KCS Group Europe

Cryptocurrency: Step right up for a miracle?

December 2022

As the pioneers and settlers spread out across the Wild West, a new type of person sprang up in the saloons and squares of the new world: the snake oil salesmen. These charmers would offer tonics promised to cure absolutely any ailment, for an unbelievable price, in a deal that the good townsfolk would be mad to pass up. Invariably, their product would be a total sham – but if the snake oil salesman could hightail it out of town with his gold before the locals found out, all he had to do was make it to the next one down the road where the whole process would begin again. And arguably, so it is with the modern-day equivalent of cryptocurrency – a lie always travelling faster than the truth.

Cryptocurrency is a broad church, but at its heart was the idea to create a series of decentralised financial networks that were not dependant on a governmental - or central - authority, and through which the creators of various digital coins could act independent of concerns over pegging the value of these to standard dollar or sterling-based metrics. It largely emerged from the new-millennium thinking that the Internet should offer greater freedoms and independence for all its users in as many forms as possible. Admirable thinking perhaps in an age of increasingly creeping suppression and control, but in retrospect the fault lines were glaringly obvious from the start: a practice with no official oversight or control, in which the major players have absolute autonomy to act as they see fit and without any compulsion to act honourably or even openly. Even the creator of the most famous cryptocurrency of all, Bitcoin's Satoshi Nakamoto, remains pseudonymous and anonymous. How could this world lend itself ultimately to anything other than fraud?

And lend itself it did. The number, variety, and losses involved in cryptocurrency scams are staggering in all three respects. Most recently, the collapse of crypto exchange FTX saw US$3.1bn owed to creditors after it was forced to declare bankruptcy, and while there is currently no direct evidence that former CEO Sam Bankman-Fried was knowingly defrauding investors, federal investigations are expected as to his mishandling of a US$32bn empire – and those with money locked in the digital wallets of the collapsed company are, if history is anything to go by, extremely unlikely to get their investment back. Others are far more blatant.

Consider Dr. Ruja Ignatova, whose own personal brand of digital snake oil – OneCoin – was worth US$25bn in customer investments despite the OneCoin token itself never existing at all, being under the leadership of individuals previously engaged in pyramid frauds and Ponzi schemes and being cited as fraudulent within a year by multiple European authorities. (Dr. Ignatova herself has disappeared and is now resident on the FBI's Most Wanted list, although it is not believed that she will surface with her old name and appearance again.)

Bitconnect's founders managed to launch a crypto scam based around a non-existent world-beating algorithm not once, but twice, making off with at least US$4bn. Faruk Fatih Ozer of Turkish network Thodex, offered an apparent swap deal of exchanging a user's cryptocurrency for 'Dogecoin' (a cryptocurrency created as a joke that invariably wound up being immensely sought-after) but froze the accounts of his clients, leaving them worthless, and got out of Dodge with US$2.2bn of their money just two days ahead of an arrest warrant.

Each of these three cases focused on a different aspect of the crypto boom – a coin itself, an algorithm, or the 'fear of missing out' – but all saw their founders exploit not only their victims, but a set of circumstances and opportunities that make crypto the prime vehicle of the day for scams. An unregulated, decentralised network whose proponents are either untraceable or unaccountable does not lend itself to confidence. And yet, driven by arrogance, over-confidence or greed, time and time again, coin offerings and crypto ventures manage to secure huge backing and, more often than not, are revealed as not cure-alls, but end-alls.

It is estimated that 98% of ventures in the cryptocurrency sphere either end up in bankruptcy or are revealed as scams. Even cases of real-life tragedy are not immune: after the 2018 sudden passing of Quadriga founder Gerald Cotten, the only individual able to provide access to approx. US$250m in digital wallets that were now 'cold' and inaccessible to his clients, there were rumours that he had faked his own death and started a new life with the money. The truth about Cotten remains unknown. Although there certainly is evidence, he was not entirely clean, faking his own death has not been proven. Certainly, some cryptocurrency ventures are genuine in the sense they are intended to provide a safe haven and alternative for those who believe that neither traditional monetary systems, nor the governments with whom they share a symbiotic relationship, can be trusted – but equally so many are fraudulent for precisely the same reasons. It is less a case of the system allowing them to be corrupt, more that the problem is, there is no system at all. And the truth is, that this may not even be the worst of it. For some, cryptocurrency is a genuine innovation that is being misused. For others, it is a get-rich-quick scam preying on the wealthy, over-confident or naïve. But it is increasingly being used by criminal gangs and rogue nation-states alike in large-scale crime and money laundering – even to the point of funding terrorism.

The anonymity conferred on any party that wishes it in the crypto-world, combined with the decentralisation and freedom that arises from the aforementioned lack of system, means that Organised Crime Groups (OCGs) and terrorists can move amounts in the billions from 'real money' to crypto, and thence onwards to as many accounts as they wish via 'blockchain bridges', through which it is extremely difficult to trace both the original provenance and ultimate destination of the funds, let alone the actors involved. Extremely difficult – but not impossible. It is apparent that one such tool, RenBridge, has been used to launder over US$500m gained from fraud, much of it believed to have associations with Russian mafia groups.

Approximately US$8.6bn was laundered through cryptocurrency in 2021 (a 30% upswing from the previous year), and with the crypto realm providing such fertile ground, is expected to 'professionalise' further. For instance, Europol has advised that professional money launderers are now carving out a crypto offering directly to their clients, promoting it above traditional laundering means, and what was previously used primarily by rogue regimes such Iran and North Korea to circumvent sanctions, on the basis it was so obscure and little-understood that their odds of going undetected were favourable, has now gained mainstream acceptance by both the criminal fraternity and their pool of victims. This is a dangerous combination. Moreover, the third wheel – the authorities – are slow to catch up. While anti-money laundering frameworks (particularly in Europe) are being strengthened, and Congress' latest amendments to the Money-Laundering Act are intended to subject the crypto-sphere to the same rigour and scrutiny as other means of potential laundering and crime, the problem remains that authorities are regularly running to just catch up.

As the global financial crisis continues to bite, and the spectre of a potential conflict with Russia, China or Iran looms large, it can be expected that increasing numbers will turn to cryptocurrency as the equivalent of doomsday 'preppers' buying tranches of remote New Zealand wilderness: something aimed at riding out the storm, no matter what. But all should be mindful that the snake oil salesmen of the Old West needed two things: the ability for the lie to outpace the truth, to be sure, but also a willing audience ready to be spun a tale without looking too closely at the man behind the curtain. After all, if something looks and sounds too good to be true, it invariably always is.