Blockchain: Revolutionary technology… or the perfect opportunity for fraudsters

Alice Hello! And welcome to Taxing Matters, your one-stop audio shop for all things tax brought to you by RPC. My name is Alice Kemp and I will be your guide as we explore the sometimes hostile and ever changing landscape that is the world of tax law and tax disputes. Taxing Matters brings you a fortnightly roadmap to guide you and your business through this labyrinth.

In case any of you miss any crucial information - or just want some bedtime reading - there is a full transcript of this and indeed every episode of Taxing Matters on our website at www.rpc.co.uk/taxingmatters.

In recent times it seems that the word Crypto is on everyone's lips. From the ever-exciting adventures of Elon Musk and his effect on the price of Bitcoin to the debate of the value of non-fungible tokens in the art world, to how Blockchain is going to revolutionise the world - or destroy it depending on what you're reading!

As the media darling topic of the day there have probably been twice as many articles warning about fraud as there have been articles singing Crypto's praises, but there will be many among us who will be thinking, "…yes, that's all very well but what does this mean?" Here are to answer these important questions I have three representatives of the founding members of the aptly named "CFAAR" or "Crypto Fraud and Asset Recovery Network"; the world's first global network of lawyers, barristers, forensic accountants, corporate intelligence and asset recovery experts, to develop and share best practice."

Chris Whitehouse is a senior associate at RPC who advises on the investigation of misappropriated assets. Carmel King is a director at Grant Thornton who specialises in asset tracing and recovery for victims of fraud and Dan Wyatt is a partner at RPC who specialises in civil cyber fraud, financial services and partnership disputes.

Chris, Carmel and Dan thank you for joining me and welcome to Taxing Matters.

So Chris if I can start with you, as I said at the outset Cryptocurrencies, non-fungible tokens, digital assets and Blockchain are on the rise but what exactly are they?

Chris I'll start with Blockchain as that is the technology that really underpins Cryptocurrency and more esoteric things like NFTs. Blockchain is an example of something called, "Distributed ledger technology" where, in a nutshell, you have a database and modifications to the database are captured in a log of transactions that are put in blocks by various nodes on the network and each block is cryptographically linked.

Cryptocurrency is a great use of that particular technology. I'll use Bitcoin, just for the sake of ease of explanation. In Bitcoin your database is a list of bitcoins and who owns them. If you have a bitcoin transaction various nodes on the network will 'compete' with one another to solve a sort of cryptographic problem that will allow them to package the transactions into a "block" that gets added to the "chain". As time goes on the bitcoin "blockchain" gets bigger and bigger and bigger as additional transaction blocks are added and the very cool factor about the technology is it resists tampering.

The technicals are complicated but, essentially, it is not possible to tamper with anything without a particular bit of information, without tampering with each subsequent block. Essentially you have a tamper-proof or reasonably tamper-proof mechanism which is decentralised amongst nodes - there is no one authority you simply have a decentralised network that allows you to have a consensus about what the state of the database is at any one particular point in time. So that's "Blockchain".

It's probably also worth touching on "NFT's" because they're so prevalent at the moment. An "NFT" or "Non-Fungible Token" is something slightly different to a bitcoin. Bitcoins are relatively indistinguishable. One bitcoin is as good as another, whereas an NFT is unique. You often see them in digital artwork, for example. An NFT would be a 'token of digital ownership' that shows a certain individual has an ownership right in something. You can trade that ownership token in the same way you would a bitcoin. So, for a piece of artwork you've created a market where it's readily tradeable - you can trace who the previous owner was – and, importantly, it means that the prime copy of a particular piece of artwork is known.

For example, in physical art if you have a copy of the Mona Lisa - and it's the original that has a certain cache value - the NFT would establish a *prime*, "this is *the* digital copy" and there would be some cache value in owning that.

NFTs are interesting because they've got a lot of potential to engage with other bits of the Blockchain eco-system like "smart contracts". To give an example, if you had an NFT linked to a piece of music you could have it so that every time that piece of music was played the owner of the NFT would receive some of the revenue. So it's got interesting interlocking potential with bits of technology like that.

Alice Thank you, Chris, that's very helpful. Dan, turning to you. As with any new technology there are new opportunities for bad-actors to use them for fraud. Has that been equally true for Cyrpto assets and Blockchain technology?

Dan Yes, thanks Alice. It has, but, I think, the first thing to say is that you get fraud in any sector. Crypto is no more, or less, susceptible - in principle - to fraud and to bad-actors and, of course, the consensus principle that Chris mentioned should, actually, guard against fraud because you have multiple different nodes of the network all verifying the position. But, as you say, with anything new, new opportunities will arise and there are plenty of imaginative people in the world to try and take advantage of those opportunities. Particularly at the moment where there is little, or no, specific regulation over Cryptocurrencies in particular. So, we're certainly seeing a huge number of cases, at the moment, coming across our desks where there has been a fraud involving Cryptocurrency in particular. I'd say there's probably four broad buckets that we're seeing.

The first bucket is your standard scam, a confidence trick. Fraudsters gain the trust of victims. The victim will end up paying for a service or product. The Crypto then disappears and there's no product, or service, in return. Often you see that in an investment management kind of setting, where people offer to trade Crypto on your behalf and give you very healthy returns. Normally what happens with these types of scams is that fraudsters are pretty clever and what they'll do at the start is they'll produce some pretty impressive results initially - probably give you some returns even, so you feel like it's going terribly well - and then you're obviously duped into giving more and more until at some point the tap is turned off.

The second bucket is just what I call your, "standard theft' - theft of access codes and passwords, hacking and so forth – and, before you know it, your very valuable Cryptocurrency has vanished from your wallet.

The third bucket is an "ICO-fraud". "ICO's" are, "Initial Coin Offerings" which is what happens when new coins are launched; basically like an IPO in the olden-days. Perhaps the most prominent ICO fraud that many of the listeners will have heard of was the one involving the "Crypto Queen" who was a lady that was behind the "One Coin" ICO which managed to get somewhere in the region of £4 billion of investments as part of its ICO before all of the money and the coins vanished.

The fourth bucket which, in many ways, is the most tragic and most interesting in some ways, is that we're starting to see frauds on frauds. So, we've seen a couple of people who've lost money through one of the three methods I've just suggested, normally one of the first two and they have been enticed to instruct an investigatory firm to trace the stolen bitcoin and find the fraudsters. They'll pay a little bit of money for the initial work, the investigations company will come back and say, "oh, great news! We've found your Crypto its in this account over here, we just need to have, XYZ-fees paid to get it back and release it back to you" at which point those amounts of money are paid. At some point along that chain of conversation it all goes quiet and it turns out that the victim of the fraud has been a victim of a second fraud and there are no recoveries and the investigatory firm turns out to be, itself, run by fraudsters.

One case in particular where the person had spent tens of thousands of pounds recovering Crypto - which is much more valuable - and then, of course, that turned out to be even further losses to the 'black-hole'.

So those are the four buckets that we're seeing most of. Once Crypto is stolen, what tends to happen is that it will be pinged around multiple different wallets and mixed in with other Crypto, both "good and bad Crypto" - the Crypto that's held bona fide and, also, other stolen Crypto. This is done to obscure its provenance and then eventually it will end up somewhere down the chain, normally after tens, or even hundreds, of separate transactions at an exit point; sometimes at a reputable exchange and sometimes it's something lurking in the dark web which is much harder to track.

What you get if you have your ten-bitcoins stolen is actually a hugely complex web of transactions where the bitcoin is split up into little bits, sent around multiple wallets and then you have to follow all the dots to work out where it ended up.

Alice And Carmel what about from your perspective, the accountancy world, what are you seeing?

Carmel We're seeing, Alice, exactly the same things as Dan has just outlined and I think there's been a really significant rise; particularly since March last year.

A lot of people are sitting at home, they're on their mobile phones, they're not really thinking about a huge amount of due diligence – it's just tapping a few buttons, or downloading an app. Particularly seeing ads on the likes of Facebook or social media and initially investing a relatively small amount, something that they can afford to play with, but very, very quickly because there are bad-actors on the other side, finding themselves under water and paying more for what they think will be a recovery.

We are also seeing romance scams, bad-actors posing as recovery specialists or posing as people who can extract the funds.

Ransomware is a growth industry - up 311 per cent in the last year, or so; a reported $350 million has been paid by victims. Now, if that's the "paid-figure" it does mean that the "attack-figure" is going to be far higher if you consider attacks that are thwarted or that are not paid. So, that's going to have been an exponential increase in Ransomware attacks as well - which are not, expressly, to do with Crypto assets, or Cryptocurrencies, but usually the payment is going to be made in that. So, from an asset recovery perspective we're looking at Blockchain analysis and we're looking at recovery techniques for items that have been paid-away in that regard.

Alice Thank you and staying with you for a second, what about the response. Has there been a uniform response from all affected sectors, the courts, enforcement agencies and governments?

Carmel In the last few years there was initially a bit of a barrier to entry, in that there was a thought that all of this belongs in some kind of 'cyber-world' and various departments were quite slow to engage and to realise that, actually, these things are frauds; they're attacks on individuals and on corporate entities and they need to be dealt with.

Taking each of those entities in turn: The courts have been absolutely excellent. It's probably fair to say that the English Court is a world leader in terms of considering the issues that we're dealing with here. As far back as 2019 *AA v Persons Unknown* considered the matter of whether or not Crypto assets constitute property and it came out in favour of the fact that it does, which meant that its capable of being subject to proprietary injunctions.

Some of the other judgments since then and some of the other matters that the court has considered has included applications for freezing orders, to protect Crypto assets that have been identified as being at exchanges and other places; disclosure orders, which will compel the exchanges to provide the KYC data that they have on account holders - which means that the anonymity that fraudsters believe they have when trading, in this kind of world, is no longer something they can rely on. Other issues have been things such as 'service out of jurisdiction', *lex situs*, and only yesterday there was a judgment handed down which considered whether Crypto assets were capable of being held on trust.

Quite a few of the law firms and barristers chambers involved in these decisions and these applications are members of CFAAR so they are very much at the forefront of this. I am pleased to say that decisions have really been coming out in favour of victims of these frauds.

In terms of enforcement agencies, I would say it has been varied. The Met Police are well known for having had two very significant bitcoin seizures.

We ran a series of webinars for the likes of HMRC, the NCA and the Insolvency Service in the last year and we've had a huge level of engagement. Attendance has been four times the level of previous webinars, which means there's a huge appetite to learn about this and some of the questions and the level of engagement was very sophisticated. You may have seen in the last month or so HMRC has sent out nudge letters to holders of Crypto assets to encourage them to pay any capital-gains tax that might have arisen from trading in those assets.

There is work to do and, I would say, on the Government side – it's engaged to a degree. We know that they are looking at the "Britcoin" which, to my mind, is a separate thing, really, from the topic of conversation today, but thinking about protecting people and creating an environment that is more reliable and encourages investment, you've got the online safety bill. Now, that only, really, goes so far. It should prevent victims of Crypto fraud by social media posts. It is a very significant gateway. People are clicking and offering £250 to something that quotes the "Richard and Judy show" because that's what gives it credibility rather than actually being a regulated asset; and it should also help with false investment opportunities. However, the online safety bill doesn't deal with advertising, doesn't deal with fake emails - I don't know about anyone else, but Rob Bryden has been emailing my spam on a regular basis encouraging me to invest in bitcoin - and it also doesn't deal with 'clone sites' which is where the bad actors are increasingly posing as recovery specialists. So there's a lot to do there.

The FCA is at the pre-regulation stage and firms who want to be involved in this space are very much engaged on that so that's a very good thing.

Finally I would say that, there is talk of extending the Proceeds of Crime Act to specifically include Crypto assets. POCA has been used for restraint seizure and to recover assets as much as a year before *AA v Persons Unknown* came out, so there has been pretty innovative use on that one as well.

Alice Thank you, Carmel. Dan, with that background, RPC and Grant Thornton are founding members of CFAAR. Can you tell us a bit more about CFAAR is and why it was created?

Dan The idea started because, as practitioners, we're pretty used to attending various industry and sector forums and groups and conferences and the like on pretty much every topic you can image. They're a really great forum and a source for learning for the industry and to build contacts so that when something happens and you need to act pretty quickly you know who to call to get a team together; but there wasn't anything in place for Crypto. In one sense that isn't altogether surprising because it's obviously a very new area - particularly in the legal world. By this time there had been a number of Crypto judgments, so it was clear that these disputes were coming and were being heard and were on the rise so that a similar network relating to Crypto would be useful. So we saw a gap.

We were very focused on building a network that was full of the brightest and the best in this area so we, carefully, spoke to various people to join as founder members to ensure that we had that real deep knowledge and expertise in the sector and also diversity of experience. So, we are not just lawyers, solicitors and barristers, we also cover other elements of the legal process.

As soon as the founder members got together, I think its fair to say there was a real 'buzz' at the network - and I think a unity of intention of what we wanted to achieve - and we wanted, really, to build a network of global professionals working in this sphere to join a community which holds meetings, seminars, roundtables, to develop everyone's skills, generate ideas and also network. So, as I said, you know who to call when an urgent Crypto fraud case comes in.

We also wanted to create a network which would have a strong voice when it comes to judicial and regulatory reviews and consultations and so forth.

All of that boils down to three objectives at CFAAR which is, firstly, creating contacts so you know who to call, secondly, a knowledge sharing and upskilling piece and, thirdly, the consultation and, although its sometimes it's a dirty word, *lobbying* for change and making sure that the industry and the legal landscape is moving in the right direction.

we've been pretty overwhelmed by the response so far. We've had nearly 900 members signed up already, that's since August, and we've had various requests, as well, for international chapters to be launched so that people can meet under the CFAAR banner in local jurisdictions. So that's something we're working to do within the next six months or so.

Alice So you've just mentioned there, Dan, a couple of future things. Chris what do you hope for the future of CFAAR and Crypto assets and Blockchain technology in general?

Chris It's very difficult to future scan exactly where Crypto will end up. The predictions about it diverge massively. It's also very difficult to say which Cryptocurrency will end up the 'top dog' in a decade's time. "Bitcoin", obviously, has the brand but other Cryptocurrencies are better, technically. I'll avoid picking a winner!

One issue that Crypto does need to deal with - and when I say, "Crypto" I'm pointing to bitcoin and Cryptocurrency like it - it's very bad environmentally, in that, to mine bitcoin it requires a great deal of energy. Many news articles will say energy used for mining, was the same as Sweden's electricity consumption. So its pretty significant.

One of the reasons electricity consumption is so high in bitcoin is it's an example of a "proof of work" method of consensus. The miners in the bitcoin network compete to transfer the cryptographic puzzle as fast as they can and the winner gets to 'mint' the relevant block. But it means that there is an awful lot of processing power to solve that puzzle. The difficulty of the puzzle scales with the number of miners and lots and lots of miners are doing the same work so its quite duplicative.

The alternative to a 'proof of work' method is a 'proof of stake' method which you see in certain other Cryptocurrencies, in particular "Ethereum 2.0" and Kadano. Again, in broad strokes, essentially - rather than having lots and lots of miners competing - you essentially have holders of the currency stake some of their currency and the more you stake the greater the chance it's you who gets to mint a block trader block. That means you don't have lots and lots of nodes competing with one another so it's a bit cleaner.

There are drawbacks to that kind of system as well but that is one example of a way the environmental issues might be solved. To recap I won't say which Cryptocurrency will merge top dog but whatever does happen the environmental aspect I suspect will be a big part of the answer.

Alice Thank you Chris and Carmel what do you see for the future?

Carmel From the prospective of a fraud practitioner, I think that 10 years ago if you lost your bitcoin in some kind of bad trade it was gone. Now, it certainly is possible to investigate and to make recoveries although it can be an expensive process and therefore for a lot of low level investors and victims it's still a lost cause - which is a difficult thing.

I think that CFAAR is going to be what members make of it. There's a massive role for the private sector in coming together and supporting the eco system and upholding the integrity of the Crypto industry.

I think that fraudsters are going to be moving on as the net tightens around them and they're not going to be dealing with the likes of bitcoin. They probably wont even be dealing with *mixers* and *tumblers* and things like that. I think they're be moving into more obscure things using bots to trade in NFT's and all kinds of things like that.

As ever its going to be up to practitioners to try and keep apace with that and keep evolving and be agile.

Alice thank you. unfortunately we're getting close to the end of our time so what final thoughts have you got for those who are interested in the world of Crypto? Beginning with you Dan.

Dan Well, I think, for consumers, I would say that it's a very exciting area to be in. There is money to be made but there's also a huge amount of money to be lost; either just through bad trading and bad investment decisions or through fraud as we've been discussing today. Enjoy it but go carefully.

And then for fraud practitioners I think that the key point is to get up to speed. This technology is not going away. It's going to increase in prominence and there'll be more and more cases going through the courts on it, so I think you need to be up to speed on Crypto and NFTs and Blockchain and the issues that arise in cases otherwise I think you'll, pretty quickly, be left behind.

Alice And Chris what are your final thoughts?

Chris I think I'll leave with a cautionary tale that builds on the frauds that we talked about earlier: the "Squid-coin" fraud that hit the headlines recently. Essentially, this was inspired by although unconnected with the Netflix show "Squid Game".

The idea behind this Cryptocurrency was investors would by the coin and, in a sort of lottery like system, you could accumulate a great deal of money. It received a great deal of media hype as its price rocketed up, not always talking about some of the misgivings people had, such as that the difficulty in actually cashing out of your position. Eventually the whole thing fell apart. Individuals behind the coin absconded with all the value and left the investors with nothing. It's a classical example of what's called a "rug-pull" by Crypto investors.

The moral of the story is, to add to Dan's point, it's a very exciting area and people, when faced with the prospect of making many multiples of their investment, perhaps aren't as street smart as they might be. So in a word "beware".

Alice Thank you and Carmel the final word is with you.

Carmel Thank you I would say that Crypto assets are ubiquitous, regardless of your practice area. It touches on taxation, it touches on estate planning, it touches on dealing with high net worth individuals or whatever geography you're interested in. Whether you're an auditor or you're involved in matrimonial and family planning there's going to be some kind of Crypto assets, sooner or later, so you do need to get to grips with it.

But I would temper that with saying it’s not a strange scary thing. It’s something that we can all get to grips with and we can find opportunity in and, if you do find yourself in trouble at the end of a fraud, CFAAR is a good group to speak to.

Alice Unfortunately that's all we've got time for in this week's episode. Tune in next time to hear Stuart Leach talking about how to protect your commercial and individual reputation, should the worst happen.

Thank you again to Carmel King, Chris Whitehouse and Dan Wyatt for joining us. You can get in touch with CFAAR via linked in and watch this space for the launch of their website www.CFAAR.co.uk.

If you have any questions for me or for CFAAR or any topics you'd like us to cover in a future episode please do email us on taxingmatters@rpc.co.uk . We'd love to hear from you.

RPC would like to thank Josh McDonald. Our original score is composed by *Inciter Music* who also produce this podcast series. To hear a full, uninterrupted version of our podcast theme go to Instagram @incitermusic and follow the link in bio.

And, of course, a big thank you to all of our listeners for joining us.

If you like Taxing Matters why not try RPC's other podcast offering "Insurance Covered" which looks at the inner workings of the insurance industry. Hosted by the brilliant Peter Mansfield and available on Apple podcasts, Spotify, Acast and our website. If you like this episode please do take a moment to rate, review and subscribe and remember to tell a colleague about us.

Thank you all for listening and talk to you again in two weeks.