

Tech evangelism: for whom we are about to deceive...

December 2021

If a tree falls in the forest and nobody hears it, does it make a sound? Or to put it in more modern terms, if a cryptocurrency partnership deal collapses because there was nobody on the other end, did you really have a deal? This curious eventuality happened to Manchester City FC last month, when a tie-up with crypto firm 3Key collapsed after only two days following fan-led internet research revealed that the firm had virtually no presence or substance.



While the putative partnership remains suspended, Man City surely have some serious questions to answer over how matters progressed this far in the first place. But they are far from alone in becoming entranced by the cryptocurrency industry; and – although no insinuation is made against 3Key – may have had a lucky escape.

Man City are not the first football club to fall into the crypto well – seventeen Premier League clubs have some form of arrangement with a crypto firm. This industry has been flirting on the edges of fraud & corruption for some time now, with reports of ‘wallets’ and their creators disappearing and investors losing hundreds of thousands in virtual currencies, or ransomware attacks where payment is demanded in Bitcoin or the like, all the better to preserve the anonymity of the perpetrators and exploit an already unregulated sector even further. Neither are they the first to withdraw from a deal, with Barcelona also abruptly terminating a partnership in November 2021 with the firm Ownix after its CEO Moshe Hegig was arrested on suspicion of fraud and financial conspiracy. This deal related specifically to the expression of ‘Non-Fungible Tokens’, or NFTs – ownership of a digital token related to an item. Not owning the item itself, just a digital asset to represent it. There have been multiple instances of NFT scams whereby a project creator, holding the purse strings, suddenly vanishes and the project is revealed to have been built on foundations of sand – most notably the ‘Evolved Apes’ scam of recent months where almost \$3 million was spirited away by a now unreachable creator.

It is not only theft conducted through such measures – it is undeniable that cryptocurrencies make money laundering and terrorist financing far easier, given the borderless nature of online transactions and the pseudonymity that is such a selling point of crypto. Over £300m GBP of laundered cryptocurrency was retrieved in the UK in just two operations, in June and July of this year. Not every cryptocurrency or NFT will be fraudulent, of course, but everything about such an opportunity screams ‘red flag’. And yet the pace

of cryptocurrency & NFT adoption continues to grow. 'Crypto evangelists' is how adherents view themselves, and this word is extremely appropriate, given that the obsession sometimes verges on the religious.

Like religion, 'the blockchain' is held in reverent awe. Like religion, the flaws are clear to see but pointing these out is considered offensive and baseless by the disciples. And like the worst excesses of religion - the snake-oil preachers and useless relic sellers – it is the very mechanism by which exploitation occurs.

All this being said, why are such dubious practices still in high demand? For the digitally-driven, younger generation it is the dreaded acronym 'FOMO', or 'Fear of Missing Out' – that not latching on to trends or hypes now will come back to haunt you, and that the compulsion is to go along with the crowd – something assuredly manipulated by the scammers. Alternatively, for others it is the necessity of having to engage with these business practices in order to do business of their own. And for a third group, it is the simple idea of 'better living through tech' – the conception that something is inherently better because of its digital nature (see the cashless society, driverless cars, the metaverse...) and so something is embraced despite its very clear flaws.

This is the trap that businesses must take care to avoid. Deeper integration with future-facing tech measures such as cryptocurrency and the blockchain is almost always unnecessary, and frequently a danger because of its very nature. Particularly in these difficult times, pressure to adopt something which is superfluous at best and an outright invitation to scammers at worst, needs to be avoided. And if an opportunity does come up, then under no account should it be pursued without extensive diligence and scrutiny – without the fear of offending those whose evangelism blinds them, perhaps purposefully, to the failings of what they are selling. *Amen* to that.

KCS Group Europe - Strategic Intelligence & Corporate Security

A leading provider of security and intelligence services, we operate discreetly in some of the world's most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients identify and deal with any risks, weaknesses and threats which could impact on their business, financially or reputationally.

Our key areas of expertise include:

Corporate Intelligence Services - New market or sector entry research - Know your customer screening

In addition, through our specialist team at KCS IS, we offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits - providing unparalleled analysis, contingency planning, and implementation.

To find out more or to arrange a meeting to discuss your business needs, please email the team at info@kcsgroupeurope.com or call (00 44) 2072451191.
