Article Information

Authors: Michael Bacina, Steven Pettigrove, Jake Huang, Luke Higgins, Luke Misthos
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: Australia introduces privacy law reforms, UK to preserve property rights in digital assets, ASIC extends reliefs for foreign financial services providers, US Congress debates the future of DeFi, FBI Fraud Reports, CryptoPunk Smart Contract Shotgun

Michael Bacina, Steven Pettigrove, Jake Huang, Luke Higgins and Luke Misthos of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

Australia introduces first tranche of privacy law reforms

Earlier today, the Government introduced draft legislation to reform the *Privacy Act 1988* (**Privacy Act**) into Parliament. The *Privacy and Other Legislation Amendment Bill 2024* (**Bill**) marks a significant step forward for Australian privacy law, aiming to make it "fit-for-purpose in the digital age".

With the introduction of this Bill, the Australian Government is seeking to legislate the first tranche of agreed recommendations of the Privacy Act Review, ahead of consultation on a second tranche of reforms. The Bill's drafting was also informed by the government's previous response to the review.

The Office of the Australian Information Commissioner (**OAIC**) warmly welcomed this first tranche of reforms to the Privacy Act, saying the Bill will:

- strengthen the OAIC's enforcement toolkit, which will include a new mid-tier civil penalty for interferences with privacy and a low-level civil penalty provision for specific administrative breaches of the Act with attached infringement notice powers;
- require the OAIC to develop a new Children's Online Privacy Code to enhance privacy protections for children in the online environment, particularly when using digital platforms;
- introduce a statutory tort for serious invasions of privacy, which would be an important addition to the suite of regulatory measures needed to address gaps in the existing privacy protection framework and address current and emerging privacy risks and harms (such as doxing).

The Attorney-General provided a more detailed overview of the bill including the proposal to criminalise doxing.

Australian Privacy Commissioner Carly Kind said,

> These are important initiatives that will have benefits for the Australian community,
>
> The enhanced civil penalty regime will add significantly to our enforcement toolkit,

And

> The statutory tort would also fill a gap in our privacy landscape by providing people with the ability to seek redress through the courts for serious invasions of privacy without being limited to the scope of the Act.

However, Commissioner Kind said much more needed to be done, and the OAIC is eagerly awaiting the second tranche of privacy reforms which includes a new positive obligation that personal information handling is fair and reasonable.

As the OAIC put it, the coverage of Australia's privacy legislation lags behind the advancing skills of malicious cyber actors. Further reform of the Privacy Act is urgent, to ensure all Australian organisations build enhanced levels of security into their operations, and provide additional tools to enforce protections for personal information.

Written by Jake Huang and Steven Pettigrove

UK Bill to preserve property rights in digital assets

In the UK, the *Property (Digital Assets etc) Bill* has been introduced into the House of Lords, marking the a leading moment in digital assets being given formal recognition as a kind of personal property.

A key issue under the common law is that personal property (that is everything which isn't land, or 'real' property as it is known at law) is that things were considered to be either a chose in possession (being a thing which could be owned like a computer or a pen) or a chose in action (traditionally a thing which a court could make orders to enforce rights in relation to – such as a share or a debt). Digital assets do not neatly fit into either the category of being a chose in possession, as strictly speaking no one ever has possession of digital assets, merely a password which can update the record of ownership on a ledger, and they do not easily fit within chose in action, as there is no issuer and no one to enforce the ownership right of a digital asset against in many circumstances.

Despite this problem, the practical approach in insolvency courts has been to recognise digital assets as property for the purposes of insolvency. This has extended to injunctive actions as was recently seen in the Australian Federal Court where Justice Collier said:

> I am satisfied that, at an interlocutory level, the definitions …[relevant to the case]… are sufficiently broad to encompass cryptocurrency assets in appropriate circumstances…

Justice Jackman recently published a speech arguing that digital assets were simply choses in action and that no third category of personal property was needed, warning that:

> the rigidity of a statute would inhibit experimentation, and suffers from the problem that you cannot regulate something in advance of its invention.

The proposed Bill is extremely short and as and in the identical form to that which was proposed by the UK Law Commission despite that position having been criticised by some scholars.

It reads as a clarifying law as follows:

1 Objects of personal property rights

A thing (including a thing that is digital or electronic in nature) is not prevented from being the object of personal property rights merely because it is neither—

(a) a thing in possession, nor

(b) a thing in action.

2 Extent, commencement and short title

(1) This Act extends to England and Wales only.

(2) This Act comes into force on the day on which it is passed.

(3) This Act may be cited as the Property (Digital Assets etc) Act 2024.

If passed, the Bill will put an end to arguments that digital assets, being software or data objects, are incapable of being property by virtue of that characteristic, and help regulators and judges apply existing laws in a way that aligns with how people have been treating digital assets for some time (like property). While not applicable outside of the UK, it will no doubt have influence over other common law countries considering how to address fundamental definitions surrounding digital assets.

Minister for State and Justice, Heidi Alexander said that the UK government would convene an expert group to advise the UK government:

> I believe the UKJT is uniquely placed to convene the expertise needed to consider the issues around control of digital assets.

Expert advice to policymakers has a key role in ensuring the law can align to the technology which it is regulating.

Written by Michael Bacina

ASIC extends reliefs for foreign financial services providers

The Australian Securities and Investment Commission (**ASIC**) has extended, for a further 12 months, the transitional relief for foreign financial services providers (**FFSPs**) from the requirement to hold an Australian financial services (**AFSL**) when providing financial services to Australian wholesale clients.

The current transitional arrangements for ASIC's "sufficient equivalence relief" and "limited connection relief" were due to expire on 31 March 2025. The further extension means the relief will last until 31 March 2026.

The development of the FFSP licensing regime

Generally, if a business or person carries on a financial services business in Australia, they will need to hold an AFSL, unless licensing relief is granted by ASIC or an exemption applies.

Before March 2020, ASIC had assessed that a number of overseas regulatory regimes – were each a "sufficiently equivalent jurisdiction" to the Australian regulatory regime. As a result, ASIC granted a blanket relief (i.e. class relief) for entities regulated in these jurisdictions from the need to also apply for an AFSL, when they provided financial services to wholesale clients in Australia.

In 2020, ASIC tried to repeal this blanket relief and introduced a foreign AFSL option for FFSPs who provides financial services to wholesale clients in Australia. Under that proposed FFSP licensing regime, FFSPs licensed in a sufficiently equivalent jurisdiction could individually apply for a foreign AFSL from ASIC, and be exempted from many of the standard AFSL obligations (a fast track approach).

In addition, the regime also established an exemption for fund management FFSPs seeking to induce certain types of professional investors in Australia to invest in their funds, a so-called "funds management relief". This relief is scheduled to be available from 1 April 2025.

Exemption to FFSP Licensing regime

Since introducing the FFSP licensing regime, the Australian Government has been working on legislation to introduce 4 additional exemptions for FFSPs from the need to apply for a foreign AFSL:-

- a comparable regulator exemption;
- a professional investor exemption;
- a market maker exemption; and
- an exemption from the fit-and-proper person assessment to fast-track the licensing process for FFSPs authorised to provide financial services in a comparable regulatory regime.

After experiencing significant delays in the past few years, the draft bill – Treasury Laws Amendment (Better Targeted Superannuation Concessions and Other Measures) Bill 2023 (**Bill**) is before Parliament. Subject to the draft being passed, the above exemptions are set to commence on 1 April 2025.

Extension of transitional relief

Given the long and bumpy law-making process for the FFSP regime and its exemptions in Parliament, ASIC has repeatedly extended the sufficient equivalence relief (as discussed above), and the limited connection relief (similar to the upcoming fund management relief, but applies to a broader range of FFSPs) since 2020. These apply to FFSPs that wish to provide financial services to wholesale clients or professional investors in Australia. They have been in place since before the introduction of the foreign AFSL regime, and many FFSPs have been relying on them in the past years, despite being technically "transitional".

The latest extensions of transitional relief to 31 March 2026 will allow Parliament further time to consider the Bill.

ASIC said the extension was necessary to:

> provide certainty for FFSPs that are currently relying on ASIC relief

After 31 March 2026, the FFSPs currently relying on the relief will be required to notify ASIC of their intention to rely on the new licensing exemption regime, unless they choose to notify ASIC earlier.

Entities that are not currently subject to ASIC relief will be able to notify ASIC of their reliance on the licensing exemption regime after it commences.

Written by Jake Huang, Steven Pettigrove and Michael Bacina

US Congress debates the future of DeFi

In a Congressional hearing on decentralised finance (**DeFi**), US lawmakers revealed a stark divide over the future of crypto-based financial systems. The House Financial Services Committee's hearing, titled *Decoding DeFi: Breaking Down the Future of Decentralized Finance*, provided a platform for both advocates and critics of DeFi to voice their perspectives.

The two-and-a-half-hour session exposed a clear split between Republicans, who supported DeFi's potential to decentralise and democratise finance, and Democrats, who focused on concerns around crime, scams, and tax evasion.

Pro-DeFi Advocates Push for a Peer-to-Peer Future

Republican subcommittee chair French Hill opened the hearing with a strong endorsement of DeFi's potential, stating that it could replace traditional financial intermediaries with autonomous, self-executing code. Hill emphasised a vision for a "peer-to-peer future" where individuals would not be at risk of having their bank accounts frozen for political reasons. His comments referenced the 2022 freeze of crypto donations to Canadian protesters, an act later deemed unconstitutional by the courts.

Crypto industry advocates, including Peter Van Valkenburgh, director of research at Coin Center, argued that regulators

have failed to provide clear guidance for compliance, making it harder for DeFi platforms to adhere to current laws, a common sentiment. Valkenburgh further emphasised that while tax evasion is a concern, it does not justify a financial system under constant surveillance and control.

Amanda Tuminelli, chief legal officer at the DeFi Education Fund, took the opportunity to highlight DeFi's inclusive nature, noting that it opens up financial access to anyone with an internet connection, bypassing the gatekeepers of traditional finance.

Critics Focus on Crime and Regulatory Non-Compliance

In contrast, Democratic lawmakers expressed deep concerns about DeFi's role in facilitating illicit activities. Representative Brad Sherman, a prominent critic of crypto, argued that DeFi primarily serves as a tool for billionaires to evade income taxes. He characterised the technology as part of a broader effort to undermine tax enforcement.

Representative Maxine Waters raised security concerns, pointing to high-profile hacks involving the Trump family's DeFi project, "World Liberty Financial." Waters questioned whether regulatory agencies like the Securities and Exchange Commission (**SEC**) and the Commodity Futures Trading Commission (**CFTC**) could adequately regulate DeFi platforms given widespread non-compliance.

Mark Hays, senior policy analyst at Americans for Financial Reform, described DeFi as a "volatile, scam-laden" industry that exposes investors to significant financial risks. Hays called for existing securities laws to be applied more rigorously to the DeFi space, echoing concerns over the lack of accountability.

DeFi at a Crossroads

The hearing provided a glimpse into the ongoing debate about how DeFi should be regulated in the US despite the passage of the Financial Innovation and Technology for the 21st Century Act (FIT21) (which mostly focuses on centralised crypto intermediaries) through the House in May this year with significant bipartisan support. Advocates on both sides are split with proponents focusing on the potential benefits of peer to peer technology and detractors focusing on security and financial crime risks. The potential for DeFi to disrupt traditional finance also poses challenges to existing regulatory and financial interests. With DeFi platforms, like Uniswap, coming under increasing pressure from regulators, the fight for a more open and transparent financial system remains real and pressing. The outcome of the next US election cycle may well have a significant impact on the shape of future legislation and regulatory enforcement, with likely ripple effects beyond the United States including on our own shores.

Written by Steven Pettigrove and Luke Misthos

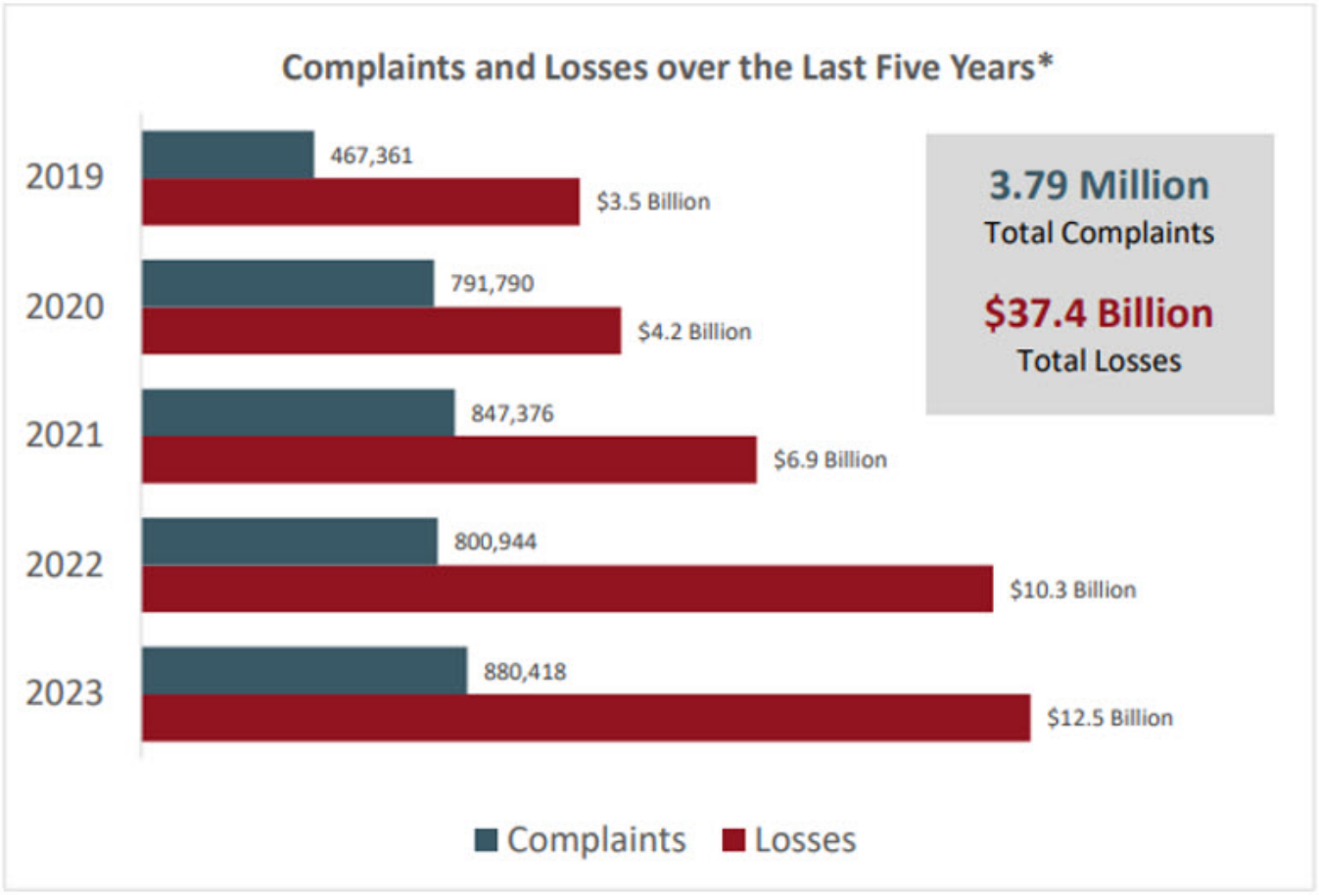
FBI Fraud Reports – how does Crypto compare?

The US Federal Bureau of Investigations (**FBI**) has a specialist Internet Crime Complaint Centre (**IC3**) which has published a standalone report into fraud with a cryptocurrency 'nexus' (Cryptocurrency Report) and quite a few media outlets have been repeating as statement in the report that 50% of all financial losses involve cryptocurrency. This is a stunning number, but looking deeper into fraud reporting, the figures aren't so clear.

In December 2023, the IC3 published their Internet Crime Report (**December Crime Report**) which said that:

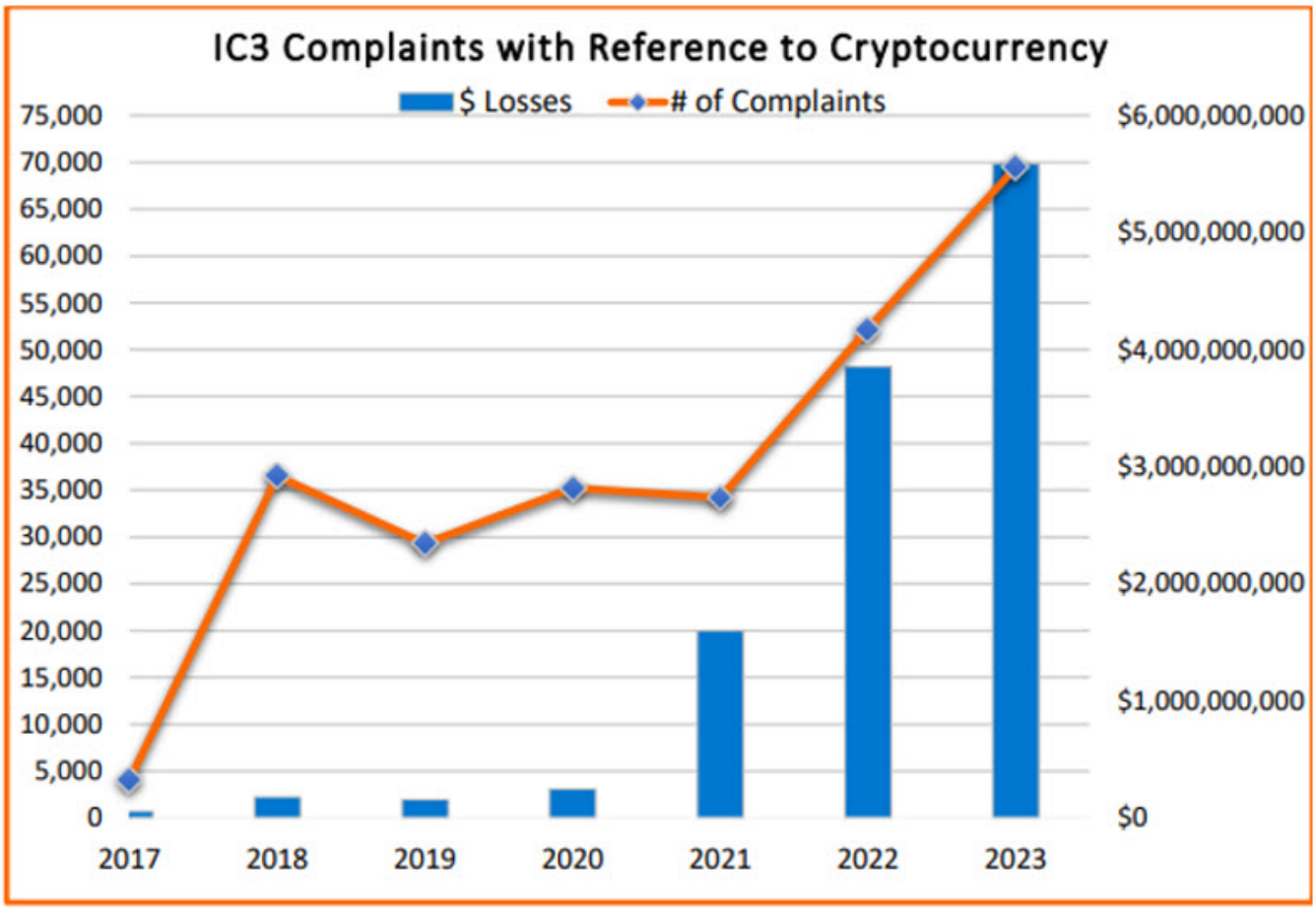
> investment fraud with a reference to cryptocurrency rose from $2.57 billion in 2022 to $3.96 billion in 2023, an increase of 53%

The IC3's December Crime Report stated that 880,418 complaints were received in 2023 and showed an increasing number of fraud complaints and losses totalling USD$12.5B in 2023:



The Crime Report also shows how the FBI categorises complaints and uses a 'descriptor' to link if cryptocurrency was involved across multiple different crimes (so looking for any reference to crypto in the report. What this means is that when a crime is reported, first the type of crime is chosen for categorisation, and then a descriptor may be added.

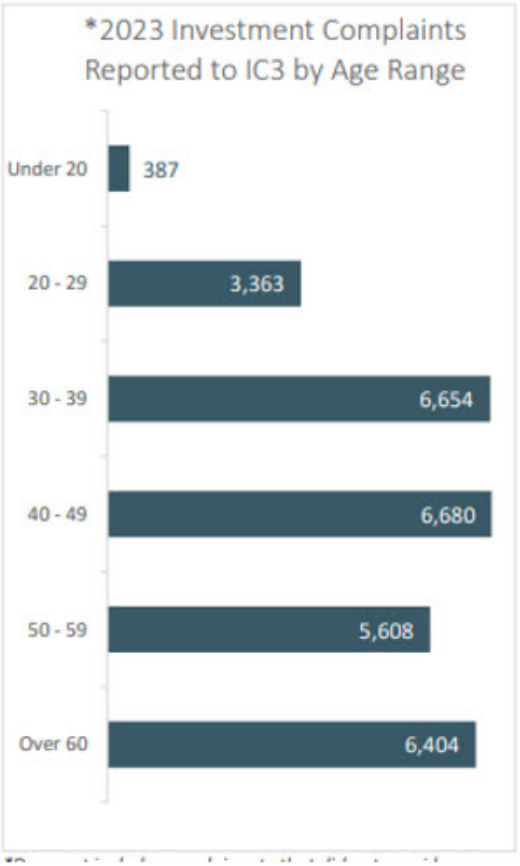
Turning to the recent Cryptocurrency Report, the number of complaints in 2023 which had a reference to cryptocurrency (it's unclear if this was in the descriptor or a new analysis has been done) was 70,000, or 7.9% of reports to IC3 which had a reference to crypto. There is no explanation as to why the figures between the two reports differ. Total losses involving these complaints is reported to be US$5.6B:



Given the December Crime Report states losses were US$12.6B, making the US$5.6B of losses of complaints referring to crypto 44.8% of the total. It's clear that the driving force of these are almost all investment scams, as reported in the December Crime Report, and that crypto-investment scams are a huge component of this:

INVESTMENT

In 2023, the losses reported due to Investment scams became the most of any crime type tracked by the IC3. Investment fraud losses rose from $3.31 billion in 2022 to $4.57 billion in 2023, a 38% increase. Within these numbers, investment fraud with a reference to cryptocurrency rose from $2.57 billion in 2022 to $3.96 billion in 2023, an increase of 53%. These scams are designed to entice those targeted with the promise of lucrative returns on their investments. [7,8]



Investment scams are a particularly insidious form of scam where victims are groomed on ways to make money, and it's unclear how many of these scams are using cryptocurrency as the lure (i.e. offering yield, trading or mining using crypto which is fake) or is using crypto as a form of payment to the scammers (this is likely to be significant). Behind every one of these losses are real people who have lost precious and hard earned wealth, and from the age distribution many of the victims are near or approaching retirement.

While those offering investment products in the USA and other jurisdictions likely already require some kind of registration or licensing, the absence of clear regulation for crypto businesses, permitting traditional investment advisors and trusted brands in crypto being able to demonstrate their compliance risks creating just the kind of vacuum where scammers can operate, while legitimate businesses struggle with laws that in many cases simply cannot be complied with. Victims in turn struggle to differentiate between a scam and a legitimate business.

This also has a second order effect of feeding a narrative that crypto is associated with crime, which may delay or create oppressive approaches to regulation which unfortunately can have the opposite effect to protecting consumers.

On a brighter note, researchers have found that the average crypto-related scams lifespan has been dropping dramatically overtime, which may suggest that scams have become more sophisticated and organised, in many cases using trafficked persons in 'slave' like conditions:

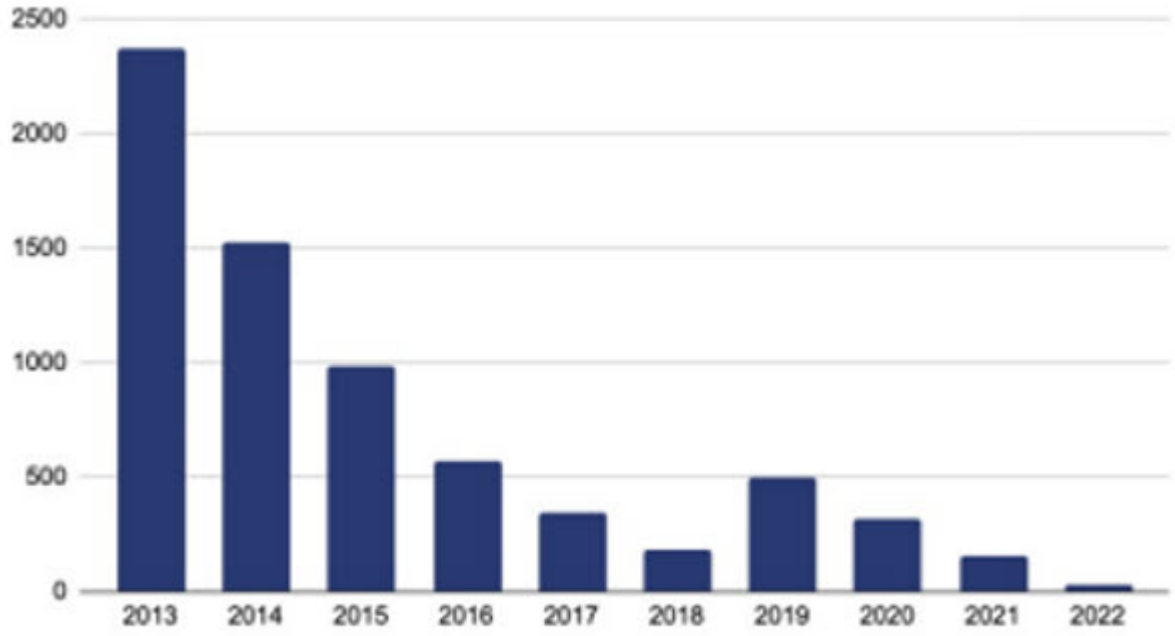


Figure 1.5. Average crypto scam lifespan, 2013-2022.

It's clear that an industry wide approach, with numerous vectors of approach, are needed urgently to combat these scams, including:

- sensible fit-for-purpose regulation without undue cost and burden to help differentiate compliant businesses and give customers affordable options for crypto investments which are clearly in demand;
- industry endorsements and voluntary codes of conduct and certification;
- fast enforcement against misleading and deceptive operators (whether or not in crypto, as it is expected AI referencing investment scams will undoubtably be on the rise);
- co-ordination between law-enforcement and industry and policy makers to help combat new scams as they arise; and
- relentless education for the community to provide a last line of defense.

Australia has had some good success with a direct attack on the top of the funnel, with thousands of scam websites being taken offline and co-ordination between Chainalysis and the Federal Policy in Operation Spincaster, with a corresponding fall in scam figures. Perhaps something the US can learn from?

Written by Michael Bacina

CryptoPunk Smart Contract Shotgun, but who has the right to bear arms?

While the death of NFTs has been called by some, many projects still maintain significant value and substantial floor prices. One of the earliest collections in particular, CryptoPunks, has maintained an impressive floor price of approximately USD$1.5M at present. With that in mind, a crafty operator has used a combination of smart contract logic and an interface having gone offline to heist ownership of a co-owned CryptoPunk (specifically Punk 2386) for around USD$20,000.

How is this possible? Well we need to go back to 2020 to the booming NFT market, and a start-up called Niftex. Niftex put forward a smart-contract protocol and web-interface to permit users to fractionalise NFTs by locking up the NFT and creating fractional parts, called "shards", which were then placed on sale for 2 weeks or until they sold out. Punk 2386 was an NFT which was fractionalised under Niftex.

The Niftex smart contracts dealt not only with the initial fractionalisation of an NFT, but also how to bring those shards together and release an NFT to a single owner. One way was to buy all the shards, but to address a situation where a shard owner was unresponsible or refused to sell at any price, a "Buyout Clause", known as a "shotgun" clause in company law.

Put under a shotgun clause:

1. one party makes an offer to buy out everyone else (usually other shareholders); and
2. the other parties who receive the offer must either, within a designated time, do nothing, and then they are deemed to have sold at the offered price, or make a higher bid back to buy out the first party, which the first party is usually forced to sell at.

The design of such a clause is to encourage proper bids for a fair value, being the price they would be willing to sell for, but assumes that the party receiving an offer is keeping an eye out for it.

On the Niftex platform all shard holders had 14 days from the buyout/shotgun clause being triggered to make a higher offer and buyout the first party, or be bought out automatically for the offered price.

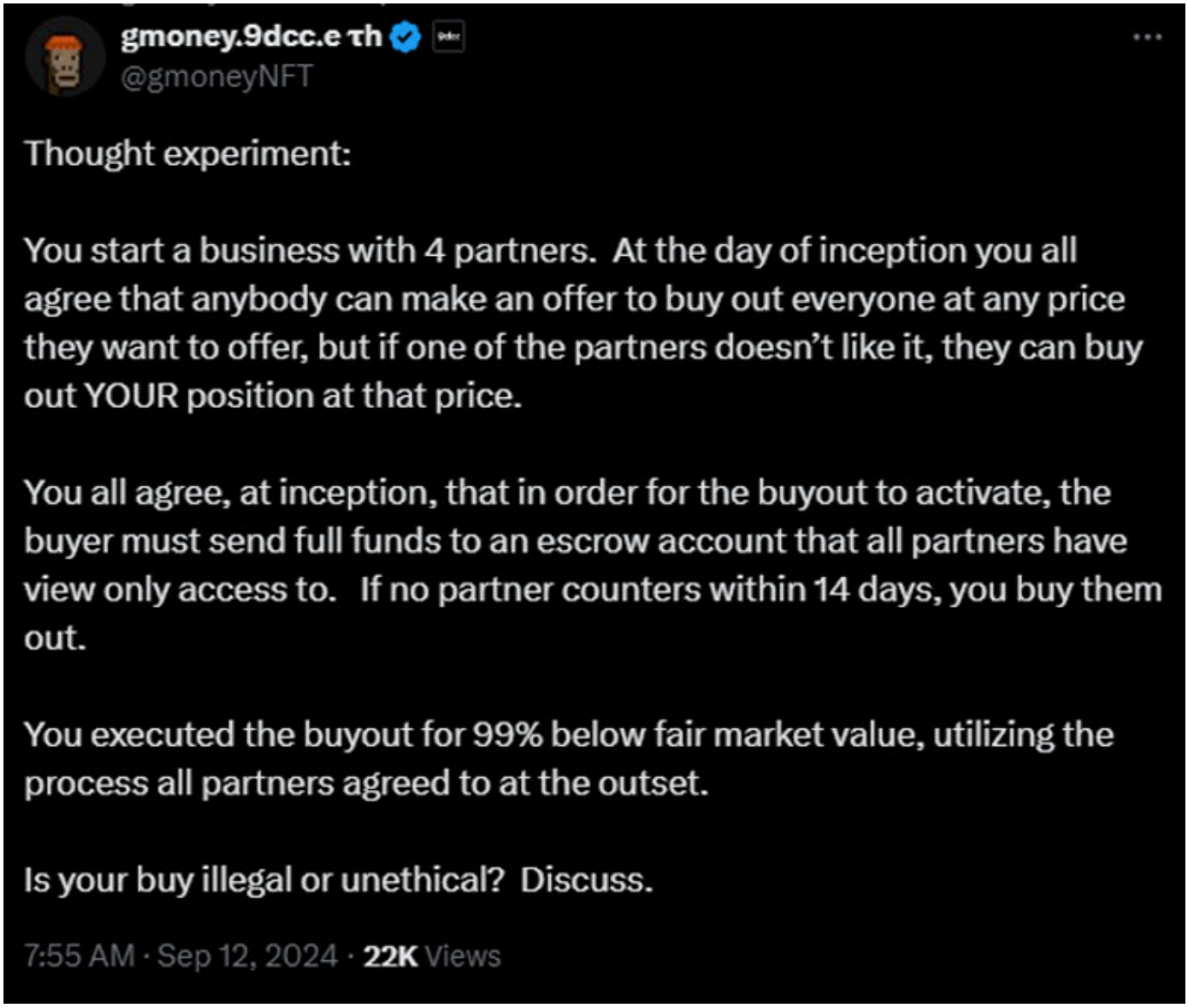
Niftex, however, shut down as the NFT market dropped, and with it whatever notification system was running on their web-interface. The smart contracts, however, are immutable and so the shotgun clause for all NFTs fractionalised on Nitfex can still be triggered by any shard holder. It is worth noting that Niftex's defunct Twitter/X account does point users to an address to monitor buyout/shotgun clause events, but it's not known if this site displayed this buyout offer.

One shard holder of Punk 2386 called the smart contract and triggered the shotgun clause, offering 10ETH or 0.001 ETH per shard (there were 10,000 shards). At least one other shard owner, known as Gmoney on X.com, became aware of the offer and attempted (with the help of some tech savvy folk) to interface directly with the smart contract to make an offer back, but said that his attempt was rejected. He has turned the situation into a thought experiment:

As a result, the unknown person obtained ownership of Punk 2386 and could accept the current bid of 600 ETH (USD$1.6M) for a fairly massive profit, they did immediately move it to another wallet. This situation raises some interesting legal questions including:

1. When users entered into the sharding arrangements, did they have sufficient notice of the terms and conditions, including the shotgun clause?
2. Does Gmoney have any claim in respect of his attempt to trigger a buyout of the original offeror, given the transaction failed (but the blockchain record shows there was an attempt to make an offer); and
3. How can other holders be sure to be on notice of other buyout attempts?

These issues go to the heart of the arguments around whether "code is law". For now, Gmoney has said on X.com "GG" to the Punk buyer, and has turned the matter into a "thought experiment" on X. So for practical purposes it seems code is law, in this case at least.



Written by Michael Bacina