Crystal

# Digital Asset, Blockchain Industry and Crime Trend Predictions 2023/4 Update

October 2023

Authored by the Crystal Intelligence Team

# Introduction

Earlier this year we published our debut Digital Asset, Blockchain Industry and Crime Trend Predictions report in which we established our predictions for how we expect criminal activity to develop in response to enforcement actions, legislation and other disruptions.

The aim was to provide professional guidance to policymakers, investigators and compliance teams who seek to understand risk.

As a follow-up to this report, and as an exercise in intellectual rigor, we have, as promised, reviewed developments over the past six months across crime, legislation and technology for accuracy and published them in this update.

Our predictions have been partially supported by events; however, in some cases, it has been necessary to update our expectations based on developments.

**Nick Smart**
Director of Blockchain Intelligence,
Crystal Blockchain

# Table of Contents

# Summary of Key Developments

- **Darknet marketplaces have not noticeably increased in number or size**, but a general trend has been observed for more sites to operate on Social Media platforms; in particular, Telegram is increasingly popular.

- Corresponding to its abundance, **fraud involving crypto assets has become increasingly localized and focused on jurisdictions lacking legal resources or frameworks to tackle it.**

- **Sanctions used against Crypto Asset Exchanges have мgenerally had a limited impact on their targets**; notably, Garantex, sanctioned by the United States Office of Foreign Assets and Control (OFAC), remains fully operational having processed over $20 bn USD since it was listed in April 2022.

# Crime

## Illicit Service Providers

**We predicted that:**

Darknet Marketplaces will increase in overall number but operate at smaller capacity to prevent disruption by law enforcement and identification by blockchain analytics tools, transitioning further to a decentralized over centralized operating model.

### Did it happen?

Sort of. Generally speaking, there has **not been an overall increase in 'Darknet' sites as we had predicted and as such, we cannot state that capacity has decreased**, though we note a trend for **more illicit marketplaces to operate on Telegram or other Social Media applications** instead of on TOR or other privacy-centric networks such as I2P, particularly across Russian language marketplaces.[1]

We believe that this is **largely due to a more streamlined and reliable User Experience**; '.onion' sites are frequently slow to load and subject to DDoS attack, and though accessibility is relatively simple with the installation of the TOR browser, discovery of illicit services is difficult and far less convenient when compared with Instant Messaging or Social Media applications.

That being said, it **does appear that illicit marketplaces are now more decentralized** and will continue to trend this way as the requirement for a store to operate a 'marketplace' on the dark web is less necessary.

**To that end, our revised prediction is:**

Illicit marketplaces will increase in overall number, however with an increasing preference for decentralization and accessibility instead of security. This poses both an opportunity and challenge for law enforcement and blockchain analytics tools; whilst collection of data and even disruption of services may be simpler, the relative ease and high speed at which new sites or communities can be set up will require more dedicated resources.

[1] privacyaffairs.com/dark-web-price-index-2023/

### What does it mean for crypto assets?

Crypto assets, notably Bitcoin, remains a highly popular method of payment for illicit marketplaces. The criminals that operate them will continue to prioritize the ability for funds to be converted into fiat currency over concerns of privacy. Despite advances in legislation and enforcement, there remains a stable 'grey' market for illicit funds to be converted.

### What things should we watch out for?

Early adoption of Layer Two network technologies into illicit platforms (i.e. Bitcoin Lightning Network), potentially frustrating detection by Blockchain Analytics tools.

Illicit vendors pivoting collection of funds from ease of conversion to protection of privacy (Bitcoin/USDT -> Monero, ZCash)

## FRAUD

## We predicted quite a few things for fraud!

> **This is what we predicted:**
>
> #1: As the increased adoption of crypto assets proliferates to new territories and regions, there will be a rise in localised fraud.

### Did it happen?

As shown in our report on Iran's relationship with crypto assets, there are indications that fraud has become more localized.[2] This has not been limited to Iran; we have detected a rise in schemes targeting consumers in India and South America. Lamentably, fraud remains very profitable overall, driven by an almost industrial approach by some groups.

What has been common between these regions is **a lack of regulation and effective supervision**; this has been readily exploited by criminals generally located offshore, as consumers **lack access to reputable domestic providers**. It is strongly acknowledged by Crystal Blockchain that regulation does not necessarily prevent fraud from occurring, particularly if it originates offshore, though it does enable recourse against rogue operators and allow the promotion of responsible local businesses in place of a fraudulent alternative.

[2] "Iran's love-hate relationship with Crypto: looking beyond on-chain data", Crystal Blockchain (crystalblockchain.com/investigations/irans-love-hate-relationship-with-crypto-looking-beyond-on-chain-data/)

**Our revised prediction is, therefore:**

Increased awareness of Crypto Assets in new markets lacking robust regulatory and enforcement frameworks will have a corresponding rise in fraud, generally originating offshore.

### What does it mean for crypto assets?

Regulation, international cooperation, and enforcement remains the key to preventing fraud. By offering a domestic licensing framework, Governments are better positioned to protect consumers through the promotion of trusted onshore entities that can be held accountable. These frameworks should be supported by concerted awareness campaigns to educate consumers of the tactics used and how to remain vigilant.

**We predicted that:**

#2: An increase in self-custody, prompted as a part of the ongoing response to scandals at centralized exchanges, results in a corresponding increase in theft from personal wallets.

### Did it happen?

There are certain limitations that make it hard for blockchain analytics tools to detect self-custodial wallets; typically, this is performed using a basic activity heuristic – we would expect a service provider to have a very high number of daily transactions, for example.
With this in mind, any trend is harder to establish as definitive, though for illustrative purposes and bearing in mind these limitations we can state that the prediction that self-custody will increase is supported by on-chain data.

However, data on theft from self-custodial wallets is more difficult to obtain at similar scales and we are highly reliant on user reported data. During the reporting period we added 1563 entities that were reported as receiving stolen funds[3]; representing an increase of almost 750% for the same period last year.[4]

[3] This does not indicate the total number of affected users; moreover, it is indicative of the thefts overall and the destination of the funds.

[4] There are several potential reasons for this variance including better and more reliable detection and labelling of stolen funds; increased user reporting and awareness; and greater blockchain coverage by Crystal's Data and Intelligence team.

**As such our prediction remains unchanged, though with an added caveat of transparency about data provenance:**

As far as we can determine overall, an increase in self-custody, prompted as a part of the ongoing response to scandals at centralized exchanges, results in a corresponding increase in reported thefts from personal wallets.

### What does it mean for crypto assets?

As with fraud prevention, greater international cooperation is needed to tackle theft overall. Initiatives to increase the efficiency and audience of theft reports across transaction monitoring tools and service providers may be effective in assisting the recovery of stolen assets; though criminals are likely to respond with more sophisticated laundering techniques, reducing the potential destinations for stolen funds will allow for more positive outcomes for victims.

**This is what we predicted:**

#3: Crypto asset signal fraud, often combined with paid promotion of projects will gain increasing levels of regulatory and law enforcement attention. Social media influencers will reduce their campaign of support following fines.

### Did it happen?

**Yes**, though lamentably, paid marketing campaigns using social media influencers remain relatively abundant albeit there has been an overall decline. Notable cases include those brought against celebrity endorsements of FTX[5], and CryptoZoo[6] among others.

[5] reuters.com/legal/ftx-celebrity-promoters-say-crypto-investors-cannot-sue-over-accounts-2023-04-17

[6] decrypt.co/120502/logan-paul-faces-rug-pull-class-action-lawsuit-over-cryptozoo-nfts

**This is what we predicted:**

#4: Deepfakes, vastly improved by advances in the efficiency and availability of Artificial Intelligence (AI) will make fraud more effective and profitable. Software such as chatGPT may be adapted for social engineering, as well as creating fake documents. This may also lead to more effective evasions of customer screening tools.

Did it happen?

**Yes.** No need to revise our prediction as we consider it extant.

**This is what we predicted:**

#5: As more Central Banked Digital Currencies (CBDCs) are launched, the possibility of vulnerabilities emerging will rise correspondingly; a theft affecting a CBDC, at the contract level is executed.

Did it happen?

**No.** Though we consider this risk as having a low chance of occurring, it remains extant.

**This is what we predicted:**

#6: Insider attacks are used as a method to cover losses by rogue crypto asset services.

Did it happen?

**No / Don't Know.** Whilst there have been several high-profile theft cases over the past months, few have been attributed to insider access. This risk remains extant.

## SANCTIONS

**Overall, we predicted fairly negative outcomes on the effectiveness of sanctions in that they would simply be sidestepped by those affected.**

> **This is what we predicted:**
>
> #1: Sanctions will continue to be of limited impact to dissuading illicit activity. However, they will be used more widely to control privacy-enhancing services. Sanctions, in their current form, will continue to have a short-term disruptive impact against illicit activity.

### Did it happen?

**No/Yes.** The mechanism of sanctioning crypto asset service providers (CASPs), and specifically addresses, has not been employed widely outside the United States Office of Foreign Assets and Control or Israeli National Bureau of Counter Terrorism Financing.

Sanctioned entities, specifically Garantex, have been able to continue operating almost unabated despite the short-term disruption achieved following their announcement as sanctioned. Sanctions against crypto asset wallets have not changed the payment behavior of many groups involved in illicit activity, such as ransomware gangs. That being said, a public announcement by Hamas that it no longer was soliciting donations in crypto assets[7] may suggest that this may not be a general trend and is effective in some circumstances.[8]

### What does it mean for crypto assets?

Sanctions are a tricky topic for crypto assets, for as long as there remains access to the broader market that does not impose sanctions due to a lack of legal sovereignty, or even deliberate ignorance, they will be ineffective. In addition, the publication of sanctioned addresses, particularly for service providers, is of limited use if the provider simply migrates to new infrastructure – a technique that we have observed in use.

For sanctions to be effective, greater cooperation is required to constrain the target's access to the market. A particular area where influence could potentially be exerted is against stable coins held against the value of an asset under the purview of the sanctioning state.

[7] reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28

[8] 'Terrorist financing trends: Crypto in decline?', Insight Intelligence newsletter.insightthreatintel.com/p/terrorist-financing-trends-crypto

**This is what we predicted:**

#2: There would be greater enforcement of sanctions against non-compliant CASPs. We stated that: Centrally issued stablecoins that continue to be traded in sanctioned countries will face legal challenges, including fines. Fines will levied against CASPs that continue to trade with sanctioned entities.

Did it happen?

**Not yet/wait and see;** though there have been increasing complaints and salacious accusations levied against the largest exchange, Binance, regarding its compliance with sanctions among other allegations, there has been no increase in penalties as yet.[9] There has also been no action against stablecoin issuers, though there has been an increase in media reporting around the use of stablecoins as a means for sanctions evasion.[10]

**This is what we predicted:**

# 3: Finally, we expected there to be specific repercussions and sanctions against owners of services that facilitated illicit activity:
Sanctions will be extended to owners of CASPs that facilitate illicit activity.

Did it happen?

**No.** This risk remains extant.

[9] Case 1:23-cv-01599: SEC vs Binance Holdings, Limited, BAM Trading Services Inc, BAM Management US Holdings. sec.gov/news/press-release/2023-101

[10] "FROM RUSSIA WITH CRYPTO: MOSCOW-BASED EXCHANGES OFFERING TO ANONYMOUSLY CONVERT STABLECOINS FOR CASH IN THE UK", Transparency International

## LEGAL

We did not anticipate any dramatic changes to legislation, largely as the policy is generally broadcast well in advance; however, we remain concerned about the credibility of blockchain analytics in investigations.

> **This is what we predicted:**
>
> Corresponding to an increase in prosecutions of alleged criminals and Service Providers, Blockchain Analytics tools will be more openly challenged for the credibility and reliability of their data; in particular, cases involving de-mixing of transactions.

### Did it happen?

**Yes.** There is at least one high-profile case against a major blockchain analytics firm currently underway in the US; an expert witness called by the defendant has made several accusations regarding the reliability of the providers clustering heuristics, describing them as 'overly inclusive'.

### What does it mean?

At this stage, it is not clear how this case will transpire though the industry is likely to question methodology and approach.

We also believed that 2023 would be the 'year of asset recovery', with greater awareness by law enforcement of the capability to trace and recover stolen or fraudulently obtained funds.

> **This is what we predicted:**
>
> Asset recovery becomes more commonplace in tandem with an overall rise in fraud. New legislation and powers to seize assets will be announced, resulting in an exodus of criminals to jurisdictions with no legal authority or capability to seize crypto assets.

### Did it happen?

Though fraud remains a major issue for crypto assets, there are indications that actions taken by law enforcement and industry are starting to bring results. Initiatives like 'Operation SHAMROCK', led by Santa Clara prosecutor Erin West, have set a precedent for others that shows it is possible for action to be taken and funds recovered.[11] That being said, the amount recovered is largely superficial in comparison to what has, and is being taken.

## TECHNOLOGY

**Though there have been several advancements in technology over the past months, we made the following predictions:**

> **This is what we predicted:**
>
> Following continued abuse, Ren is forced to shutter in 2023 leaving the market open for cross-chain bridging, creating opportunities for a new *de-jour* service to emerge by certain illicit groups.
>
> In particular, TRON supporting bridges will be more sought after alongside a corresponding trend for fraud to use this network.

### Did it happen?

**Yes/sort of.** The front page of Ren's website is now down[12], and the bridge page shows a message from Kroll and states that all assets into Ren have been taking into custody. TRON bridges are not necessarily more abused than any other. It is clear that cross-chain protocols offer a key capability for anyone wishing to slow fund tracing efforts and present a unique area of risk that must be managed carefully by receiving service providers.

[11] "This Bay Area prosecutor wants to help police nationwide take on 'pig butchering' scams" cyberscoop.com/erin-west-pig-butchering-cryptocurrency-scams

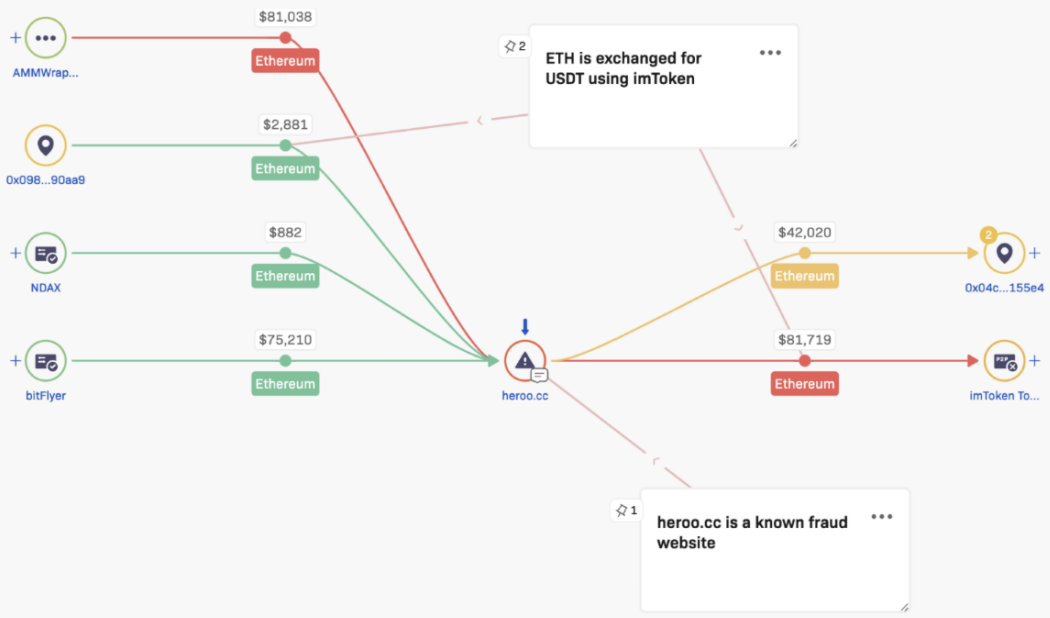
[12] renproject.io

April 11, 2023 –We wish to inform the Ren community that FTX Trading Ltd. (d.b.a. FTX.com), West Realm Shires Services Inc. (d.b.a. FTX US), Alameda Research LLC, Maclaurin Investments Ltd., and certain of their affiliates (together, the "FTX Debtors"), which had purchased the shares and all of the assets of the Ren Protocol entities, authorized and directed the Ren Protocol entities to transfer of all cryptocurrency assets into the FTX Debtors' cold storage wallets for safeguarding, in advance of possible shutdowns of infrastructure and systems. The cryptocurrency assets will be transferred to distinct segregated wallets cold storage wallets designated for these assets transferred by Ren, separate from the other Debtor cold storage wallets.

Case-related information can be found on the docket of the chapter 11 cases and on FTX Debtors' claims agent website at https://cases.ra.kroll.com/FTX/.

FTX

There is also an emergence of new services that have gained notoriety for use by criminals and nation state threat groups such as 'Sinbad', a custodial mixing service, and IMTOKEN, a token swapping service that has found utility for several fraud groups converting Ethereum or USDC to USDT.



We also missed a fairly significant development; the proliferation of Layer Two technologies, such as the Lightning Network for Bitcoin, and Optimism, for Ethereum.

**To that end, we offer the following revised predictions:**

Decentralised Protocols, particularly those that enable automated swapping of tokens or cross chain transactions, will remain critical points for criminals seeking to launder funds post theft or fraud.

In the mid-term, Layer 2 payment systems will spread in popularity and grow in complexity, posing great challenges for crypto asset service providers and blockchain analytics tools.

## Conclusion

While some of our initial predictions in the 2023/4 update of our Digital Asset, Blockchain Industry, and Crime Trend Predictions report have been partially supported by events, it is essential to acknowledge the dynamic nature of this space and the need for ongoing analysis and adaptability.

Key insights from this update include:

**1. Darknet Marketplaces:**
We noted a shift in the location of illicit marketplaces, with a trend towards operating on social media applications rather than privacy-centric networks. This shift is driven by the improved user experience and accessibility social media platforms offer.

**2. Illicit Service Providers:**
The prediction that illicit marketplaces would become more decentralized has been reaffirmed, emphasizing law enforcement and compliance teams' need for resources and vigilance.

**3. Crypto Assets and Fraud:**
Despite advances in legislation and enforcement, crypto assets, particularly Bitcoin, remain popular for illicit transactions. We observed an increase in localized fraud schemes targeting regions like India and South America, highlighting the importance of regulation and supervision to combat fraud.

**4. Self-Custody and Theft:**
As more users turn to self-custody solutions, we noted an increase in reported thefts from personal wallets. The trend of self-custody is expected to continue, requiring enhanced awareness and security measures.

**5. Social Media and Crypto Asset Fraud:**
The prediction that crypto asset fraud, combined with paid promotion of projects, would attract regulatory attention and reduce influencer campaigns has materialized, with notable cases involving celebrity endorsements.

**6. Sanctions:**
Sanctions have had a limited impact on dissuading illicit activity, and their effectiveness remains debatable. More extensive international cooperation is needed to make sanctions more effective.

**7. Asset Recovery:**
With new legislation and powers to seize assets, asset recovery efforts have become more common. However, the impact varies, and criminals may seek refuge in jurisdictions with limited legal authority.

**8. Technology:**
Layer Two technologies like the Lightning Network and Optimism have grown in popularity, posing challenges for crypto asset service providers and blockchain analytics tools. Decentralized protocols for automated token swapping and cross-chain transactions remain critical for criminals seeking to launder funds.

In this ever-evolving landscape, policymakers, investigators, and compliance teams must remain vigilant, adapt to emerging trends, and continue collaborating to address digital asset and blockchain industry challenges.

The future of this space will be shaped by technological advancements, regulatory developments, and the ability to stay ahead of criminal activities.

**To learn how Crystal can help transform your approach to crypto compliance, please book a demo here.**