Decoding Crypto Crime

A Guide for Law Enforcement

OSCE Organization for Security and Co-operation in Europe

Disclaimer

Decoding Crypto Crime

A Guide for Law Enforcement

Organization for Security and Co-operation in Europe

Table of contents

Acronyms, abbreviations and key terms with explanations

5th AML Directive	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance). This directive added crypto assets to its scope. By 10 January 2020, Member States must implement the required laws and regulations to follow this directive.
AML	Anti-money laundering – Refers to laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income.
CASP	Crypto asset service providers – Entities that offer services related to crypto assets to the public. These services can encompass a wide range of activities, including but not limited to: 1. Exchange Services: Facilitating the buying and selling of crypto assets for FIAT money or other crypto assets. 2. Wallet Providers: Offering custodial or non-custodial wallets to store, manage, and transfer crypto assets. 3. Transfer Services: Enabling the transfer of crypto assets from one address or account to another. 4. Financial Advisory: Providing advice on the buying, selling, or holding of crypto assets. 5. Custody Services: Holding and safeguarding crypto assets on behalf of clients. (See p. 20 for more information.)
COE	Council of Europe – An international organization dedicated to upholding human rights, democracy, and the rule of law in Europe.
CTF	Counter-terrorism financing – Refers to policies and actions to prevent the funding of terrorist activities. It seeks to detect and halt the flow of money, from both legitimate and illicit sources, to groups intending to carry out acts of terror.
ERC20 Tokens	Ethereum request for comment 20 Tokens – Implemented in 2015, this is a technical standard used for creating and issuing smart contracts on the Ethereum blockchain.
EU	European Union – A political and economic organisation of 27 European countries that are located in Europe.
EPE	Europol Platform for Experts – A Europol lead space for law enforcement experts to share knowledge, best practices and non-personal data on crime.
EUROPOL	European Union Agency for Law Enforcement Cooperation – The European Union's law enforcement agency that assists its Member States in their fight against serious international crime and terrorism.
FATF	Financial Action Task Force – An intergovernmental standard setting body founded to develop policies to combat money laundering and terrorism financing.

FinCEN	The Financial Crimes Enforcement Network – A bureau of the United States Department of the Treasury that collects and analyses information about financial transactions.
FIU	Financial intelligence unit – A government agency responsible for collecting, analyzing, and disseminating financial information and intelligence on suspected money laundering and terrorism financing activities.
IP	Internet protocol – A set of rules governing the format of data sent over the internet or other networks.
LER	Law enforcement request – A request made by law enforcement agencies to companies or individuals seeking information for investigations.
MiCA	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. This is a new EU Regulation governing crypto assets. It will be in force from 30 December 2024.
ML	Money laundering – The illegal process of making large amounts of money generated by a criminal activity falsely appear to have come from legitimate sources.
MultiSig Wallet	Multi-signature cryptocurrency wallet – Type of cryptocurrency wallet that requires multiple private keys to authorize a transaction.
OCEEA	The OSCE's Office of the Co-ordinator of Economic and Environmental Activities
OSCE	Organization for Security and Co-operation in Europe – A regional security organization in Europe focused on promoting dialogue and comprehensive co-operation across military, political, environmental, and economic dimensions.
OSINT	Open source intelligence – Information collected from publicly available sources used in an investigation context.
OTC	Over the counter – The trading of virtual assets securities between two parties with or without a central exchange or broker.
UNODC	United Nations Office on Drugs and Crime – An office operating within the United Nations responsible for producing and disseminating data on drugs and crime.
VASP	Virtual asset service provider – A term introduced by the FATF to denote an entity that conducts activities or operations for virtual assets. (See p. 20 for more information.)
VPN	Virtual private network – Technology that allows to create a secure connection over a less secure network between an individual's computer and the internet, sometimes but not always to hide the location of the user.

Introduction

Goal of this guide

This document serves as a comprehensive guide for law enforcement officers, including police officers, prosecutors, state and federal agents, as well as tax and forensic specialists who have been newly introduced to cryptocurrencies and other virtual assets. It's tailored for those who are increasingly tasked with investigating crimes related to crypto assets.

It focuses on the most common types of scams and fraudulent behaviour, explains the best practices for officers, which actions to take and what type of information can be recorded from potential victims, especially during the initial evidence-gathering process at local police stations.

This guide has been written and designed to be a guide for law enforcement officers. It purposefully does not cover areas of cryptocurrencies that are unlikely to be important in police cases in connection with individual victims.

It also intentionally focuses on the interactions between law enforcement and natural persons. Information on STRs (Suspicious Transaction Reports) or SARs (Suspicious Activity Reports) used by financial institutions or financial intelligence units (or their equivalents) has been disregarded.

Multiple issues had been identified in the current way cryptocurrency cases have been dealt with, for example, due to incomplete data collection, investigators reported that they had to get in contact with victims to gather information like a cryptocurrency wallet address, without which an investigation remains impossible. Officers need to understand which information is vital to collect and which is not. Such miscommunication often results in days of delays, since victims may not fully understand which information is relevant for law enforcement.

This knowledge gap is not just an inconvenience; it has been exploited by criminals who recognize that technology is globally available from day one, while best practices in cryptocurrency investigations continue to lag behind. In response to this growing challenge, we have developed this guide that outlines how law enforcement should proceed in investigations and in assisting potential victims who report a cryptocurrency-related crime.

Recognizing the complexities of the topic and the diversity of legal situations and practices across various different OSCE participating States, our goal is not to offer an exhaustive guide, but rather a practical manual that can be used on an ad hoc basis by first line law enforcement agents that receive reports from citizens. It is intended to prompt conversations on how to enhance internal best practices, particularly if existing guidelines do not cover cryptocurrencies. The most common fraudulent practices have been summarized as they stand today and introductory material is provided to facilitate a deeper understanding of the subject.

This guide serves as an essential stepping stone in bridging the gap between law enforcement and the constantly changing world of virtual assets. It should be recognized that the Web3 space in which cryptocurrencies operate is rapidly evolving and that this guide may need to be supplemented with additional knowledge.

This guide emphasizes not only the tools and strategies necessary for effective investigations, but also aims to foster collaboration and continuous learning within the community. The ultimate aim is to equip law enforcement officers with the knowledge and confidence needed to confront the unique challenges posed by cryptocurrency-related crimes.

Structure of the guide

The primary aim of this guide is to educate law enforcement officers who are new to the field of virtual asset crimes, and to support victims reporting such crimes. With this objective in mind, the guide is structured as follows:

Firstly, a concise overview of digital assets is offered. Digital assets can be thought of as a large umbrella term that includes subjects like cryptocurrencies such as Bitcoin and Ethereum. An explanation of what they are and how they are similar or different from one another will be provided. Their differences and similarities will be examined to ensure a clear understanding. Additionally, the potential uses and misuses of cryptocurrencies and the technology that supports them will be discussed.

After establishing a foundational understanding of virtual assets, the guide presents the common crimes associated with them. It then describes standard protocols for dealing with these crimes, identifying which can be quickly addressed and which require more thorough investigations. The guide also covers evidence collection for each crime, questions to ask victims, data to share with virtual asset service providers, and information that can be obtained from virtual asset exchanges.

Accessibility and language simplification: Due to the complexity of the field, the authors have used simplified, non-technical language to make this report accessible to beginners. By avoiding jargon, the aim is to ensure that the content is clear and understandable for all readers. Finally, the guide offers victim support resources and presents various suggestions that can help prevent cryptocurrency-related crimes.

Background

Investigations centred around crypto assets might appear intimidating at first, particularly given the misconceptions surrounding the difficulty of asset recovery. It is a myth that once a national currency has been converted into a cryptocurrency like Bitcoin, the funds are irretrievably lost, leaving victims helpless and forcing investigators to close their cases. This perception was accurate until a few years ago, but times have changed.

This progress in technology has opened new doors, similar to how DNA verification has allowed cold cases to be reopened and solved. We can now reopen previously closed cryptocurrency cases. The ever-growing accessibility of tools designed to detect and review cryptocurrency transactions on blockchain and changes in international law allows us to determine the perpetrators of cryptocurrency criminal cases. These tools are becoming increasingly user-friendly and widespread, heralding a change in the investigative landscape.

Despite all of these tools, we do still see many investigations conducted by local police officers closing prematurely due to limited understanding and knowledge. Contrary to common belief, cryptocurrency transactions can be traced. By accurately recording data at the onset, there's a heightened likelihood of linking transactions to a potential suspect, seamlessly merging virtual and tangible evidence.

In recent years, several OSCE participating States have begun integrating cryptocurrencies and other virtual assets into their national anti-money laundering regulations in line with updated standards issued by the Financial Action Task Force (FATF). This development means that companies operating with cryptocurrencies must now adhere to processes initially designed for traditional banking institutions. They are requested to verify the identities of their customers, scrutinize the sources of funds, and monitor where cryptocurrencies are being sent.

Recognizing these shifts, the OSCE Virtual Asset Expert team has decided to launch a support guide specifically tailored to members of local law enforcement units. This guide will not only illuminate the new possibilities in cryptocurrency investigations, but also empower law enforcement officers with the knowledge and tools they need to pursue justice in this complex and evolving field.


30 OSCE MINISTERIAL COUNCIL
osce
IT'S ABOUT PEOPLE
SKOPJE
Interpretation Languages
CH 0 - Floor
CH 1 - ENG
CH 2 - FRA
CH 3 - GER
CH 4 - SPA
CH 5 - RUS
CH 6 - ITA
CH 7 - ALB
CH 8 - MKD


OSCE
Valiant Richey
OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings
Helga Maria Schmid
OSCE Secretary General
OSCE


Mariia Sulialina
Deputy Head of the Center of Civil Education "Almenda", Ukraine
Hadja Lahbib
Minister of Foreign Affairs of Belgium
Stefano Baldi
Permanent Representative of Italy to the OSCE
Dorota Woroniecka-Krzyżanowska
Polish Center for International

About the OSCE

The OSCE is the Organization for Security and Co-operation in Europe. It operates as a regional security organization with the purpose of promoting dialogue and co-operation and takes a comprehensive view of security, encompassing everything from the military and political to the environmental and economic dimensions.

The OSCE was established during the Cold War in 1975 and currently consists of 57 participating States. These States are predominantly in Europe, where much of the work of the OSCE is focused, but also include Canada and the United States in North America, as well as countries such as Kazakhstan, Kyrgyzstan and Uzbekistan in Central Asia. It operates on the principles of comprehensive security, which encompasses military, political, economic, environmental, and human dimensions.

In Europe, the OSCE works to foster stability and address security challenges. Its primary aim is to prevent conflicts and promote regional co-operation through mechanisms such as diplomatic negotiations, conflict resolution initiatives, and arms control agreements. In addition, there is work that the OSCE does to support democratic and human rights, such as monitoring elections.

When it comes to the topic of financial crime and crypto crime, the OSCE helps to combat these challenges by facilitating intelligence exchange and capacity-building among its participating States, which works to improve the flow of cross-border information. This is important work, since crypto crimes are by nature not limited to a single country or currency, and thus cross-border co-operation is vital.

The OSCE also encourages the establishment of legal frameworks and robust regulatory measures to tackle both classic money laundering and terrorist financing, as well as to implement measures to detect and prevent illicit activities involving cryptocurrencies. This includes ensuring that participating States comply with international anti-money laundering (AML) and counter-terrorism financing (CTF) standards.

Training programmes and workshops are run by the OSCE in aid of this, with the intention of improving the expertise of law enforcement agencies, financial institutions, and other relevant actors in dealing with financial and crypto crimes. These efforts aim to improve investigative techniques and the use of cutting-edge technologies to detect and combat cybercrime and crypto-related criminal activities.

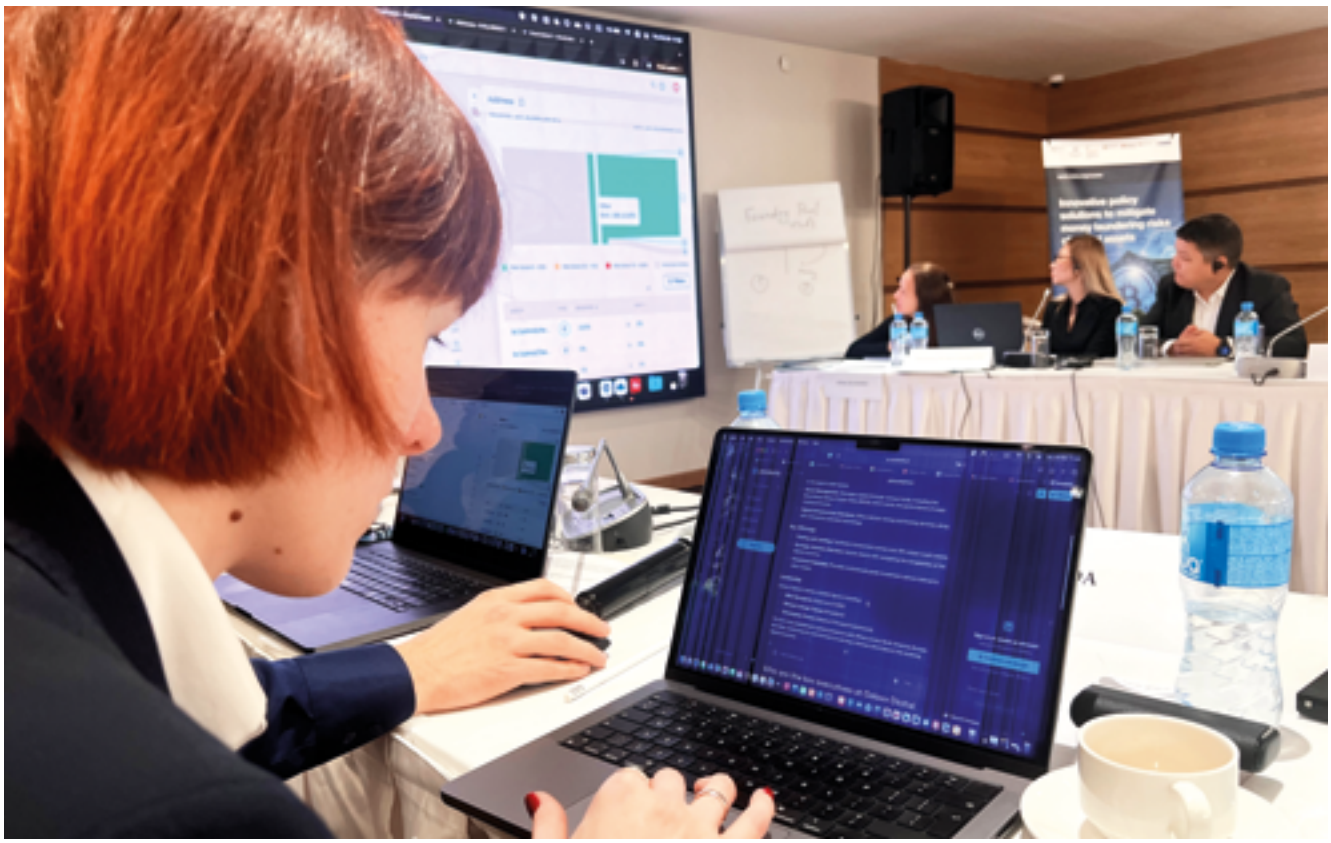
For the purpose of this publication, the OSCE is responding to the need of specific participating States to address the risks posed by the use of virtual assets for criminal purposes and for the circumvention of international sanctions. This addressing of risk is the essential goal of the project “Innovative policy solutions to mitigate money laundering risks of virtual assets”, which is being led by the OSCE’s Office of the Co-ordinator of Economic and Environmental Activities (OCEEA).

The ultimate objective of this project is to build the capacities of national authorities to counter these virtual asset specific vulnerabilities. Throughout the implementation of the project, the OCEEA, together with the United Nations Office on Drugs and Crime’s Global Programme against Money Laundering (UNODC GPML), has continued to assist three countries in Eastern Europe and Caucasus — Georgia, Moldova, and Ukraine — in bringing their virtual assets (VA) and virtual assets service provider (VASP) regulatory framework in compliance with the FATF Recommendations while providing relevant law enforcement agencies in these three countries with capacity-building and technical support.

To enhance the efficiency of the project, the OSCE team has partnered with the UNODC, which has contributed its in-house expertise and practical training programmes on cryptocurrencies, money laundering (ML) and terrorist financing (TF) risks, investigation, seizure and confiscation, regulation, and customer due diligence. The OCEEA continues to support relevant authorities, such as central banks, compliance departments of key financial institutions, financial intelligence units, general prosecutor’s offices, ministries of justice and internal affairs, by assisting in drafting regulations and instructions for personnel, organizing awareness-raising activities and facilitating interagency and international co-operation in the investigation of crimes conducted with the use of cryptocurrencies.

This publication has been created as a part of the innovative policy solutions to mitigate money laundering risks of virtual assets projects, financed by Germany, Italy, Poland, Romania, the United Kingdom, and the United States.

OSCE Organization for Security and Co-operation in Europe



Greta Barkauskienė leading a workshop for investigators in Astana, Kazakhstan. Drawing on her extensive expertise as an AML expert and as the national tactical co-operation group co-ordinator for the Lithuanian PPP Center of Excellence in Anti-Money Laundering, she brings best practices from both public and private stakeholders to empower beneficiary countries.

Investigators' workshops held in Tbilisi, Georgia, focused on key aspects of cryptocurrency asset seizure, including the preparation of secure facilities for potential confiscations. These workshops were closely linked to a follow-up exercise aimed at enhancing skills in identifying, transferring, and recovering cryptocurrency assets on the Blockchain. Photo: Michal Gromek.

Understanding digital assets: A simplified guide

Understanding digital assets: A simplified guide

This section will cover the differences between various digital assets, FIAT and cryptocurrencies. We will also distinguish the differences between various types of cryptocurrencies and the infrastructure around them.

There is often confusion as to what the difference is between digital assets, virtual assets, crypto assets and cryptocurrency.

Simply put, a **digital asset** is the broadest term. It is an asset that exists in digital form. This includes images, videos, music, as for example in MP3 format, documents, and virtual currencies.

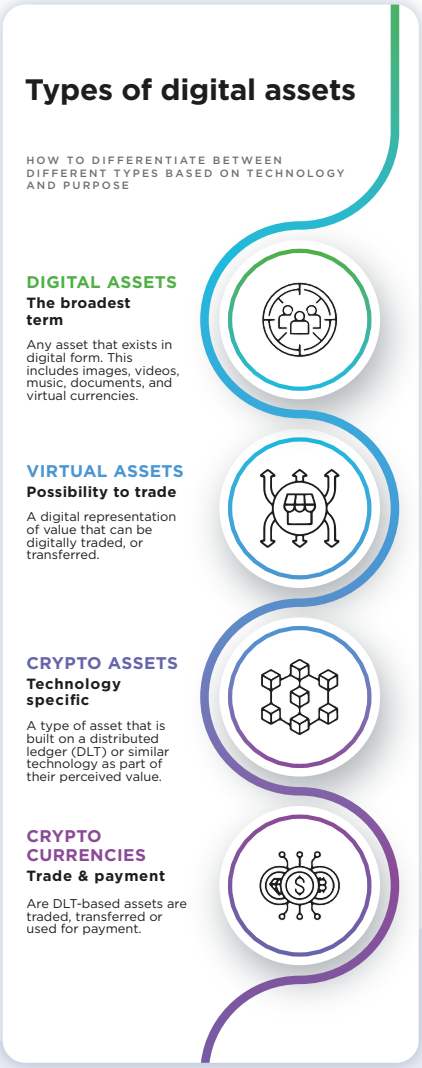
A **virtual asset** is a narrower set of digital assets. According to the FATF,[1] virtual assets (crypto assets) refer to any digital representation of value that can be digitally traded, transferred or used for payment. It does not include digital representation of FIAT currencies.

By contrast, a **crypto asset** has an even narrower niche. It is an asset that stores value but must be transferred by distributed ledger technology (DLT). Blockchain is a type of DLT. You can have a virtual asset like a coin in an online game that is not a crypto asset because it is transferred between players in the game without employing distributed ledger technology. Blockchain is currently the most prominent type of distributed ledger technology, but there are other DLT technologies, such as Hashgraph, Iota Tangle, R3 Corda and multiple others. For the purpose of this guide we are focusing on blockchain-based finance.

Within digital assets, there are many different types of assets, including cryptocurrencies, which are new types of currency that work using blockchain technology, and non-fungible tokens (NFTs), which are image-based assets.

Thus, once a crypto asset is developed to be traded, transferred or used for payment, we would refer to it as a cryptocurrency. You may also come across the term virtual currency, which is often used interchangeably with cryptocurrency. The distinguishing factor between cryptocurrency and virtual currency is the underlying technology. Cryptocurrencies use blockchain, whereas virtual currencies are not necessarily built on blockchain.

This guide will predominantly focus on crimes committed with cryptocurrencies.



With the permission of the author (from Alexandra Andhov, Computational Law, Karnov, 2022).

1 Financial Action Task Force, source: https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20(crypto%20assets)%20refer,digital%20representation%20of%20fiat%20currencies (accessed: 26 Sept. 2023).

Cryptocurrencies vs. FIAT

Traditional coins and paper money, known as "FIAT currency," have been the backbone of our economies for centuries. But with the rise of technology, new forms of money have emerged, blurring the lines between the tangible and the virtual. When individuals make electronic transfers of FIAT currency from one person to another, they use "e-money." E-money, or electronic money, represents our familiar FIAT currency in a digital form, facilitating electronic transactions without changing its value. E-money is a digital representation of fiat currency.

Contrary to FIAT, cryptocurrencies operate in a decentralized environment. They aren't tied to any government or central bank, and various factors, including demand, technology, and trust, determine their value. Bitcoin, a leading name in this realm, has showcased the potential of these currencies, with its value soaring to remarkable heights. Back in 2021, it reached a value of over $64,000 per coin. Cryptocurrencies, such as Bitcoin and Tether, are not guaranteed by any government or central bank. Whilst not anywhere near as old as FIAT currency, virtual currencies are not as novel as most people presume. One of the first virtual currencies — E-Gold — was already introduced almost 30 years ago, in 1996.

Summary of E-Gold

One of the first popular virtual currencies was called "E-Gold." First established in 1996 by Douglas Jackson and Barry Downey, E-Gold allowed users to open an account with a value denominated in grams of gold (or other precious metals) and the ability to make instant transfers of value to other E-Gold accounts.

In 2005, E-Gold had 2.5 million account holders, performing daily transactions at a typical value of US$6.3 million. It was popular due to its efficiency, low fees, and global accessibility. However, its lack of strict regulations also attracted illicit activities. In 2007, E-Gold was indicted by a grand jury in the United States, whereby the company was accused of money laundering, conspiracy and operating an unlicensed money-transmitting business, ultimately leading to the shutdown of E-Gold by the US courts in 2009. E-Gold spawned a range of copycats, such as e-Bullion.com, Pecunix.com and others.[2]

It is important to be specific when discussing this field, since virtual currencies can refer to both e-money and cryptocurrencies. This can quickly become confusing. In this guide, we focus on cryptocurrencies.

Underlying technology: Blockchain

Blockchain is a type of distributed ledger technology (DLT). This new technology first emerged in 2008 in a white paper published by Satoshi Nakomoto.[3] It is defined as being decentralized, since there is no single control center or person in charge. Instead, changes can be made by any user, but they have to be accepted by a majority of users to become permanent.

There are many different blockchains. Blockchain simply refers to the underlying technology. Imagine each blockchain as a building. While each can look very different on the outside, and each building can have a very different purpose, when you look underneath, nearly all buildings have been built with bricks and cement.

Just as with buildings, some blockchains can be accessed by anyone without needing permission, while some require approval before you're allowed to join.

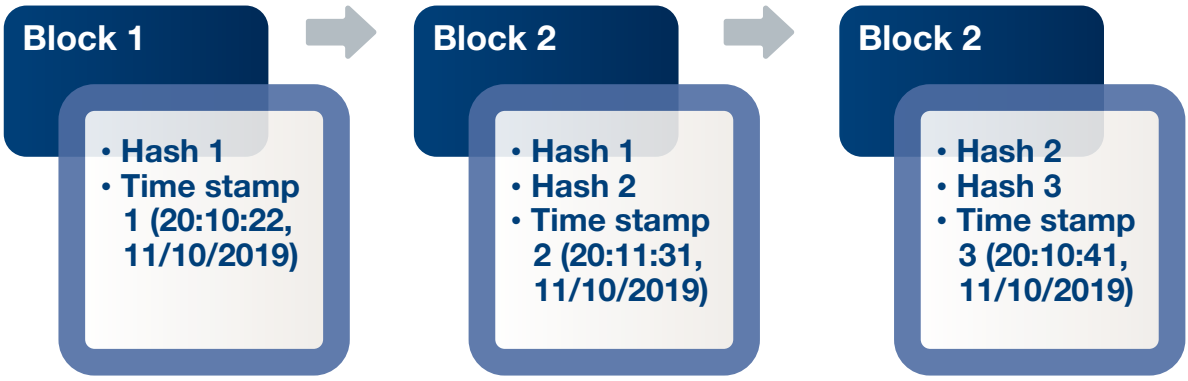
2 "Feds accuse E-Gold of helping cybercrooks", NBC News, May 2007. (Available: http://redtape.nbcnews.com/_news/2007/05/02/6346006-feds-accuse-e-gold-of-helpingcybercrooks (accessed: 24 August 2023). "Internet currency firm pleads guilty to money laundering", The Industry Standard, July 2008. Available at: http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering (accessed: 24 Aug. 2023). *Synopsis of e-gold Transactions (1996) E-Gold.* Available at: http://www.e-gold.com/unsecure/synopsis.htm (accessed: 24 Aug. 2023).

3 Nakamoto, S. (2008) A peer-to-peer electronic cash system, Bitcoin. Available at: https://bitcoin.org/en/bitcoin-paper (accessed: 26 Aug. 2023).

In this regard we distinguish between public and private blockchains. Public blockchains are called "permissionless" and tend to require less transparency or control, while "permissioned" blockchains are often used for enterprise purposes and require the person wanting to join to be approved.

The blockchain is named this way because users add or change "blocks" of data, and these blocks are tied together in a chain chronologically (by time). When one user makes or uploads a new block (for example, a new transaction with a bitcoin), all other users on the blockchain have to validate the new block using "consensus methods" (this involves quite complex mathematical equations, to ensure it can be trusted). Because the blocks are all linked together, it is nearly impossible to go to a previous block and change it. This means that the system cannot be tampered with. Any new information, including changes of old information, is recorded in a new block.

Blockchain works by allowing all users connected to that chain to see the entire history of the chain (the "ledger"). Therefore, with a bitcoin blockchain the users can see every transaction that has occurred. This allows investigators to conduct investigations. Because of the distribution of the blockchain ledger to every user, blockchain is called "distributed ledger technology" or DLT. It is like a "google sheet" upon which everyone can collaborate and see the previous versions. Since everything is visible and cannot be altered without everyone being able to see it, there is a high level of transparency, trust and security. There is also a high level of resilience to attacks: Because every single person has a copy of the blockchain and there is no centralized version, even if one user ("node" in blockchain terminology) gets attacked and fails, the system can still operate.



With the permission of the author (from Alexandra Andhov, Computational Law, Karnov, 2022).

Types of cryptocurrencies

There are two ways of distinguishing between cryptocurrencies:

- **Whether they are convertible or nonconvertible**
- **Whether they are centralized or decentralized**

These distinguishing characteristics are described in more detail below.

Convertible and non-convertible currencies

Convertible currencies have an equivalent value in FIAT currency and can be exchanged back for "normal" money. This convertibility is not guaranteed since cryptocurrencies are not backed by any government or institution. The convertibility of a cryptocurrency to a FIAT currency is based on the market and private offers being accepted. This is the type of cryptocurrency where most crimes occur. Examples of convertible currencies include Bitcoin and E-Gold.

Non-convertible currencies are like the gold coins that stay within a computer game. Crime committed with these is less likely, since they don't hold real world value. However, some individuals find a way to trade them outside the boundaries of the game they exist in, making them convertible outside the game, even if it's against the game's rules. For example, somebody can transfer "collected gold coins" from one

player to another player in a game, with the transaction paid offline in cash.

Centralized and decentralized currencies

Centralized cryptocurrencies are overseen by a single authority that issues the currency, sets its rules, maintains a payment ledger, and has the power to withdraw it from circulation.
Centralized currencies can be convertible or nonconvertible. Non-convertible currencies are always centralized (since, for example, one can't have a currency within a game without the game being in charge of the currency). When exchanging a centralized convertible currency, the exchange rate is determined by market supply and demand, or it is fixed by the administrator. A good example of a centralized currency is E-Gold.

Decentralized currencies, on the other hand, lack a central authority and operate based on a peer-to-peer network. Think of a decentralized system like the internet. Just as there is no one supervisor in charge of the entire internet, a decentralized system doesn't have one main controller. Even though most people use the internet daily, there's no single company that is paid; instead, various providers are paid for different services. This is how the blockchain network technology behind cryptocurrencies like Bitcoin is used. Transactions are managed through the network and there is no other monitoring by any authority.

A selection of ten cryptocurrencies with the largest market caps as of 23 August 2023 are listed below, as based on the link in the footnote.[4]

Name	Symbol	Market cap (23 Aug. 2023)	Comparable to the gross domestic product of the following country[5]
Bitcoin	BTC	$514,912,135,787	Sudan
Ethereum	ETH	$201,475,414,760	Haiti
Tether USDt	USDT	$82,835,552,223	Somalia
BNB	BNB	$33,285,580,473	Andorra
XRP	XRP	$27,991,699,189	Curacao
USD Coin	USDC	$26,005,195,827	Lesotho
Cardano	ADA	$9,357,776,591	St. Vincent and the Grenadines
Dogecoin	DOGE	$8,965,846,112	Northern Mariana Islands
Solana	SOL	$8,792,761,272	Samoa
TRON	TRX	$6,938,358,042	American Samoa

Pseudo currencies and privacy coins

Pseudo-anonymous currencies involve accounts that use pseudonyms, meaning that while transactions aren't directly tied to personal identities, some identifying information remains. For instance, a typical FIAT currency bank account used to purchase cryptocurrency is linked to identifiable data. Coins within this category include Bitcoin and Ether.

Conversely, privacy coins offer greater anonymity by employing advanced cryptographic methods to obscure transaction details and associated identities, making it challenging to trace them back to the original user. Examples of such coins are Monero and Zcash.

4 All cryptocurrencies (2023) CoinMarketCap. Available at: https://coinmarketcap.com/all/views/all/ (accessed: 24 Aug. 2023).

5 Based on the World Bank GDP data (current US$), https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=false (accessed on 23 Aug. 2023).

Crypto wallets

A cryptocurrency wallet is where cryptocurrency is stored. A useful analogy is to imagine how money is stored around the globe today.

Money comes in different forms. Some of it is stored in gold bars hosted by large banks, some of it circulates in the form of paper banknotes, online bank transfers or cryptocurrencies. Cryptocurrency wallets come in different forms as well: an app on the phone, a device that looks like a USB drive, or just a piece of software (a bit similar to your email address) to which you will have access after typing in a login and password. Even though there are different kinds of cryptocurrency wallets, they use the same technology. Most have 12-, 18-, or 24-word recovery passwords that can re-open the wallet.

Crypto wallet addresses

Cryptocurrency wallet addresses are similar to a bank account number. Having somebody's bank account number doesn't mean having access to somebody's money. Crypto wallet addresses have long, complicated sequences with many case-sensitive letters and numbers. Here are two examples:

A cryptocurrency wallet for the currency TRON
TYm3NTSyk85t9UHSd68DY4vGWQADHXpaXJ

A cryptocurrency wallet for Bitcoin
Bc1qu5z7kn0v2krhglsnan4c0m5f76xk69p53wjwgh

The difference between traditional bank account numbers and crypto wallet addresses is that compared to a crypto wallet address, a lot of information can be gathered from a bank account number. Law enforcement can easily decode an IBAN number and contact the relevant authority.

An IBAN is an international bank account number. It can have up to 34 letters and numbers. It starts with the country's code, a two-digit safety check, and then details about the bank and the account. Sometimes different countries format these bank details differently. For example:

IBAN:

- **LT44 32500 47338696265**

  LT identifies the Republic of Lithuania,

  32500 identifies the Revolut Bank UAB

  47338696265 is the account number of the user[6]

If an IBAN bank account number like this appears in an investigation, the officer would know to contact the Lithuanian Bank Revolut. This information can be obtained from so-called "IBAN validators," such as iban.com or https://wise.com/gb/iban/checker. Then the process to obtain personal information about the account user can be started.

For pseudo-anonymous cryptocurrencies like Bitcoin, no law enforcement office will be able to identify personal information about the account holder based on an account number like this: bc1qu5z7kn0v2krhglsnan4c0m5f76xk-69p53wjwgh.

In order to find identification information of the owner, a specialized software is needed, as for example, a **blockchain analytics provider**.

Blockchain analytics providers can reveal the identification information of users and track transactions across different cryptocurrencies, a common tactic

6 IBAN and financial institution codes, Bank Of Lithuania, https://www.lb.lt/en/iban-and-financial-institution-codes (accessed 25 Sept. 2023).

used with stolen cryptocurrencies. The ability of such providers to identify which financial institutions or crypto exchanges (VASPs – vrtual asset service providers) have this identity information depends on the laws of the country in which they operate. For this reason, international actors like the OSCE are helping their participating States align with international best practices in this area.

Crypto wallet explorers

Because the leading types of public blockchain are open to everyone, one can look through all of the transactions that happen in a wallet using a "crypto wallet explorer."

A crypto wallet explorer is a search engine designed specifically to navigate blockchain data. It provides detailed information about individual blocks, transactions, and associated wallets. Think of it as "Google" for blockchain transactions.

Watch out:

One might need a different wallet explorer for each type of cryptocurrency. Best practice is to type the name of the cryptocurrency one desires to review and add the expression "wallet explorer" or "blockchain explorer" into a search engine to review the leading providers. Such services are generally free.

Main uses of crypto wallet explorers:

- **Transaction verification:** Wallet explorers allow users to verify that a transaction has taken place. When someone claims they sent cryptocurrency, an explorer can be used to confirm this by searching for the transaction using the transaction ID or a wallet address.
- **Auditing and record-keeping:** For individuals or businesses that need to maintain records of transactions, explorers can provide detailed information when a transaction occurred, how much was sent, and the involved addresses.
- **Research and analysis:** Developers, researchers, and analysts often use wallet explorers to study the overall health and activity of a blockchain. They can see how many transactions are taking place, the size of transactions, and more.
- **Wallet balance:** By entering a wallet address into an explorer, one can view the balance of a particular cryptocurrency wallet and see its transaction history.

Free wallet explorers:
It is easy to find crypto wallet explorers for each type of cryptocurrency simply by typing "best free XXX cryptocurrency wallet explorer" into a normal internet search engine.

Using these tools, anyone can explore and verify transactions on a blockchain, even without owning cryptocurrency or having an in-depth knowledge of the technology. In the same way we can search the internet with solid search tools, we can search blockchains.

Exchanging cryptocurrencies

Similarly to "normal" money, one needs to use a specific platform to exchange one type of cryptocurrency to another or to FIAT currency. There are three main types of platforms: peer-to-peer exchanges (P2P), centralized exchangers (CEX) and decentralized exchangers (DEX).

P2P stands for **peer-to-peer**, and thus person-to-person or, more often, user-to-user (since legal entities can sell or offer their assets). Here users are not buying from the exchange itself, but from other users. An example of such a P2P exchange that has ceased operation was the Finnish provider called LocalBitcoin.com.

Such exchangers sell their own virtual assets and do not match users with each other.

Peer-to-peer changes are subject to AML and CTF regulation[7] and require detailed user information. They also must follow certain rules in the countries they operate.

Decentralized exchanges claim that they function like automatic file converters (e.g., .doc to .pdf). They are mostly used for crypto-to-crypto transactions and less frequently for FIAT-to-crypto exchanges. Funds involved in decentralized exchanges require specialized support for tracing.

This is just the tip of the iceberg. There are also new types of exchanges, as the above-mentioned decentralized exchanges, OTC exchanges, mixers and tumblers. This is a rapidly evolving technology that is being developed with the purpose to hide traces of users' transactions. Many OSCE participating States are taking actions to limit the usage of such tools.

Mixers and tumblers

Mixers and tumblers are services designed to enhance the privacy and anonymity of cryptocurrency transactions. Their primary function is to mix the funds of various users, thereby obfuscating the original source of the funds.

7 This applies only for crypto-exchanges operating in countries that have implemented the FATF's recommendation 15, which requests countries to incorporate financial entities dealing with cryptocurrencies into their AML and CTF framework.

Mixers

These are centralized or decentralized services that mix cryptocurrency funds from various sources to hide their origin. Users send their cryptocurrencies (like Bitcoin) to a mixer, which then shuffles these coins with other users or its own coins. Once the "mixing process" is complete, the service sends the equivalent amount of coins minus a fee to the user's specified address, making it difficult to trace the origin of the coins. However, centralized mixers are operated by a single entity, which can potentially log the transactions. The Europol EC3 team is offering courses in demixing, courses available for confirmed law enforcement only.

Mixer-like related services in traditional banking

Mixers operate similarly to conventional banks where funds are deposited and withdrawn. Consider a large financial institution where various individuals deposit money. If this institution aggregated all these deposits and then dispersed them to account holders without specifying the origin of each dollar, this would resemble the mixing process. Funds are overseen by a known entity, such as a centralized mixer, and once inside, these funds intermingle with others. Leading blockchain analytics providers claim to offer automatic or manual "demixing" services for most of the leading mixers, allowing these providers to review the transactions across such services.[8]

Tumblers

Tumblers are similar to mixers, and in many contexts the terms are used interchangeably. The primary goal of a tumbler is also to improve transactional privacy. Some consider tumblers as more sophisticated versions of mixers. They use advanced algorithms to ensure the mixed coins cannot be linked back to their original sources.

Tumber-like related services in traditional banking

Tumblers can be compared to bank accounts in countries that are defined as tax havens, or offshore banks reputed for offering enhanced confidentiality and privacy. Such banks typically employ intricate structures and services tailored for privacy and asset safeguarding. In the realm of cryptocurrency, tumblers utilize cutting-edge mathematical algorithms to maintain the anonymity of transactions, affording a more refined level of concealment than standard mixers. Tracing a transaction across a tumbler is complex and time-consuming, but not impossible.

Differences and similarities

While both mixers and tumblers serve the same purpose of enhancing transactional privacy, the nuances between them often come down to their methods and level of sophistication. It's like comparing basic web browsers to those offering enhanced privacy features. Both allow you to browse the internet, but one offers more advanced tools for maintaining anonymity.

VASPs and CASPs

A virtual asset service provider (VASP) undertakes the following activities:

- Facilitating the exchange between virtual assets and FIAT currencies;
- Facilitating the exchange between one or more forms of virtual assets;
- Facilitating the transfer of virtual assets from one wallet to another,
- Providing financial services related to the sale of virtual assets.

There are a number of terms used interchangeably when it comes to VASPs. "VASP" was decided on by the Financial Action Task Force (FATF). However, "CASP," standing for crypto asset service provider, is commonly used in the EU instead of VASP. The number of services defined under CASPs is wider than those of VASPs. The terms "exchanges" and "brokers" are also sometimes used, but they represent only one of many types of VASP or CASP.

8 The author was unable to confirm or deny those claims prior to the editorial deadline of this publication.

Protocol for handling digital asset-related crimes

Protocol for handling digital asset-related crimes

The four most important pieces of information to collect

When a potential victim arrives at a police station and claims that they have been subject to cryptocurrency fraud, there are four vital pieces of information that must be collected.

Cryptocurrency transactions are irreversible — once they are completed and have entered the blockchain, it will require significant effort to return those funds to the victim. And yet, while the effort is truly substantial, it is not impossible.

Time

The first key element is time. Cryptocurrency transactions do not always immediately enter the blockchain. There is often some amount of time when the funds are held at a bank or a licenced cryptocurrency broker before being recorded on the blockchain. Establishing whether this is the case, is the first and most crucial question, since it offers the chance to still reverse the transaction.

Financial institution

The next most important question is to ask the victim which cryptocurrency broker or financial institution was used when the FIAT currency was transferred.

If the transfer has been conducted to a broker in a low-risk jurisdiction that has enforced anti-money laundering regulations on financial institutions, there is a possibility that the transaction can be stopped.

Size

The third most important question is the size of the transaction, since large amounts of funds crossing the anti-money laundering threshold are subject to verification by a VASP or CASP. If the victim has made a large transfer to a licensed exchange, it may be possible to contact this exchange and stop the transfer from being changed to cryptocurrencies.

Type of cryptocurrency

Finally, the last key question is what type of cryptocurrency or virtual asset has been purchased. Some types can be easily traced, such as Bitcoin. Other types of cryptocurrency known as privacy coins, such as Monero and ZCash, have been designed to make tracing and investigations more difficult, but even these are possible to trace with some effort.

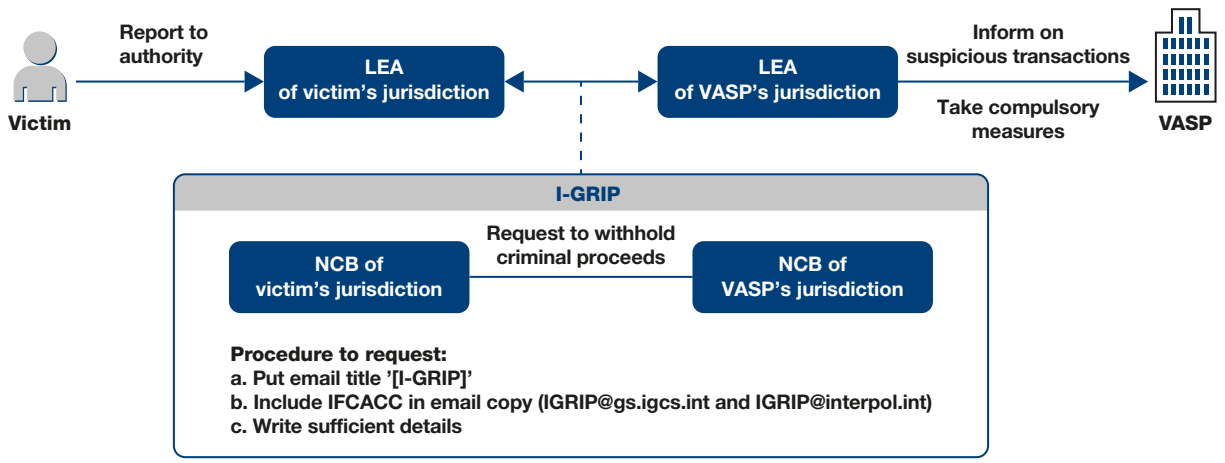
If the transaction from the victim's bank account is very recent, all efforts should be placed on stopping it from entering the blockchain. Receiving a case at the station and passing on for pre-investigation to other colleagues who might only pick it up days later can significantly decrease the chances of success.

Here are three examples that are common and illustrative of this concept:

Example 1: If in the case of a potential victim, the transfer of FIAT from an international bank is, for example, initiated on Friday evening and this is reported to law enforcement on Saturday morning, then it is still possible to contact the bank and stop the transaction. If the victim has not contacted the bank, they should immediately do so.
(See INTERPOL'S IGrip solution, p. 23)

Example 2: Even if the victim has transferred a larger amount from their bank account to a cryptocurrency broker and the transfer has already left the victim's account, there might be information in the customer bank account showing the name of the VASP/CASP to which the transfer has been sent. In this example, if the transfer has been sent to one of the larger brokers, such as Binance, the customer should immediately contact their customer service via a chat window or send an email with a title: **"Urgent: Stop exchange – fraud"** to fraud@nameofthebroker.domain or compliance@nameofthebroker.domain to inform them that the transfer coming from a particular IBAN, of a particular size and in a particular timeframe is not to be processed.

Members of law enforcement can also request the funds to be stopped, via for example Binance's Government Law Enforcement Request System: https://www.binance.com/en/support/law-enforcement.
Larger brokers or exchanges and other VASPs usually have a proceeding in place that can help enforcement agencies to locate and stop the transfer. The majority of players in the industry will have email addresses like compliance@name-of-the-broker.com or fraud@name-on-of-the-broker.com that can be used to report urgent cases.



Source: Image courtesy of INTERPOL

At the same time, the LEA of the victim's jurisdiction can make a stop payment request through INTERPOL with a tool called **Global Rapid Intervention of Payment** (I-GRIP). This is a channel to the LEA of the jurisdiction where the VASP is located. INTERPOL launched I-GRIP to make international co-operation speedy enough to effectuate initial stages of asset recovery.

Once the LEA of the jurisdiction where the VASP is located receives an I-GRIP request, they can take necessary measures to withhold the criminal proceeds from being processed further in accordance with their national law. The necessary measures can take various forms. They can simply inform the receiver VASP about the suspicious transaction, so the VASP can make its own voluntary business judgement to suspend the suspicious account or even to recall the transactions. Also, LEAs can utilize their administrative power to mandate a VASP to suspend the suspicious account. Additionally, the LEA can open their own domestic criminal investigation parallel to the investigation carried out by the I-GRIP requesting jurisdictions and issue a criminal seizure order against the suspicious account.

If the legal framework in the OSCE participating State allows it, another possibility might be to file the case immediately, together with the potential victim's reporting, since time is one of most crucial aspects in cryptocurrency investigations.

Example 3: If the potential victim is not fully sure to which cryptocurrency broker the funds have been sent and there are abbreviations of letters and numbers that look similar to this on the transfer details:

`1C5Eu4UpeK5djG3QiKwhcLELtFwHT146dG`

this could indicate that the funds have been or will be exchanged to a cryptocurrency wallet. Such wallets can be compared to bank accounts or an email postbox, where funds are stored. With a bit of skill funds in such a wallet can be recovered or frozen. Even though such a combination of letters and numbers looks unusual for individuals who are unfamilar with cryptocurrency, for investigators experienced in the space, such combinations of letters and number provide information similar to a credit card number. Having a cryptocurrency wallet address is similar to having a credit card number, but without personal details such as the name or the issuing bank. A credit card number indicates the issuer of the card and the card's type. Similarly, once a cryptocurrency wallet address has been reported by a victim to law enforcement, with the help of external tools there are possibilities (which are not always successful) to connect a wallet address to a particular cryptocurrency or a specific VASP or financial intermediary.
(For more information, see the section "Further tools for virtual asset crime investigations," p. 47.)

9 INTERPOL, Guidelines for Seizing Virtual Assets (October 2023), p. 40.

Best practice for each type of transaction

There are three types of transactions on blockchains that are relevant for investigators to know about, since they may need the co-operation of virtual asset service providers (VASP).

Type of transactions	Description	Impact for the investigation
FIAT currency to cryptocurrency	A victim has completed a pay in, via bank transfer, card payment, mobile pay or cash in a national currency to a VASP, which exchanges funds into cryptocurrencies.	**Best practice 1** **Try to stop or revert a transfer to a cryptocurrency broker if possible.** The largest failure at the reporting stage is to record the suspected crime and assign a person within the office to conduct a pre-investigation. This delays the initial contact with the victim. If there is no delay, the transaction potentially could still be stopped. If the transaction has been completed outside of banking hours or on the weekend, it may still be possible to stop the outgoing bank transfer from being undertaken, since some banks process bank transfers the next business day. If the transaction has been completed with a card payment, it may be possible to get in touch with a card issuer to potentially return or stop the transfer of the payment. A key aspect is to find out which financial institution carried out the bank transfer. This will be visible on the bank statement. **Best practice 2** **If stopping the transaction is unsuccessful, try to identify which VASP the transfer has been sent to, with the goal for them to stop the transaction and freeze the funds if possible.** If the cryptocurrency broker operates in a low risk country that has introduced AML/CTF regulations for cryptocurrency assets, then it is possible to contact the broker without a delay and request the funds to be frozen or returned, if they have not already been exchanged. Sometimes this process can be initiated by the victims themselves. Brokers might then stop the exchange of the funds, since AML laws indicate that funds can only be transfered if the origin of the funds is known and it is clear where the funds are being sent. Letting the VASP know that the destination of a cryptocurrency wallet is a scam will force them to take action to stop it due to money laundering regulations.

Type of transactions	Description	Impact for the investigation
		Although this depends on the internal compliance policies of the VASP, a temporary freezing of funds for a couple of business days will allow law enforcement or prosecutors to step in with an official request to return the funds. This is possible if one acts quickly and the cryptocurrency broker is responsive. If both processes failed, the third possibility is to contact the VASP that has been identified and ask for all evidence from their databases about the identity of the user that has created an user account (since it is likely to be the scammer, or a fake identity), their identification information and the transaction hash.
Cryptocurrency to cryptocurrency	A victim reports fraud that is exclusively within the blockchain technology, with no links to traditional financial institutions that process FIAT currencies. For example, a fraud has occurred in which a user has been tricked into purchasing a different cryptocurrency product (such as NFT, Staking, etc.), resulting in financial losses.	**Best practice 1** **Search for potential licensed financial intermediaries, so-called "centralized exchanges," that have been involved in the exchange. If they can be found, it may be possible to collect identity information about the parties involved through this intermediary.** **Best practices 2** **Often, victims have been subject to social engineering, which leaves a significant amount of cybersecurity traces. For example, suspects often ask victims to connect with them via remote-display management apps, emails, phone calls, initial bank transfers, sms, or communicator messages.** In this scenario, the victims are usually experienced with blockchain based finance. The initial task is to collect the most accurate and updated transfer information: transaction times, the types of currencies used by the victim, information about cryptocurrency wallets, receipts, emails, sms confirmations, and other types of information. (More details can be found in the next section "Gathering evidence," p. 27).

Type of transactions	Description	Impact for the investigation
Cryptocurrency to FIAT currency	A victim reports the theft or loss of funds	In this scenario, the victim already possessed cryptocurrencies that have been sent to a cryptocurrency exchange and then have been exchanged to a national currency to be most likely paid out by means of a bank transfer or in cash at a physical office. Similarly to transfers from FIAT to cryptocurrency, here there is a need to search for the financial intermediary that has conducted the exchange into the national currency and initiated the bank transfer. If a large amount is involved and the financial institution is located in a low-risk jurisdiction, then this institution must review where the funds have come from, a step that is conducted manually by compliance employees. If such a review occurs, it usually takes place between 24 hours to a couple of business days from the time of the transaction. If possible, type in the cryptocurrency wallet address into a blockchain-wallet-explorer to check it and review if it is connected to a financial intermediary that could be contacted (see the section “Further tools for virtual crime investigators,” p. 40, for more details). If such a search is unsuccessful, then one must use a dedicated software (a blockchain analytics provider) that might indicate whether an address has been connected to a known financial institution.

Gathering evidence

Gathering evidence

Gathering information from an individual

10 pieces of information crucial for an investigation

- **Nature of the asset:** which cryptocurrency project or NFT was involved, including its name, symbol, and specifics of the underlying technology.
- **Transaction details:** Information on transactions made by the victim, such as date, time, amount, currency, and transaction IDs (for example receipts from a VASP).
- **Wallet addresses:** Details of the cryptocurrency wallet addresses involved, both of the victim and the suspected scammer.
- **Communication records:** Any communications the victim had with the alleged scammers, be it via email, social media, chat applications, phone calls or forums.
- **Promotional material:** Any advertisements, online posts, or other promotional materials related to the virtual assets that have been received by the victims. With copies of emails, make sure the hyperlinks are included in them, ideally on USB drivers. Warning! While recording such material, do not click on any hyperlinks provided in the electronic material as they might be infected.
- **Platform details:** Any details of the VASP (see the section "VASPs and CASPs," p. 20) platform or exchange where the victim purchased the cryptocurrency asset. For information on how to request data from VASPs, see the section below, "Requesting data from VASPs," p. 29. The names of exchanges can often be found on transaction receipts.
- **Referral information:** Information on how the victim got to know about the asset, be it through a referral, an online advertisement, word of mouth, etc.
- **Coding anomalies:** If available, any evidence of manipulated code that prevents selling or any other anomalies. Any hyperlinks to websites used to support the crime, and depending on the jurisdiction, when the victim has detached its financial data, any login credentials that would help law enforcement to understand the software.
- **Financial records:** Bank statements, credit card statements, or other financial records showing the transfer of funds related to the investment.
- **Identity information:** Any details that can help identify the scammer, such as usernames, social media profiles, email addresses, or any other contact information that has been used during the interaction with the victim on the victim's computer.
- **Technological anomalies:** Has the victim installed any software apps during the process of being scammed? Has this software been uninstalled or is it still on the computer? Is it possible to determine the source or origin of the software?

If a cryptocurrency transaction has not been suspended, it is vital to obtain the cryptocurrency wallet address where the funds were either sent to or received from.

Collecting cryptocurrency wallet addresses

What are the most crucial pieces of information needed for an investigation on the blockchain?

Transaction details: Cryptocurrency wallet address and Hash numbers

A common failure is the incorrect recording of the relevant cryptocurrency wallet addresses, since these involve long strings of numbers and letters.

Example 4: When recording a cryptocurrency wallet address, etc., the number zero "0" can easily be confused with the letter O, or the letter q with g, A best practice is to type a recorded cryptocurrency wallet address into an internet search engine, like google or bing, to see whether it can be identified. If the address does not come up immediately, a wallet explorer tool can be used.
(See also the section "Further tools for virtual asset crime investigators," p. 47.)

If the cryptocurrency wallet address is correct, there will be instant information displayed that allows one to extract the following information:

Always for Bitcoin:

- **Amount of the transaction:** You can see the amount of Bitcoin that was sent or received in each transaction.
- **Time of the transaction:** A timestamp indicating when a transaction was included in a block is visible.
- **The current balance of the cryptocurrency wallet:** You can view the total amount of Bitcoin currently in the wallet.
- **Transaction Hash:** This is a unique identifier for every transaction, like a transaction-ID used by payment service providers serving as its "fingerprint."

Available at some services but not all:

- **Transaction size:** Some services provide details about the size of the transaction, often exchanged in leading FIAT currencies such as USD or EUR.
- **Timezone customization:** Certain platforms offer the ability to change the default UTC timezone. For instance, users can adjust it to their local timezone, aiding in evidence collection.

Is it possible for one cryptocurrency wallet address to store different types of cryptocurrencies?

The potential for a user to employ a singular application to access various virtual assets using identical credentials is embodied by the multi-signature (MultiSig) wallet. MultiSig utilizes a single application to manage diverse virtual assets with the same credentials, streamlining the process of handling different cryptocurrencies.

Much like how banks assign unique account numbers for various currencies—one for USD, another for EUR—cryptocurrencies based on different blockchain technologies, such as Bitcoin and Tron, require unique wallet addresses.

MultiSig wallets do not necessarily require multiple individuals; instead, they refer to the use of multiple private keys to authorize a transaction. One person could possess multiple private keys, or multiple individuals could be involved in asset management, each with their own private key.

A visualization of this concept can be likened to the distinction between smartphone types and the operating systems or applications they support. Certain apps are designed exclusively for Apple's iOS and require an iPhone, while others are tailored for Android and won't function on Apple devices. However, various apps developed by different programmers can run on the Android platform and be sourced from the Google Play Store. Similarly, cryptocurrencies unified by a common technology, such as ERC20 tokens built on the Ethereum blockchain, can be managed within a single Ethereum-based wallet address.

This mirrors how a single app store facilitates the download of numerous apps developed on the same platform. Likewise, cryptocurrencies developed on the same blockchain, like Ethereum, can be consolidated within a single Ethereum-based wallet address, allowing for a more streamlined user experience.

Requesting data from VASPs

If the victim doesn't know to which virtual asset service provider (VASP) the money has been sent, they might have a receipt showing wallet addresses. If not, this data can be often visible using a blockchain analytics provider software. Such providers are registered in countries where laws clearly state that virtual assets must follow anti-money laundering guidelines. As per these rules, VASPs must verify the identity of their users and record transactions. For example, within the European Union, according to the Fifth EU AML Directive, VASPs across the EU Member States must be registered and must comply with a variety of anti-money laundering obligations.

If the victim knows which VASP the funds were sent to or came from and still has (or can recover) the login credentials, then the first step is to extract all transfer information from the exchange. This transfer information will include conducted transactions, the cryptocurrencies sent and their cryptocurrency wallet addresses.

If the victim is unsure where the funds have been transferred or from where they were sent, the name of the VASP can sometimes be found on the victim's bank statement or card statement.

Some of the names of virtual assets or exchanges include PanCake Swap (https://pancakeswap.finance/); Wasabi Wallet (https://wasabiwallet.io); Doge Coin (https://dogecoin.com/); and Shit Coin (https://www.investopedia.com/terms/s/shitcoin.asp). While these would not be instantly familiar to those not active in the cryptocurrency world, they are commonly used.

Even platforms that claim to be fully decentralized, such as Uniswap, offer a transaction history possibility for users in .csv that can help with an investigation.

With hundreds of exchanges worldwide, only a few names might be easily recognizable to the general public or law enforcement.

If an individual cannot retrieve access to their account at a VASP, it remains possible to reach a centralized VASP or a cryptocurrency wallet (custodianship provider) for help.

Following best practices, VASPs will usually not provide any information over the phone, so there is a need for a Law Enforcement Request (LER) to the VASP or other financial institutions that processed the exchange of the victim's funds. The process of filling in an LER to a VASP is described on page 22.

The information you're likely to receive from a centralized VASP is the following:

- First name
- Last name
- Date of birth
- Copies of identity documents[10]
- Size of completed transactions
- Timestamp of transactions[11]
- FIAT and cryptocurrency of the transaction[12]
- Size of the agent's commission
- Confirmation time of Sanction Screening and Politically Exposed Person Screening and the types of watchlists that have been used.
- **Cryptocurrency wallet address** or addresses if multiple transactions and currencies exist
- Transaction hashes to conducted transactions

It is less likely but still possible to receive the following information:

- Customer number or ID registered within the agent
- Declared residence address[13] of the customer
- Registered address of the customer[14]
- Social security number, depending on the country where the platform is registered
- Interactions between the agent (VASP/CASP) and the customer (often in the form of a PDF, since customer service is often conducted with external software providers such as Intercom or ZenDesk)
- All documents providing proof of funds – uploaded to and from the users
- IP address (which might be misleading since users tend to use VPNs)
- Device used for login, such as a mobile phone or a desktop computer
- Browser and the version used for accessing the service: Opera, Chrome, Safari, Internet Explorer or similar
- Background checks on the customer, conducted with Open Source Intelligence (OSINT)[15]
- Comments of VASP employes with regard to a particular user or its transactions
- Any blockchain analytic investigations conducted on the user or its transactions by VASP employes
- Any enquiries about the particular user from other law enforcement agencies or financial institutions
- Any transaction that has been initiated by the user but not completed
- For physical offices or ATMs, there might be a video recording of individuals using the premises
- Request all of the documents the users have uploaded (including proof of source of funds and proof of source of wealth), as well as all interactions with customer service

Police officers can collect more information from the victim about their own bank account details, which helps filter the information collected from VASPs. This information will only be available for FIAT to crypto transactions (not for crypto to FIAT transactions).

- The bank account number of the victim that was used to conduct a transfer to and from a VASP account.

10 This can include a passport, identity card, or e-identification. However, this process is vulnerable to the same issues as traditional cybercrime, such as the use of fake or collectible items that imitate real identity documents (for example, "collectable documents" available on websites like dokumencik.pl).

11 It is important to determine which time zone the timestamp refers to. For example all Bitcoin blockchain transactions are registered with UTC (London time) independently of where the user comes from. The problem of connecting incorrect transaction timestamps to other evidence has sometimes been critical.

12 Both virtual assets and FIAT.

13 If allowed in the jurisdiction, it is possible to review whether the platform has other customers registered at the same address who have conducted transactions.

14 Whether the platform extracts such information from a public data basis.

15 Which might include extractions from publicly available data sources, such as criminal record certificates or information about the UBO of particular ventures, that might have been extracted by compliance employees of the platform.

- Phone number: Some users use their phone's payment system

- Card information from the credit, debit or prepaid card that was used for the transaction. The provider's account might have additional information such as a second level of confirmation via a mobile bank app or the SMS service called 3D secure that could be obtained

- For countries using "open banking," additional information might be available from payment service providers that conduct those transactions (if those transactions have been completed using open banking)

Format information for VASP data

For optimal efficiency, it's advisable to obtain the required transactional data in a ".csv" format, facilitating straightforward integration into law enforcement systems. Typically, responses to Law Enforcement Requests (LERs) are delivered in two formats:

- A ".pdf" where the Virtual Asset Provider offers direct responses to inquiries made by the Law Enforcement Agency (LEA)

- A ".csv" file comprising transactional data

Often, VASPs maintain a folder with consolidated customer data. This folder includes crucial documents such as proof of funds (POF) and other uploaded files. Large VASPs normally have a set way of responding to law enforcement requests. When interacting with smaller institutions, law enforcement may be able to specify their preferred data format for receiving the required information.

However, customer identity can sometimes be captured in diverse formats, such as a ".pdf" or a ".jpeg" of an ID document or a video that exists in formats like ".avi" or ".mov".

It is recommended to refrain from requesting ".xml" or ".xls" files from VASPs. Specifically, the use of ".xlsx" files is discouraged due to cybersecurity concerns. There's a risk that data provided by VASPs in ".xlsx" format could harbour viruses, particularly in the macros embedded within the file, which may compromise the security of LEA computer systems.

Reliability of obtained IP addresses

An Internet Protocol (IP) can often be obtained from a VASP through a law enforcement request process. An IP address is a unique identifier of a device like a smartphone or a laptop on the internet network. Think of an IP address as a unique set of numbers, like a phone number. For example, 193.46.242.201 points to Stockholm, Sweden. But just as one landline phone number can be shared by multiple family members in a house, thanks to a technology called NAT (Network Address Translation), multiple devices can use the same IP address.

VASPs often claim that they can export IP addresses which have been captured during the login process of users, however the reliability of this information for investigations ought to be questioned. IP addresses only show which device accessed the internet, not who specifically used it. They can be camouflaged by scammers using virtual private networks (VPNs), and therefore should only be used in cases in which there is other evidence that can link the user's IP to potential criminal activity.

Companies providing internet access to users' homes (called internet service providers, "ISPs") can often identify who used a specific IP address at a certain time. During an investigation, such companies might be requested, to connect the address to particular users who signed a contract for their services. Unfortunately, even if the user does not use VPN, this information is not always reliable. Since users might provide WIFI networks without passwords, there could be times when someone else's IP address is used.

Knowing an IP address alone doesn't always provide exact information about who performed a specific action online. In environments such as public offices, schools, or workplaces, multiple individuals might share the same internet connection, further complicating the attribution of online actions to a specific individual.

Finally, VPNs are engineered to hide a user's actual IP address by projecting the appearance that the connection originates from a different location. However, even with a VPN there might be a possibility to connect a certain user behaviour with visits of particular websites, associating them with a particular IP within a specific timeframe. This implies that while VPNs enhance user anonymity, they do not render online actions completely untraceable. Discerning entities might still be able to link online activities to individual users under certain circumstances.

Collecting IP addresses

Arguments for:

- **Traceability:** IP addresses can serve as a starting point to trace back potential suspects or identify the origin of suspicious activities. There might be a possibility that they can be connected to other investigations.

- **Deterrence:** Knowing that IP addresses are monitored may deter potential criminals from using their own networks for illicit activities.

- **Collaborative evidence:** In conjunction with other pieces of evidence, IP addresses can help to build a stronger case against suspects.

Roman Bieda conducting a hands-on workshop for investigators in Kazakhstan. As a former product owner of a blockchain analysis tool and an expert witness in courts in Europe and the United States, he focuses on sharing not only knowledge, but also best practices and insights into the challenges faced during the evidence collection process. The aim of the OSCE workshops are to ensure that challenges experienced in one participating State do not need to be repeated in others.

Arguments against:

- **Inaccuracy:** Since multiple devices can share a single IP address, and with the use of VPNs and other obfuscating tools, relying solely on IP addresses might lead to misidentification.

- **Privacy concerns:** Collecting IP addresses en masse may infringe on individuals' privacy rights, especially if done without proper justification.

- **Resource Intensive:** Tracing and verifying IP addresses, especially when VPNs or other masking tools are involved, can be time-consuming and divert resources from other vital investigative activities.

In conclusion, while IP addresses can provide additional insights about a device's activity and location of a particular device at a given time, they don't conclusively identify individual users. Investigations based on IP addresses are only useful when approached with caution and seen as part of a larger toolkit.

Other documents to request

In some OSCE participating States, companies that handle virtual assets (like cryptocurrencies) are considered "obliged financial institutions" or intermediaries. This means they have to regularly monitor their customers' activities. They are required to review customers and transactions that exhibit suspicious behaviour, often employing blockchain analytics tools to identify potential sources of risk. Once these checks are conducted and documented, law enforcement can request to see them.

For example, in the Republic of Georgia, companies providing exchange services that are registered with the National Bank of Georgia are obligated to use specialized tools to analyse blockchain transactions. **This ensures a layer of transparency and security in monitoring the flow of virtual assets.**

If law enforcement agencies lack access to such blockchain analytics tools, they can request the VASP to share details for the investigation. This information could be in an accessible and editable format, such as a PDF or an image file.

This implies that while the tools are instrumental in maintaining the integrity of transactions and identifying illicit activities, there are procedural and legal considerations to be observed when sharing information derived from these tools. For example, multiple blockchain analysis providers and compliance solution providers might have specific protocols and agreements in place that limit the sharing of sensitive or editable information even with law enforcement — without prior authorization. This might create problems for VASPs to be willing to disclose reliable information vs. being obliged to limit evidence due to agreement constraints.

Taking cases to court

Taking cases to court

Prosecutors of virtual asset cases

To ensure that prosecutors have a solid foundation to work from, law enforcement officers should be well-versed in evidence collection related to anti-money Laundering (AML) activities, especially in the rapidly growing field of virtual assets and cryptocurrencies.

Investigative stage

- **Seek digital evidence:** Understand and monitor the transactions on blockchain technology and distributed ledgers.
- **Analyse information:** Recognize patterns that might suggest money laundering, such as rapid and high-volume transactions on cryptocurrency exchanges.
- **Follow digital leads:** Trace the flow of assets across multiple virtual wallets and platforms, using specialized software if needed.
- **Evaluate the credibility of all received identification information**, received from VASPs (See challenges with "Copies of Identity documents," p. 30)

Trial or investigation preparation

a. Case overview:

- There should be a focus on crypto wallets, IP addresses, transaction timestamps, and the amounts exchanged in the digital realm.
- The first intention should be to understand the conversion of virtual assets to tangible assets, like property or goods, and trace their origins.

b. Identifying the type of offence:

- Recognize the signs of cryptocurrency being used for money laundering, such as through "tumbling" or "mixing" services that aim to obscure the source of funds. Some of the leading blockchain analytics providers offer "demixing services" which claim to be able to disassemble the transactions that have been processed across a mixer. If the case is of severe importance there are demixing services offered by both blockchain analytics providers and courses on demixing offered by law enforcement agencies like Europol.
- Use the ledger of blockchain transactions to prove the elements of the crime.

c. Linking criminal activity to assets:

- Trace any movement from cryptocurrency wallets to the purchase of tangible or other virtual assets. This could involve looking at the movement of cryptocurrency from an exchange to a private wallet and then to another entity or service.
- Identify any anonymizing services or techniques used, and attempt to trace assets despite these challenges.
- Recognize patterns that may indicate criminal intent like money laundering, such as splitting large amounts of cryptocurrency across multiple wallets or using privacy coins like Monero or Zcash.

Presentation of evidence:

- Clearly explain how cryptocurrencies and blockchain work, since many court officials may not be familiar with this technology.
- Present a clear and concise digital trail of the money laundering process, from the source of the illicit funds to their final destination. It has been recommended to create visual props and to use easy non-technical language when presenting evidence, since many prosecutors or judges might not yet be fully familiar with the complexities of cryptocurrencies.

Additional evidence:

- Crypto exchange records: These can provide user activity details, wallet addresses, IP logs, transaction amounts, and dates.
- Blockchain analysis software: Such software can visualize the flow of digital currencies.
- Digital wallet examinations: Investigate hardware wallets, mobile wallets, and desktop wallets. They might have records, transaction history, or metadata that can be useful.
- IP address tracking: Track the IP addresses associated with transactions to locate the geographical location of the suspects. (see p. 31 for the limitations of IP addresses)
- Collaboration with international agencies: Due to the decentralized nature of cryptocurrencies, international co-operation can be crucial for tracking cross-border transactions. However, such co-operation is usually started at a later stage by a leading investigator.[16]

By collecting comprehensive evidence related to cryptocurrency transactions and activities, police officers can provide their investigation colleagues as well as prosecutors a robust base to build their case and ensure that culprits are held accountable.

16 Finance Intelligence Units that work together with the Egmont Group have developed an exchange system mechanism that can be accessed here: https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf (accessed 15 Feb. 2024)

Recommendations and contacts for complex cases

Recommendations and contacts for complex cases

Dedicated teams and expertise

Leading providers of blockchain analytics software frequently establish dedicated teams composed of experts in both the realms of cryptocurrency and investigative processes. These teams specialize in assisting law enforcement agencies in navigating the intricacies of blockchain analytics, ensuring that the tools are used to their maximum potential. It is recommended to check your agency's intranet to see which departments are already using blockchain-based analytics software, since colleagues in those departments are likely to have the most insights into this matter.

Training and certification

Recognizing the complexities of blockchain technologies and the importance of robust knowledge management, many blockchain analytics software providers also offer structured training programmes. These programmes often culminate in various levels of certification, which not only validate the skills of law enforcement personnel but also amplify their efficiency in handling blockchain-related investigations. While some services, like consultancy support, may require additional funding, the long-term returns in terms of enhanced investigative capabilities can be substantial.

External support for in-depth investigations

Beyond in-house teams and training, there is an expanding spectrum of external commercial providers adept at conducting exhaustive investigations of cryptocurrency transactions on the blockchain. These entities operate as contractors, offering their specialized skills to law enforcement agencies. Their expertise can prove invaluable, especially in complex cases where in-depth analysis and multifaceted investigative techniques are required. Law enforcement agencies like INTERPOL or Europol offer dedicated support and training for investigators (see section "Co-operation with experts on digital assets," p. 51). If your team would like to join available training events, please contact VirtualAssets@osce.org for additional information.

Proceed with caution

However, while the advantages of external providers are numerous, agencies must also be cognizant of potential challenges. Engaging external entities like consultancy agencies or blockchain-based analytics providers in sensitive investigations can introduce complications in case proceedings. There is also the critical matter of data security. The transfer of sensitive information to external parties must be approached with utmost caution to ensure that data integrity is maintained and that there is no inadvertent breach of confidential information.

Maciej Szulc leading a train-the-trainer workshop in Gdansk, where policymakers from OSCE participating States share best practices for resolving complex cases and assisting national stakeholders. The focus extends beyond content quality to effective delivery methods.

Support for victims

Support for victims

Challenges victims should be warned about

Victims of one cryptocurrency scam can easily fall prey to another. Organized fraud rings don't just strike once, but instead target their victims repeatedly and strategically. Below are details of common secondary scams:

- The "Saviour" Deception: After an individual's initial entanglement with a scam network, a different wing of the same syndicate extends an offer, pretending to be a professional who can help recoup their lost investments. This seemingly generous offer comes at a price, with the victim expected to pay a service company to recover the lost funds. After the funds have been transferred, the "saviour" often disappears, together with lost funds.
- The "Whistleblower" Ruse: In another guise, scammers might pose as disgruntled ex-employees of the fraudulent enterprise, asserting inside knowledge that can supposedly help victims reclaim their assets. The process is the same as with the saviour — funds must be paid in advance and then the contact person usually disappears.
- The Mirage of Legal Recourse: These are scenarios where victims are approached by a legal professional who pledges to get the money back, particularly when VASPs come into play. After the vicitm agrees on an hourly rate, these lawyers claim to have created extensive documents, sometimes exceeding 40 pages, that often detail fundamental cornerstones of the anti-money laundering (AML) and counter-terrorism financing (CTF) legislation but have limited legal value. Unfortunately, the documents that have been used are mostly generic and 99% of them remain unchanged, so the VASP is flooded with the same documents with minor customizations. Victims are charged exorbitant rates for these largely redundant efforts. It is essential to realize that with most VASPs, transactions, once executed, are irreversible. Claiming "credit card chargebacks" has slim chances of success. Hence, such legal action points are usually of low value and rather deplete a victim's wallet.

Olga de Truchis, an OSCE Virtual Asset Expert and Co-Driver of the Europol Financial Intelligence Public–Private Partnership (EFIPPP) Crypto-Assets Workstream, led a session on best practices for traditional financial providers in managing financial crime risks associated with virtual assets and virtual asset service providers. The workshop, hosted at the premises of the National Bank of Latvia (Latvijas Banka), included representatives from four additional OSCE participating States.

Selected types of crimes committed involving cryptocurrencies

Selected types of crimes committed involving cryptocurrencies

Below are details about the most common types of crimes committed with cryptocurrencies. At the very least, one should be aware of these types of crimes, but also know that this is not a comprehensive list.

Cryptocurrency investment schemes

What is it?

Cryptocurrency investment scams are some of the most common types of fraud schemes. Initially, this scam targeted wealthy senior citizens in high-income countries. However, the tactics have evolved, with stock market investors and those nearing retirement increasingly being targeted. It is crucial to remain vigilant and attuned to the evolutions of this scam in the future.

This scam works by scammers contacting wealthy individuals and presenting them with lucrative investment opportunities. Typically, a scammer, pretending to be a seasoned crypto investor, approaches unsuspecting individuals displaying significant amounts of wealth.

Different types of this scam

There are usually different types of claims:

- **Upfront fees:** Scammers lure individuals with the promise of high returns on investments. However, to initiate the process, they mandate an initial commitment, from 250 EUR to 1000 EUR (or equivalent in the national currency in question) usually at the lower end of this range.Upon receiving this initial payment, a scammer simply disappears post-payment, leaving the victim financially diminished with no prospective investment to show for it.

- In a more complex approach, the process involves a live video call, during which the scammer showcases a “financial account” that is claimed to belong to the future victim who is experiencing a substantial influx of money. While these accounts are designed to appear legitimate, they are actually design copies and have no connection to traditional financial institutions.

- Sometimes victims receive a “first payout” of for example 50 EUR to 100 EUR, which the scammers claim to be interest on their investments, to lure the victim to pay more.

- **Identity theft:** To create an illusion of legitimacy, scammers might request personal identification details of the victim, purportedly for fund transfers or deposits. However, instead of assisting in an investment, they gain unauthorized access to the personal and financial details of the victim. Victims forget to block their identity documents at the financial institution, or even send copies of this information to the scammer.

How to address it

- **Do not complete any additional transfers.** Often scammers speak about small transfer costs, or payout costs that appear very small in comparison with the total amount of the scam. Example: a 600 EUR fee for a 60,000 EUR scam.

- **The vicitm should not break the contact.** Usually by the time a victim approaches law enforcement, their contact with the scammer has already been broken. But if it is not, then it might help the investigation for the victim to maintain their contact to enable a search for the cybercrime tools being used.

For users who are less experienced in investments, finance or the usage of online tools, scammers often install remote-access software.

This software is primarily designed for remote access, control, and support. It allows users to remotely access and control their desktop or laptop and servers from anywhere. The victim often installs such software with the help of a scammer. Once the connection has been established, the victims often forget to uninstall the software. Traces left with the software can be a good support for law enforcement investigation, if secured correctly.

Depending on the type of software, there are various types of features, including:

- **Remote control:** Users can control a computer from another location as if they were sitting right in front of it. This is useful for troubleshooting issues, providing remote support, or accessing files.
- **File transfer:** Software that allows users to transfer files between computers. This sometimes leads to the instalment of a "keylogger," a type of spyware that monitors everything the user types and can share it with scammers for years after it has been installed on a computer.
- **Remote access:** This lets scammers access the victim's computer or server remotely and modify files, install programs or initiate connections.
- **Mobile access:** This allows the remote control of devices from smartphones and tablets.

- **Victims should** not uninstall any software that has been placed on their devices, since these might leave cybersecurity traces useful for investigations. However, the victim should be aware of the possibility of having software on their device that tracks what they are typing, or that keeps the camera turned on, etc. If this is the case, the vicitm should limit the use of their device.
- **Review what personal information has been released.** If possible, change bank logins, and order new passwords for e-identification tools if such tools are used.
- **Review the section on secondary scams** found above on p. 38.
- **The appropriate steps to take depend on the victim's specific situation.** For further details, see the section "Best practice for each type of transaction," p. 24.

A further twist to this scam is the use of fake celebrity endorsements. Scammers misappropriate real photos and combine them with fabricated accounts or promotional materials, making it appear as if renowned personalities vouch for the scheme.

Extortion and sextortion

In cases of extortion, individuals often receive a sophisticated email falsely informing them that a hacker has obtained access to the victim's computer and can connect to the camera of a laptop or a smartphone. When it comes to sextortion, the claim is usually that the hacker filmed the victim during an act of masturbation.

What is it?

An individual receives an email from a scammer. This email says that the scammer has hacked the victim's computer or smartphone and obtained access to the camera. In sextortion cases, the scammer then claims that they have recorded footage of the victim during an act of masturbation and will publish the video if the victim does not pay them in cryptocurrency.

The victim is prompted to transfer funds to a specified cryptocurrency wallet within a tight deadline to prevent the release of such purported footage to business and private contacts, who the hacker claims to have found on the device. As "evidence" of their claims, the hacker typically provides a list of usernames and passwords associated with various websites, suggesting that the victim used identical credentials across multiple adult content sites.

An original email message sent to the author of this publication:

Topic: I recorded you - (here the scammer passes on the password that was found in the breach)
Date: 2023-06-22 3:32
Sender: “Save Your Life “ <xxxxxxxxxf@xxxx.ga>
Receiver: XXXXXX@xxxx.com

Hi, I’m a hacker and programmer, I know one of your passwords is: (password of the user extracted from password leaks)

Your computer was infected with my private malware, because your browser wasn’t updated/ patched, in such a case it’s enough just to visit some website where my iframe is placed to get automatically infected if you want to find out more - Google: “Drive-by exploit”.

My malware gave me full access to all your accounts (see password above), full control over your computer and it was possible for me to spy on you over your webcam.

I collected all your private data, recorded a few videos of you (through your webcam) and I RECORDED YOU SATISFYING YOURSELF!!!

I can publish all your private data everywhere, including the darknet, where very sick people are, and the videos of you, send them to your contacts and post them on social networks and everywhere else!

Only you can prevent me from doing this, and only I can help you out. There are no traces left, as I removed my malware after my job was done and this email(s) has been sent from some hacked server…

The only way to stop me is to pay exactly 400$ in bitcoin (BTC).
It’s a very good offer, compared to all that HORRIBLE shit that will happen if you don’t pay!
You can easily buy bitcoin here: www.xxxxxxx.com, www.xxxxx.com , www.xxxxxx.com or check for a bitcoin ATM near you or Google for other exchanges.

You can send the Bitcoin directly to my wallet or create your own wallet first here:

www.login.xxxxx.com/en/#/signup/, then receive and send to mine.
My Bitcoin wallet is: **17yshaYmvdp4yjU3WoCwowh6HHjTfEGDuG**
Copy and paste it; it’s (cAsE-sEnSEtiVE).
You got 3 days.

As I got access to this email account, I will know if this email has been read.

If you get this email multiple times, it’s to make sure that you read it, my mailer script is configured like this and after payment, you can ignore it.

After receiving the payment, I remove all your data and you can live your life in peace like before. Next time, update your browser before browsing the web!

Nina-Louise Siedler, in Riga, leading a workshop for policymakers from five participating States, sharing insights from virtual asset regulatory roundtables. The session focused on pan-European legislation related to virtual assets, aiming to identify regulatory shortcomings and highlight novel developments of relevance to the participating States.

How to address it

Best practices in supporting victims who report extortion emails.

- **Stay calm:** If the user has received a sextortion email, there is a need to remain calm. The example of the email presented above shows that criminals use strong adjectives, with the goal to instil fear, create urgency, and induce shame as well as panic.

- **Victim shall not engage** with the sender in any way: Sextortion emails usually do not send anything as proof, or contain attachments. If there are any links sent with the email, the user shall not open them.

- The user must be prohibited from exchanging FIAT to cryptocurrency and transfering it to a suspect cryptocurrency wallet.

- **Verify cryptocurrency wallet:** One way to assess the authenticity of a cryptocurrency wallet address is through tools commonly referred to as "wallet explorers." For instance, the mentioned cryptocurrency wallet can be examined using the following link:

  https://www.blockchain.com/explorer/addresses/btc/17yshaYmvdp4yjU-3WoCwowh6HHjTfEGDuG.

- Upon initial investigation, which remains free of charge and takes less than 10 seconds, it becomes evident that this wallet has received multiple transactions. This often contradicts the hacker's claim that this is a unique and singularly used cryptocurrency wallet address. Multiple transactions suggest that several individuals may have transferred funds to it.

- **Using the market of stolen account credentials for the advantage of the victims:** Victims may use free-of-charge services like: https://haveibeenpwned.com, which allow them to check if their data has been exposed to data breaches by combing through billions of leaked account details. By entering their email or username, users can see if their information appears in any known breaches. If the attacker showcases a password that is being used, change it immediately across all platforms where it's employed.

When investigating individuals suspected of extortion, tracing payments to their cryptocurrency wallets is essential.

By doing this, one can see if any wallets are tied to official financial platforms, which can help law enforcement identify who sent money to the suspect. While paying into an extortion wallet isn't a crime, those who did might have relevant information or faced similar threats from the same person, which can aid an investigation.

At the OSCE Secretariat Vienna, training is held for Ukrainian policymakers on regulatory gaps in virtual assets, with a focus on decentralized exchanges.

"Rug Pull" scams

Exit scams, pump-and-dump scams, or "rug pull" scams (after the metaphor "pulling the rug out from under someone") are schemes in which scammer create a lot of excitement around a new digital asset. It can be any type of digital asset, not just a new cryptocurrency. Such scams have been pulled with projects and non-fungible tokens (NFTs), too. Scammers then quickly exit the project, stealing investors' money and leaving the digital asset worthless.

What is it?

The objective of this type of scam is to get as many buyers or investors as possible for the new digital asset, and to artificially inflate its perceived value to be as high as possible. Once the scammers have collected enough money, they vanish (the "exit" of the exit scam) and take the money for themselves. This exit can happen quickly, with everyone suddenly disappearing, or over time, with money slowly taken out of the scam and the developers intentionally producing fewer developments of the asset. In the case of the latter, it can sometimes be hard to distinguish between a true "rug pull" fraud or just a badly handled, unsuccessful project.

In either case, the exit of the scammers means the asset is shown to be fake and becomes valueless. The victims are left either with multiple coins or tokens that are worth a fraction of what they paid for them, if they can find a buyer, or the digital asset contains a code that indicates the asset can't be sold at all.

Phishing scams

Phishing scammers is a common scam in many areas of the internet. It is also a common and effective scam related to digital assets.

What is it?

Scammers pretend to represent an official business with legitimate-looking websites or company documents and send out thousands of emails and messages with links leading to their fake version of a website. This website is created to allow logins and store every visitor's personal information as well as all crypto addresses and passwords (called "crypto wallet keys") that they type. This is especially important for crypto crime, since unlike other kinds of accounts, if a crypto wallet's private key is stolen, then the account is nearly impossible to retrieve. This means that the funds within the wallet are lost forever.

Different types of of this scam

According to a report released by one blockchain analytics provider,[17] new types of phishing scams involve playing off of "FOMO" (fear of missing out) in new crypto investors, by getting victims to send money to the wrong account in the hope of buying an NFT. This meant that victims lose only the amount of money they sent to the wrong account, not their entire wallet.

17 Illicit Crypto Ecosystem Report. (2023), available at: https://www.trmlabs.com/report (accessed: Aug. 2023).

Another type of scam variation gaining popularity is "address poisoning," in which a scammer creates an address that resembles one to which the intended victim previously sent funds. The scammer then sends a small amount of cryptocurrency to the target in the hope that they will unwittingly make a future payment to the same scam address in place of their intended recipient.

What can be done to avoid it?

People should be aware of fake phishing links and check all links.

Double-check addresses:

- Always double-check the address one is sending funds to, especially when dealing with large amounts. Do not rely solely on clipboard functions (the so-called copy-paste function), since malware can manipulate them to paste cryptocurrency wallet address other than what the victim believed to have copied.

- Use bookmarks for frequently visited crypto sites. This avoids the risk of mis-typing or landing on a phishing site that looks similar.

Enable additional security measures:

- It is recommended to use two-factor authentication (2FA) wherever possible. This adds an extra layer of security, making it more difficult for scammers to access accounts.

- Regularly update and run anti-malware software to detect and remove potential threats on your device. Some malware strains are designed to monitor crypto transactions or to modify clipboard data.

Use password managers: Password managers are software tools designed to store, manage, and auto-fill passwords. They also often allow users to create safe notes that can securely save cryptocurrency wallet numbers for various online accounts.

Man-in-the-middle attacks

What is it?

In this type of scam, scammers don't directly target a victim, but instead intercept the data transmission when someone accesses their cryptocurrency account on a public or unsecured wifi network, that is, where the websites visited and the information sent from computer to website is not private. The scammers collect the crypto wallet address, login details and the wallet keys, and then use this to take over the account.

How to address or avoid this?

This type of scam can be avoided with the use of a virtual private network (VPN). These are fairly cheap, usually only 3 to 4 EUR a month. VPNs encrypt the user's connection to the internet, making it harder for unauthorized individuals to see what websites are visited or what is typed. It also conceals the user's original IP address, allowing for anonymous browsing and stopping the user's actual geographical location from being visible. This allows users to have remote access to their organization's resources, or for them to bypass censorship.
(See more in the section "Collecting IP addresses," p. 31.)

Fake websites imitating cryptocurrency exchanges

What is it?

Instead of creating a fake cryptocurrency, the scammer creates websites that look like cryptocurrency exchanges. When the victim goes to this website to exchange their type of cryptocurrency for a different type or for FIAT currency, the scammers steal their details and the deposited cryptocurrency.

How to address or avoid this?

To bolster security, always employ two-factor authentication (2FA) when logging into your exchange. This additional layer of verification can involve receiving a one-time code via SMS or email, which you need to input during the login process. Alternatively, if the OSCE participating State offers an e-identification solution, consider utilising it for an added measure of protection during sign-in.

Secondary scams

There are also secondary scams that occur after a victim has been scammed once. These are covered in the section "Support for the victims," p. 37.

From left to right: Marcin Zarakowski, Michal Gromek, Anna Pajewska, and Nina-Louise Siedler, who led an independent workshop focused on the challenges and advantages of supervizing virtual asset service providers (VASPs) for the Ukrainian delegation. The session included representatives from key Ukrainian institutions, such as the National Bank of Ukraine (NBU), the State Financial Monitoring Service of Ukraine (SFMS), the Ministry for Digital Transformation, and the National Securities and Stock Market Commission (NSSMC). The workshop was hosted at the Polish Ministry of Finance, which continues to generously offer its facilities free of charge for a series of training sessions for Ukrainian delegates.

Further tools for virtual asset crime investigations

Further tools for virtual asset crime investigations

Blockchain analytics tools

A good blockchain analytics tool or wallet explorer means that police officers can conduct part of their investigations without needing to rely on information from VASPs, which can be slow or incomplete. Furthermore not all VASPs are yet using blockchain analytics tools.

Why this matters:

Law enforcement agencies frequently request information about the current balance of specific cryptocurrency wallet addresses from VASPs. While VASP compliance teams are equipped to respond to these queries, doing so becomes a considerable administrative task. A more efficient alternative is to input the cryptocurrency wallet address into a wallet explorer, which then quickly provides the needed information for a majority but not all leading cryptocurrencies.

Information offered by wallet explorers:

- Current balance in cryptocurrency and major FIAT currencies, e.g., USD.
- Total funds received by the cryptocurrency wallet.
- Total funds sent from the cryptocurrency wallet.
- Timestamps for transactions. (Note: transaction times may vary based on the cryptocurrency's time zone).
- Fees incurred on the blockchain.
- Source cryptocurrency wallet addresses (from where funds were transferred).
- Destination cryptocurrency wallet addresses (to which funds were sent).

To those unfamiliar with blockchain analytics, this data might seem superficial. However, for investigative purposes, it can provide valuable insights, such as showing a pattern of many small incoming transactions, coupled with fewer large outgoing transactions. This type of pattern might suggest activities resembling those of a drug dealer.

Real-world examples:

The following wallets have been found to have been used in criminal cases:

- Cryptocurrency wallet linked to a sextortion case: Blockchain Explorer
- Cryptocurrency wallet associated with the Twitter Hack, a wallet explorer that collects feedback from users, and Chain Abuse

Similar to all open source intelligence sources, any data obtained from such explorers should be approached with scepticism and verified before drawing any conclusions.

Examples of free blockchain analytics tools:

- Block Explorer: This is a straightforward tool that provides detailed information about Bitcoin blocks, addresses, and transactions. It is a good starting point for beginners.
- Etherscan: This tool is specifically for the Ethereum blockchain, and can offer detailed transaction and address analytics.
- Blockchair: This tool covers multiple blockchains, from Bitcoin to Ethereum, making it versatile for those looking to analyse different networks.

Olga de Truchis and Greta Barkauskiené, OSCE Virtual Asset Experts and Co-Drivers of the Europol Financial Intelligence Public–Private Partnership (EFIPPP) Crypto-Assets Workstream, participated in the EFIPPP April 2024 Plenary at Europol's headquarters in The Hague. Together, they facilitated knowledge-sharing sessions in which participants from various countries, including OSCE beneficiary countries, explored and discussed emerging modus operandi of organized crime in the virtual asset space.

Blockchain analytics providers

Blockchain analytics providers are the commercial counterparts of wallet explorers.

They use specialized software designed to monitor, analyse, and visualize activities on blockchain networks. These tools help investigators to uncover patterns, follow transactions, and gain insights into the vast and complex world of blockchain.

Beyond the data available by using a wallet explorer, blockchain analytics providers offer:

- **Tracking & tracing:** Most analytics tools can track and trace the journey of a cryptocurrency transaction from its source to its destination. This is vital for understanding the flow of funds and identifying any potential illegal activities.
- **Visualization:** These tools often provide visual schemes and charts to make it easier to grasp large amounts of data at a glance and connect cryptocurrency wallets to financial institutions, or link transactions or wallet providers together.
- **Risk assessment:** By analysing transaction patterns, some tools can assess the risk associated with particular wallets or transactions, offering valuable insights for financial institutions and regulators.
- **Comprehensive data:** These tools can pull and integrate data from various blockchains, giving users a holistic view of the cryptocurrency landscape that can be helpful for larger numbers of of investigations.
- **Demixing services:** Some providers claim that their services are able to display transactions across mixers and tumblers, which are services designed to enhance the privacy and anonymity of cryptocurrency transactions. (For more information, see the section "Mixers and tumblers," p. 19, as well as the discussion of demixing services in the section "Taking cases to court," p. 34.)

By leveraging these tools, investigators can better understand the intricate dynamics of the blockchain world, ensuring informed decisions and a deeper comprehension of this revolutionary technology.

At the HQ of the National Bank of Georgia, the Virtual Asset Team has received crucial support from OSCE Virtual Asset Experts over the past two years. As a result, Georgia's score in MONEYVAL has been elevated to "Largely Compliant" with FATF Recommendation 15.

Co-operation with experts on digital assets

Co-operation with experts on digital assets

When dealing with digital assets and their associated reports at a law enforcement agency (LEA) station, collaboration with external entities becomes essential. These entities include international police organizations, banks, and specialized units within certain countries. Their expertise aids in the effective handling of investigations.

Identifying local expertise

It is invaluable to identify local members of a law enforcement agency who have experience in virtual assets. Having their contact details can be beneficial for the following reasons:

- **Purpose:** To field questions and gain insights during reporting processes.
- **Example:** The United Kingdom's National Crime Agency (NCA) has created a dedicated crypto unit that can act as a sound board for complicated cases. Inspiration for how to organize co-operation within law enforcement with regard to virtual assets can also be found in the Typologies Report 2023 compiled by Council of Europe.[18]

International support

Europol Platform For Experts (EPE):

- **Description:** This is a free platform for hands-on assistance on virtual assets for members of LEAs.
- **Eligibility:** To be eligible for the EPE (https://epe.europol.europa.eu/), a country must be a Member of the European Union or be part of a so-called operational agreement.[19]
- **Benefits:** EPE offers best practices on virtual asset investigations. It also provides access to webinars, as well as contact details to stakeholders, conferences, and other learning resources.
- **Joining process:** If an OSCE participating State is part of the operational agreement[20] Budapest Memorandum (list provided separately), they can apply for access. The process involves:
  - Contact the designated authority at o3 (at) europol.europa.eu using a work email and specify what connects you to virtual assets and how your knowledge will benefit others.
  - Clearly specifying the reason for joining, specifically as related to virtual assets.
- **Who can join:** While the platform is primarily designed for law enforcement officials, experts outside of this circle both public and private

18 Look out for 'Case Boxes' -Typologies Report 2023 - Money Laundering and Terrorist Financing Risks in the World of Virtual Assets, Moneyval, Council of Europe https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4 (accessed 25 Feb. 2024).

19 Agreements & Working Arrangements with Countries. Europol https://www.europol.europa.eu/partners-collaboration/agreements (accessed 26 Nov. 2023).

20 Agreements & Working Arrangements with Countries. Europol https://www.europol.europa.eu/partners-collaboration/agreements (accessed 26 Nov. 2023).

can also apply. However, the depth of accessible information might be limited for non-law enforcement professionals.

- **Cost:** There's no fee involved. Access is entirely free.

In October 2019, Europol launched two educational games called "Cryptopol." They have been updated several times, and feature multiple cryptocurrencies. They remain free of charge for agents from EU Member States. See: o3@europol.europa.eu.

INTERPOL's Financial Crime and Anti-Corruption Centre (IFCACC)

INTERPOL's Financial Crime and Anti-Corruption Centre (IFCACC): This is a centre dedicated to countering transnational financial crimes in order to safeguard global financial systems.

Eligibility: Addressing the growing concern of globalized financial crimes, INTERPOL introduced IFCACC as a consolidated response to assist in battling these challenges. This extends beyond mere law enforcement, being also relevant to international bodies and stakeholders.

Benefits: IFCACC facilitates:

- Support in fraud, payment crime, and cross-border inquiries from law enforcement.
- Assistance in anti-money laundering, asset recovery, and understanding of virtual assets.
- Oversight in anti-corruption practices, from sports-related concerns to high-level political discrepancies.

Joining process: Since IFCACC operates on a multi-agency model, potential collaborations involve:

- Establishing contact with the INTERPOL General Secretariat or with the INTERPOL National Central Bureau, which usually sits under a State's ministry of justice and its judicial police.
- Demonstrating clear alignment of goals against financial crimes and corruption.
- Expressing potential areas of collaboration or needs.

Who can join: In addition to law enforcement, financial institutions, international entities, and private sector representatives can engage with the IFCACC. However, the depth of collaboration might vary based on the nature and purpose of the association.

Cost: Since INTERPOL is an international organization, there is no cost associated with engaging with its General Secretariat.

For additional information about the IFCACC and I-GRIP, see:

- IFCACC@interpol.int
- IGRIP@interpol.int

For further information related to virtual assets technicalities, members of law enforcement can send an email to: innovation@interpol.int

Additional resource: members of law enforcement agencies can request INTERPOL's Guidelines for Seizing Virtual Assets: vaguidelines@interpol.int

UNODC virtual assets programmes against cybercrime and money laundering and investigation workshops

Overview:
Led by the United Nations Office on Drugs and Crime (UNODC) team, this comprehensive workshop series offers an in-depth exploration of virtual assets, financial crime, and the pivotal realm of compliance.

The curriculum is structured into basic, advanced, and cascade sessions, defined as training-the-trainers, the latter encouraging the propagation of industry best practices. The workshops blend rigorous theoretical constructs with tangible exercises, equipping participants from law enforcement with invaluable skills in tracking, investigating, and adeptly managing virtual assets.

Eligibility:
This specialized training is curated for professionals spanning various sectors, such as law enforcement, financial institutions, technology enterprises, and educational fields. It stands as an invaluable resource for policymakers, regulators, investigative officers, and all professionals intent on decoding the complexities of virtual assets, blockchain dynamics, and the art of financial crime mitigation.

Key focus areas:

- **Virtual asset essentials:** Delve deep into the genesis, evolution, and intricate facets of continuously evolving virtual assets and their underpinning technologies.
- **Transaction dynamics:** Decode the life cycle of blockchain transactions, from inception to culmination.
- **Blockchain in-depth:** Uncover the processes through which transactions are logged, ratified, and archived on the blockchain.
- **Blockchain forensics:** Become proficient in real-time transaction surveillance and discerning patterns employed by malefactors to obscure their identities.
- **AML/CTF tactics:** Assimilate how to calibrate anti-money laundering and counter-terrorism financing protocols to align with the metamorphic landscape of virtual assets.

- **Risk governance:** To familiarize participants with the gold standards in mitigating the distinct risks tethered to virtual assets.
- **Asset oversight:** To provide the participant best practices in the art of aptly confiscating and stewarding virtual assets amidst probes.

Enrollment steps:
Prospective attendees can:
- Review forthcoming workshop timelines and secure their spots.
- Ascertain potential fee concessions based on their professional spectrum via the specified form.
- Thoroughly peruse and concur with the explicit training terms of engagement.

Target audience:
The workshops are tailored to resonate with a diverse audience, encompassing investigators, legal aficionados, financial regulatory personnel, tech pioneers, journalists, and more. They serve both the public and private sectors, catering to those captivated by virtual assets and correlated fiscal norms.

Fee Structure: Estimates for a training session charges range from USD10,000 to USD20,000 depending on the participant count. Preferential pricing is potentially accessible for public sector delegates, academicians, non-profit entities, and media personnel.
Further information on the training scope can be requested by contacting the UNODC Virtual Assets Training Division via email:
cryptocurrency@unodc.org

Additional features:
The e-learning platform of UNODC can be found at the following link:
https://www.unodc.org/elearning/en/courses/course-catalogue.html

Basel Institute on Governance

Basel Institute on Governance:
This is an independent, non-profit organization focused on enhancing governance and countering financial crimes globally. Based in Basel, Switzerland, it also operates in various African countries, collaborating closely with the University of Basel.

The Basel Institute's cryptocurrency workshop: Offers a comprehensive 4-day virtual training centred on the fundamentals of cryptocurrencies, financial crime, and anti-money laundering (AML) compliance. The course encompasses a practical money laundering scenario, guiding participants through tracing blockchain transactions for illicit activities.

Eligibility: Open to professionals across the spectrum, from law enforcement, financial sectors, businesses, and even students. The content is tailored to benefit policymakers, regulators, investigative journalists, and anyone interested in virtual assets, blockchain, and financial crime mitigation.

Benefits: The Basel Institute workshop offers insights into:
- **Cryptocurrency basics:** Understanding the foundation, emergence, and scope of virtual assets, distributed ledger technology, and more.
- **Transaction mechanics:** Grasping how the Bitcoin network functions, cryptography, and transaction management.
- **Blockchain & mining:** Learning how transactions are secured, stored, and validated in the blockchain.
- **Blockchain analysis:** Techniques for real-time transaction monitoring, anonymity evasion by criminals, and tool utilisation.
- **Due diligence:** Adapting AML/CTF programmes to new payment modes.
- **Risk management:** Best practices and sources for managing virtual assets risks.
- **Asset seizure:** Procedures and nuances in crypto asset confiscation, wallet management, and more.

Who can join: The course is tailored for investigators, lawyers, AML/CTF professionals, members of financial intelligence units, FinTech practitioners, journalists, and more. It is designed for both public and private sector professionals interested in navigating the world of virtual assets and financial crime.

Cost: CHF 750 per person with a reduced rate of CHF 300 for specific members, such as those in the public sector, academics, non-profits, and journalists.

For more details:
info@baselgovernance.org

Course details and registration links for available dates can be found on the Basel Institute's social media platforms.

FinCrime Fighters Foundation

The FinCrime Fighters Foundation is a Stockholm-based foundation that has been created by experts of the Digital Asset Task Force of the Global Coalition To Fight Financial Crime. The goal of the tool has been to receive quick and reference-supported answers to issues connected with blockchain based finance and Web 3.

The foundation provides a free token pool to the generative AI Assistant, dedicated exclusively to public and private financial crime fighters. The team is constantly uploading and reviewing newest reports, including material from the OSCE that has been released publicly. Regulations can be searched with a Chat GPT-like system to help practitioners to be up to date on regulatory changes on a daily basis.

https://www.fincrimefighters.com/

Recommendations for law enforcement post-reporting

Recommendations for law enforcement post-reporting

- **Provide immediate support:** Ensure that victims are given immediate guidance on how to secure their remaining digital assets and reduce the risk of further financial loss. This could involve guidance on how to change passwords, secure wallets, or shift assets to a more secure platform.
- **Financial counselling:** Connect victims with financial counselling services that can help them understand their loss, potential tax implications, and strategies to recover or mitigate losses over time.
- **Educate:** Launch public awareness campaigns and workshops about such scams. The more informed the public is, the harder it becomes for scammers to deceive potential investors.
- **Collaborate with exchanges:** Work closely with cryptocurrency exchanges to track and possibly freeze scammers' assets, making it harder for them to cash out their ill-gotten gains.
- **Cross-jurisdictional collaboration:** Since digital scams often cross borders, collaborate with international law enforcement agencies to trace, apprehend, and prosecute culprits.

Mariam Grigalashvili sharing insights from Georgia and the National Bank of Georgia with colleagues from the Central Bank of Armenia in Yerevan during a workshop focused on cryptocurrency taxation and its relationship to AML and CTF policies.

Summary and principles of co-operation with the OSCE

Summary and principles of co-operation with the OSCE

The OSCE's Virtual Assets Support Initiative

Who we are

The OSCE Virtual Asset Expert Team is uniquely poised to respond to the evolving challenges presented by virtual assets for policymakers and law enforcement. Drawing on nearly nearly fifty years of of excellence in providing technical expertise, we assist policy members and law enforcement in navigating the complexities of virtual assets within the OSCE's 57 participating States.

The value we create for law enforcement and policymakers

- **Cutting-edge knowledge:** Our training equips law enforcement and policymakers with up-to-date insights and strategies, tailored to address challenges unique to the realm of virtual assets.
- **Operational efficiency:** With hands-on training, we provide the logistics, book venues, invite pre-vetted virtual asset experts from OSCE participating States, propose an agenda, and put together the learning objectives.
- **Training & expertise development:** We offer comprehensive virtual assets training programmes. Our team, which is a mix of policymakers, law enforcement, members of compliance teams of traditional banks, and WEB3 companies, prioritizes hands-on learning, with a limited but concise theoretical component. The primary focus is on practical exercises, ensuring real-world applicability. Notably, past participants have seen direct results, including the successful investigation of complex money laundering cases.
- **Resource provision:** We collaborate with leading blockchain experts. This hands-on experience with professional tools empowers members to implement their learning effectively in deep-dive sessions and workshops, in which we translate complex developments into exercises.
- **Case analysis:** Our training often encompasses real-time case studies and legislative support that visualize on-going developments to ensure that we resolve challenges before they actually happen.
- **Scalability & continuity:** Our cascade-training system includes a "train-the-trainers" model, in which we equip experts with the ability to return to their own jurisdiction to disseminate this knowledge further. This ensures a wider reach and continuity in expertise development in home countries.
- **Building a safer digital environment:** By ensuring that policymakers and law enforcement are well equipped to deal with virtual assets, we contribute significantly to creating a more secure and transparent digital financial landscape.

Join us in shaping the future of cybersecurity and ensuring a safer, more transparent digital realm for all.

Get in touch with us at:
VirtualAssets@osce.org

A short selection of further reading

A short selection of further reading

United Nations Office on Drugs and Crime (UNODC)

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies (2014)

Despite being published by UNODC more than ten years ago, in 2014, this comprehensive 200-page document delves deeply into various terms, and provides context for terms described in this review. It also features detailed self-assessment questionnaires:

https://www.unodc.org/documents/middleeastandnorthafrica/money-laundering/FULL10-UNODCVirtualCurrencies-final.pdf.pdf

Organization for Security and Co-operation in Europe (OSCE)

Handbook for Dealing with Virtual Currencies in Criminal Proceedings (2022)

https://www.osce.org/files/f/documents/2/0/522754.pdf

U.S. Department of Justice

The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets (2022)

https://www.justice.gov/d9/2022-12/The%20Report%20of%20the%20Attorney%20General%20Pursuant%20to%20Section.pdf

Published by the U.S. Department of Justice, the report serves as a companion to the International Law Enforcement Cooperation Report and updates the Cryptocurrency Enforcement Framework. It provides a comprehensive overview for future reference.

About the author

This review was created by Michal Gromek, a leading virtual asset expert in the OSCE project aimed at mitigating money laundering risks associated with virtual assets and cryptocurrencies being conducted at the Office of the Co-ordinator of OSCE Economic and Environmental Activities (OCEEA). Gromek is a former Chief Compliance Officer of the Stockholm-based Nasdaq-traded VASP Safello. He chairs the Digital Asset Task Force within the Global Coalition to Fight Financial Crime, a collaboration established between Europol, the World Economic Forum, and London Stock Exchange Risk Solutions. Gromek is also an executive team member of the Global Coalition to Fight Financial Crime. He continues to conduct training sessions for governments and law enforcement agencies, providing support in crafting legislation to prevent challenges faced by OSCE participating States. He gained his expertise through former roles as a FinTech executive and as a programme director of the Executive Education division at the Stockholm School of Economics. He worked with on Fintech and Virtual Assets Compliance for over a decade. His findings have been published on Forbes.com, as well as in a number of books and journals.

Acknowledgements

A significant enhancement to this guide has been the review and contributions made by Dr. Alexandra Andhov. Her legal expertise and insights have greatly elevated the accuracy, relevance, and depth of the content presented. With her background as associate professor at the University of Copenhagen Faculty of Law, she provided invaluable assessments and recommendations in the writing of this document. Dr. Andhov is experienced with the intersection of law and technology, contributing to a significant number of projects in this area, particularly as the co-founder and chief legal officer of the Financial Crime Fighters organization.

To ensure the highest possible readability and quality, the document language was edited by multiple individuals, predominantly by Grace Marshall, ensuring clarity and coherence throughout the publication. As the Secretary-General of the Global Coalition to Fight Financial Crime, she helped adapt the information for a general audience.

In addition to Ms. Marshall, Denisse Rudich provided many hours of support in assessing and editing the document, bringing her extensive experience within the space to the table. Her insights into both the content and the language were indispensable.

Further editorial support was provided by Greta Barkauskienė, Emilia Pachomow, Sungyong Kang, and Vincent Danjean. Additional review and suggestions for edits were conducted by the INTERPOL Financial Crime and Anti-Corruption Centre (IFCACC), particularly by Mona Hessein, as well as members of the European Cybercrime Centre (EC3), specifically Gert Jan van Hardeveld.

The OSCE's OCEEA team is thankful for such strong support.

Our sincere thanks to the Latvian Financial Intelligence Unit for their crucial role in identifying and selecting ecosystem leaders for a study visit to the Baltics focusing on virtual assets. We also extend our appreciation to the Polish Ministry of Finance for its continued support in providing training facilities. Furthermore, we are deeply grateful to the many institutions and individuals from a wide range of sectors whose contributions were instrumental in the successful progress of the project.

Notes

OSCE Secretariat
Office of the Co-ordinator of OSCE Economic and Environmental Activities
Economic Governance Unit
Wallnerstrasse 6
1010 Vienna, Austria
E-mail: virtualassets@osce.org
www.osce.org/eea

Organization for Security and Co-operation in Europe