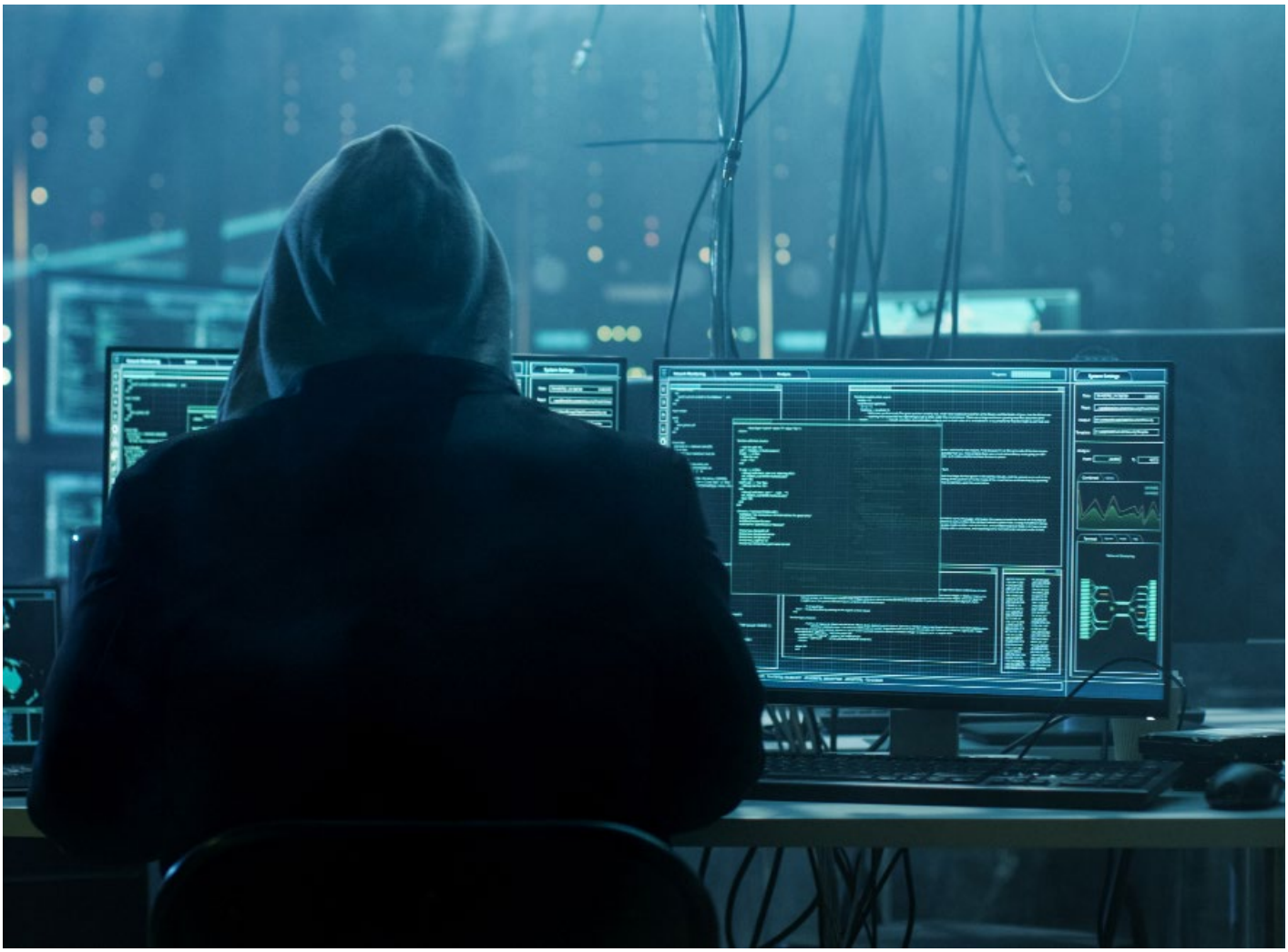
Deloitte.



Financial crimes with cryptocurrencies
What happened last year?

Crypto assets are changing the world and are also introducing new types of financial and non-financial risks. As this market is fairly new and partially regulated or supervised, those using or interacting with crypto assets can be vulnerable to financial crime risks. Although the cryptocurrency market offers many opportunities, companies and individuals should act with caution to mitigate the risk of financial crime associated with crypto assets.

Our financial crime experts have analysed trends on the crypto market for 2022 and 2023 and identified the most common financial crime typologies observed. This article provides snapshots of existing or potential risks for you and your business. In addition, we share insights into how you can protect yourself and your business and how we at Deloitte can support you.

An Old Friend for Criminals: Malware & Ransomware

Malware and, more specifically, ransomware is one of the most commonly used tools to steal funds from victims.

The term "malware" is used to describe any kind of malicious software: ransomware is a specific type of malware used to hold the victim's data, or systems, hostage. The intention is to prevent the victim from accessing these, and then to demand payment in return for regaining access: or to threaten to publish sensitive data, and then demand payment for not publishing. The majority of ransomware variants use centralised exchanges to launder the money they have taken.

In January 2023, BaFin issued a warning regarding "Godfather", a malware affecting banking and crypto industries in Germany. "Godfather" operates by imitating commonly used banking and cryptocurrency websites. When customers attempt to login, their login information is sent to cyber-criminals. To collect the codes for two-factor authentication, the virus also sends the associated notifications. The cyber-criminals were then able to access customers' accounts and wallets using the login information obtained. Approximately 400 banking and cryptocurrency apps, including ones based in Germany, were reportedly targeted by this malware in 2022.

Due to the significant risk of ransomware, in March 2023, FATF published guidance explaining how ransomware can be detected and how personal data (including financial data) can be protected. The FATF report examines the methods used by criminals to carry out ransomware attacks, including how payments are made and laundered. It proposes a number of actions that countries can take to more effectively disrupt ransomware-related money laundering, such as building on and leveraging existing international cooperation mechanisms, developing the necessary skills and tools to quickly collect key information, tracing financial transactions and recovering virtual assets. The FATF has also finalised a list of potential risk indicators that can help public and private sector entities identify suspicious activities related to ransomware.

Trade Without Oversight: Darknet Markets

Darknet markets offer a space for trading of illicit goods, including stolen personal data (used for identity theft), stolen credit card information, hacked crypto wallets, and even hacked social media accounts. Darknet markets have however experienced a drop in income since 2021. The Darknet market revenue reached $1.5 billion overall in 2022, a decrease from $3.1 billion in 2021.[1]

This drop is largely attributable to the seizure of Hydra. On 5th of April 2022, the German Federal Criminal Police Office (Bundeskriminalamt – BKA) announced the seizure of Hydra's Germany-based servers and cryptocurrency assets. The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury also sanctioned Hydra at the same time. Both federal agencies from the U.S. and Germany worked together on this coordinated operation. At the time, Hydra was the largest Darknet market by revenue and functioned as an intermediary for drug trafficking, sale of stolen documents (e.g. Personal IDs) and illegal cryptocurrency exchanges (in particular with Russian rubles) for the purpose of money laundering.

Next Generation Stealing: Hacks & Digital Thefts

One of the major risks associated with crypto assets is hacking which represents a significant problem for market confidence. Cryptocurrency theft totalled more than $3.5 billion in 2022, according to publicly reported attacks (e.g., $612 million was taken from Ronin Bridge, $321 million from Wormhole Bridge, and $190 million from Nomad Bridge). This figure is almost 51% greater than in 2021. Tokens, stable coins, and wallets are all targets for hackers, and they can be stolen directly from exchanges. Once obtained, hackers can trade them on centralised and decentralised exchanges to launder their stolen assets.

Not So Clever: Smart Contract Scams

Smart contracts are a useful feature of decentralized finance (DeFi), as they allow the provision of financial services, such as loans, without the need for conventional intermediaries. This can help people who are, for example, struggling to get a loan from a traditional bank to obtain the financial services they need.

Smart contracts are digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met. Smart contracts "live" in decentralised blockchain networks, meaning the data's security is dependent on the network's applied security protocols. A study released in 2018 by five researchers from the NUS School of Computing in Singapore , found that around one in twenty smart contracts are at risk for hacking. The study identified that three types of smart contracts are particularly vulnerable – those which either lock funds indefinitely, leak funds to arbitrary users, or are susceptible to being ended by any user.

Automated verification and DeFi security audits are the two main solutions to address smart contract risks, but they are not currently in common use. The FBI recommends that DeFi platforms establish real-time analytics, monitoring and rigorous testing to mitigate the associated risk; DeFi platforms are also advised to develop an emergency response plan.

Jackpot for Fraudsters: Online Casinos

Online gambling websites which accept fiat (e.g. €,$..) and crypto assets and provide unlicensed or unregulated gambling services can be used by criminals to launder money. Online casinos with no (or limited) KYC requirements allow criminals to keep their identities anonymous during the client onboarding process. Money laundering via casinos is not new and it is not restricted to online casinos. Generally, money launderers simply convert cash into casino chips, gamble on low-risk games, then convert the chips back to money which can be presented as casino winnings. Either way, illicit funds laundered via this method are very difficult to detect.

[1] "How Darknet Markets Fought for Users after Hydra's Collapse." Chainalysis, 16 Feb. 2023, https://blog.chainalysis.com/reports/how-darknet-markets-fought-for-users-in-wake-of-hydra-collapse-2022/#:~:text=Total%20darknet%20market%20revenue%20for,from%20%243.1%20billion%20in%202021.

[2] "Top Crypto Crimes in 2022." Coinfirm, 25 Jan. 2023, https://www.coinfirm.com/blog/crypto-crime-report-2022/.

[3] NUS School of Computing, 2018, Finding The Greedy, Prodigal, and Suicidal Contracts at Scale, https://arxiv.org/pdf/1802.06038.pdf. Accessed 29 Mar. 2023.

Selling Dreams: Exit Scams & DeFi Rug Pulls

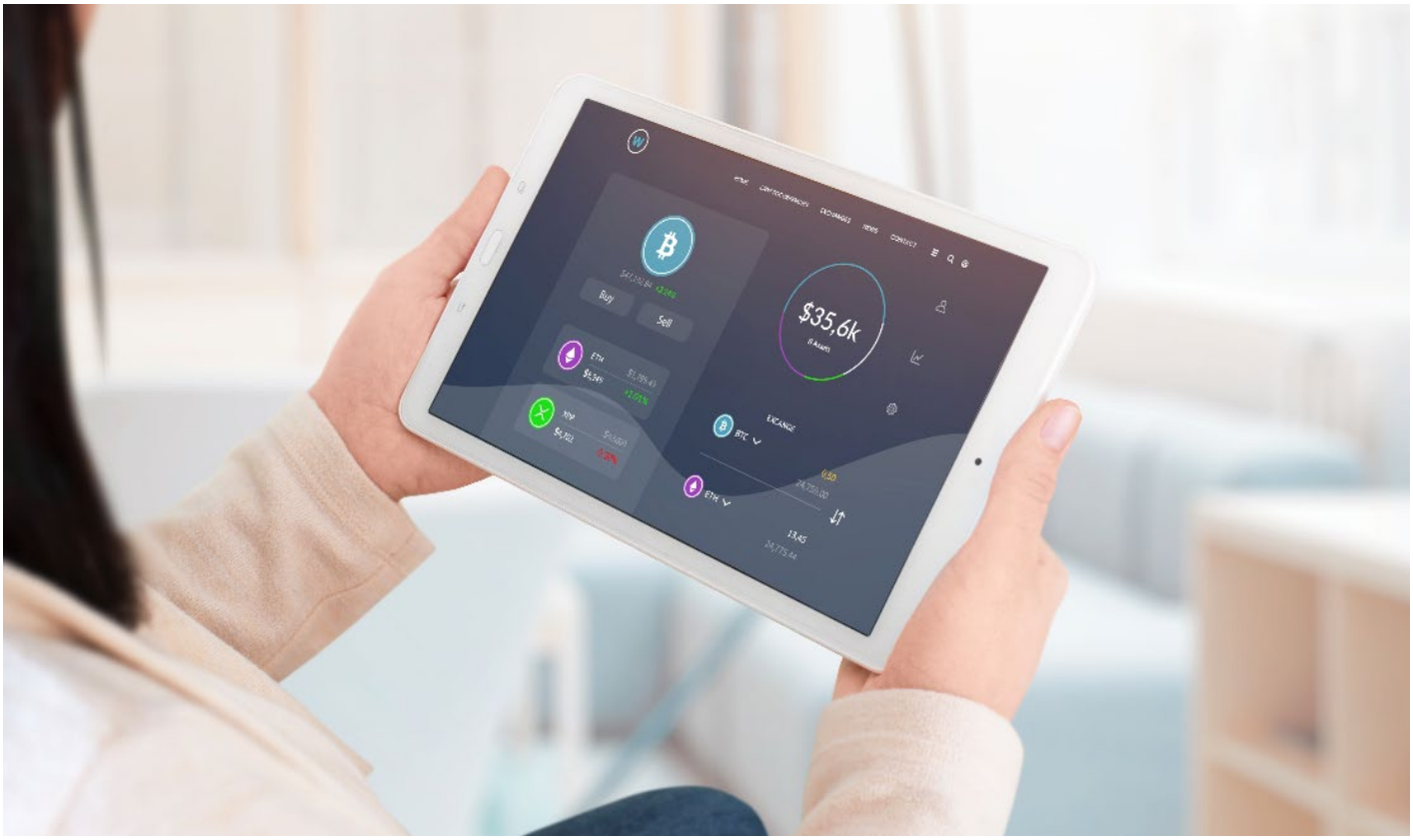
When the purported developers or promoters of a cryptocurrency collect funds from a group of investors, then take the funds collected without providing the promised asset, this is to be considered an "exit scam." The DeFi rug pull is a particular kind of exit scam that happens when a cryptocurrency project is completely abandoned. The funds collected are subsequently taken by the makers or promoters. These techniques echo those involved in a 'Ponzi Scheme' but with a modern touch to involve crypto assets. In particular, an exit scam is comparable to a Ponzi scheme that eventually comes to an end with the operator running away.

More than 125,000 rug-pull scams took place in 2022, up 50% from the previous year.[5]

Using a Front Man: Money Muling & Crypto ATMs

One of the most common methods used by criminals to transfer money is "muling"; use of real people who open accounts (usually legitimately) and transfer money on behalf of criminals. An example of this occurred recently in the U.K. University students responded to job advertisements promising them £500 to £1,000 per week to serve as brokers for cryptocurrency asset transfers. Agents of a criminal organisation then instructed them to open accounts on cryptocurrency asset exchanges and deposit money in round amounts of £700 in fiat currency into their bank accounts. This served as a mean for criminals to use cryptocurrency exchange accounts to launder the proceeds of fraud.

The awareness of the public is vital in fighting against this scheme. Money mules are becoming increasingly common at crypto ATMs in Europe, including those using fake or stolen IDs. Crypto ATMs are easy to use for criminals as they allow criminals to avoid the traditional financial system's controls over financial crime. There are around 1,200 crypto ATMs in Europe, including Russia.[6] Crypto ATMs provide a reliable method for rapidly transferring digital assets into fiat, or vice versa; in many jurisdictions, crypto ATMs remain unregulated or of unclear regulatory status.



[4] A Ponzi scheme is an investment scam that involves convincing victims of high returns and low risk with the help of fake reports. The profit for initial investors is financed with the money of newer investors. It is similar to a pyramid scheme and is used in different variations to this day. Ponzi scheme organisers often use the latest innovations, technology, or products to entice investors and give their scheme the promise of high returns.

[5] Strohe, Miriam. "2022 Gab Es 50 % Mehr Rug Pulls Als Im Vorjahr." Cryptomonday.de, CryptoMonday, 25 Jan. 2023, https://cryptomonday.de/news/2023/01/18/2022-gab-es-50-percent-mehr-rug-pulls-als-im-vorjahr/.

[6] Zandt, Florian. "North America and Europe Lead Bitcoin Atm Charge." Statista, Statista Inc., 7 Sep 2021, https://www.statista.com/chart/25707/number-of-bitcoin-atms-by-region/

It Never Gets Old: Phishing

Most people are familiar with phishing which is in fact deceptive emails aiming to steal sensitive information (personal data, passwords, account information etc.). An effort to steal cryptocurrency through phishing often targets a user's private key. In conventional finance, this would be comparable to obtaining login details for the user's bank account. Phishers may also target crypto assets through use of a deceptive smart contract. If a user approves this contract, the phisher is given permission to transfer the victim's cryptocurrency.

Phishing emails can be seen as simple to detect. It is however difficult to prevent them, especially for crypto assets and decentralised finance, given the lack of a centralised IT security system.

Vulnerable Means: Crypto Tokens

Crypto tokens (fungible tokens representing a set value or utility) do not always require KYC information from investors or documentation proving the source of the cash they used to buy Initial Coin Offering (ICO) tokens. As a result, such tokens are vulnerable to being used as an intermediary by criminals for money laundering. Criminals buy a token with illegally gained (potentially through the use of malwares or ransomware) crypto assets. Then, the criminals use an exchange that permits trading in tokens to exchange their tokens for fiat money or for other crypto assets. Once this trade is complete, it is very difficult to detect the source of the funds.

Same Method Different Tools: NFTs

A Non-Fungible Token (NFT) can be understood as a unique identifier showing ownership of a specific (often digital) asset, such as art, goods, or items in online games. Usage of NFTs is increasing on an ongoing basis. Purchasing of goods and services to obscure the source of financial assets is a well-established method of money laundering. NFTs can also be used for this scheme. NFT markets are also an easy targets for "rug pulls" – scams in which an NFT seller flees with money from the purchaser while failing to provide them with the NFT the purchaser was promised.

Papa Smurf is All Eyes and Ears: Peel Chain

Peel Chain is a method for funding a protracted string of minor transactions to conceal huge sums of Bitcoin gained illegally. Low amounts are repeatedly transferred (or "peeled") from a person's assets via an exchange where these illicit funds may be converted to fiat money. This technique is conceptually similar to Structuring or Smurfing. It can be considered to be an adaptation of the traditional Smurfing method for use on crypto assets. The most significant difference between Peel Chain and Smurfing is that when criminals successfully use Peel Chain techniques, the link to the first address where the stolen money is kept will remain hidden. In 2022 the US federal authorities arrested two people attempting to clear stolen crypto assets worth $4.5 billion which had been stolen in 2016 from Biftinex.[7] As Peel Chain was used in this theft, it was not possible to trace or recover all the assets stolen.

Off The Beaten Track: Mixers Like Tornado Cash

Crypto mixers play a vital role in crypto asset laundering by obscuring transaction flows. A crypto mixer is a service that combines the crypto assets from multiple users to mask the sources and owners of the cash. This kind of anonymity would ordinarily be difficult to establish due to the transparency of Bitcoin, Ethereum, and the majority of other public blockchains. Mixing services are not generally illegal, but a small number have been associated with services advertised to illegal dark web vendors, cybercriminals, and other illicit actors. The market also has observed the rapidly accelerating use of privacy wallets emerge as a favoured money laundering vehicle, privacy wallets have overtaken mixers as a preferred tool for laundering illicit funds.

In 2022, Tornado Cash was sanctioned by the U.S. OFAC (Office of Foreign Assets Control) for enabling users to launder billions of dollars in crypto assets, including $455 million suspected to have been stolen by North Korean hackers.[8] The restrictions block U.S. businesses and people from transacting with Tornado Cash and froze its U.S. assets.

[7] Ponciano, Jonathan. "Feds Seize $3.6 Billion in Stolen Bitcoin, Arrest Couple Five Years after Massive Crypto Exchange Hack." Forbes, Forbes Magazine, 9 Feb. 2022, https://www.forbes.com/sites/jonathanponciano/2022/02/08/feds-seize-36-billion-in-stolen-bitcoin-arrest-couple-five-years-after-massive-crypto-exchange-hack/?sh=173f7c607c95.

[8] News, Luke MacGregor/Bloomberg. "U.S. Sanctions Crypto Platform Tornado Cash, Says It Laundered Billions." The Wall Street Journal, Dow Jones & Company, 8 Aug. 2022, https://www.wsj.com/articles/u-s-sanctions-virtual-currency-mixer-tornado-cash-11659971832?mod=article_inline.

With Great Features Comes Great Responsibilities: Financial Crime Risks for Financial Institutions

Increasingly, financial institutions are announcing their intention to provide services related to cryptocurrencies, including custody and exchange. This new service portfolio brings with it new attention from criminals. Financial institutions can be directly exposed to all financial crime risks related to crypto assets, including institutions which do not directly provide these services. If a financial institution's customer has connections to Virtual Asset Service Providers (VASP) or other companies that deal with cryptoassets, they will be exposed to the related risk. The question numbered as '19 i3' in Wolfsberg Questionnaire (v1.4) may help to assist those risks.

To mitigate the associated risks, financial institutions should pay particular attention to high-risk customer behaviours such as sending funds to a VASP, transacting with a high-risk jurisdiction, offering trading in privacy coins[9], and transactions which include frequent payment references to cryptoasset related terminology (e.g. Bitcoin, Ethereum, crypto), and a lack of KYC requirements.

Our Service Offering

Our team continuously stays on top of developments in the crypto market in regards to regulatory requirements and financial crime typologies.

Our service offering includes (but is not limited to) ensuring compliance with local and global regulatory requirements such as the German AML Act (GwG), Transfer of Funds Regulation (TFR), Markets in Cryptoassets (MiCa), and supporting processes for client due diligence, transaction monitoring, and suspicious activity reporting to the German Financial Intelligence Unit (FIU).

[9] A type of cryptocurrency known as a "privacy coin" uses technology to make it almost impossible to connect a specific person to a transaction, ensuring the anonymity of all participants and the secrecy of information such as the transaction amount and the parties involved.

Contacts

Peter Schadt
Partner
Tel: +49 89 29036 8352
pschadt@deloitte.de

Deloitte.

Issue 01/2024