PiperAlderman

Article Information

Author: Michael Bacina
Service: Blockchain

The 4 biggest security issues you need to understand before buying cryptocurrency or tokens

Cryptocurrencies are finally getting significant press coverage as their prices rise and create huge gains for early investors. But there are some key security issues that any investor needs to consider before getting into this market.

Cryptocurrencies are finally getting significant press coverage as their prices rise and create huge gains for early investors. But there are some key security issues that any investor needs to consider before getting into this market.

Michael Bacina, Partner discusses.

How big is this market getting?

The combined market capitalisation of cryptocurrencies and associated tokens has drifted above US$100 billion dollars with a daily volume in the three largest currencies (Bitcoin, Ether and Ripple) of over US$1.5 billion.

Token Sales

In recent weeks and months a staggering number of token sales have raised mind boggling amounts of money in incredibly short periods of time for businesses with little more than a whitepaper and a moonshot goal.

Some significant token sales in 2017 include Aragon raising US$25M in 15 minutes, Tezos raising US$232M and Bancor raising US$150M in only 3 hours. Despite the risks in the cryptocurrency token market, the secondary market for tokens have seen initial token investors make significant returns in many tokens.

For example as at today Tezos tokens are almost double their debut price:

So, how do I get a piece of this action?

By now, a whole lot of regular folk without much knowledge of cryptocurrency are seeing these massive returns on tokens and cryptocurrencies and want to get in on the action. People have figured out how to buy some Ether or Bitcoin (using an exchange like BTC Markets or an agent like CoinSpot) and are ready to support a token sale/try to gamble their money on a token issue.

But, before **you** dive in and risk your hard earned cash on a token sale (or more concerning, your superannuation) there are four critical security issues that you need to understand. These risks are very real, and in the unregulated and irreversible work of blockchain, you can and should take steps to protect yourself. Obviously none of this article is financial advice and you should only invest what you can afford to lose.

Risk 1: Fake addresses

If you are going to participate in a token sale, you're going to need to manually type the web address of the page you are going to visit in order to send your crypto currency for tokens.

Don’t use hyperlinks.

This may seem annoying (it is!) and pretty technologically backwards (it is!) but there are so, so many examples of individuals who were fooled by fake twitter accounts and fake websites using misspelled URLs (particularly for myetherwallet.com) and of course, those sites provide fake payment details that go somewhere other than where the user was expecting. And once money is transferred to a cryptocurrency wallet it’s gone and cannot be retrieved.

Over time, as “Web 3.0” deployment really gets underway, solutions like the Mist browser and platforms offering better security for token sales will help address this problem. Until then, the only safe solution is typing in the address yourself. Some say to use Google and check the issuer website, but nothing beats typing it yourself.

Risk 2: Fake wallet details

This one is a bit harder, as seen in the recent CoinDash incident, if a hacker gains control of a website and changes the wallet address during a token sale, then the funds sent to that wallet address are gone.

There isn’t much you can do on this one right now, other than to read everything available in background about any token issuer and decide whether you trust their backend security and to check Etherscan.io to see if anyone has reported that the address is a scam.

There are services setting up token sale platforms which are advertising a greater emphasis on the security of the sale which may provide more comfort but this is a “black swan” risk anyone in token sales currently faces.

Also gaining more popularity is the Ethereum Name Service which effectively replaces the 20 character wallet address string with a domain name word, again providing some greater certainty but in doing so creating a risk that someone will make a misspelling of that domain (see Risk 1 above!).

Risk 3: Market manipulation

The recent “flash crash” of Ethereum on the GDAX market highlights that these immature marketplaces have significant manipulation going on, likely on a regular basis.

In my opinion any person investing in this market using margin trading or using stop loss strategies is playing with fire. In a traditional, highly liquid market, these are valid ways strategies to manage risk, but the “flash crash” was mostly driven by 800 or so margin calls and stop loss orders which functioned precisely as programmed in the face of a market with barely any buy orders, dropping the price to 0.10c at one point before it rebounded.

So, be very, very wary of margin loans or stop-loss orders.

Risk 4: Hot wallet risks

One of the biggest risks I see newcomers to cryptocurrencies exposing themselves to is leaving their funds on the website on which they bought them. Doing so leaves your funds in a ‘hot wallet‘. If the website holding your hot wallet is hacked, you may lose your funds and if the company running the site goes down (or is located offshore) you will have little practical recourse to sue the operators for not properly securing your funds.

It’s painful and annoying to do, but you really, really, really, really need to learn cold storage as soon as you own any cryptocurrency and ideally you should be considering purchasing a cold storage wallet (the most popular is Trezor and there is a handy guide to using it here). You can also create paper cold storage wallets or just download your currency to your computer. Any of these are safer than leaving your money online. Recently I was at an event where the presented asked a crowd of 200 odd people “how many of you own cryptocurrency?” – almost every hand went up. In response to the question “how many keep their currency in cold storage?” only three hands went up.

So learn about cold storage and use it.

What’s next?

The token market will continue to be volatile, as will the cryptocurrency market, and with dozens and dozens of token sales coming up, there will be no shortage of opportunities.

Let’s hope that security will get a greater focus from those at the backend and that money lost will only be from incorrect investment choices, rather than a redistribution from those with less security knowledge to those with more.

It’s easily within your hands to get a cold storage wallet, type in those URLs if you want to take part in a token sale, keep an eye on the wallet addresses advertised and to steer clear of margin lending and stop loss orders to at least manage some of the risk.

Good luck.

Disclaimer: The author owns cryptocurrencies, and none of the above is, or is intended to be, investment or financial advice.