

What goes up, must come down. (Unless it keeps going up).

By Mark Laing

Bitcoin has been poking its face into the mainstream media again last week, after the market price of a ‘coin’ rose by 50% in a month – almost reaching its 2017 all-time high of £15,000 – before falling away again to around £12,500. The price is currently even more volatile than usual and so there’s every chance that, by the time this article goes live, there will be another chapter in this latest tale of up-and-down.



Even if you don’t follow the fluctuating cryptocurrency market, you may be subconsciously aware of big price rises because they tend to bring with them a much more visible trend: scams, aimed squarely at the kind of people who don’t know a lot about the subject.

Have you seen the social media posts, masquerading as news articles, in which a popular TV celebrity is talking to an interviewer about their recent investments in cryptocurrency - “*Ant and Dec DOUBLE their personal fortune in six weeks with bitcoin!*” - and so on? Or how about the emails that urge “*Don’t miss out on the Bitcoin price rocket!*” along with a link to a trading website where you can jump onboard the hype train?

While most of us will roll our eyes and click the ‘spam’ button, it is the unfortunate truth that many people are drawn into these stories of instant riches and find themselves defrauded of huge amounts of money. We recently investigated a case in which a professional investor lost around £120,000 after he signed up to what looked like a legitimate cryptocurrency trading platform, only to discover it was operated by conmen.

Financial scams are just the tip of the iceberg when it comes to cryptocurrency and crime: terrorism funding, large-scale drug distribution, blackmail, ransomware, and child abuse on-demand... All have horrific consequences for victims, and all perpetrated by those who seek to abuse cryptocurrency as a way of making money.



Criminals choose ‘crypto’ because it offers anonymity, but the truth is that most of it is not really anonymous at all; it is ‘pseudonymous’ at best. There are defined lines of enquiry. Over the last three years, we at BLD have developed a clear investigation strategy to help investigators trace and de-anonymise the users of cryptocurrency.

Earlier this month, bitcoins worth \$955 million, known to be linked to a long-closed drug marketplace called The Silk Road, were moved to an 'anonymous' address. Roughly 48 hours later, with the assistance of crypto-investigators at Chainalysis, the US authorities successfully seized these bitcoins after identifying the custodian.

Whether your work involves criminal investigation, asset recovery, financial compliance, or civil conflict resolution – you need to understand the fast-growing world of cryptocurrency and how you can work with it. Our resident crypto-specialist, Mark Laing - a former cybercrime detective and certified training partner of Chainalysis themselves - delivers a range of training solutions, from one-day awareness seminars to our City & Guilds Assured Cryptocurrency Investigation training course. See website for more details!