

March 19, 2019

I have a degree in Computer Science and I've started 3 companies in the technology and distributed systems software space.

I'd like to comment on the first three questions, the first following an observation stating that crypto assets are commodities and not securities:

"1. Are there factors in addition to those noted above that we should consider?"

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?"

My comment is as follows:

These token schemes are all centrally controlled, sometimes anonymously, and were foisted on the public so the people who created the tokens could make millions.

The tokens are presented as "coins" or "money" and the public is given promises that they can get rich selling the tokens to someone else at a higher price in the future, when the "coins" might be "worth millions".

At their core, they are all zero sum pyramid schemes. The only potential "value" they have is their utilization for illegal transactions.

One of the primary ways the people who created these tokens got people to use them is pushing use cases of smuggling, drug purchases, ransomware and the like, along with explaining that governments would not be able to track individual users or block transactions between parties.

Everyone who started a token scheme began by giving a large number of their tokens to themselves. They then attempted to create a market for the tokens where they could exchange those tokens for money by getting other people involved in their scheme by giving them tokens or allowing them to print their own tokens by utilizing their own computing resources. Many of these attempts have been successful.

The token systems themselves are generally controlled by 2 different parties.

The first centrally controlling entity is the small set of developers behind the software that runs the token scheme. They have the ability to block or reverse transactions, determine which token ledger is the true ledger, increase or decrease the number or rate of token issuance and change transaction parameters by changing the software that manages the token ledger and associated transaction processing.

The second controlling party is the party that runs the computers that actually process transactions. In Bitcoin, this is any group that controls a majority of hashing process power. They have the ability to block transactions, roll back transactions and double spend tokens.

The first group, the developers, are the true central control and they generally state that if the group processing transactions acts in a manner the developers don't like, the developers will roll back the transactions of the transaction processors and block the ones who act in a manner they disagree with.

I've never understood how any government can see any of these schemes as legitimate. None of them are any different from me selling people casino chips marked with my name, calling them money and saying they will go up in value because I will only issue 100 casino chips. Then I would process transactions between individuals, keeping a ledger of who owns what by not by name, print fake prices of the casino chips to show people the price going up and promote them as the "new form of money".

The technology behind the tokens is slow, wasteful and insecure.

Insecure because you must have trust in the transaction processors and developers who maintain the system.

Since, at their core, the systems are designed to facilitate illegal transactions and get people to buy worthless assets for money, the average person buying into these schemes will lose their money. As a zero sum game, it is impossible for them not to.

The best approach to dealing with all these schemes is to enforce the existing laws against running pyramid schemes.

Eric Swildens