

THE HUMAN FACTOR
The limits of AI in investigations

CORRUPTION RECOVERY
Tracing stolen government funds

CRYPTO FRAUD
Crime, forensics and recovery

CDR

**Commercial
Dispute
Resolution**

www.cdr-news.com

April 2023

ESSENTIAL INTELLIGENCE:

Fraud, Asset Tracing & Recovery

Contributing Editor:

Keith Oliver
Peters & Peters Solicitors LLP

TA THE INTERNATIONAL ACADEMY
OF FINANCIAL CRIME LITIGATORS

**PETERS &
PETERS**



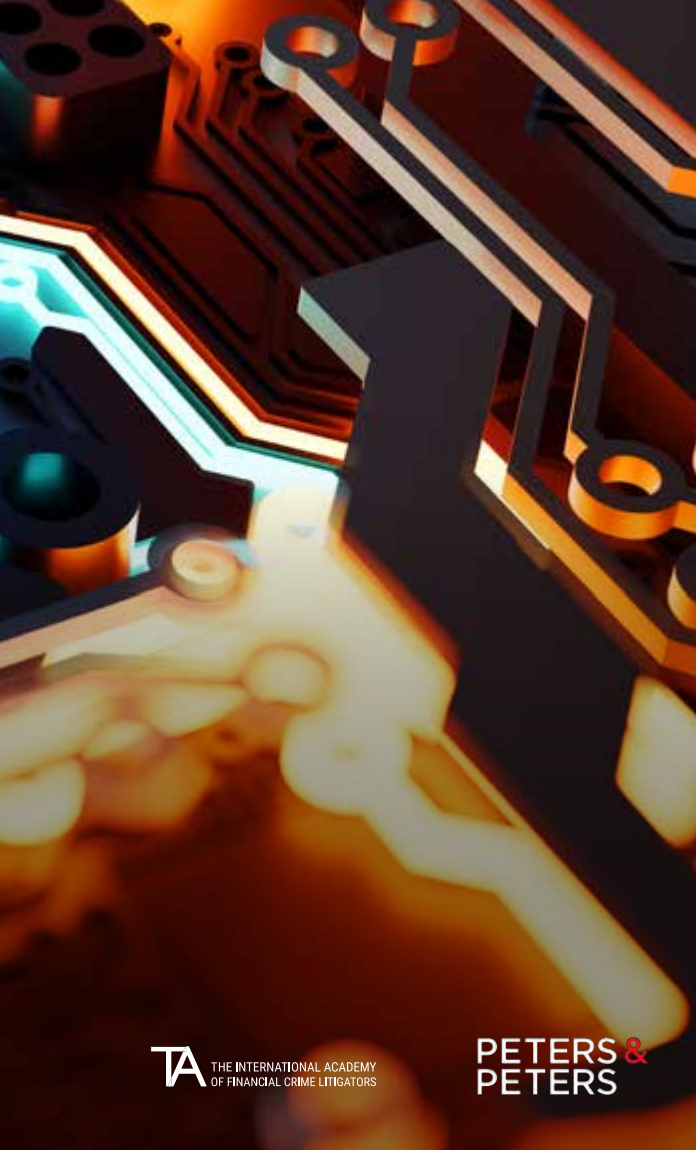
ESSENTIAL INTELLIGENCE:

Fraud, Asset Tracing & Recovery

EXPERT ANALYSIS CHAPTERS

- 8** Latin America: part of the global picture
Andrew Mizner
Commercial Dispute Resolution
- 11** Hi Ho (Crypto) Silver: Has the sheriff finally ridden into town?
Andrew Stafford KC, Calvin Koo & Timothy de Swardt Kobre & Kim
- 19** Crypto and forensics
Mansi Mehta & Hakob Stepanyan BDO
- 26** Cryptocurrency fraud and asset recovery
Syedur Rahman Rahman Ravelli
- 34** Insolvency and asset recovery in corruption matters
Angela Barkhouse Quantuma

- 41** Why we make such a mess of financial crime compliance – lessons from regulatory inspections
Nigel Webb Interpath
- 48** The English courts and international asset tracing
Olga Bischof & Theodore Elton Brown Rudnick
- 56** Why the need for human investigators will always exist
Olena Morozovska, Matt Taylor, Tom Stanley & Anastasia Beck K2 Integrity
- 62** Q&A with Joana Rego, co-founding partner at Raedas



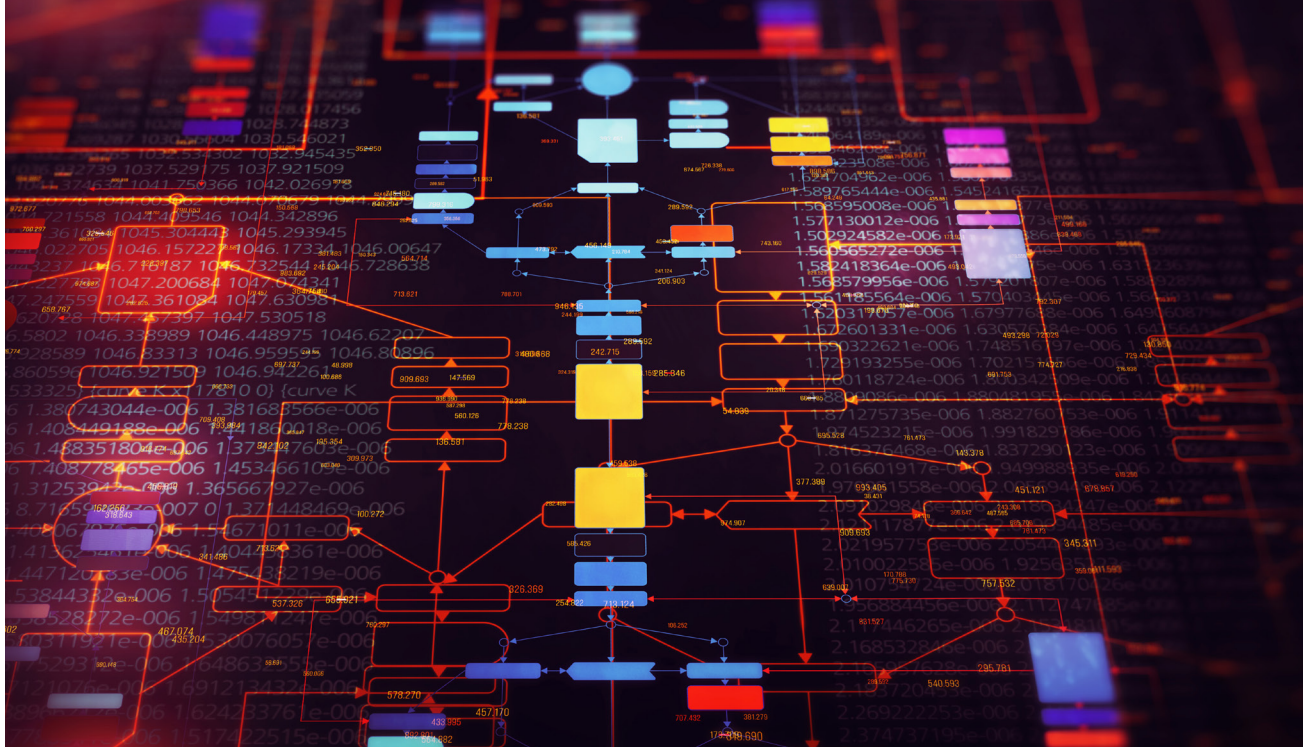
TA THE INTERNATIONAL ACADEMY
OF FINANCIAL CRIME LITIGATORS

**PETERS &
PETERS**

JURISDICTION CHAPTERS

- 67** **Bermuda**
Keith Robinson, Kyle Masters, Sam Stevens
& Oliver MacKay **Carey Olsen**
- 75** **British Virgin Islands**
Alex Hall Taylor KC, Richard Brown,
Tim Wright & Simon Hall **Carey Olsen**
- 87** **Cayman Islands**
Sam Dawson, Denis Olarou & Peter Sherwood
Carey Olsen
- 95** **Cyprus**
Andreas Erotocritou & Elina Nikolaidou
A.G. Erotocritou LLC
- 105** **England & Wales**
Keith Oliver & Caroline Timoney
Peters & Peters Solicitors LLP
- 117** **Germany**
Dr. Michelle Wiesner-Lameth, Tabitha
Schulze-Bünthe & Sarah Landsberg
act **AC Tischendorf Rechtsanwälte
Partnerschaft mbB**

- 127** **Guernsey**
David Jones, Simon Florance & John Greenfield
Carey Olsen
- 137** **Hong Kong**
Dorothy Siron **Zhong Lun Law Firm LLP**
- 151** **India**
Nitya Jain, Abhilasha Khanna & Samudra Sarangi
Panag & Babu
- 161** **Ireland**
John O'Riordan & Peter Bredin **Dillon Eustace LLP**
- 171** **Japan**
Hiroyuki Kanae & Hidetaka Miyake
Anderson Mōri & Tomotsune
- 181** **Jersey**
Marcus Pallot & Tabitha Ward **Carey Olsen**
- 189** **Liechtenstein**
Moritz Blasy, Nicolai Binkert & Simon Ott
Schurti Partners Attorneys at Law Ltd
- 195** **Singapore**
Wendy Lin, Joel Quek, Jill Ann Koh & Leow Jiamin
WongPartnership LLP
- 205** **Switzerland**
Dr. Claudia Götz Staehelin & Dr. Florian Baumann
Kellerhals Carrard
- 215** **United Arab Emirates**
Sara Sheffield, Max Davis, Peter Smith & Karl Masi
Charles Russell Speechlys
- 225** **USA**
Oren J. Warshavsky, Gonzalo S. Zeballos, Geoffrey
A. North & Tatiana Markel **BakerHostetler**



Crypto and forensics



Mansi Mehta
BDO



Hakob Stepanyan
BDO

At the beginning of 2023, over 420 million users worldwide owned cryptocurrency. In the last few years, we have seen public companies putting cryptocurrencies on their balance sheets, nation states adopting them as legal tender, and entire ecosystems being built around various layer one protocols. Today we have sophisticated financial products, retail transactions and a growing wave of institutional adoption of digital assets. Other than traditional cryptocurrencies, we have also seen an increasing adoption of Central Bank Digital Currencies (CBDC), Non-Fungible Tokens (NFTs), Decentralised Finance (DeFi) and Stable Coins in this evolving landscape. In addition, the recent crypto fallouts and bankruptcies highlighted that these episodes were not a crypto or a blockchain failure. The blockchain technology was resilient at its core. The fundamental reasons for these debacles were lack of internal controls, corporate governance, stress testing and risk management.

With the increase in global crypto adoption, criminals have found a way to use, abuse, and circumvent this network to their benefit. The illicit actors tend to gravitate to what they can exploit and adopt varying levels of sophistication to engage in criminal activity utilising digital assets. They have also capitalised on the industry's openness and anonymity to broaden their illicit activities. Since cryptocurrencies and other blockchain-based digital assets are a relatively new field, our understanding of the risks associated with them will keep evolving, and we still have a long way to go in understanding the full technical and economic implications.

Looking ahead, we can expect more traditional white-collar crime to enter the cryptocurrency space. We have already seen bad actors use cryptocurrency to evade sanctions, and as users become more sophisticated, so it is likely we will see digital assets used in bribery and kickback schemes. Criminals may also exploit the lack of uniform crypto accounting standards to manipulate financial statements.

For any organisation looking to engage with digital assets, the key to mitigating risks associated

- ➔ with crypto crimes are strong corporate governance, robust controls, compliance technology and employee competency. Should an organisation fall victim to crypto-related financial crime, there exist investigative tools that aid in the identification and recovery of funds. In this chapter, we will explore these tools and preventative measures that combat the risk of falling victim to crypto crime.

Old crimes with new currency

Crypto crimes are essentially financial crimes conducted on the blockchain. Financial crime is not new, but crypto crime is the latest creative mechanism to transfer funds illegitimately (e.g., to illicit wallet addresses on the blockchain). While darknet markets, money laundering and ransomware payments dominate the news cycle, by far the largest portion of illicit crypto asset activity is represented by scams, hacks, exploits and fraud. Below we will explore some of the common financial crimes involving crypto assets.

- **Frauds and scams**

“Rug pulls” (stealing initial investor funds) in the crypto industry were popularised during the “initial coin offering” (ICO) phase, now rebranded as “initial exchange offering” (IEO) or “initial decentralized exchange offering” (IDO). No matter the delivery method, the perpetrators’ objective is to issue tokens to raise



funds for a project and then abandon it at a later date. One of the more notable recent rug pulls was the Squid Game inspired meme token SQUID, a play-to-earn token that launched on the Pancakeswap decentralised exchange in October of 2021. The token drew in tens of millions of dollars from retail investors and rose in price from less than a penny to \$3,000 in 11 days. After the anonymous developers sold their tokens and extracted all the liquidity, they disappeared. All channels of communication, including the project website, were shut down.

- **Market manipulation**

Though the SEC has been actively enforcing laws against market manipulation since the early 2000s, the digital assets space is particularly challenging because of its global nature and developing regulatory landscape. A common market manipulation tactic is the pump and dump scheme where influencers or “project teams” embark on a campaign to amass a large community around a token launch or to reinvigorate interest in a particular token, only to draw exit liquidity for large holders to sell their otherwise illiquid cryptocurrency.

- **Hacks**

Criminals use hacks to steal private keys and drain cryptocurrency from victims’ wallets, with smart contract exploits one of the most common in DeFi platforms. Smart contracts are simple lines of code that are designed to self-execute the terms of an agreement between two parties, provided certain conditions are met. They have a wide range of applications that remove the need for intermediaries. However, many contain vulnerabilities that can be exploited. Once a smart contract is launched, most of the time, it is difficult to integrate the patch to correct the security flaws. Hackers have used these security vulnerabilities to steal funds from DeFi platforms and cross-chain bridges. 2022 was marked by several failures and thefts to the tune of \$3.8 billion.

- **Ransomware attacks**

Ransomware attacks have become more prevalent as cryptocurrencies allow for larger payments without the ability of a centralised intermediary, such as a bank, to freeze or track the payments. The attacker intrudes into a



victim's systems to encrypt the computer network and demand a cryptocurrency payment in exchange for a decryption key to recover the files. These attacks are a substantial and evolving threat to organisations and critical infrastructure, and the resulting damage extends beyond the extorted ransom. In 2021, a cybercrime group attacked an oil pipeline's devices on its network, stole files, and threatened to release them to the public. The company was forced to pay over \$4 million worth of cryptocurrency in ransom in order to restore the system. While the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) eventually recovered most of the funds, the attack was still highly disruptive, shutting down gasoline and jet fuel supply for large swathes of the pipeline's customers. In this case, the silver lining was the successful collaboration between the FBI and the DOJ. The recovery was an important milestone, as it was the inaugural event for the DOJ's newly created Ransomware and Digital Extortion Task Force.

- **Darknet Markets**

One of the earliest adopters of cryptocurrencies due to their pseudonymity, darknet markets are the illicit websites hosted on the dark web, which facilitate the illegal sale of drugs, arms, human trafficking and money laundering by enabling settlements in cryptocurrency. Although authorities were able to leverage the public blockchain data to shut down many of them, few remain in operation and rely on privacy coins to evade authorities. In April 2022, the joint task force that included the German federal police, FBI, Drug Enforcement Administration, IRS Criminal Investigation division, and Homeland Security successfully took down Hydra, the world's largest Russian-language darknet market notorious for fiat off-ramp services and mixers for cybercriminals as well as drugs, weapons and many illegal goods, among others.

- **Terrorism financing**

Nearly 20% of terrorist attacks were identified as crypto financed or linked to digital assets, and several terrorist organisations use cryptocurrency as a preferred source of fundraising to finance their operations. For instance, Hamas, designated as a terrorist organisation by both the United States and European Union, is noto-

rious for soliciting crypto donations through their website and Telegram channels, which is why it is important to stay vigilant with transaction monitoring and sanctions screening tools to keep track of wallet addresses belonging to sanctioned entities.

- **Sanctions evasion**

In recent times, sanctions evasion has become a popular topic of discussion among government officials, regulators and law enforcement, because sanctioned individuals are using crypto to move their wealth and evade sanctions. However, cryptocurrencies have been a popular tool for sanctions evasion by autocratic regimes for several years. Some look to cryptocurrency mining or issuing a virtual currency to evade sanctions, while others use state-sponsored hacking groups to steal funds through vulnerability exploits and other scams.

What ties all these illicit activities together is money laundering. For many of the bad actors, the end goal is to use the open and permissionless nature of public blockchains, along with the pseudonymity of crypto wallets and anonymity preservation techniques, to launder their ill-gotten gains and eventually transfer the funds to an "off-ramp" which converts cryptocurrency to fiat currency. This off-ramp can be a cryptocurrency exchange, an ATM, an over-the-counter desk, or a peer-to-peer marketplace. As we can see, crypto-asset-related financial crime is largely similar to traditional financial crimes. To identify and recover the proceeds from criminal activities, investigators will need to leverage traditional forensic accounting tools and techniques, along with detailed analysis of blockchain data to monitor and track transactions. With the limited exception of a few sophisticated illicit actors, the transparency of public blockchains significantly reduces friction for investigators to follow illicit movement of funds.

Blockchain analytics tools and investigative techniques

What happens on blockchain stays on blockchain

Tracing funds on the blockchain follows a similar procedure to traditional financial investigations – conducting digital forensics, reviewing documents and records, and analysing transactional data. In a

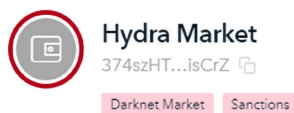


crypto investigation, the investigator will look for transaction identification (Transaction ID), wallet addresses, and in rare cases, seed phrases and private keys. Once identified, the investigator can follow crypto assets across different wallets, chains and jurisdictions with the help of sophisticated blockchain analytics tools and intelligence software.

Public blockchains are inherently transparent – all transactions are recorded in a public ledger that identify users by their wallet addresses, making this a good starting point to an investigative plan, even though the ledger may lack names, locations and other personally identifying details. Using blockchain intelligence software, investigators can uncover more ownership attribution data and perform forensic analyses that can identify the perpetrator and the end location of stolen funds. These tools are especially helpful when it comes to analysing large transaction volumes, and we will cover their capabilities below.

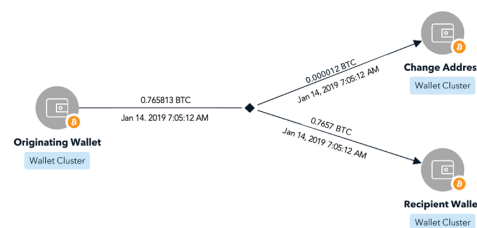
Attribution data

One of the key benefits of using a leading blockchain intelligence software tool is the rich attribution data. This means that the software provider has already conducted research using open-source intelligence, artificial intelligence and deep learning algorithms to provide information that ties wallet addresses to real world owners such as exchanges, darknet markets, individuals and organisations. The user may apply additional labelling and attribution data customised to his or her investigation to identify the illicit actors and entities involved in crypto crimes. Shown below are attribution tags applied to a blockchain wallet address, “374szHTL2KPyAmxtZTBYiJZN9aAA-QisCrZ”, associated with “Hydra Darknet Market”, a sanctioned entity.



Address clustering

In order to identify multiple wallet addresses that belong to the same user or entity, we rely on clustering algorithms that group related addresses together. Clustering helps identify additional wallets belonging to investigation targets, associates and counterparties. Two of the most common clustering methodologies are the common-input-ownership heuristic and change address heuristic detection algorithm. These algorithms will use an outgoing transaction and the return of the remainder to identify wallets that may be associated with one another. Below are three addresses that have been clustered together and associated with the owner of the originating transaction wallet.



Transaction mapping

When reviewing a transaction in a block explorer, we are presented with a substantial amount of useful details about the transaction, including the transaction hash, date, originating wallet address and recipient address.

Block explorer extract

Advanced Details			
Hash	1052-df1b 0	Time	22 Feb 2023 04:41:05
Age	10m 1s	Inputs	1
Input Value	0.00444171 BTC	Outputs	2
Input	\$105.53	Output Value	0.00441967 BTC
Fee	0.00002304 BTC	Output	\$104.99
Fee/B	\$0.55	Fee/B	10.240 sat/B
Fee/KB	16,000 sat/vByte	Size	225 Bytes
Weight	573	Weight Unit	4.021 sat/WU
Coinbase	No	Witness	Yes
RBF	Yes	Locktime	0
Version	1	BTC Price	\$23,759.46

Overview

JSON

From

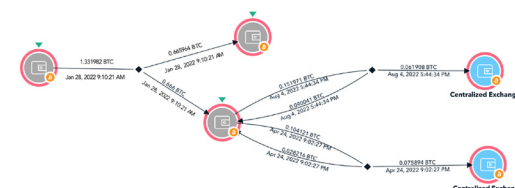
1 bc1qpkhstg75mabcmhup8tckr77375m73h 0.00444171 BTC - \$105.53

To

1 18C4vHML3poxuKdYyq28589fwQ51vk 0.0039932 BTC - \$94.81

2 bc1qpkhstg75mabcmhup8tckr77375m73h 0.00042853 BTC - \$10.10

With blockchain investigation tools, we can map the history of the transaction and any associated wallets in a fraction of the time it would take to search and keep track of each transaction manually. Additionally, the transaction map is more visually digestible and allows investigators to identify patterns and anomalies. Below is a map of the transaction flow related to a ransomware attack. In the transaction map below, we start with the ransomware operator’s clustered wallet attempting to obfuscate asset tracing by breaking up the outgoing transactions in what can be described as layering. However, thanks to the visualisation capabilities of the blockchain visualisation tool, we can follow the transaction to a centralised exchange. The crypto asset tracing exercise in this scenario leads to the identification of stolen funds that end in a compliant off-ramp exchange with anti-money laundering (AML) and know your customer (KYC) protocols, which means it will comply with court orders to freeze assets and share the illicit actor’s identification.



Some of the challenges we run into while investigating crypto transactions include privacy coins, mixers and non-compliant exchanges, which tend to be popular in the laundering process. In recent years,

we have seen chain hopping quickly become common practice for sophisticated illicit actors. Because different blockchains are not interoperable, some will attempt to obfuscate a transaction path by moving funds through multiple blockchains using dark web swapping services, “atomic swaps”, bridges, and decentralised exchanges. For example, the stolen funds may be converted from one cryptocurrency to another using a decentralised exchange where users are not required to provide documentation and go through KYC procedures. Although this complicates the transaction tracing exercise, a well-trained investigator can leverage attribution data and the powerful visualisation tools available in the blockchain intelligence software to follow along. In an ideal scenario, the transactions will be traced to a compliant exchange where KYC data is readily available and will follow court orders to freeze funds.

Preventative measures – corporate governance and best practices

Prevention is better than detection and recovery

There exists an entire spectrum of proactive and preventive measures that institutions and individuals may adopt to limit their exposure to criminal activity related to cryptocurrencies while navigating through this dynamic and niche digital asset ecosystem.

Prior to offering crypto-related products or services, transacting with cryptocurrencies, or adding cryptocurrencies to the balance sheet, institutions should take preventive measures to limit their exposure to crypto-related criminal activity. Organisations should review and update their policies and procedures, internal controls and educate their employees. It may also consider implementing transaction monitoring tools and engage with custody solution providers to ensure the safeguarding of their crypto assets.

If an entity wants to manage its own crypto wallets, then private key management becomes a critical piece from a trust and reliability perspective. Other than implementing strong mechanisms to safeguard the recovery phrase and private keys of the crypto wallet(s), the organisation may also assess establishing multi-party computation (MPC) or multi-signature wallets for private key security. MPCs are a relatively new method which does not require private keys to be stored in a single place. Instead, MPC breaks a private key into encrypted shares and divides it among multiple parties. These parties will independently compute their part of the private key share to produce a signature without revealing the encryption to the other parties, which means there is never a time when the private key is formed in one place; instead, it exists in a fully “liquid” form. In contrast, in a multi-signature setup, each person, or entity responsible for signing a transaction has a unique signature generated by a distinct private key. Depending on an organisation’s or an individual’s needs, one or both options are critical deterrents from hacks, phishing scams, or the many other methods of theft plaguing the industry.

One of the most important considerations for mitigating losses would be to conduct a comprehensive due diligence process prior to engaging in a crypto project. For custodians and centralised exchanges, it is important to understand how they are utilising cold storage (a signing device that stores a user’s private keys offline), whether they are comingling customer funds, and how they are securing private keys. With the collapse of several crypto-exchanges, organisations should be mindful of organisational structure, corporate governance, and the capabilities of those in leadership positions. Whether it is an investment platform or an acquisition target, scrutinising these attributes, along with risk management and transparency, could





enable efficient decision-making processes. For decentralised projects, certain aspects may be more easily analysed than others. For example, the code may be open source and available to review for vulnerabilities, but the founding team and developers are anonymous. Or, the review of the code reveals the economic model, governance model, and token issuance schedule, but there may not be any disclosures about pre-mined/minted tokens that were distributed to early investors, venture capitalists, and related parties. As such, the individual or organisation should make sure there is a firm understanding of the value add provided by the project along with existing risks and tradeoffs prior to making outsized investments.

These measures related to corporate governance and internal controls can assist in mitigating external and internal threats, such as fraud, hacks, loss of private keys, asset misappropriation, and fraudulent accounting and reporting, while helping establish effective compliance framework and best practices in this evolving landscape.

Way forward

Mobile and social media was web 2.0. It changed everything. Crypto and blockchain is web 3.0

This bear market for cryptocurrency has been extremely revealing by exposing everything from poor risk management to outright fraud. The outlook may seem dismal, until you look further into the projects that continue to build. From infrastructure to new products and services, we see entrepreneurs, project teams, venture capitalists, and regulators continuing to innovate, monitor and invest – the bear market will pass, and adoption will continue.

As the size of the market continues to grow, so will the prevalence of financial crimes. Besides the transparent nature of the public blockchains, law makers, regulators and enforcement bodies are becoming increasingly more sophisticated in their approach. Additionally, increased compliance and regulatory clarity can help mitigate the illicit activities. Ultimately, it will be up to the industry players to develop more robust code and implement safeguards to build confidence. Much of this has already started to take place with the increase of cybersecurity firms offering protocol and smart contract code audits, DeFi protocols integrating with crypto security firms to offer compliant institutional onramp support, and Web3 foundations partnering with compliance organisations to improve on-chain security, to name a few. In the coming months and years, we will see increased demand from users and regulators for stronger consumer protections. This will mandate decentralised and centralised exchanges to apply stronger scrutiny in the tokens they list.

For those who find themselves at risk of crypto-asset-related financial crime, there are three measures they can take to mitigate this risk:

1. Adopt blockchain analytics and intelligence tools to monitor and trace crypto transactions.

2. Implement robust controls and governance practices, which include leveraging private key management and custody solutions.
3. Conduct comprehensive due diligence prior to engaging in a crypto ecosystem.

Note

Reach out to authors for further citations and references. All graphs are sourced from TRM Forensics for illustrative purposes. **CDR**


At **BDO**, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the US, and in over 160 countries through our global organisation, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, LLP, a Delaware limited liability partnership, is the US member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

 www.bdo.com




Mansi Mehta is a Director in the Forensics practice of BDO USA LLP with more than 16 years of domain expertise in handling fraud, risk and compliance advisory engagements. She has led high-profile fraud investigations, business processes & system reviews, due-diligence assessments, and cyber forensic engagements, including those for the US Department of Commerce, Securities and Exchange Commission (SEC), foreign government agencies, global banks, and multinational corporations. Mansi's global experience in Asia, the Middle East and North America has enabled her to develop deep expertise in business process optimisation, internal control assessment, data analytics and product management roles. Mansi is a key member of the "Council of Blockchain and Crypto" at BDO, focusing on compliance governance, risk assessment and due diligence of Web3 and crypto projects. She speaks regularly on the topics related to crypto governance and blockchain analytics.

 mansi.mehta@bdo.com



Hakob Stepanyan serves as a core team member of BDO Forensics' Blockchain and Digital Assets Initiative. Having worked with cryptocurrency-centric and -adjacent companies since 2017, he helps the team enhance advisory services related to blockchain-based digital assets. While at BDO, Hakob also has held a traditional forensic accounting roles on a monitorship regarding export control compliance.

A Certified Fraud Examiner, Hakob has assisted clients in a range of industries across multiple jurisdictions. For example, he worked on multi-jurisdictional monitorships and internal investigations regarding compliance, anti-bribery, and corruption at the Forensic Risk Alliance (FRA). He has also assisted with pre- and post-M&A due diligence and ability-to-pay modelling.

 hstepanyan@bdo.com