentralized digital currency are always “creating” new units of the currency. Some Proof-of-Stake and other alternative consensus algorithm cryptocurrencies started out with every single unit of the currency being available to the “initial stakeholders.” Instead of rewarding those responsible for consensus (e.g. “Miners” or “Stakers”) with “new units” of the currency, they reward them with automatically collected “transaction fees.” Some cryptocurrencies will not allow a transaction lacking a minimum fee—which sometimes vary by transaction type—and for others there is no fee required but it motivates inclusion of a transaction in the consensus by allowing those which create a new “block” send the fees of all included transactions to their own wallet and enforcing a maximum number of transactions allowed in a block and/or a maximum size in bytes allowed in the block.

Further, even in Bitcoin (as well as other cryptocurrencies), the chance of any one miner creating new unit is very small so they aggregate their computing power into “pools” and the pool they are a part of measures their power and gives them a share of the new unit, which when created goes to the owner of the pool’s wallet initially before the owner distributes it to the miner’s wallets. An individual miner may only help the pool create a single unite in a whole year, but will get a share of all units the pool creates based on their computing power.

Finally, I have some questions on your rulings that I think your document should clarify. The first of which pertains to your ruling on “Bitcoin ATMs.” I would argue that they do not act as an intermediary between a buyer and a seller even if they involve a third party. The ATM acts more like a private, automated, trader for the owner. When someone deposits cash into a Bitcoin ATM, it either draws from its own bitcoin supply or purchases bitcoin from a third party. The bitcoins purchased from the third party go directly into the ATM’s wallet, not the users. The ATM then sends the funds to the user. The ATM does not purchase bitcoins for the user, it purchases bitcoins to restock itself so that it may fulfill the user’s request. The owner of the Bitcoin ATM is like a vending machine owner who buys soda to stock his machine. The only difference is that the vending machine automatically purchases the product and restocks itself when needed. This restocking process is invisible to the user and the user has no say in who the

machine purchases its bitcoins from. The machine is not an interface between buyer and seller, but an automated trader which resupplies itself.

A similar concept applies when the user sells their BTC at the machine for cash. The machine only has a set amount of cash it can distribute and it cannot automatically restock its cash supply. If it runs out, the owner must physically open the machine and add the cash to it which is like restocking a vending machine.

My last question is to how this applies to FinCEN rulings that exchanging convertible virtual currencies counts as money transmission. You should clarify how or if the State of Illinois will enforce compliance with FinCEN rullings.

Sincerely,

Colin M. Lacina