Can You Trust the Price? What's behind Crypto's Irrational Buoyancy

"Markets can remain irrational longer than you can remain solvent." – John Maynard Keynes

A banking executive asked me a question last week as we discussed the latest round of irrational pricing in the crypto markets.

"What's the only thing backing virtually any modern currency, crypto or fiat?"

Although he is two steps from a national bank's C-suite and I'm a VC expert in corporate law, we agreed 100% on the answer. I'll bet you do too, because if you have a basic economic education, the answer is obvious: *Trust*.

You could argue that based on the deliberate decentralization of governance in blockchain and crypto, trust has a different definition for those of us in the crypto world than it does to my tightly regulated banking friend.

To that I would say, the mechanisms may differ, but in the end, trust is trust, and the entire point of cryptocurrency's existence is our need to be able to trust in the independently verified value of our money, regardless of its form.

Three recent events are causing me to question the rationality of crypto investors, and the stability of the crypto marketplace and governance. While they have not shaken my ultimate trust in blockchain technology and cryptocurrency as a revolutionary example of decentralized governance, they do leave me shaking my head.

Tether's Serious Valuation Issue & Governance

Tether came clean, after being drug into court by New York State regulators, admitting that they only have 75 cents backing every Tether Coin, while courting investors by still touting a 1:1 USD stablecoin valuation.

Remember, the attraction of stablecoin is its bid to bridge the gap between crypto and fiat currency by attaching a 1:1 valuation to a reserve asset, thus lowering volatility.

This not only makes reserve asset backed coins attractive to buyers by reducing the wild highs and lows of, for example, Bitcoin. In theory, it also makes them more user-friendly to everyone from a bank to your corner grocer.

Because they can trust it.

It's why we've seen a stablecoin explosion with Gemini Dollar, Paxos, USD Coin, True USD, etc.

But stablecoin must be solidly backed by its reserve asset, and independently, rigorously, and regularly audited. Otherwise, trust in the currency erodes.

As I reported in my earlier article on Tether's governance mess, Tether's leadership made a series of suspect moves that could point to them being more concerned about shielding themselves than protecting their asset and their users.

They went from promising full and independent audits, to hiring a firm to do what amounted to not much more than a press release claiming the coin was stable, to surreptitiously removing its own internal guidance statement on independent audits from its website.

Are these the actions of a trustworthy entity?

I can't speak to Tether's motivations: those are up to the New York courts to decide. But I can say that if I had a client make the moves Tether's leadership made, I would worry. Their behavior is exactly the kind that makes some jurisdictions still consider cryptocurrency highly suspect, which will only lead to more regulatory oversight.

So, you'd think when the news of their scandal spread, Tether would tank, right?

A month later, it's still trading at $1.00, as if it was still backed 1:1.

Komodo's Broken Wallet

We hear a lot of jokes these days about "Big Brother," but Komodo's recent "fix" to protect their users' privacy and currency would be right up Orwell's upside-down oversight alley.

Essentially, Komodo's leadership used the very same vulnerability in the Agama wallet they were trying to protect their users from, to commit some hefty pickpocketing.

They went into all of their users' Agama wallets and took their coin, amassing some $11.84 million KMD and $750,000 BTC, ostensibly to keep hackers from exploiting the crack in the wallet's armor, so those bad actors wouldn't steal the coin.

Aside from the giant allocation mess they've just created for themselves – because who can say which asset belongs to whom, since Komodo is a privacy coin BTC fork – they've opened up a host of ethical, governance, and regulatory issues.

Was Komodo's leadership protecting their users' rights, or their asset? You can read more about Komodo's headaches, here.

And, if the governing body of a cryptocurrency felt, even with the best intentions, that they had the right to swoop in and protectively seize millions in coin, do their rights trump those of their contracted users?

At this point, I'm wondering who you should be more afraid of: the hackers or the asset developer.

So, thousands of Komodo users are now at risk of losing their coin, and possibly their privacy, as leadership struggles to recover some of its tattered reputation and shift users to other wallet options.

You would assume that Komodo would see a massive fall-off in valuation after such an erosion of trust. Yet, Komodo's market price has inexplicably risen.

Lord of the Zcoin: One Sigma to Rule Them All?

Zcoin is a privacy coin that used its own distinct privacy protocol, dubbed the Zerocoin Protocol, to differentiate itself from ZCash and Horizen's zero-knowledge protocols that hide user data and allow users to purchase coins anonymously.

Specifically, Zerocoin was designed to allow you to move a public ledger coin to a private wallet, protecting the identity of the owner. However, there is a flaw in the Zerocoin Protocol that renders any expectation of privacy for Zcoin users worthless.

And the insistence on calling the protocol's failure a cryptography error, rather than a code or human one, seems to be slapping a new name on their mistake to make it seem somehow less odious to the public.

We may never know if the error was in the cryptographic algorithm, in key management, or in some other area, but in a recent interview, I believe Zcoin's founder, Rueben Yap, provides a clue. Keep reading and I'll explain.

If the very reason your coin is valuable – its privacy assurance – is breeched, you would think that the price would plummet. Instead, like Komodo, Zcoin has risen from its mid-May 2019 low of $7.22 to hold steady between $11 and $12.

And if that's not strange enough, when Rueben Yap took to the internet via various interviews to reassure Zcoin's users of the stability of their upcoming "greatest ever" privacy protocol – the Sigma Protocol – the story only gets stranger.

Zcoin leadership acknowledges that there is no longer an expectation of privacy with their cryptocurrency, and are urging users to remain patient while they put the mysterious Sigma Protocol through its paces in Testnet and Mainnet testing (due to conclude mid-July 2019).

Which to me sounds like they're selling promises they don't yet know if they can keep.

And almost as if he wanted to reinforce my cynicism, Yap gave an interview to hackernoon that is one of the weirdest things I've ever seen.

Specifically, Yap states that the Zerocoin Protocol was based on decades-old open-source code from a competition in 1991, that he and Zcoin's leadership trusted had been broken apart by its original developers and disposed of.

And I kid you not, he said they disposed of it "Lord of the Rings-style" by entrusting 1/6th of the code key to each of six developers.

Who then promised to destroy their portion of the Zerocoin "One Ring."

> "*It's kinda like they split the key up into 6 pieces like splitting the ring up. Then each of them destroys their part of the ring as long as one person destroyed their part of the ring, it can never be made whole again.*"

So, in case you are as confused as I was initially, what this boils down to is that Zcoin's vaunted privacy protocol, which was also used by PIVX, Gravity Coin, and VEIL, was based on a bunch of coders and developers promising to destroy their back door into the system.

Once again, the entirety of a cryptocurrency's distinct value was based on trust, and that trust was broken. Although in this particular case, I can't begin to understand Yap's expectation that a developer would destroy his only way back into the system he created.

Which is why I will not hold my breath over when their Sigma Protocol will launch.

Further, it's why I am again scratching my head, attempting to understand the vagaries of overenthusiastic Zcoin investors. Because while Zcoin has surged and held, VEIL bottomed out in May and has not recovered.

What does this mean for Crypto Insiders?

What this tells us is that there is a disconnect between reality and market prices. What this means for valuation remains to be seen, and as I said, my faith is not shaken, although my rational mind is.

So, I'll leave you with this poker adage: If you're at the poker table for more than five minutes and you don't know who the sucker is – you're it.

SOURCES:

https://support.komodoplatform.com/support/solutions/articles/29000029932-agama-security-announcement

https://www.crypteron.com/blog/the-real-problem-with-encryption/

https://hackernoon.com/zerocoin-protocol-sigma-protocol-and-privacy-coins-7761db50a0c2

https://cryptoslate.com/zerocoin-exploit-found-zcoin-attacked-other-privacy-coins-at-risk/

https://www.chaac.tf.fau.eu/2018/04/12/zerocoinzcoinpivxzoinsmartcashhexxcoin-attack/

https://zcoin.io/#

https://www.nasdaq.com/article/know-your-coins-public-vs-private-cryptocurrencies-cm849588

https://zcoin.io/zcoin-development-update-27-may-2019/