Andrew Brookes via Getty Images

FRAUD

As cryptocurrencies surge, so do the scams

The number of investment frauds involving digital assets such as bitcoin has rocketed in recent months. But authorities are striking back with some success

Alex Wright

Fuelled by celebrity endorsements, cryptocurrencies have soared in popularity among investors over the past year. Unfortunately, the fraudsters have noticed this trend.

The number of crypto scams in the UK has more than doubled over the past year. A record 720 cases were identified in January alone, according to Action Fraud, a British reporting centre for cybercrime.

This figure is likely to be the tip of a global iceberg. In the US, for instance, the Federal Trade Commission reports that the number of bogus investment opportunities grew 12 times over between October 2020 and May 2021, causing almost 1,000% more in losses than the total reported during the equivalent period of 2019-20.

Worse still, a report by the Bank for International Settlements in 2018 estimated that a quarter of all initial coin offerings (ICOs) could be fraudulent. It based this finding on information gleaned from newspapers and white papers – and on the percentage of cryptocurrency websites that had been discontinued after their ICOs.

The problem has become so prevalent that the UK's Financial Conduct Authority (FCA) has warned investors buying cryptocurrencies that they should be "prepared to lose all their money". Other finance industry regulators around the world have issued similar caveats.

"There has been an exponential growth in cryptocurrency-related fraud in recent years," says Sam Tate, partner at international law firm RPC and head of its team dealing with white-collar crime. It recently requested data from the FCA under the Freedom of Information Act 2000. This revealed that investigations into unauthorised cryptocurrency ventures had risen from zero in 2016-17 to 52 in 2019-20.

"It's the type of risk that everyone should be worried about, whether they're a small investor or a giant bank," Tate says.

Cryptocurrency fraud has become a global business conducted by perpetrators ranging from state-authorised hackers to international criminal gangs, he adds. "National boundaries aren't respected when it comes to cryptocurrency fraud. This makes it even more difficult to track and tackle the problem."

The classic crypto fraud occurs where investors are targeted by criminals offering the lure of a get-rich-quick scheme that is in reality a Ponzi scam. Using fake websites, mobile apps, emails and social media adverts, they trick investors into handing over their money with the promise of eye-watering returns, which never transpire.

There are several variations on this common scam. They include fake social media accounts, where criminals impersonate celebrities to encourage investors to participate in fraudulent investment schemes. For example, the accounts of high-profile Twitter users – including those of Joe Biden, Barack Obama and Elon Musk – were recently hacked, offering giveaways aimed at duping followers into investing in a fake bitcoin scheme. Other examples include two-for-one scams, which promise investors they can double their money by sending their cryptocurrency to a wallet, from which it is then stolen.

Then there are exchange hacks – where criminals exploit weaknesses on exchange platforms to steal funds – and rug pulls, in which crypto developers list a token, encourage parties to invest and then run off with the tokens and exchange these for a more stable currency. Other popular tactics employed by fraudsters include setting up an exchange to take investors' money, which then can't be withdrawn.

Some even use phishing to take over an investor's wallet before stealing their data and credentials. This could be done through a Sim-swap attack, "where fraudsters trick the customer support staff of cellphone operators into giving them control of someone else's phone number", says Mriganka Pattnaik, CEO and co-founder of blockchain transaction company Merkle Science.

Alternatively, scammers might use fake messages that appear to come from trusted businesses. "The messages will convince users to visit a link that they control and enter their log-in credentials, which are then stolen," Pattnaik says.

In all of these scams, the investor will often never see their money again. And, by the time they realise what has happened, the fraudsters are long gone.

"Like any new asset class with the potential for high returns, there is the risk that fraudsters will try to take advantage of it," says Tony Lewis, a partner in the dispute resolution team at law firm Fieldfisher. "At the same time, cryptocurrency is unregulated, so it's easier than traditional bank accounts and other authorised investment schemes for fraudsters to exploit."

The problem has been exacerbated by the rise in older investors trying to obtain better returns on their capital while interest rates on savings are so low. The number of over-55s buying cryptocurrency tripled between 2019 and 2020, according to the FCA. The elderly and vulnerable are easy prey for old-fashioned telephone scams, too. In total, £113m was lost to cold callers and other criminals promoting fraudulent crypto investments last year alone, according to data seen by the *Investors' Chronicle*.

Even more experienced investors have been stung. Apple co-founder Steve Wozniak lost the equivalent of $70,000 (£50,000) when fraudsters bought seven bitcoins from him using a stolen credit card, which they later cancelled.

Because criminals often operate undetected, law enforcement agencies and financial watchdogs have either been largely powerless to prevent many of these scams or been overwhelmed by the sheer volume of cases. And because courts were operating well below capacity during the pandemic, there is a huge backlog of cases waiting to be processed.

But there have been some successes, notably when the Federal Trade Commission obtained a settlement against a scheme named the Bitcoin Funding Team, recouping almost $500,000 of investors' money. The scheme's promoters had falsely promised that participants could earn large sums by paying cryptocurrency to enrol in a chain referral scheme, but never delivered.

Tate believes that the authorities need to come up with an advertising campaign that warns of the risks associated with cryptocurrencies. A more joined-up approach among regulators to tackling the problem is also required, he adds.

"They need to target the kind of people who are likely to be interested in these types of schemes," Tate says. "The UK's National Crime Agency does a lot of advertising about this subject on social media. But, if there were an internationally recognised kitemark of approval for some of these currencies, it would go a long way to tackling the problem."

Investors can find it difficult to distinguish reputable cryptocurrency providers and schemes from bogus ones, especially given the perception that cryptocurrencies are largely safe, with retailers such as Starbucks and Whole Foods accepting bitcoin payments.

This means that investors must do their due diligence on the product and company they are investing with and where their money will be kept, relying on trusted news sources for their information and using only recognised exchanges that give them full access to their funds.

Investors can also use software such as Chainalysis KYT to analyse and verify transactions, identifying illicit activity, suspicious wallets or connections to the dark web, says Jacob Sever, co-founder and chief procurement officer of Sumsub, a verification specialist. A high risk score highlights unreliable sources that shouldn't be accepted, he adds.

Big companies are doing their bit to counter the scammers. Facebook and Google have both banned bitcoin adverts on their websites, for instance, while NatWest now directs its mobile app users to a warning screen advising them to beware of cryptocurrency scams after it saw a record number between January and March 2021.

Nonetheless, there's still a long way to go in the fight against cryptocurrency fraud. "The key message is that investors should do their homework thoroughly beforehand," Pattnaik says. "The rule of thumb is: if a scheme sounds too good to be true, it probably is."

> **The rule of thumb is: if a scheme sounds too good to be true, it probably is**

> **National boundaries aren't respected when it comes to cryptocurrency fraud. This makes it even more difficult to track and tackle the problem**

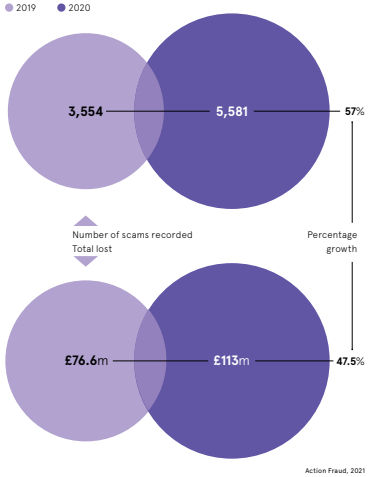
720

cryptocurrency scams in the UK in January 2021 alone, equivalent to 23 a day

Action Fraud, 2019

THE NUMBER AND COST OF SCAMS INVOLVING CRYPTO INVESTMENTS BOTH INCREASED SIGNIFICANTLY LAST YEAR

Data for the 12 months to the end of December 2020



Action Fraud, 2021

Commercial feature

How cryptocurrencies could become a reliable everyday payment method

The price volatility of cryptocurrencies such as bitcoin might make them seem unsuitable for everyday use but newer stablecoins show how blockchain technology could be used for payments in the future

"Paper money is going away." Tesla founder Elon Musk is perhaps more prescient than even his most ardent followers believe. He made the comment in a 2019 podcast, a year before Covid made us all go contactless.

Yet Musk was not talking about the move from cash to card but about cryptocurrencies.

"Crypto is a far better way to transfer value than a piece of paper," he said.

But Musk's vision of this future crypto-world is unlikely to see us all ditch banknotes for bitcoin. In the past year, the value of one bitcoin has fluctuated between US$9,000 and US$62,000. Not great for making traditional payments.

This is where stablecoin comes in.

A stablecoin is a digital token that is transacted over blockchain in the same way as cryptocurrencies but, crucially, backed by a so-called fiat currency, such as the pound Sterling or the US dollar. Notably, the stablecoin model does not require the mining of each token, an energy-intensive process that has seen Musk temper his support for bitcoin.

Tether tokens (USDt), the market-leading stablecoin, is pegged to the US dollar, for example.

This provides a robust method of exchanging value while using a familiar accounting unit.

Much of the enthusiasm for cryptocurrencies – a market worth more than $1.18tn – has focused on the trading opportunity. That same volatility that makes bitcoin less useful for everyday transactions is exactly the sort of volatility that can make you huge gains. Or indeed huge losses.

It is this volatility which has led financial regulators to warn that cryptocurrencies are a bubble waiting to burst.

But perhaps the most exciting use of cryptocurrencies is yet to be realised. The potential for stablecoin to become a payment method for everyday transactions has many vested interests in the cosy and well remunerated world of banks and other financial institutions alarmed.

Tech Daily

Take the credit card industry. In 2019, Visa generated profits of US$12.1bn on revenues of US$23.0bn while Mastercard made profits of US$9.7bn on US$16.9bn. The business of issuing plastic and enabling payments globally is lucrative. They earn from cardholders, through annual fees, interest and other stealthier charges, but also from merchants, such as retail shops and websites, who are charged hefty interchange fees.

They also make money from selling customer data. With increasing concerns around data privacy, many welcome the onset of Web 3.0, where data is shared independent of third parties.

In its 2020 annual report, Mastercard said, "Technological changes, including... cryptocurrency and blockchain technology...could result in new technologies that may be superior to, or render obsolete, the technologies we currently use in our programs and services. Moreover, these changes could result in new and innovative payment methods and products that could place us at a competitive disadvantage and that could reduce the use of our products."

Stablecoins such as tether tokens have the potential to be low-cost forms of payment because the use of blockchain means financial institutions and their eye-watering fees are kept out of the loop. It is little wonder that credit card companies and other financial institutions recognise the existential threat that cryptocurrencies pose.

Developments in cryptocurrencies mean that feeless or very ultralow fee transactions are being enabled, opening up their wider use. Tether tokens, for example, are already increasingly being used for micropayments.

Researchers at Germany's Bielefeld University believe subscription services, like Spotify and Netflix, may embrace the use of such crypto-enabled micropayments to offer access to smaller chunks of content.

It is the young who will usher in this new world.

One recent study of young people in Russia found that more than a quarter believed that, within five years, most stores would accept payments in bitcoin and that, within ten years, cryptocurrencies would be issued by the state and replace cash. In the UK, some 43.6% of millennial investors in a survey for law firm Michelmores said that cryptocurrency was a valid alternative to traditional banking.

If young people have anything to do with it, Elon Musk's prediction about paper money will be proven right and soon.

> **Perhaps the most exciting use of cryptocurrencies is yet to be realised**