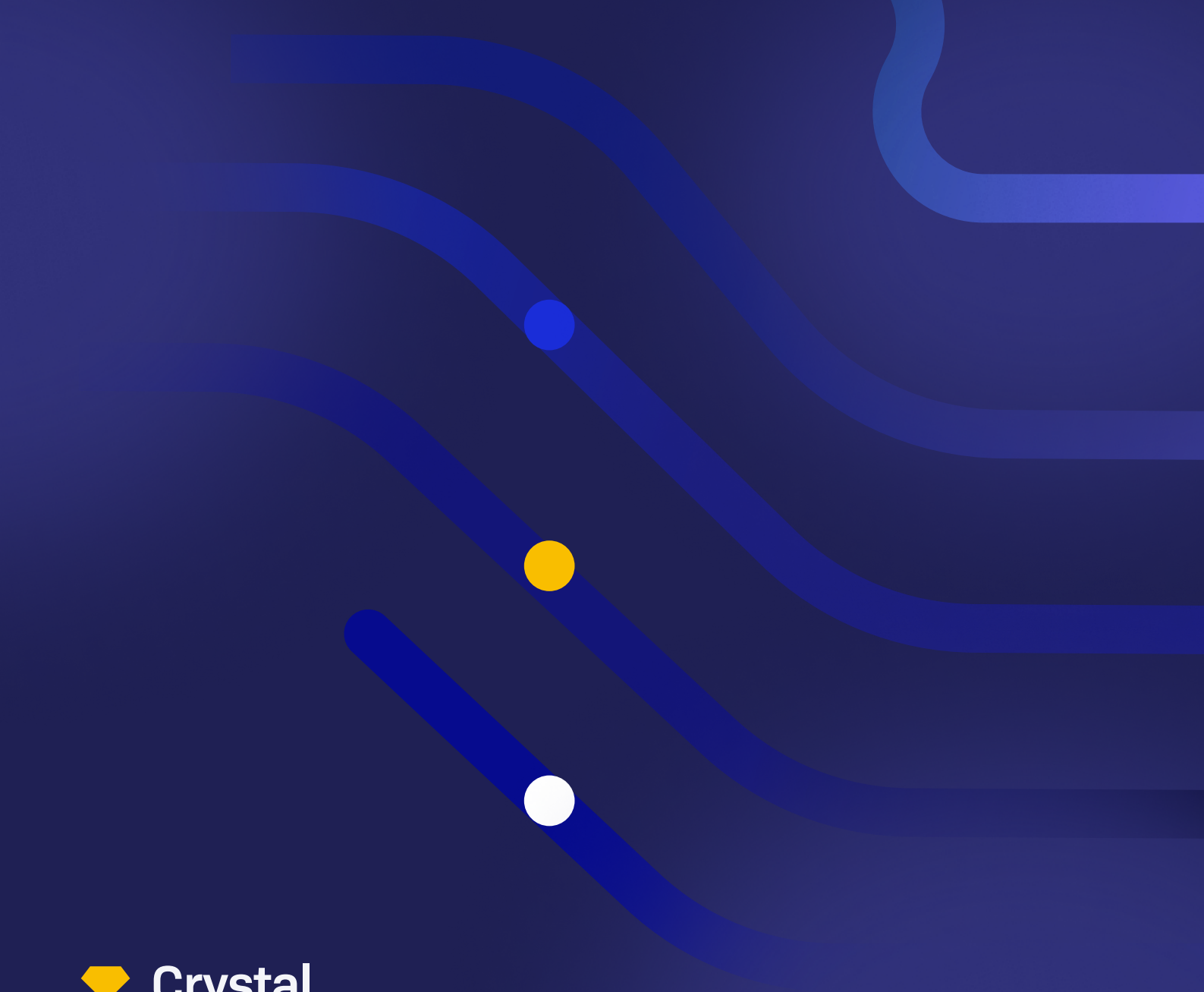


Crystal

Digital Asset and Crime Trend Predictions 2023/4

March 2023

Authored by the Crystal Blockchain Intelligence Team

Foreword

Though the general principles of financial crime remain largely the same, criminals and other illicit actors continue to seek new ways raise, store, move, and spend crypto assets. This report establishes our predictions for 2023; how we expect criminal activity to develop in response to enforcement actions, legislation and other forms of disruption. We will periodically revisit this report throughout the year to see if our predictions are true, and make adjustments accordingly.

We aim to provide professional guidance to policymakers, investigators and other compliance staff who are seeking to understand risk, and those that create them.

Nick Smart
Director of Blockchain Intelligence,
Crystal Blockchain

Table of Contents

Introduction

For this report, we set about trend forecasting by researching and formulating predictions based on the behaviours we observe at the intersection of digital currencies, blockchains, regulation and financial crime.

By identifying the source, tracing the evolution, and recognising patterns of trends, we can provide law enforcement agencies, financial institutions and VASPs with an image of the future, and what possible actions to pursue.

To do this we research and identify specified markers which we detail below and predict how they are likely to affect future behaviour. Through this process, we can identify trends that will affect the digital currencies industry.

There are different types of forecasts:

- Long term forecasting, also known as 'macro trends', look at broader directional pointers that indicate the way society is changing.
- Short term forecasting provides a much more prescriptive sense of what may happen in the next 6 – 12 months.

Prediction Confidence Levels

- HIGH: 70-95% chance of occurring
- MODERATE: 40 – 69% chance of occurring
- LOW: >39% chance of occurring

We assign confidence ratings to our predictions based on the quality and availability of information we have obtained. It is not a quantative methodology, as some evidence may be more compelling in support of a particular course of action than another.

Predictions we are most confident in are rated high, which is usually indicative of several credible, reliable sources that support the hypothesis stated.

For predictions of moderate or low confidence, we lack the same quality of evidence or there are too many variables for us to be certain.

Low confidence predictions may have no direct evidence, or are believed to be unlikely during the timeframe specified due to other technical limitations.

Crime

Illicit Service Providers

We assess, with moderate confidence 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.

In detail: Following the shut down of Hydra marketplace in 2022, several alternatives have since appeared including OMG!OMG!, Mega, and Black Sprut – though we have reasonable grounds to suspect that they operated by the same individuals.

Larger services represent a greater vulnerability to disruption by law enforcement efforts, as well as attack by rival service providers. Operating several smaller sites may afford greater resilience and reduce the impact of disruption activity. Conversely, the more sites operated by a single group, the more likely that they in turn will be exposed to criminal activity against them i.e. thefts, hacks, and denial of services.

Impact:

- Ultimately this poses a greater challenge for the industry seeking to understand a larger network of illicit service sites.
- Proactive intelligence gathering against these targets may offset the risks posed by them, including looking for mentions of 'preferred' exchange services on various forums to mitigate both counterparty and individual service risks.

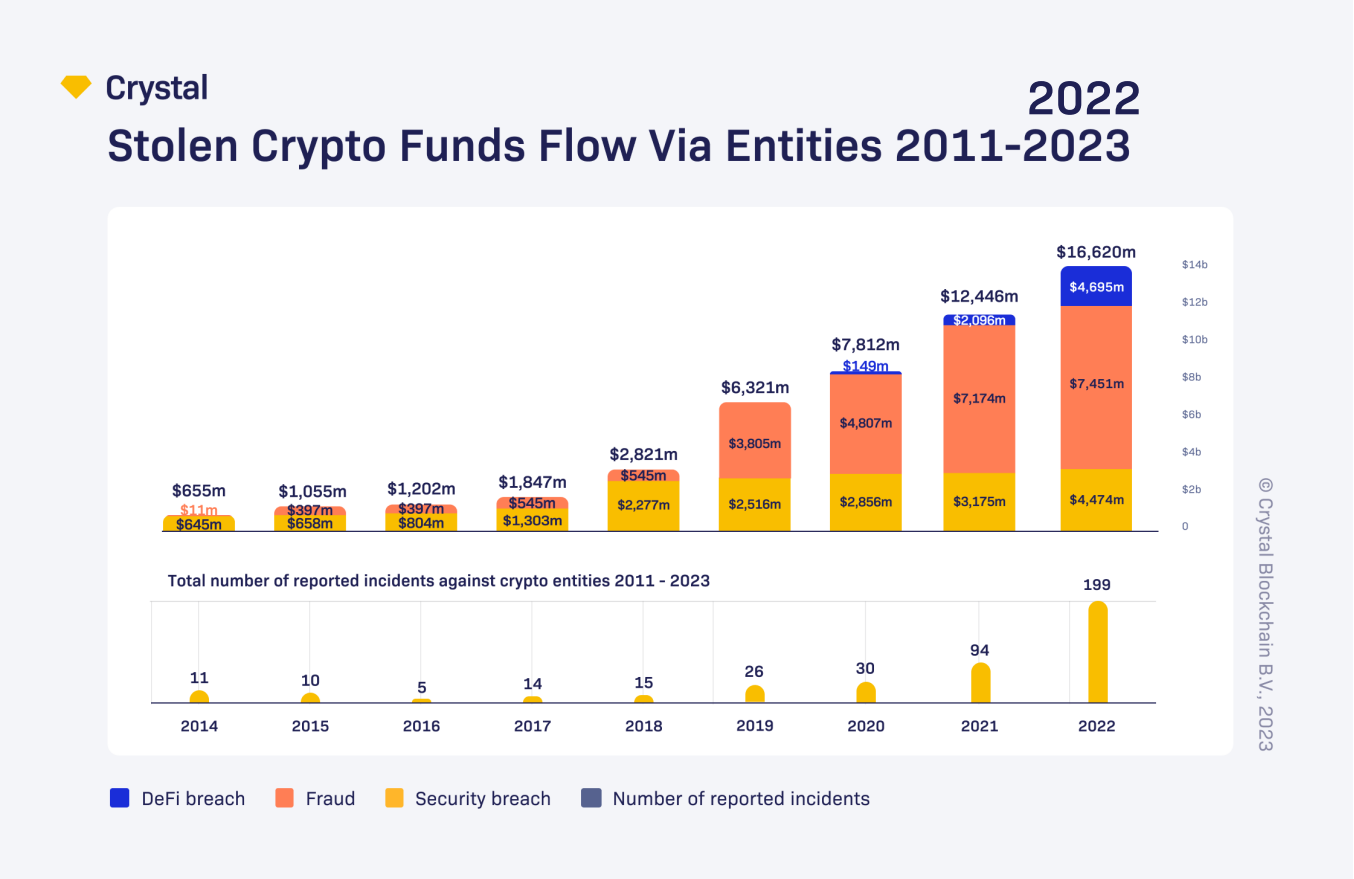
FRAUD

We assess, with high confidence that:

1. As the **increased adoption** of crypto assets proliferates to new territories and regions, there will be a rise in **localized fraud.**

In detail: Overall, all types of fraud have risen in recent times, however crypto assets are increasingly the ***de jour*** choice for criminals either directly – by taking crypto assets from victims, or indirectly, by using crypto assets as a vehicle to solicit attention from victims

Figure 1: Flow of stolen crypto funds via entities 2011- 2022.



As legislation often follows adoption, the opportunity increases for criminals to exploit inexperienced regulators who are unwittingly providing credence to their schemes. We have already noted an increase in crypto asset frauds targeting native speakers in the Middle East and North Africa regions.

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.**

In detail: To some extent, this has materialized already against NFT owners, who often use a self-custodial solution like MetaMask and are frequently targets of malware and social engineering.

However, as more users are compelled to self-custody, which we have identified in a corresponding increase in unhosted wallets, these users will be a greater target.

We assess, with moderate confidence that:

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.**

In detail: Following several high-profile legal actions against celebrities, such as Kim Kardashian by the United States Securities and Exchange Commission, many have distanced themselves from promoting crypto asset projects. Though there are often disclaimers in their correspondence – 'this is not financial advice' – this has not held up to legal scrutiny. Coordinated campaigns to raise the price of an asset, including a more conventional stock or bond, are under much greater attention and we expect there to be a corresponding level of enforcement.

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.**

In detail: Though perhaps not a true 'deep fake', there has been at least one high profile campaign targeting users of FTX in the past four months with a dubbed likeness of the platforms founder, Sam Bankman-Fried. Similarly, there have been several technical demonstrations of AI greatly enhancing the presentation of documents either used in, or to solicit directly, acts of fraud.

We assess, with low confidence that:

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

In detail: Throughout 2022, there have been many successful attacks against smart-contracts resulting in almost $3 billion USD of losses. It is assessed that a government-backed CBDC would represent an extremely high-payoff target for a criminal in terms of remuneration, or even a state-level group seeking to undermine the credibility of the target's financial system.

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

In detail: Amidst ongoing speculation as to the individual responsible, during its shuttering, funds from FTX were removed from the exchange and reported as stolen. There is a remote chance that this was not an external actor, but someone from within the service seeking to profit themselves. We believe that this incident may set a precedent to rogue businesses, who may seek to hide their own malfeasance through staged loss of funds.

SANCTIONS

We assess, with moderate confidence that:

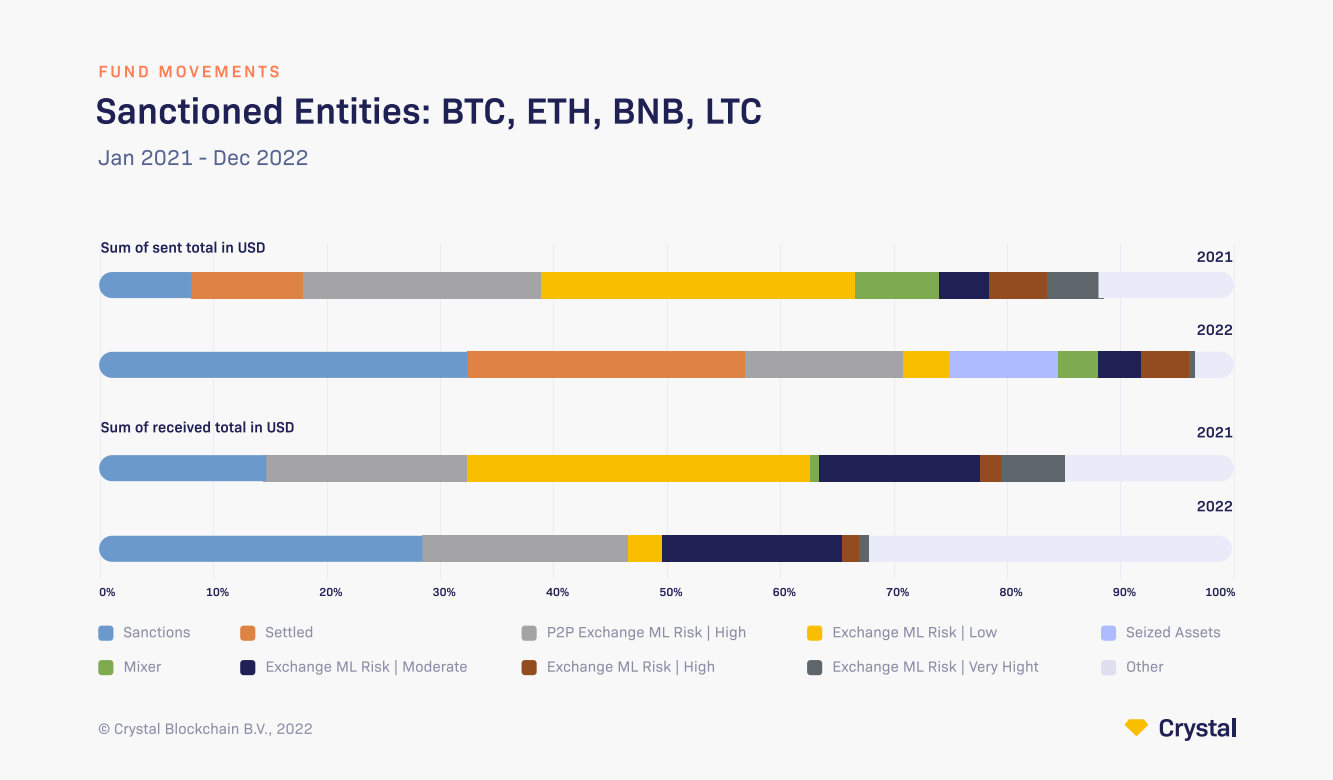
1. Sanctions will continue to be **of limited impact to dissuading illicit activity**, however, will be used more widely to control privacy-enhancing services.

In detail: Whilst not yet levied against a specific exchange, regulations from several jurisdictions – including Dubai's Virtual Asset Regulatory Authority in the United Arab Emirates – have outright disallowed privacy enhancing crypto asset types. We expect that this trend may be extended to services that provide support for these types from offshore locations.

2. Sanctions, in their current form, will continue to have a **short-term disruptive impact against illicit activity**.

In detail: Despite the US Office of Foreign Assets Control placing several Russian crypto asset exchanges under sanctions (Chatex, SUEx and Garantex), this has had little lasting effect - against at least Garantex who continue to operate. By not demonstrating a lasting disruptive effect, it is certainly an effective strategic message to those operators who maintain political differences.

Figure 2: Fund movement January 2021-December 2022 relating to sanctioned entity



3. Sanctions will be **extended to owners of Crypto Asset Service Providers** that **facilitate illicit activity.**

In detail: Recent action against Bitzlato, including the arrest of its founder by US authorities in joint operation involving international law enforcement is a precedent that we expect to continue as authorities seek a lasting disruptive effect against those who are facilitating criminal activity.

4. **Centrally issued stablecoins** that continue to be t**raded in sanctioned countries will face legal challenges, including fines.**

Fines will be levied **against Crypto Asset Service Providers** that continue to **trade with sanctioned entities.**

In detail: There have been several fines levied against crypto asset businesses who have failed to comply with sanctions regulations during 2022. We expect that businesses who are either complicit, or ignorant of sanctions breaches will face even steeper penalties as the supervisory regimen matures.

LEGAL

We assess, with moderate confidence that:

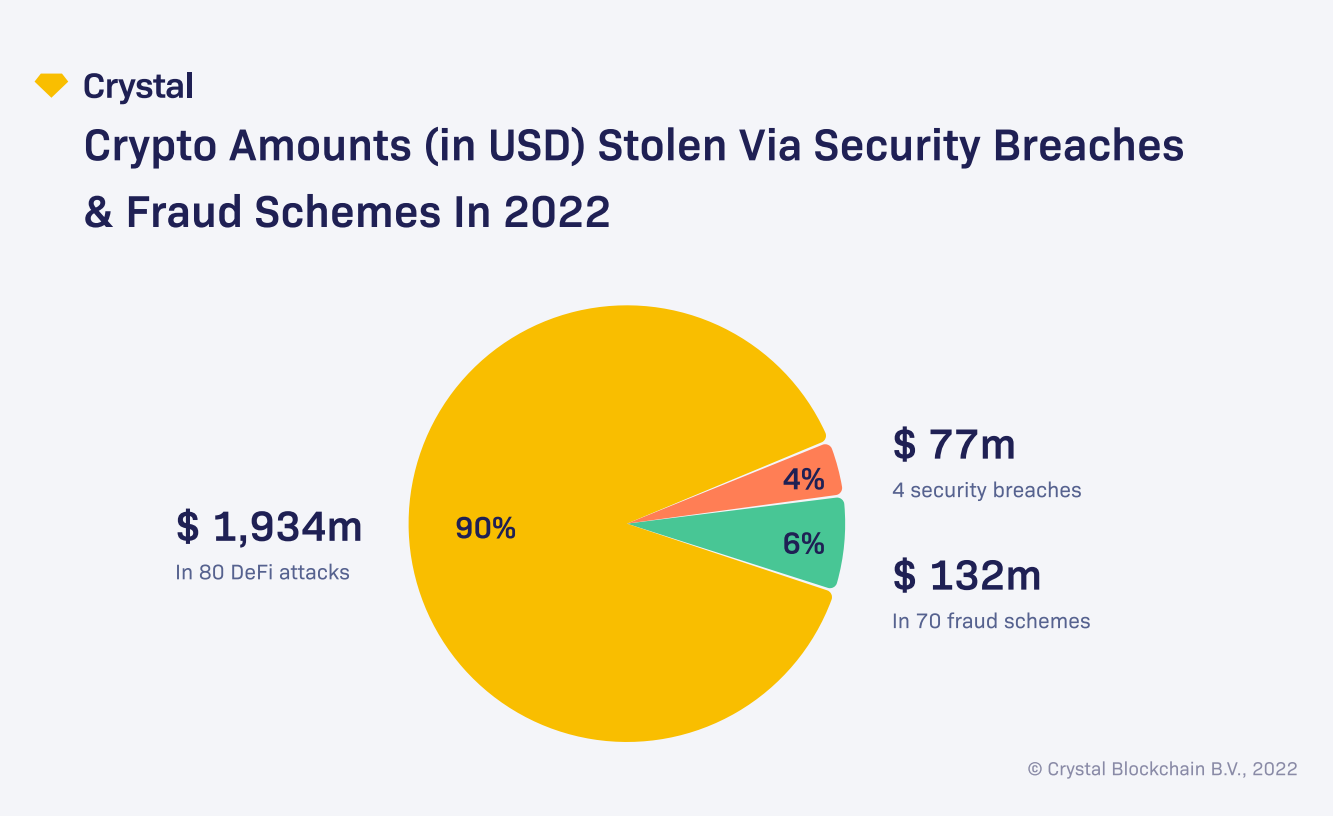
1. Corresponding to an increase in prosecutions of alleged criminals and Service Providers, **blockchain analytics tools** will be more **openly challenged for the credibility and reliability** of their data; in particular, cases involving de-mixing of transactions.

In detail: As blockchain analysis has become increasingly valuable to law enforcement and prosecution, there has yet to be a significant legal challenge to this form of evidence.

Whilst there are now several solutions available to the market that claim to perform de-mixing of transactions, this methodology may not stand up to scrutiny under legal examination. We expect this to be tested as defence lawyers become more familiar with the technical limitations of blockchain analytics tools.

2. **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.**

Figure 3: Crypto amounts in USD stolen through security breaches and fraud 2022



TECHNOLOGY

We assess, with moderate confidence that:

1. 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 detail: As noted by many observers, Ren has been consistently abused by criminal groups following thefts; it has gained favor with the North Korean linked 'Lazarus' group and as such, has a particularly tarnished reputation. With plummeting liquidity, as well as a notoriety for being used by criminals, we do not expect Ren to remain a viable option much longer.

2. **TRON supporting bridges will be more sought after alongside a corresponding trend for frauds to use this network.**

In detail: TRON has risen steadily in popularity as a Layer 1 blockchain over the past year and correspondingly has seen a rise in abuse by frauds; its main advantages being its speed and support for key stablecoins and tokens, such as USDT.

In summary, our top predictions are:

- Localized fraud will rise with the increased adoption of crypto assets in new territories and regions.
- We expect even more Darknet Marketplaces to appear.
- As more Central Banked Digital Currencies (CBDCs) are launched, the chances of one such CBDC being hacked increases.
- Sanctions will continue to have limited impact on preventing illicit activity.
- Blockchain analytics tools will be more openly challenged for the credibility and reliability of their data.