Sam Volkering's
CRYPTO NETWORK

FRONTIER TECH INVESTOR

How to spot and avoid crypto scams

Frontier Tech Investor is issued by Southbank Investment Research Limited. Registered in England and Wales No 9539630. VAT No GB629 7287 94.

Registered Office: 2nd floor, Crowne House, 56/58 Southwark Street, London SE1 1UN. Southbank Investment Research Limited is authorised and regulated by the Financial Conduct Authority. FCA No 706697. https://register.fca.org.uk/.

ISSN 2398-2470

Contact Us

To contact customer services, please call us on 0203 966 4580, Monday to Friday, 9.00 am - 5.30pm

...continued on next page...

How to spot and avoid crypto scams

By Sam Volkering
Editor, *Frontier Tech Investor*

One of the hardest things for people new to crypto is to appreciate the shift in the balance of power.

That's the shift away from centralised, third-party institutions to you.

It's a difficult thing to get your head around considering how we've been conditioned our whole lives to trust these third parties, like banks, currency exchangers and central banks.

However, in crypto one of the underlying principles is that the control and power over your finances and wealth exists with you.

A popular term in crypto is "you are your own bank". In many respects, that's true. There are of course ongoing developments that make that concept a lot easier for people new to this space and help take the daunting aspects out of it.

But it's also a very liberating concept that really puts your destiny (as cheesy at that sounds) in your own hands.

Of course, with this shift in power, and the responsibility on you to be more engaged and active in how you navigate this world, comes elements of risk.

As outlined in the special report "The Ultimate Starters Guide to Crypto", there are ways to help mitigate risks by using things like hardware devices to store your crypto and ensuring you understand how to properly allocate and manage your capital.

However, one of the biggest things I think you can also do is to understand some of the traps and pitfalls in the world of crypto that are thrown at you from malicious operators.

There are scams and fraud in all aspects of finance, both in the traditional financial world and crypto. Most people aren't too bad at identifying and knowing a scam in the traditional world – albeit there's still far too much of it.

However, in crypto, due to inexperience, a lack of knowledge and understanding and because it's all still so new, people really struggle with some of the scams and fakery that occurs.

Having been around crypto for over a decade now, I've pretty much seen it all when it comes to the scams in crypto. They can be highly sophisticated and are all designed with one goal in mind – to separate you from your crypto, your money, your wealth and to take it from you.

...continued on next page...

That's why this report is probably one of the most important ones you'll have access to. In it I go through a number of the more common scams that you will likely see and have thrown at you.

Being able to identify them, flag them and importantly avoid them will save you a lot of heartache and pain. It will also help to build your knowledge store to help others avoid as well.

This isn't a definitive list though. Scams and fraud are always evolving in all aspects of crypto and non-crypto finance. You should always stay vigilant, and if you're ever in doubt about something, you can reach out to me for more assistance in identifying a scam by emailing me at frontiertechinvestor@southbankresearch.com.

Here are three of the biggest, but yet apparently easiest ones to fall for, scams.

1. The "trusted" news report

Over the last few years, on and off I've received emails from people who'd recently bought and read my crypto book and subscribed to one of my services.

They're often thrilled to start their crypto journey. However, being new to crypto they are often also on the brink of getting sucked into a scam right off the bat.

In one such email was a simple question… Could I direct them to the websites that show the bitcoin investments the Dragons from Dragons' Den had been making and how to join up?

Straight away this rang huge alarm bells for me. But with a very brief and simple search it was easy to find this is one of the prominent bitcoin scams doing the rounds.

What was really worrying about this particular scam is the fact just a day after the subscriber reached out, I got a similar email in my own inbox.

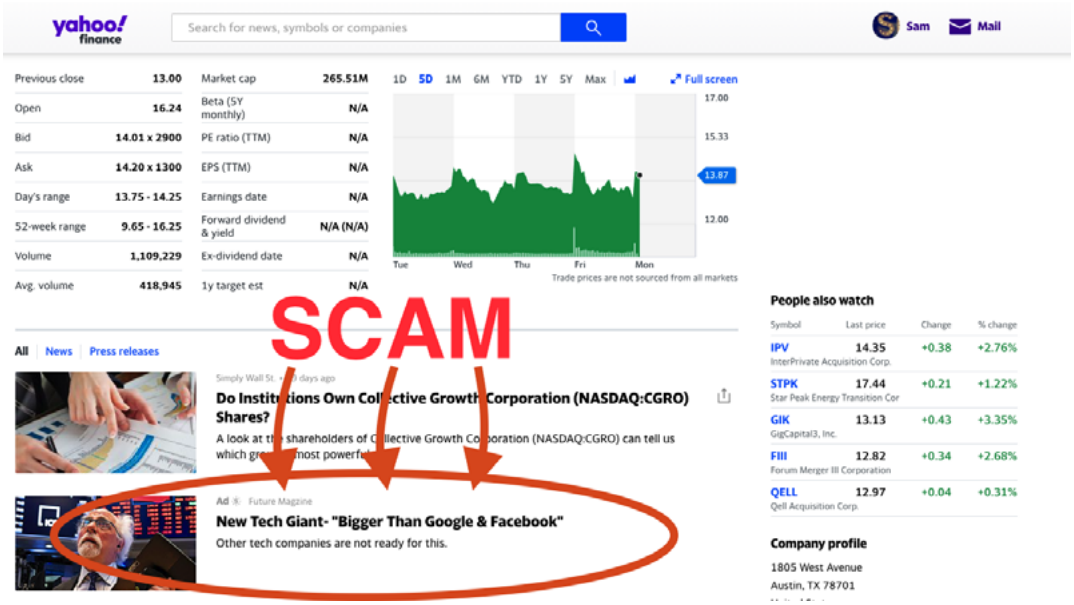
So, before we dissect this scam, let's take a look at it. Once you see what these look like, you can more easily spot them if they find their way into your emails or social media.

You also sometimes see them on reputable sites such as Yahoo Finance disguised as an advert.

Just recently I saw one pop up as I was looking on Yahoo Finance. I clicked through to see what it was, and it was a link through to the scam bitcoin site, Bitcoin Revolution.

…continued on next page…

I made some annotations on the screenshot to point out the scam.

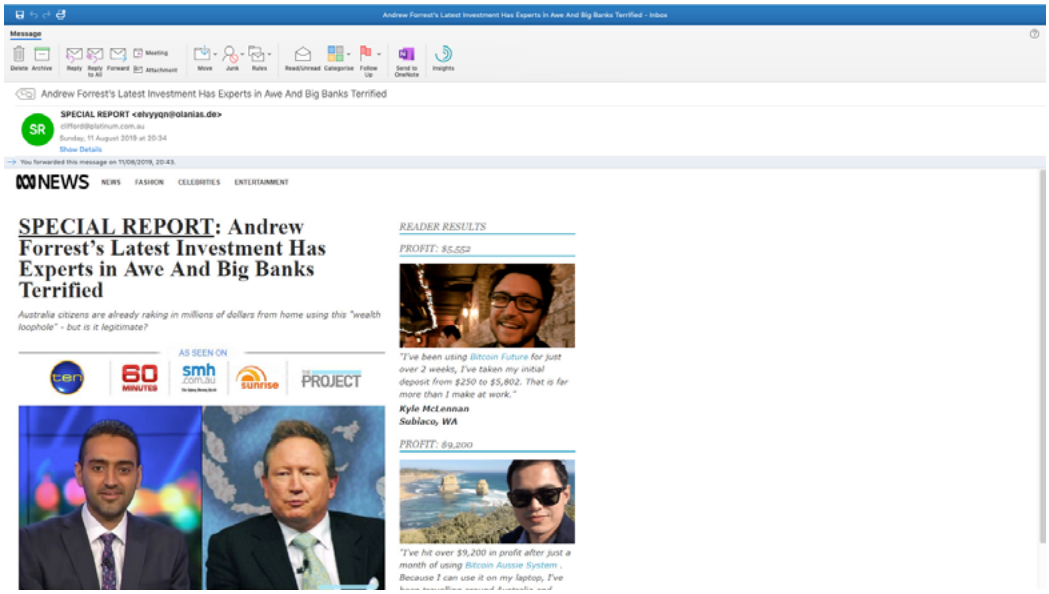


Source: screenshot from Yahoo Finance

When they appear as an email you often see them also disguised as a news report, or a "special report" from a reputable news agency.

In the image below is another email I got from a reader in Australia with the same scam, but in a completely different country. Same thing tweaked for a local audience.

In this one the ABC News is Australia's national broadcasting station, a bit like the BBC in the UK. But it too is suggesting that a prominent, wealthy Australian business leader has made money from this bitcoin system and you can too.



Source: screenshot from editor's email

...continued on next page...

On the face of it this looks reasonably legit. It looks like a report from the Australian ABC News site. It's got "As seen on" and Channel 10, 60 Minutes, SMH, Sunrise, The Project – all mainstream mass market news outlets. Then there are even "reader results" over to the side about this "profitable" system.

Let me be clear, this is a scam. Similar ones saying that Dragons' Den investors have been investing in this system are also scams. They use all kinds of tricks and traps to try and convince you they're legit.

I've seen ones saying Richard Branson made money from it, Deborah Meaden has and even more recently that Holly Willoughby endorses this system.

These are all fake claims and link to scams.

You can even see statements from the likes of Richard Branson and Deborah Meaden addressing these scams, here and here.

You also find that in the fake news reports, emails and ads for all these things that images can link out to a scam site.

These sites are almost always bitcoin and crypto trading "systems" with names like Bitcoin Revolution, Bitcoin Loophole, BTC Future, and other such variations.

You also find they have a very similar homepage, with more fake news reports, fake testimonials, fake figures and all enticing you to send in a little money that is traded for you and then multiplies almost instantly.

They usually have three or four tiers of membership that allows traders to work on your behalf. Starter, Premium and VIP levels are pretty common, each with minimum cash deposit amounts from around £500 to £5,000 and even £50,000 for the "VIP" levels.

It's all rigged to get you started, and then to pile more and more money in as they use fake figures and numbers to suck you in to sending them more and more money.

It's quite easy to recognise these scams as these sorts of people or news stations never actively promote bitcoin and crypto trading systems.

If in doubt, open a new browser window or tab, go to the claimed news site – in this instance, the BBC, ABC News or CNN or whatever – then search for the report the scam ad or email is referring to.

Similarly, do a Google search for "Deborah Meaden Bitcoin" or "Richard Branson Bitcoin" or "Dragons' Den Bitcoin" or "Holly Willoughby Bitcoin" and pages of information about these being a scam pop-up. Realistically you should be doing this kind of preliminary research on everything to do with crypto.

The reputable, quality, ethical and professional services, platforms and advisories can easily be found. You can find information about the company, about the people, about

...continued on next page...

the services, there are contact details and other avenues for contact including social media where questions and queries will be answered.

If you can't get any of that, then red flag city, folks.

And then if you're still not sure about something, use me! Reach out to me and I'll look at it for you. I've been around long enough to know what's an outright scam or not.

You can email me with concerns or questions about potential scams or reach out to me on social media. To help keep your crypto experience that little safer I'm always available to help where I can.

2. Online impersonators and "send one, I'll send two back"

One of the more brazen scams is when people try to impersonate other people on social media. They will then typically build some level of trust to then request payment or trading of some sort.

Perhaps they'll also request signing up to or joining a site they're in control of as well.

I've come across this a couple of times recently. One was an attempted scam on me, another was a sadly successful scam on a reader.

In my example, I had "Saifedean Ammous" reach out to me on Twitter with a direct message. Saifedean is of course a prominent bitcoin figure and one of our interviewees from our The Next Bitcoin series of videos.

The message to me on Twitter was simple enough at first. Just a "Hello Sam" and "How are you going?"

I knew from the outset it was a scammer, because I know the Twitter handle of the real Saifedean. But I figured let's entertain this and see where it goes.

One thing to note is impersonators have to have a unique "handle" on a site like Twitter, so they will do subtle variations to try and sneak it past you. For example, an upper case "i" looks exactly the same as a lower case "l" hence making things very difficult to see. Or sometimes they'll add "_" to the end of a name, again just to try sneak past your first defences.

Anyway, the best way to deal with online impersonators is to remember a golden rule – anyone who ever actively asks you to send them crypto on social media is not to be trusted.

No one of any reputation will ever ask you for crypto, ask for your details, your private seed to your devices, passwords or anything like that.

In the instance of my scammer impersonator, I thought I would try and get the scammer to send me some crypto – trying to scam the scammer! *Note: I would have*

...continued on next page...

donated it to charity had they actually sent me any.

This scammer, however, was trying to get me to go to a trading site to log in and register. I had a look at the site, and as predicted it was exactly like the other scam trading sites out there, like Bitcoin Revolution (and others) mentioned above.

Once again, different levels of trading service from Premium to VIP, all promising to deliver returns once you've paid for the level and added funds to your account.

But these direct message scammers are cunning.

They will keep coming back to the point of making you transfer them some crypto in order to get access to something, whether it be a site, a "new opportunity", some kind of inside info or in exchange for another crypto or bonus amount of crypto.

It's really a sort of variation on the "send me one BTC and I'll send you two back" scams that get around social media.

Now if you've never seen those, it's a very basic concept. These impersonator accounts promise to send back more crypto that you send them.

They never do, they're just chancers that you should always ignore.

These direct scammers will also try and emotionally manipulate you to feel guilty that perhaps you don't trust them, or make you feel bad or get you hyped with raging FOMO (fear of missing out) to trick you into their world.

They'll often talk about things like "their family" to make you feel empathy for them, or any kind of trick they can find to lull you in.

Or they just leverage off another well-known name to make you think you're dealing with that genuine person… except you're not.

A reader of mine found this out the hard way when they were recently tricked into sending a scammer around one third of their crypto investments believing they were interacting with another prominent crypto name, Teeka Tiwari.

They ended up converting a bunch of crypto to BTC and sending it over to the scammer. I had a look at the BTC address, and sadly this scammer address has been in operation since July this year and so far has seen 45.15 BTC received into it – that's about $871,000 worth!

The scam site they were trying to get the reader on to in that instance was called netcointrade.com. Can you start to see now how these scam sites do variations on names to try and appear legitimate?

If you see that site, beware it's a scam. It's not hard to figure it out. It has all the red flags you'd expect that I talk about above. But also there are all these awards they highlight: "Best Execution Broker (Asia Pacific) 2014" and "Most Trustworthy

...continued on next page...

Enterprise Award 2017".

Only problem is that you can do simple Whois domain searches for most sites to find out more information. In this instance, netcointrade.com was only registered in mid-September 2020.

How do you win awards from years ago when you've only been in existence for a year? Again, these are just some of the red flags you need to be aware of, to look for and to check.

If *anyone* reaches out to you on *any* social media platform directly to get you to transfer them crypto, don't.

If they try to get you to sign up to a trading site where you have to transfer money into an account to get started and see the profits roll in, don't.

Even if it's someone you think is a reputable, professional person, don't reply to any requests on social media, ever.

Reputable, professional people will have reputable, professional avenues of contact.

Let's do a quick role play to see what you've learnt so far…

Let's say I reached out to you directly on Twitter from my actual legitimate Twitter account and asked you to send me 0.1 BTC so I could test a new wallet for you and then I'd send it straight back.

Would you send it to me to test?

Answer: NO.

Hell no you wouldn't. And you shouldn't.

That's because I'd never ask that. You might think it's my actual legitimate account, but it won't be.

And if it was my actual account, then it's likely I've been hacked!

Never fall prey to these people on social media. If you were ever unsure, or even if you thought you were absolutely sure, still reach out through the professional channels to verify the person.

With me for instance you'd call or email Southbank Investment Research to get a hold of me through official channels. Only then would you find out if it was me or not.

If you're trying to verify someone on social media, and you can't find any professional or official channels to contact them – they're not worth contacting and you're clearly being scammed.

...continued on next page...

I'm just saying – blanket rule, never send anyone anything without 100% verifying who they are. And *never send any money, any crypto, any funds, and "systems"* through social media channels no matter who asks for it.

Stick by those rules and you'll save yourself a lot of heartache when the scammers knock on your door – *and here's the thing, they will come at you at some point* so you better be ready for it.

3. Phishing for your crypto

This is perhaps the most advanced and sophisticated scam that is very hard not to fall for. But you must know what to look for.

It's the "phishing" attempt. That means they are trying to get you to divulge information, data and credentials that will allow the scammers access to your exchange accounts, your hardware devices and your crypto holdings.

They are very smart and look very legitimate, but they are scams.

Ones going around at the moment are phishing scams related to the Ledger hardware wallet. These impersonate communications from Ledger asking you to head to links to give information or to download something or reset your passwords.

For example, I recently got a text message recently purporting to be from Ledger.

Now if you own a Ledger hardware wallet and get this text message, it would put the fear of God through you.

The text message says (or a variation of),

> *Alert (Ledger) You just sent 0.027099 BTC (0/4 confirmations). Please visit ledger-chain.co.uk within 40 mins if you need to cancel*

I had an email from a subscriber not long after with this exact text in it. It was also the exact same text that I received as well. Even down to the exact BTC amount.

If you received an email like this, it is a phishing attempt.

The site that it links to will have malware on it that is designed to try and get access to your Ledger pin code or your crypto wallet private keys. If it's not malware, then it may ask for those details.

Be warned, *do not go to that site, do not click on those links, do not give any information about your hardware device.*

If you've headed to those links, run a thorough and detailed anti-virus and malware sweep of your computer. And even then, I would suggest using a different computer or phone to connect to your Ledger device.

...continued on next page...

Never click on anything like this as it is a phishing attempt. Ledger has information about the increasing sophistication of phishing attempts on its support site.

If you're ever worried about transactions taking place on your Ledger device, just go and check your public wallet address on a blockchain explorer.

Admittedly, getting this text message myself was a little worrying. So I just went to blockchain.com and searched my wallet address. Nothing had moved or taken place I didn't already know about.

You can always check your crypto wallets and all the transactions on the respective blockchain searching for your public wallet address.

Emails are doing the rounds as well with similar attempts to scam you, saying they're from Ledger but they're really not.

I got one recently that said,

> *Your Ledger has been deactivated.*
>
> *Unfortunately, due to the new KYC (Know Your Client) regulations, you're required to confirm your identity:*
>
> *https://docs.google.com/document/d/e/2PACX-1vR3MpYfOK11QNZSF4L7zhL-78_S4A4U2hDbpcvfcyAba5uLbz1BCGbVEHUsWkNHGg30yqpXnE3/pub?embedded=true*
>
> *Sincerely,*
> *Ledger Verification Team.*
> *Q29P-M8W12TW*

This is a scam. It went straight to the bin. The scammers will find ways to get email addresses. They will blanket send these emails. They will even make them look like legitimate corporate emails. They're not.

Companies like Ledger will never send an email asking for your details, private seed, phrases, passwords, pin numbers, anything like that. All downloads and software updates will be through the verified applications and devices when connected.

Ledger also has great resources on its site about phishing that you can access here.

Conclusion

There you have it, a few things to be aware of and to ensure you keep an eye out for when it comes to scams in crypto.

Remember, you don't need to use "systems" and trading robot sites to earn and to build your crypto wealth. Most of the time they're complex scams and will do you in rather than help you out.

...continued on next page...

And remember, if you're *ever in doubt* contact me at frontiertechinvestor@southbankresearch.com and ask for help. I've seen it all and will be able to provide more guidance.

Regards,

Sam Volkering
Editor, *Frontier Tech Investor*