Date: 12-11-19
Received from: Aniello Zampella <aniello@coinbtm.com>

Hello all,

Commenting on:https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/pr_guidance_regarding_listing_of_vc

Speaking as the 14th Licensee here.

Hope this email finds you all well and in good health. I feel honor-bound to comment on this proposal based on my license.

With respect to & considering the documented and reported transgressions of other licensees which I've sent over via email in the past, I feel this new proposal for "self-regulation" in this field is preposterous and riddled with flaws given people's tendencies to shirk responsibility whenever the rules are not enforced. Ironically, that means I'm arguing this proposal is not being strict enough... it's far too lax.

Down to business:

As mentioned in person during my first annual exam, I fervently believe seven simple words are enough to protect the average consumer from many problems faced today. Those words are explicitly stated here: "If it ain't bitcoin, it's a shitcoin". Meaning: all "digital assets" or "convertible virtual currencies" or whatever you want to call them EXCEPT bitcoin are, in my humble opinion, an anathema to the overall financial system and merely serve as vehicles for charlatans to sell dreams to the uninitiated and unwashed masses. They all exist because someone somewhere said "I want to ride the next unicorn! it's too late to get bitcoin." (failing to understand that no, it's not too late and it breaks down into 8 decimal points) Each and every one has a centralized development and governance structure which is much more closely related to a security (like stock equity in a company) than to a commodity or land, or anything that remotely stores value for a prolonged amount of time. They depend heavily on marketing to generate interest and stay relevant. They solve nothing which a well-built application couldn't do better.

The only real solid point of a blockchain is to 100% verifiably send value from point A to point B without being forced to rely on any type of custody or third party.... and bitcoin does this and has done this flawlessly for just about a full decade. Bitcoin has no "creator" (anymore) that can decide to just change the consensus or rules on a whim. It is the closest thing to "a tangible thing" in the digital asset space. That "thing" of scarcity is able to then soak up wealth / value, and is best used as a hedge against inflationary currencies the world uses on a daily basis. Think of it as a time capsule for your wealth... Can be even as little as $1 or much more.... but the point is you take X wealth from the inflationary world, place it into a disinflationary asset (bitcoin) and then on a rainy day some time in the future (2+ years) when you look back in that disinflationary time capsule the USD value of the asset will invariably be greater than when you first put it there. The expectation being that on that rainy day you would need to tap into the wealth you have stored in BTC to "get something done" like buy a house or pay for a child's college, etc. Whether that value appreciation occurs in the future is always a lively debate, however the past decade of bitcoin history and my expertise in the industry has led me to these conclusions.....

Frankly speaking, the technical underpinnings for many of these "blockchains" is laughable, and no company would be able to always protect its users from protocol malfunction or the dreaded "51% attack" which is present on all Proof of Work blockchains. As an example and from a high level: it would

right now only take a nefarious entity approx $75k per hour to attack the "Bitcoin Cash" blockchain and place oneself in control of block generation and transaction mining. This has happened before, and it will happen again. Anyone engaging in financial activity with such a blockchain risks having their transactions reversed completely by said bad actor. This means an attacker can defraud others by sending the asset to an exchange to trade or directly converting it with another party into a different asset, and then re-organizing the blockchain with new & different versions of the same transaction where the attacker never sent the coins to the (now-defrauded) exchange or other party. Since the attacker was 51% in control of the network, they can re-write the chain's history with impunity.
For Ethereum Classic, this amount is a paltry 10k per hour. Right now. Anyone can attack Ethereum Classic and re-write the history of transactions for only about $10k per hour... This in my humble opinion, does not sound like something that the general public should ever be exposed to. We are in the business of protecting consumers, are we not? By comparison, bitcoin would be costing well over half a million dollars per hour to even attempt the attack - and if the attack was successful on bitcoin, there would be no way to spend those defrauded coins because the value of the market would plummet as soon as people realized what happened rendering the attacker's efforts into a Pyrrhic victory. Kind of a catch-22 protection at the end of a very expensive road that a potential attacker would be faced with.

Let's take the exact wording, for instance:

"A proposed DFS web-page that will contain a list of all coins that are permitted for the Virtual Currency Business Activities of the VC licensees, without the prior approval of DFS, which list may be updated from time to time, as long as such listed coins have not been subject to any modification, division, or change after their listing on the DFS web-page"

The list is: Bitcoin, Bitcoin Cash, Ether, Ether Classic, Litecoin, Ripple, Paxos Standard, and Gemini Dollar.

There's much wrong to unpack in the end of that paragraph & this list of "coins"... I know you guys mean well here, and please don't take this the wrong way, but I'm telling you that you don't know what you're talking about.... These software protocols / code repositories all go through such frequent updates & modifications as to render this list moot before the period at the end of this sentence. Bitcoin updates approx every 6-8 months based on community-driven code reviews. Ethereum updates almost every 2 months as per the schedule of the Ethereum Foundation and Vitalik's whims. Bitcoin Cash updates every month or two, desperately trying to shove in features that other blockchains discuss or implement first, as if that somehow mattered. Etcetera...

There are things in each of the code updates that change at any given time that can force a blockchain/currency to become completely "different" from what it was, and yield a completely separate blockchain (hard fork) resulting in two separate and incompatible things.....

This can happen intentionally or unintentionally. Then there are other things which are benign to network consensus and are as simple as typo fixes in the readme files. And there is everything in between. So, this begs the question: where does one draw the line? The ultimate problematic answer is, you simply cannot: it is a binary all-or-nothing choice. You either certify "the thing" (and its main advertiser/hype man/development team) is ok to trade with, or you don't. You cannot say the entity will "self certify" the code because it can and will evolve beyond your control and purview.... In the recent hard fork that happened on Ethereum not even a week ago, we noticed our beloved Gemini's own exchange Ethereum hot wallet ran "out of gas" when processing withdrawals! This was because the ETH developers did not properly disclose the code changes and their impacts to the wider community, and Gemini was obviously not sufficiently made aware of, nor prepared properly, for a production change like that to happen.... This behavior puts customer funds at risk! Luckily for Gemini and Ethereum as a whole, I don't believe any customers lost tokens, they just had their time wasted... But it goes to show

the slap-dash nature of "alt-coin" development. Don't fall for that marketing term. Again, remember: if it ain't bitcoin, it's a shitcoin.

Also with regards to Ethereum, there still exists a very real possibility that the "bloat" of its blockchain/state quickly becomes so massive that software clients become unable to sync and connect with other peers.... Attempting to sync up new nodes to this behemoth history tree is..... troublesome.... to put it nicely. On most servers it is flat out impossible. Ethereum's main "killer app" is and has always been "minting your own coin" .... which is ridiculous in and of itself.

Bitcoin Cash - is a complete fraud masquerading as "the real bitcoin" and was perpetrated by Roger Ver to try and capture the development roadmap and "brand" of bitcoin. It is constantly marketed to digital asset newcomers AS bitcoin itself, which is fraud. But there is no Bitcoin Company to press charges for false advertisement since bitcoin is just an open source software protocol and this "thing" is marketed as something it is not... While I don't have very nice things to say about any alt-coin, this particular one is extra bad specifically due to this insidious underlying bait-and-switch foundation.

As for Ethereum Classic, really? is this a joke? That made the short list? Real quick: The difference between ETH and ETC is that when the first DAO's "smart" contract got hacked and was drained/locked of all user funds, the community decided to re-write the Ethereum chain history to "fix" that event in a contentious hard fork. Vitalik Buterin, who is effectively the issuer of Ethereum, pretty much decides the path of the development and that was his call to make... Plenty of people were (in my mind, rightfully) arguing that the "smart contract" which was exploited was the fault of the programmer who wrote it poorly, and that blockchain transactions *should be* immutable when confirmed in blocks, therefore people needed to learn a hard lesson to not blindly throw their money into things they didn't do research on..... This chain with the hacked coins still exists, was somehow included in the short list, and no one really uses it for any kind of daily activity.... as mentioned earlier you can 51% attack it for pretty cheap overhead.

These kinds of smart contract "bugs" have occurred again since that birth/split of ETC, too... See Ethereum Improvement Proposal 999 for one big example -> https://github.com/ethereum/EIPs/blob/master/EIPS/eip-999.md which is basically a "bailout" for the crappy Ethereum developers, which has so far been completely rejected by the community - leaving the affected ~530k ETH still unspendable. Any persons who had some ETH in that hosed contract will never have access to it again unless an Act of God (Vitalik) changes the ETH codebase and sneaks it into the repository.

Litecoin - as with all the others, there's no real use for litecoin... this coin has persisted based solely on marketing: "it's the digital silver to bitcoin's gold" But, again this is glossing over the simple fact so many uninformed people miss..... you get 8 decimals of precision with bitcoin, so you don't necessarily need to have 1 full bitcoin, you can send 0.00000001 bitcoin even to cover whatever debt or move value.... this was before people were comfortable with decimals and thought you needed to send full coins to be worth something.

Then we have Ripple - it's a pre-mined security, vast majority of the tokens are held by Ripple Labs. They control the entire supply of XRP and periodically sell it, similar to securities, to raise "real" capital for their own purposes. So, if we can sell securities like XRP, does that mean I can start selling fractional shares of AAPL and MSFT or AMZN from my kiosks? Walks like a duck.....

Paxos Standard and Gemini Dollar are not actually crypto currencies. Any "stablecoins" are not crypto currencies at all. Those two in particular are supposedly the type where they are digital representations of real US Dollars held in custody bank accounts somewhere domestically. When you think about it, there is no discernable difference in those "dollars" and the dollars in your PayPal account balance. The

issuers can freeze accounts and restrict movement of funds. How and why these are things that exist is still beyond me, aside from wanting to move fiat for 24/7 arbitrage.

The Federal Gov't can cleverly obsolete them, instantly, by allowing, or rather by mandating, normal ACH and wires to happen 24/7. Signature Bank and Silvergate Banks both have their own internal fiat-transfer networks for this very purpose. There would then be no need for any stablecoin if it worked bank to bank instead of just internally.... Think like venmo, but by default for everyone and every bank account. They really should hurry up, too. Because stablecoins, not crypto, are by far the best way to launder large sums of money. As a quick example from today's news feed.... this kiosk operator in Canada is now going to offer all manner of stablecoins in their kiosks. https://www.cryptoninjas.net/2019/12/11/canadian-crypto-atm-network-instacoin-adds-support-for-7-stablecoins/ Why? With any stablecoin, there's no price volatility and it's tied to the value of the fiat analog (usually USD), which all familiar goods and services are priced in. Again, how these things exist is beyond me. If it was known that stablecoins were going to be around long term, a criminal enterprise would be wise to convert their illicit finances into stablecoins, since they are readily transmitted across any jurisdictional borders and do not suffer value volatility day after day (aside from typical central-bank induced inflation)

This system of "digital dollars" was tried before with LibertyReserve and the Feds shut that down after awhile, too... https://en.wikipedia.org/wiki/Liberty_Reserve Fun Fact: LR is likely what gave rise to the first stablecoins back in 2014..... They are easy to convert between themselves too, so you can trade GUSD for USDT or PAX etc.... try following some funds there to get a freeze on some GUSD after it's been traded or converted into USDT. Good luck.

So now, there are these "regulated" stablecoins which have actual dollars in banks, that can be traded amongst regular people all across the world for other stablecoins of "equal value" that may or may not have dollars backed in bank accounts or used to more easily pay for goods & services, because it's straight fiat without the govt, bank, or processors..... what could possibly go wrong with that? Do you think anyone can be 100% sure that the issuers of these stablecoins know the true identities of the bearers of these tokens when they later get used to do some shady stuff after having been traded back and forth a bunch of times? Ha! Good luck... Ever really ask them to prove it *en masse*?

It is my belief that when offering a financial service to the public, it should be with a very long term forecast outlook, similar to a traditional bank. The entity should be required to secure its own assets and provide a time-idempotent interface for the public to trade with the entity. That means running one's own independent blockchain node software and not third-partying it with a custody wallet provider. Too much systemic risk, if something happens to that third party, you are dead in the water.

This notion of wanting to provide "more coins" feeds into a broader consumer-based gambler mentality... and that's kinda weird. We are not trying to push penny stocks on people and call it the next revolution in finance are we? Seems rather disingenuous... The ones who make out the most in this endeavor are the exchanges which facilitate the trades... since they take a commission fee on the trading activity. The ones who lose out the most are the average consumers who arguably don't do enough proper research before FOMO takes hold and they throw money at any ticker on the screen.

Without going into the technical details on these things, it is easy to succumb to marketing buzzwords, the "razzle dazzle" and slick talking / promises of grandeur for what is ultimately a powerful but complex technology / system.

It's bad form to offer a token and then de-list it because of poor volume/performance/etc ... so if you are going to offer XYZ coin, in my opinion, you better be prepared to provide support and updates for that blockchain for the life of your company. Token de-listings generally mean the tokens become

worthless for anyone who holds them, as they immediately suffer from even less liquidity and the inability to exit positions or utilize said tokens in any fashion. That means you ultimately helped those people lose money by initially facilitating that nonsense. No bueno.

I do not believe it to be wise for the fox to be allowed to guard the hen-house. Even though I am the fox in this analogy and it is in my personal interest to lobby for less restrictions, not more. I feel it is in everyone's interest to limit the types of "tokens" traded. Not everyone is as frank and honest as that assessment, however....

It smells like this proposal is the result of lobbying efforts from Coinbase/Gemini/itBit to rubber stamp more coins for trading, so they can accumulate more fees from said trading.... Curiously though, my company never receives customer inquiries for supporting anything besides bitcoin. Hence, why I believe this to be a biased proposal request that does not fully analyze the scope of effects which would likely promulgate as result of this change..

Therefore, in conclusion, and with the utmost respect, I humbly suggest that NYDFS continues to evaluate, case-by-case, each entity and perform rigorous checks on their controls and procedures.

That's my 2 satoshis. If you made it this far, thank you very much for reading through my thoughts.

Best Regards,

--Aniello Zampella
Founder / CEO
Cottonwood Vending LLC
BitLicensee #0000014