Regulation within crypto currency markets: By Alexander Larsen, IRM subject expert

Published on February 5, 2018

by Victoria Robinson MA, MCIM

Author Alexander Larsen
President of Baldwin Global Risk Services Ltd
United Kingdom

According to Reuters: “Japan’s financial regulator said on Friday it had ordered all cyrpto currency exchanges to submit a report on their system risk management, following the hacking of over half a billion dollars of digital money from Coincheck.”

Whilst the whole premise of blockchain technology and crypto currencies revolves around it being essentially unhackable, the exchanges that trade these currencies are vulnerable. The introduction of system risk management (which we assume to be risk

management of the software/operating systems and servers) checks is a step forward for the crypto currency space although it only covers one area of exposure linked to the crypto currency market.

History of incidents

Crypto currency has been a booming market with increases in some major coins in the high 1000's of percent over the last year. This rise, coupled with a lack of regulation, has seen the crypto currency world being hit with a number of negative incidents from Ponzi schemes to fraud, scams and hacking incidents.

Bitconnect, which as of writing of this article, is trading at roughly $8.60, a huge fall from its height of over $300 a month ago, is an example of a potential major Ponzi scheme which has lost $2.4 billion worth of value over 10 days.

The subpoena by US regulators of crypto exchange Bitfinex and its relationship with Tether is another concern to the crypto currency market with many claiming Tether to be a scam. Tethers are tokens backed by US dollar deposits, with each tether always worth one dollar. These tokens should be backed by dollars but thus far the company has yet to provide evidence of its holdings to the public and has not had any successful audits as of yet.

There have also been a large number of Initial Coin Offerings (ICO's), used to raise money for start-ups by issuing tokens/coins, which have raised vast sums of money only for the owners to disappear with all the money, whilst others have been less deliberate but have been just as devastating to investors. A crypto currency called Tezos, raised $232 million last year, but suffered internal power struggles, which has left the project in disarray.

This brings us to the current concern in Japan of cyber attacks of exchange platforms. Cyber attacks and hacking attempts of exchanges have been frequent with Bitfinex, coinbase and kraken amongst others having been closed down for days at a time during 2017 due to a number of hacking attempts. It is the successful hacking incidents which are the most worrying however, with successful hacks such as MT Gox, which cost almost 350 million and two attacks on Youbit which led to it's bankruptcy. The most recent coincheck hacking was worth 500 million, a record, and it is this which has caused Japan to act.

Regulation

Last year, China took a definitive stand on regulation on crypto currencies which sent shockwaves through the market. Some feel it was perhaps heavy handed with ICO's being banned, bank accounts being frozen, bitcoin miners being kicked out and nationwide banning on the internet of crypto currency trading related sites. Others however believe that it has been a positive step, and has encouraged other governments to take regulation seriously and hopefully take a more balanced approach. It certainly isn't in the interest of governments to stop ICO's, which provide many positives including innovation, but they should certainly regulate them from a consumer protection, taxation and organised crime standpoint.

Implementing regulation also removes uncertainty for investors as well as the companies who are involved in ICO's. Uncertainty is the source of many risks and often a negative certainty is better than uncertainty as it allows a focus within set parameters.

It's important to remember that too little regulation doesn't offer protection and too much stifles innovation.

How to regulate

There are a number of ways to regulate crypto currencies and the following are just some examples:

1) Framework for ICOs

New ICO's are currently not subject to much in terms of regulation globally. One of the problems is determining how they should be treated with some being considered securities. As a fund raising vehicle, there could certainly be a framework that lays out key requirements of an ICO such as a company needing to be registered in order to issue a token, transparency in terms of individual members of the registered company as well as perhaps introducing a few requirements that regular IPO's require such as implementing risk management. Currently in USA, ICOs are expected to adhere to Anti Money Laundering (AML)/Know Your Customer (KYC) practices.

2) Regulate exchanges

Exchanges, which is where much of the transactions take place in terms of trading coins, is a logical area of focus when it comes to regulations

South Korea's financial services commission for example, has stated that trading of crypto currencies can only occur from real-name bank accounts. This ensures KYC and AML compliance. According to the FSC, the measures outlined were intended to "reduce room for crypto currency transactions to be exploited for illegal activities, such as crimes, money laundering and tax evasion,"

Regulators should focus on regulation that encourages transparency and minimises anonymity.

1) Tax Laws

Clarity needs to be brought into the tax laws in terms of when investors should pay capital gains. The USA has been quite quick to ensure that crypto-to-crypto transactions are now taxable and not just crypto to Fiat currency transactions. This is not the case in the UK however, where things are less clear and will become even more so, once crypto currencies start to introduce dividend like behaviour.

2) Reserve requirements of exchanges

Most banks and stock exchanges are required to hold a certain amount in reserves in order to survive any major downturn or crash. This should most certainly be the case for crypto currency exchanges too especially considering the volatility which sees crashes of 60% several times a year with some crypto currencies falling 90% before recovering. This is also known in part as systemic risk which could be what the Japanese financial regulator defines as system risk.

3) System risk management

As we have seen from this Japan story, one way of ensuring more protection and reliability is by ensuring there is regulation around system risk management on exchanges. There should be minimum requirements protecting against hacking, phishing and other cyber related attacks. The requirements could be scaled against value of the exchange, number of users or number of daily transactions.

It's important to note that much is being done to reduce the risks of hacking incidents such as the concept of a decentralised exchange. This would essentially be a crypto currency exchange on the blockchain, much like the crypto currencies themselves. This

would reduce hacking significantly and whilst it is not currently practical, it could be the standard of the future.

Self-Regulation

The Crypto Currency market gets a lot of negative publicity and much of this could be rectified if there was more self-regulation. It would also reduce volatility within the market and bring about positive change. This refers to both exchanges and ICO's alike.

The Japan Blockchain Association (JBA) for example has established self-regulation standards which includes the use of cold wallets amongst its 15 crypto exchange members (of which Coincheck was one of them) and are now looking to strengthen the standards further following this recent incident.

Risk Management in the Crypto Currency Space

Risk Management, as with all organisation's, plays a vital role in meeting and exceeding objectives whilst providing resilience and stakeholder confidence. Exchanges and companies that are raising/have raised ICO's should ensure that Risk Management is part of their business. Identifying risks and opportunities, assessing them and implementing response plans should be standard. Cyber risks, reputational risks, operational risks, system risks and strategic risks should all be considered and prepared for, which would minimise market disruption and reduce the likelihood of financial ruin. At the very least they owe it to the investors who have funded them.

For investors, with volatility so high, the rewards are great but so are the risks. Investors should ensure that they only invest what they can afford to lose, do their due diligence on their investments which includes understanding the technology, the team and look for a

prototype rather than a wild concept. Additionally, investors should always be on the lookout for phishing scams and suspicious emails.

Finally, even the most optimistic investor should at least consider that crypto currencies are a speculative bubble that could burst.