U4 Helpdesk Answer

U4 Helpdesk Answer 2023:8

Cryptocurrencies, corruption and organised crime

Implications of the growing use of cryptocurrencies in enabling illicit finance and corruption

Cryptocurrency is becoming an increasingly popular tool for organised crime groups (OCGs) to conduct illicit activities. OCGs can exploit the inherent pseudonymity and decentralised nature of cryptocurrencies to conduct money laundering and other crimes related to corruption. Criminals can use cryptocurrencies instead of the formal banking system to move large sums of money which entails a potentially lower risk of being detected by law enforcement or the traditional financial institutions which are required to submit suspicious transaction reports.

The development sector can play an important role in mitigating the risks associated with the criminal use of cryptocurrency. Relevant actions include coordinating the development and implementation of regulatory and legislative frameworks, educating the public about the risks of cryptocurrency use and strengthening law enforcement agencies' capacity to dismantle criminal networks.

28 March 2023

AUTHOR

S Elsayed (TI)

tihelpdesk@transparency.org

REVIEWED BY

Sophie Lemaître (U4)

Vincent Freigang and Matthew Jenkins (TI)

RELATED U4 MATERIAL

- Blockchain as an anti-corruption tool (2020)
- Overview of international fraud operations relating to corruption (2020)

Query

Please provide an overview of the role of cryptocurrencies in the financing of organised crime.

Contents

Caveat

The virtual assets industry encompasses not just cryptocurrencies like Bitcoin and Ethereum, but also non-fungible tokens (NFTs) and other digital assets. However, this Helpdesk Answer focuses primarily on cryptocurrencies, not least as the studies suggest that, as yet financial crime represents only a small portion of overall trading activity related to NFTs (Elliptic 2022).

MAIN POINTS

- Cryptocurrency is not only restricted to cybercrime but is used for all types of crimes that involve the transmission of monetary value. This includes money laundering, financial sanctions evasions and other corruption related crimes such as bribery and embezzlement.
- There are constraints associated with the use of cryptocurrencies in criminal activities, such as the volatile value fluctuations, which contribute to the reluctance of criminals to use cryptocurrencies for long-term investments.
- International development agencies can play a role in mitigating the criminal use of cryptocurrencies. This includes coordinating the development and implementation of regulatory and legislative frameworks, encouraging bilateral and multilateral coordination to establish networks for experience sharing, and supporting platforms for public-private collaboration.
- However, resources spent by donors to curb crypto-related corruption imply an opportunity cost. Donors will need to determine whether the same resources would be better spent on improving traditional law enforcement practices or other development priorities.
- This is a pertinent consideration given that although the use of cryptocurrency in criminal activities is increasing, cryptocurrency transactions related to criminal activities represent only a limited share of the criminal economy compared to cash.

Background

Cryptocurrency is defined by Choo (2021) as a "virtual medium of exchange that exists only electronically; it has no physical counterpart such as a coin or dollar bill, and no money has been staked to start it".

With this definition in mind, it is important to note that a plethora of different terms can be used to refer to cryptocurrency, including digital currency, virtual commodity, crypto-token, payment token, cyber currency, virtual asset, and electronic currency (Ibrahimi and Arif 2022).

Cryptocurrencies are one type of crypto-asset created using blockchain technology, with a three-dimensional structure described as a "peer-to-peer electronic cash system" by inventor Satoshi Nakamoto. This system includes a universal value representative, infrastructure for issuance and audit trail, and rules governing money supply and transaction processes. Despite being organisationally decentralised, the rules are predefined and dictated by the open-source algorithm (OECD 2019).

Cryptocurrencies further depend on encryption algorithms for their creation and operation, functioning both as a currency and a virtual accounting system. To use cryptocurrencies, one must possess a cryptocurrency wallet which can be a software-based cloud service or stored on a computer or mobile device. The wallet acts as a tool for storing a user's encryption keys which confirm the person's identity and enables them to access their cryptocurrency (Oswego State Univeristy of New York 2022).

In 2009, Bitcoin was introduced as the first decentralised cryptocurrency, rapidly gaining popularity partly due to the lack of third-party intermediaries, such as formal financial institutions, in transactions, which was an attractive feature to many users (Chohan 2017). By using blockchain technology, Bitcoin enabled direct and secure payments without the need for an intermediary such as a central bank or public authority (Chohan 2017).

Cryptocurrencies are decentralised as they do not require a central authority to manage and control transactions. Instead, transactions are conducted using encryption algorithms and cryptographic techniques validated by all users of the system to ensure security (Ibrahimi and Arif 2022). This means that once data is entered, it cannot be reversed. This immutable characteristic of blockchain implies that cryptocurrency transactions are permanently recorded and accessible to anyone. Moreover, this means that erroneous or fraudulent transactions cannot be undone; there is no central authority that can provide recourse in such cases.

By 2022, over 12,000 distinct cryptocurrencies existed with more than 300 million users worldwide. The cryptocurrency market has been steadily growing with over 18,000 businesses now accepting cryptocurrency payments (Ibrahimi and Arif 2022).

While Bitcoin remains the largest player with a market capitalisation of around US$755 million, Ethereum is valued at around US$360 million , and Tether at approximately US$82 million. More than 80 other cryptocurrencies have a market capitalisation of at least US$1 million each while over 100 other cryptocurrencies have market capitalisations in the hundreds of thousands of US dollars (Ibrahimi and Arif 2022).

From a developmental perspective, the impact of cryptocurrencies is a complex issue. On the one hand, advocates of cryptocurrencies claim they are a means to promote inclusive development by providing a decentralised, secure, and transparent

means of conducting financial transactions. For example, cryptocurrencies can facilitate cross-border payments and remittances, potentially supporting financial inclusion for the unbanked or underbanked, as well as providing access to alternative sources of capital for entrepreneurs and small businesses (Holtmeier and Sandner 2019). On the other hand, opponents raise concerns related to the potential negative effects of cryptocurrencies on economic development. One major concern is their high volatility and rapid fluctuation in value, making it difficult for businesses and individuals to plan and invest for the long term (Pierangelo and Jayant 2023). Moreover, cryptocurrencies have tapped into the longstanding desire for "get-rich-quick" schemes, and increases in market prices are largely driven by recruiting more and more investors. Such speculative investments can result in a financial bubble, which in turn can result in sudden drops in value of the virtual assets, resulting in large losses to investors. For example, Bitcoin reached a price of US$ 70,000 in November 2021, but later fell by nearly 75% by November 2022, causing large losses for numerous ordinary investors, including many in low- and middle-income countries (Al-Arabiya News 2022).

Cryptocurrencies also have an environmental impact. The significant energy demand of the cryptocurrency mining process has resulted in an upsurge in the consumption of fossil fuels, thereby exacerbating climate change (Christos and Bruce 2022).

Kutera (2022) points out that the decentralised, distributed and dependable nature of cryptocurrencies has played a significant role in transforming them into a worldwide trading platform. Regrettably, these very same characteristics have also rendered them appealing to criminal elements (Albrecht et al. 2019). The explosive growth of this industry is likely to result in a significant increase in crypto-related criminal activities and virtual asset-based money laundering (Larkin 2022). Indeed, a recent report by Europol indicates that the use of cryptocurrency for illicit purposes and the concealment of illegal gains has surged in both scale and complexity in recent years (Europol 2022).

This Helpdesk Answer aims to provide an overview of the use of cryptocurrencies to perpetrate corruption related offences as well as their broader function in assisting organised criminal activities, particularly as a tool for money laundering. The Answer then identifies potential measures to alleviate these risks.

The link between cryptocurrencies and organised crime

According to a 2022 Europol report on cryptocurrencies and criminal finance, the revolutionary nature of this technology has hindered a timely legislative and law enforcement response. Anti-money laundering and combating the financing of terrorism (AML/CFT) and know-your-customer (KYC) processes were not originally designed to address risks associated with cryptocurrencies.

The surging popularity of digital currencies has fuelled their increasing application by organised criminal groups. Indeed, Europol (2022: 3) notes that "the criminal use of cryptocurrency is no longer confined to cybercrime activities, but now relates to all types of crime that require the transmission of monetary value".

Money laundering operations now reportedly constitute the highest proportion of illegal acts committed using cryptocurrencies, ahead of other

types of offences such as fraud (Europol 2022). In each of these instances, cryptocurrencies can help perpetrators of financial crime to camouflage the origin of illicit assets. For example, cryptocurrency mining involves the use of powerful computer systems to solve complex mathematical equations and validate transactions on a blockchain network. While the process of mining itself is not inherently illegal or fraudulent, it can provide an avenue for money laundering.

Criminals can use the proceeds of real-world crime, such as drug trafficking or extortion, to fund cryptocurrency mining, resulting in newly minted digital coins with no direct link to criminal activity. These coins can then be sold back into fiat currency, providing a neat way of laundering dirty money (KYC360 2020; Out-law Analysis 2022). There exist criminal service providers dedicated to facilitating the transfer of criminal profits using cryptocurrencies (Europol 2022).

Verifying the criminal origin of wealth held in or laundered via cryptocurrencies is very challenging. As such, the extent of the use of cryptocurrencies to launder funds obtained from conventional offline criminal activities is hard to determine (Europol 2022). This is because in such cases, the cryptocurrency is not transferred from addresses that have previously been linked to criminal activities. Rather, proceeds of crime in fiat currency are initially transferred into cryptocurrencies (e.g. via an exchange or the above-mentioned mining services), with no immediate indicators pointing to the criminal origin being visible on the blockchain (Chainalysis 2022).

Consequently, the unlawful use of cryptocurrencies is now no longer restricted to "on-chain" crimes such as blackmail scams or ransomware attacks carried out by cybercriminals who demand payment in cryptocurrencies. Nor is it restricted to use for money laundering. Rather, cryptocurrencies are now used to perpetrate all manner of offences that entail the exchange of monetary value, including to purchase illegal goods and services that relate to "off-chain" crime such as narcotics, contract killings and child sexual exploitation material (Campanelli 2017).[1]

Attributes of cryptocurrencies that make them attractive to organised criminal groups

Anonymity/pseudonymity

As cryptocurrencies operate without the involvement of central banks, they circumvent the traditional banking system entirely. Users do not have cryptocurrency accounts in the traditional sense. Each unit of each cryptocurrency is monitored with a specific set of access keys that authenticate every individual coin. The holder of the coin is given a private key which serves to validate them as the legal owner of the assets (Chohan 2017) and transactions are recorded anonymously on the blockchain (Europol 2022).

While users are not obliged to disclose personal information when conducting financial transactions within the cryptocurrency system, the pseudonymous ID number of their cryptocurrency wallet is typically public (Albrecht et al. 2019). Moreover, most blockchains are accessible to the

[1] Additionally, apart from their role in enabling the transfer of illicit gains, cryptocurrencies could also become the target of theft through various forms of malware (Europol 2022). The theft of crypto assets such as digital coins is, however, beyond the scope of this Helpdesk Answer.

public, and these features can allow the monitoring and tracing of cryptocurrency transactions. Mario (2021) therefore argues that, while cryptocurrencies can offer a degree of pseudonymity, the public nature of the blockchain and the ability to trace transactions mean that they are not entirely anonymous (Oettler 2021). This point is underscored by US criminal sanctions recently imposed on individuals and cryptocurrency exchanges implicated in assisting North Korean hackers to launder stolen funds through cryptocurrency (Spencer 2022). In this case, the pseudonymity of cryptocurrency was exploited by criminals to facilitate illegal activities, but the blockchain technology and public availability of blockchain data ultimately allowed law enforcement agencies to trace the transactions.

However, various services and stratagems can amplify anonymity and impede the efforts of law enforcement. For example, identification is not required to exchange transactions of up to €1,000 in cash at some Bitcoin ATMs. One could potentially carry out multiple exchange transactions over a period of time or use multiple Bitcoin ATMs (Ibrahimi and Arif 2022).

In addition, in countries in which law enforcement authorities do not have the required capacity or resources to overcome the pseudonymity of the system, the use of cryptocurrencies can serve as an effective means of obfuscating illicit transactions and is therefore likely attractive to criminals (Bains et al. 2022).

Cryptocurrency onramp/offramp

Cryptocurrency "on-ramps" refer to the process of converting traditional currency into cryptocurrency, allowing individuals to enter the crypto market. This can be done through a variety of means such as buying cryptocurrency directly with a credit card or bank transfer, using a cryptocurrency ATM or earning cryptocurrency through mining or staking. Conversely, a crypto offramp refers to the process of converting cryptocurrency back into currency, allowing individuals to exit the crypto market. This can be done through similar means such as selling cryptocurrency for fiat money on a cryptocurrency exchange, withdrawing funds from a cryptocurrency ATM or using a peer-to-peer cryptocurrency marketplace.

This ecosystem might pose risks for money laundering as it allows individuals to access and exit the market and facilitate the flow of funds between traditional financial systems and the crypto market (Phadtare 2022). The key to identifying potential crimes involving cryptocurrencies is being able to link pseudonymous wallet IDs and transactions to real people. As such, on-ramps like cryptocurrency exchanges which are often required to verify their users' real identity are a vital source of potentially incriminating information for law enforcement (iDefy 2022). However, criminals are aware of this and often seek to provide false ID documents when registering with a cryptocurrency exchange (Coin Desk 2021). Where cryptocurrency exchanges do not conduct robust due diligence, dirty money can be easily transformed into apparently "clean" cryptocurrency.

Regulatory ambiguity/lack of regulation

Cryptocurrencies are difficult to scrutinise or arraign due to their decentralised structure. In principle, they have the capability to destabilise fiat currency and establish a section of the economy that is not directly governed or regulated by the state (Holtmeier and Sandner 2019). This risk has

prompted certain countries, including India and China, to impose stringent laws on cryptocurrencies. In contrast, some countries such as Japan have implemented legislation and regulations accepting cryptocurrencies as a legitimate mode of currency. Nonetheless, most governments are only now commencing discussions about how to regulate cryptocurrencies (Albrecht et al. 2019).

Within the European Union, there is a legal requirement under the 5th Money Laundering Directive for cryptocurrency exchanges and cryptocurrency wallet providers to identify their customers. In various other countries, similar measures exist to promote scrutiny and transparency in cryptocurrency transactions. However, these policies are notably absent in many parts of the world (Bele 2021). Furthermore, individuals can also purchase cryptocurrencies via cryptocurrency ATMs,which offer a greater level of privacy as many providers do not require the identification of their customers or have inadequate verification protocols.

Global reach

Cryptocurrencies enable an almost instant transfer of funds across borders and offer criminal organisations a means to easily transfer funds while evading cross-border limitations, exacerbating the AML/CFT risks associated with cryptocurrency (Moritz and Philipp 2019; Campanelli 2017; FATF 2014). Unlawful funds can be transferred to other financial jurisdictions where criminal organisations operate to shield their wealth from confiscation during the layering phase of the money laundering process (Albrecht et al. 2019).

The traditional banking system relies on central authorities to validate transactions while the decentralised nature of cryptocurrency validation spans multiple countries and bypasses conventional central authorities (Europol 2022). This allows for rapid cross-border transactions and the exploitation of regulatory gaps between jurisdictions. Mutual legal assistance requests between national authorities can be slow and ineffective, causing delays in the pursuit of justice, while criminals can collaborate across borders almost instantaneously using digital technologies (University of Luxembourg 2015).

The role of cryptocurrencies in facilitating corruption

The characteristics of cryptocurrencies described above mean that they can potentially be used to facilitate corrupt practices (Campanelli 2017). A study by the IMF using cross-country regression analysis indicates that more cryptocurrency use is empirically associated with higher levels of perceived corruption (Marwa, Nikolay and Honda 2022). While the IMF paper does not seek to explain a causal relationship, it notes that cryptocurrencies may be used to transfer the proceeds of corruption. In the view of the authors of this Helpdesk Answer, the correlation between high levels of corruption and extensive use of cryptocurrency could potentially also be explained by the fact that countries with high levels of corruption tend to have weak political and financial institutions which may reduce trust in the formal banking system.

Some commentators have argued that cryptocurrencies can facilitate corrupt transactions online by reducing some of the constraints on corrupt behaviour such as transaction costs and the risk of being caught (Ibrahimi and Arif 2022). For instance, parties to a corrupt deal can potentially reduce the chance of being detected by the authorities where they use the anonymous web

browser Tor and cover their tracks with web applications designed to obscure the origin and destination of transactions, such as Bitcoin Fog or Dark Wallet (Lawrence 2015).

The following section provides an overview of how cryptocurrencies can be used to enable different types of corruption crimes.

Bribery

There are numerous ways in which bribes can be channelled to public officials, including cash payments, inflated commissions, and expensive travel arrangements (UNODC 2022). With the advent of cryptocurrencies, a new avenue has been opened for corrupt transactions. Historically, the commission of bribery required a face-to-face interaction between the perpetrator and the recipient or their intermediaries. If the exchange was not cash-in-hand, bank transfers could provide a traceable record of the exchange. Given the pseudonymity of cryptocurrencies and the large resources required to trace crypto assets, corrupt parties can discreetly transfer bribes to officials' cryptocurrency wallets to reduce the risk of detection (Ibrahimi and Arif 2022).

As such, the potential of cryptocurrencies in facilitating bribery transactions is a growing concern for law enforcement agencies around the world. The Association of Certified Fraud Examiners (AFCE) has examined a hypothetical scenario that illuminates how cryptocurrencies could be used to transfer bribes between a construction company and a city official (Lawrance 2015). In this scenario, Bitcoin is used to transfer the funds in an anonymous manner, making it difficult for authorities to detect the illicit activity. The construction company sets up anonymous Bitcoin wallets through a used laptop connected to a public Wi-Fi network at a coffee shop and the company manager makes weekly deposits into the wallet via anonymous Bitcoin ATMs. The bribe is then transferred to the city official via Bitcoin Fog, a tool on the Deep Web that further obscures the transfer of funds. The city official cashes out the bribe money using local Bitcoin traders and ATMs while on luxury vacations, leaving little to no trace of the transaction. With the benefits of anonymity and the lack of detection methods, bribery using Bitcoin poses a significant challenge for law enforcement agencies. Even with a whistleblower disclosing general details of the scandal, investigators would likely face dead ends (Campanelli 2017).

The increasing use of cryptocurrencies in bribery and kickback payments appears to be a growing trend. According to the findings of the Association of Certified Fraud Examiners (ACFE 2022), 8 percent of fraud cases worldwide in 2021 involved the use of cryptocurrencies. Of these cases, 48% related to the payment of bribes and kickbacks, while 43 % involved the conversion of embezzled assets into cryptocurrencies.

Case study

A real-life scenario for the use of cryptocurrency as a medium for bribery took place in 2022 when two Chinese intelligence officers were charged with attempting to obstruct a US federal investigation into a sophisticated cyber espionage campaign. The officers allegedly offered a bribe to a potential witness in the investigation in exchange for the witness's silence and for the destruction of evidence. The bribe was intended to be paid in cryptocurrency to reduce the risk of detention. Nonetheless, the incident came to light due to an investigation by US authorities and charges were brought by the US Attorney's Office for the Eastern District of New York. The defendants are currently believed to be in China. The investigation in question involves a hacking group known as APT10

which has been linked to the Chinese Ministry of State Security (US Department of Justice and US Attorney's Office 2022).

Embezzlement

Alongside bribery, cryptocurrencies can play a role in cases of embezzlement as the lack of regulation and the pseudonymity of cryptocurrencies can facilitate the misappropriation of funds (Campanelli 2017). For example, cryptocurrencies could be used in embezzlement schemes where public officials embezzle public funds and use cryptocurrencies as a vehicle to store the stolen funds. Given the hurdles to connecting pseudonymous cryptocurrency wallets to real people – particularly in countries where law enforcement lacks expertise and resources – a perception that using cryptocurrency lowers the risk of being caught for embezzlement could potentially reduce the constraints on corruption. Conceivably, this might lead to a rise in the number of people prepared to embezzle funds.

Case study

In South Korea, a government official was recently accused of embezzling approximately US$3.24 million from the national health insurance service. The official converted US$2.8 million of the embezzled funds into cryptocurrency and fled the country in early February. The incident has raised concerns about the vulnerability of government funds to fraud and theft in the cryptocurrency sector (Alper 2022).

The role of cryptocurrencies in facilitating other forms of IFFs

Illicit financial flows (IFFs) refer to "Financial flows that are illicit in origin, transfer or use, that reflect an exchange of value and that cross country borders" (UNODC 2020). IFFs are generated by illicit activities such as corruption, money laundering and terrorist financing as well as other crimes such as tax evasion. These flows can be transferred through various means, including but not limited to cash smuggling, remittance transfers, transfer pricing, trade financing and shell companies. These channels may vary in their degree of complexity but can all be used to conceal the true nature and source of the illicit funds.

Aidan Larkin, CEO of Asset Reality, points out that cryptocurrencies have become a favoured tool for criminals to conceal the origin of their illegal earnings, and as such are an increasingly relevant component of IFFs (Larkin 2022). Supporting this claim is the 2022 report by the blockchain analysis company Chainalysis (Chainalysis 2022). The report reveals that cryptocurrency addresses received the equivalent of US$14 billion in illicit funds in 2021, an increase of approximately 80% from the previous year (Chainalysis 2022).

According to Europol (2022), cryptocurrencies also provide an avenue for evading taxes and transferring funds across international borders undetected. They have become an important component of money laundering schemes (Bele 2021). Cryptocurrencies are a popular method of payment for illegal goods and services available on the dark web. The Europol 2022 report outlines a growing trend where criminals involved in fraud rely heavily on cryptocurrencies and ransomware attacks in which perpetrators encrypt a victim's

data and demand payment in cryptocurrency. In all these cases, the criminals seek to obscure the source of their illegitimate assets using cryptocurrencies (Europol 2022).

Money laundering

The ability of cryptocurrencies to aid the transfer of illicit funds across international borders without detection has made them increasingly important for organised crime groups (Bele 2021).

The use of cryptocurrencies for money laundering generally follows the placement-layering-integration pattern, but with some unique characteristics. Because cryptocurrencies are anonymous at the point they are created, the initial placement stage of the process is often unnecessary. Creating a new account, or "address," is simple, quick, and free. This allows criminals to execute large-scale money laundering schemes with thousands of transfers using computer scripts at a low cost. Additionally, the rapid increase in exchange rates of certain cryptocurrencies, with some showing growth rates of up to 10,000%, makes it easy to justify sudden wealth from cryptocurrency investments (UNODC 2022).

So-called privacy coins are a type of cryptocurrency that allows for even greater anonymity in blockchain transactions compared to traditional cryptocurrencies. These privacy coins allow for the concealment of information about user addresses, including the balance and origin of the coins, from third parties, unlike traditional cryptocurrencies where anyone can view an address's balance and transaction history (UNODC 2022). In addition, cryptocurrency mixing refers to a technique that involves sending funds from multiple sources to one address. Blending and splitting them into multiple portions allows users to obscure their origin, making them almost impossible to trace (UNODC 2022).

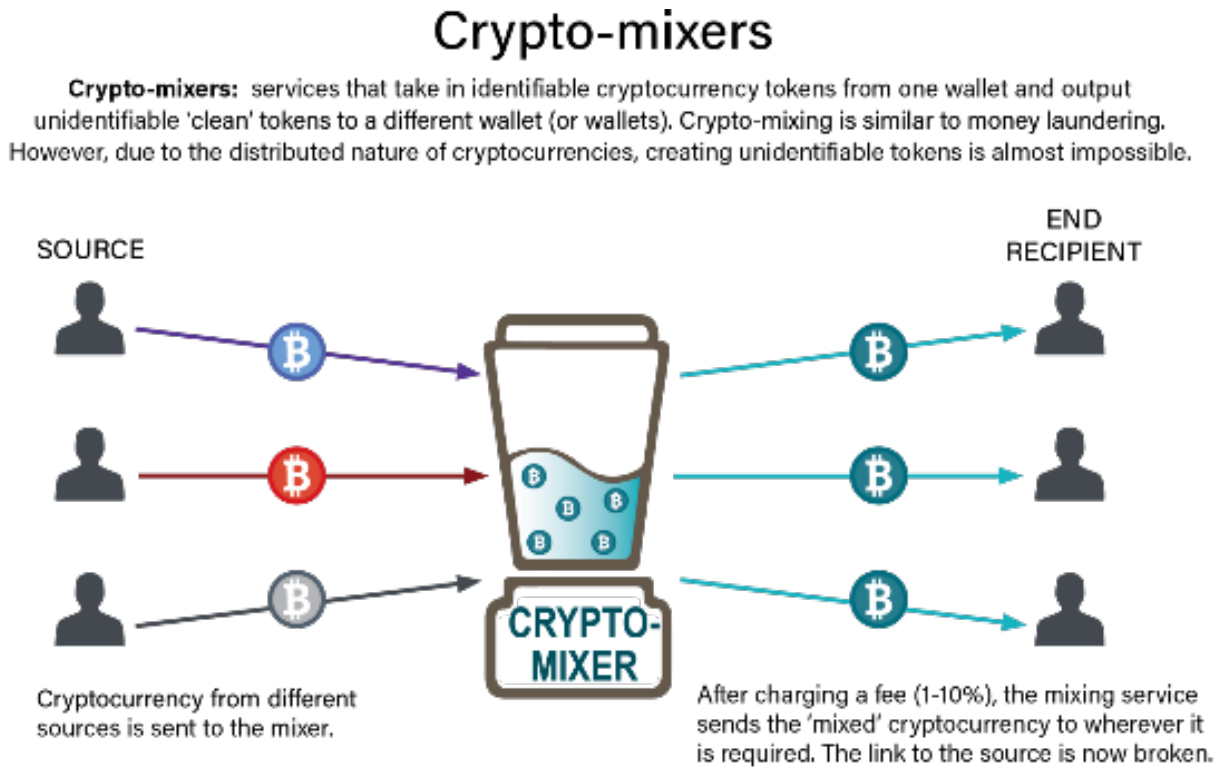

Figure 1: Crypto=Mixers (UNODC 2022)

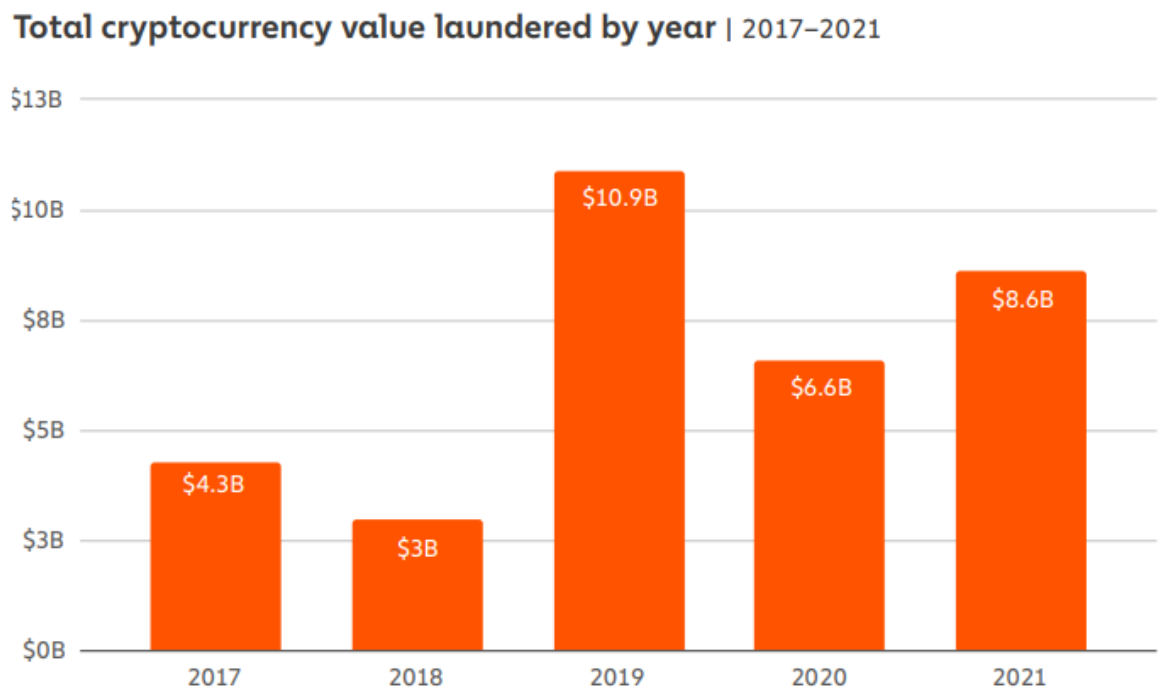

Figure 2. Total cryptocurrency value laundered 2017-2021. Source: Chainalysis 2022.

According to the 2022 Europol report, there has been a notable increase in the employment of cryptocurrencies for money laundering practices with a significant number of criminal networks incorporating cryptocurrencies into their modes of operation in recent years (Europol 2022). Also, Chainalysis reports that the significant expansion of both legitimate and illegal use of cryptocurrency led to a 30% surge in cryptocurrency related money laundering activities in 2021, with an estimated US$8.6 billion worth of cryptocurrencies being laundered (Chainalysis 2022).

The Financial Action Task Force (FATF) (2014) report on virtual currencies notes that criminal networks that provide money laundering as a service have embraced cryptocurrencies and are offering their services to other criminal organisations. These networks have access to established infrastructure such as multiple bank accounts, deep knowledge of the banking system, and are well-versed in the use of financial technology (FinTech).

Marketplaces are available on the dark web where money laundering cryptocurrency service providers are advertised. These marketplaces also provide information on how to convert cryptocurrencies into cash, such as by exchanging Bitcoin for prepaid debit cards or gift vouchers (Ibrahimi and Arif 2022).

The services of professional money laundering networks are often used by other criminal groups and can include the acquisition or trade of cryptocurrencies, the conversion of illegal assets to legitimate ones, and the ultimate withdrawal of funds into criminal accounts. These professional networks pose a major risk as they facilitate the underlying predicate crimes.

Bitzlato

In January 2023, US authorities announced the arrest of Anatoly Legkodymov, the owner of Hong Kong based cryptocurrency exchange Bitzlato, for allegedly laundering hundreds of millions of dollars for criminals on the platform. Legkodymov, a 40-year-old Russian national living in China, was arrested in Miami. The US Deputy Attorney General called Bitzlato a "haven" for criminality and accused Legkodymov of not implementing proper security measures to prevent money laundering and other crimes on cryptocurrency platforms. Bitzlato's main client was Hydra, a major dark net marketplace shut down by US and German authorities last year (US Department of Justice 2023).

QQAazz Money Laundering Ring

In 2020, Europol announced the arrest of 20 people in connection with the QQAazz criminal network which is believed to have laundered tens of millions of euros from cybercrime and other illegal activities (Europol 2022). The operation involved cooperation between law enforcement agencies from Europe, the US and Australia, and resulted in the seizure of assets worth several million euros, including cash, cryptocurrency, and real estate. QQAazz is accused of providing money laundering services to other criminal organisations, using a complex network of shell companies and fake invoices to conceal the origin of funds. The network is also alleged to have provided virtual private network (VPN) services and bulletproof hosting to cybercriminals, allowing them to carry out their activities anonymously and evade detection.

e-BTC

In 2017, the US Attorney's Office for the Northern District of California indicted a Russian national and his Bitcoin exchange, e-BTC, on 21 charges, including money laundering and operating an unlicensed money-transmitting business, for allegedly being involved in an international money laundering operation that facilitated more than US$4 billion worth of cryptocurrency transactions. The defendants are accused of using their exchange to help criminals launder money and evade law enforcement by providing them with anonymous access to cryptocurrency (United States Attorney's Office 2017).

Liberty Reserve

In May 2013, the US Department of Justice charged Liberty Reserve, a money transmitter based in Costa Rica, and seven of its employees with money laundering and operating an unregistered money-transmitter business (US Department of Justice 2016). According to the statement by the Department of Justice, the company enabled criminals to distribute, store and launder the proceeds of illicit activities like credit card fraud, identity theft and narcotics trafficking by conducting more than 55 million illegal transactions involving over US$6 billion anonymously and untraceably. The Department of Treasury identified Liberty Reserve as a primary money laundering concern and cut it off from the US financial system under Section 311 of the USA Patriot Act. Liberty Reserve had over a million users worldwide, including 200,000 in the US, and used its own virtual currency, Liberty Dollars, which was denominated and stored in US dollars. Users could pay an extra fee to hide their account numbers and make the transfers untraceable. After discovering the investigation by US law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued operating

through shell companies, moving millions of dollars across several countries (Europol 2022).

Silk Road

In 2013, the US Department of Justice charged the alleged owner of Silk Road, a website that enabled users to anonymously buy and sell illegal goods and services with narcotics trafficking, computer hacking and money laundering conspiracies (FATF 2014). According to the FATF 2014 report on virtual assets and potential AML/CFT risks, Silk Road was a black-market cyber bazaar that operated globally, with thousands of vendors selling illegal goods to over 100,000 buyers, generating over US$1.2 billion in total sales revenue. As the report highlights, Silk Road's payment system functioned as an internal Bitcoin bank with each user having at least one Silk Road Bitcoin address. The website operated on the Tor network, and only accepted Bitcoin for payment, allowing for anonymity and the concealment of users' identities. Silk Road used a "tumbler" to obscure the trail of illicit proceeds. The Justice Department seized the website and over 173,000 Bitcoins, worth more than US$33 million at the time, from seized computer hardware. The individual was arrested in San Francisco in October 2013 and indicted in February 2014 (FATF 2014).

Financial sanctions evasion

The recent imposition of comprehensive economic sanctions by the United States and other nations against Russia has heightened attention to the potential use of cryptocurrencies to evade financial sanctions (Cox 2022). With close relationships to the ruling elite in Russia, corrupt individuals are able to secure and retain control over misappropriated assets. Like other modes of payment and means of transmitting money, cryptocurrency and crypto-exchanges are vulnerable to exploitation by criminal actors who aim to circumvent economic sanctions (Europol 2022). The characteristics of cryptocurrencies that are commonly exalted, including pseudonymity, decentralisation and digitalisation, are now giving rise to concerns among government officials, regulators and lawmakers in the context of these sanctions. As observed by Pouneh et al., the intelligence community in the United Kingdom identified that Russian money launderers are increasingly providing cash to crypto-asset services, thus enabling them to transfer significant volumes of funds (Almasi et al. 2023)

A recent report by TI Russia (2023) reveals how dirty Russian money is being funnelled into the UK through dark crypto exchanges that operate without any AML controls. The process of transfer is uniform across different exchanges, involving an advance payment in the Ethereum token USDt to a specific crypto wallet address, after which a courier delivers the cash to a designated location in London within the same or the next day. The study shows that several shadow crypto exchanges exist in the UK, offering cash without proper KYC procedures, a clear violation of current UK laws. This practice creates a significant risk as it exposes the financial system to exploitation by criminals and corrupt officials seeking to launder their illicit profits (TI Russia 2023).

Case study

In October 2022, five Russian and two Venezuelan nationals were charged with global sanctions evasion for various offences relating to a global procurement, smuggling and money laundering network. The defendants allegedly procured US military technology and Venezuelan sanctioned oil through shell companies and cryptocurrency to support Russia’s military industrial complex. They were involved in a complex web of cryptocurrency and shell companies to evade export controls and

perpetuate the shadowy economy of transnational money laundering (US Attorney's Office 2022).

Mitigation strategies for development agencies

When cryptocurrencies are used for illegal activities, it can undermine the integrity of financial systems, create instability and erode trust in institutions (Holtmeier and Sandner 2019). This can make it more difficult for businesses to operate and for countries to attract investment. In addition, the criminal use of cryptocurrency to enable illicit activities such as human trafficking and drug trafficking has significant implications for development actors working to promote human rights, social justice and peacebuilding (Larkin 2022).

Thus, the involvement of development actors including international development agencies, government organisations, NGOs and donor organisations, in mitigating the risks of the criminal use of cryptocurrency is essential to promote sustainable development in countries where they operate (OECD 2019; Basel Institute on Governance, Europol, Interpol 2021).

Development actors can play a significant role in several aspects such as raising awareness among stakeholders, offering capacity building for government officials and law enforcement authorities in partner countries, providing technical assistance to develop legal and regulatory frameworks, promoting international cooperation, and supporting innovation in the use of cryptocurrency to address developmental challenges.

Several actors have issued recommendations to minimise the risks of organised crime groups abusing cryptocurrencies, some of which may help guide development practitioners (Basel Institute on Governance 2022; Basel Institute on Governance, Europol, Interpol 2021; Larkin 2022). The recommendations they make can be clustered under the themes presented in the following sections.

Strengthening the regulatory environment

The potential abuse of cryptocurrencies to facilitate crime including corruption underscores the need to improve monitoring and oversight of the industry to deter illegal activities (Bains et al. 2022). Numerous commentators on the topic are calling attention to the worrying absence of appropriate legal frameworks needed to prevent the use of cryptocurrencies by criminal groups (Ibrahimi and Arif 2022; FATF 2021; Basel Institute on Governance, Europol, Interpol 2021; Larkin 2022).

National legislative and regulatory environment

Many governments around the world have begun to implement national regulatory and legal frameworks to prevent the use of cryptocurrencies for money laundering or other illicit activities (Ibrahimi and Arif 2022). According to an UNCTAD policy brief, by November 2021, 41 developing countries had taken regulatory measures in response to cryptocurrencies, a significant increase from 15 countries in 2018. These measures included prohibiting banks and financial institutions from dealing with cryptocurrencies, banning crypto-exchanges from providing services to individuals and enterprises, and imposing income taxes on capital gains from cryptocurrency trading. Nine developing countries, including Algeria, Bangladesh, China, Egypt, Iraq, Morocco, Nepal, Qatar and Tunisia, have gone so far as to ban cryptocurrencies outright. Furthermore, several jurisdictions, such as

Australia, Bahamas, Greece, Romania, the Philippines and Uzbekistan, are implementing national anti-money laundering and anti-terrorism financing laws that apply to crypto-exchanges (UNCTAD 2022).

Acknowledging the growing significance of cryptocurrencies and the need to ensure that regulatory frameworks are fit for purpose, international organisations play a significant role in establishing and promoting standards for countries to develop legislative and regulatory frameworks related to cryptocurrencies. For example, FATF has revised its recommendations to explicitly affirm their applicability to financial transactions involving virtual assets. Furthermore, FATF included two new definitions, "virtual asset" (VA) and "virtual asset service provider" (VASP) in the glossary to ensure clarity in its recommendations (FATF 2021). Development actors could choose to support partners in developing countries to implement legislation to govern cryptocurrencies through technical assistance or the seconding of experts.

In addition, international development agencies could play a role in supporting coordination and cooperation between national agencies in developing countries responsible for AML/CFT. This could be achieved by providing technical support to countries to establish interagency working groups or task forces that enable policymakers, regulators, supervisors and law enforcement authorities to co-operate with one another and any other relevant competent authorities (FATF 2021).

International cooperation to harmonise regulation

The legality of cryptocurrency varies from country to country. As mentioned above, some countries have taken a more restrictive approach to cryptocurrency, while others have been more permissive (Ibrahimi and Arif 2022). This inter-country variation in terms of the regulatory and legal frameworks calls for improved international cooperation to counter the use of virtual assets in illicit activity.

Acknowledging the significance of legal clarity and a harmonised regulatory structure in blockchain based applications, in 2021 a tripartite Working Group on Criminal Finances and Cryptocurrencies recommended that countries "strengthen the existing international cooperation channels between law enforcement and virtual asset service providers (VASPs). This includes both formal and informal cooperation between law enforcement agencies and judicial authorities, as well as with VASPs based in other jurisdictions" (Basel Institute on Governance, Europol, Interpol 2021).

In this regard, international development organisations could play a role in enhancing international cooperation in multiple ways, such as developing communication channels through workshops, establishing platforms and practitioner networks as well as supporting regional initiatives to foster information sharing and experience exchange (Larkin 2022). In addition, international development agencies could provide support to overcome challenges in the practical application of international cooperation that arise due to inter-country discrepancies in how they implement legal and regulatory frameworks. This could be achieved by contributing to cooperation networks, such as the Egmont Group or CARIN network, which can offer extensive support for obtaining information or conducting an investigation (Larkin 2022).

Supranational institutions could also play a role in establishing unified regulatory and legislative frameworks. For example, the European Commission has sought to address the fact that the legal and regulatory landscape in Europe is currently disjointed, with different countries adopting different positions (European Parliament Think Tank 2022). Accordingly, the EU has

approved a legislative proposal to regulate crypto assets and update specific financial market regulations (Ibrahimi and Arif 2022).

Virtual asset recovery

To facilitate the freezing and confiscation of virtual assets, the Working Group on Criminal Finances and Cryptocurrencies recommends cryptocurrencies be treated like traditional assets such as jewellery or artwork (Basel Institute on Governance, Europol, Interpol 2021). In their view, this approach not only helps in "restoring stolen funds but also acts as a deterrent to potential crypto-enabled crimes and money laundering involving virtual assets" (Basel Institute on Governance, Europol, Interpol 2021). In addition, the group recommends breaking down silos between government agencies working on traditional fiat money and cryptocurrency to improve the effectiveness of AML/CFT measures (Basel Institute on Governance 2022).

The joint working group also emphasised that the implementation of already established asset recovery practices like pre-seizure planning and public-private collaboration has been highly effective in several jurisdictions, enabling the recovery of significant amounts of cryptocurrency, which can then be converted into fiat currencies through auctions or exchanges (Basel Institute on Governance 2022).

Capacity building and use of new technology

The next section considers how to develop the expertise, resources and capacity required to clamp down on the use of cryptocurrencies for criminal purposes. Broadly speaking, law enforcement agencies in both high income and low-income countries have the same needs in this regard. However, the sophisticated investigative approaches, knowledge and software required are not cheap to acquire or develop.

International development organisations could shoulder some of the cost implied in developing the expertise and capacity that law enforcement agencies in low and middle-income countries (LMICs) will require to trace digital assets. This could, for instance, involve training workshops for frontline staff to detect cryptocurrency related crimes or secondments between law enforcement authorities in the donor's home country and partner countries.

Such investments naturally imply an opportunity cost, however, and considerable resources will be needed to acquire expertise and technology able to trace cryptocurrency transactions. Donors will need to determine whether the same resources would be better spent on improving traditional law enforcement practices or other development priorities. This is an especially pertinent consideration given that Europol (2022: 3) notes that the "value of cryptocurrency transactions related to criminal activities still represents only a limited share of the criminal economy when compared to cash and other forms of transactions".

Strengthen investigation approaches

In addition to revising regulatory and legislative frameworks, cracking down on the use of cryptocurrency to facilitate organised crime and corruption will require equipping investigators with the tools and expertise necessary to trace and track cryptocurrency. Without proactive investigations, the probability of detecting uses of cryptocurrency linked to corruption is essentially zero (Larkin 2022).

The Working Group on Criminal Finances and Cryptocurrencies has recommended that countries "invest massively in capacity building especially for those in law enforcement and the private sector in a position to detect virtual assets-based money laundering" (Basel Institute on Governance, Europol, Interpol 2021). However, this should take into consideration the limitations in the availability of resources in LMICs.

Promote the use of new technologies and techniques

To keep up with criminals when it comes to virtual asset-based money laundering, law enforcement agencies need to rapidly develop and adapt their investigative technologies and techniques (Basel Institute on Governance 2022).

This requires recognising the potential for money laundering through new forms of cryptocurrencies and other virtual assets such as NFTs and developing procedures to address these risks. Traditional techniques like undercover investigations and so-called controlled delivery[2] need to be adapted to crypto related risks and deployed alongside techniques like crypto tracing financial investigation, which may involve using private sector expertise (Basel Institute on Governance, Europol, Interpol 2021).

In parallel with the development of novel investigative techniques, the FATF recommendations recognise the importance of adopting new technologies to support investigations. FATF identifies various tools that countries should use to crack down on unlicensed or unregistered virtual asset service providers (VASPs), including blockchain analytics and web-scraping tools (FATF 2021). This is important because unlicensed VASPs offer an easy way for criminals to transfer the proceeds of crime onto and off the blockchain.

Raise awareness and crypto literacy

There is a perceived need to increase understanding among law enforcement officials and prosecutors of how crypto assets and services can facilitate organised crime and money laundering (Basel Institute on Governance 2022).

Europol (2022) also suggests that enforcement authorities develop standard operating procedures to handle digital evidence and secure seized assets, and that visualisation tools can help prosecutors to follow the money (Europol 2022). However, mitigating the risks associated with the illicit use of cryptocurrencies requires countries to undertake not only awareness raising efforts but also substantial action to adopt appropriate legislation in the domains of domestic and international criminal law (Basel Institute on Governance, Europol, Interpol 2021; Ibrahimi and Arif 2022; Basel Institute on Governance 2022).

Beyond raising the awareness of law enforcement agencies in partner countries of the risks associated with cryptocurrencies, development agencies could also sensitise donor governments to the need to regulate the industry to prevent harmful effects in LMICs, such as a growing volume of IFFs. Finally,

[2] According to the European Union Agency for Criminal Justice Cooperation, controlled delivery is "an investigative tool. It permits transportation of illegal or suspect consignments to enter, cross or exit the territory of one or more member states… with the knowledge, and under the supervision of, the competent authorities of the involved states, to progress the investigation of the offence and identify potential suspects" (European Union Agency for Criminal Justice Cooperation 2022).

development agencies could also consider funding public information campaigns in partner countries to increase citizens' knowledge of the risks of investing their savings in cryptocurrency.

Public-private collaboration

The time pressure for investigators is notably heightened when dealing with virtual assets, as transactions can be undertaken within minutes which necessitates swift action to restrain or freeze assets (Basel Institute on Governance 2022).

Effective public-private cooperation can prove instrumental in preventing assets from vanishing during an ongoing investigation (Larkin 2022). According to the Working Group on Criminal Finances and Cryptocurrencies, the private sector has the potential to be an ally for law enforcement by aiding in the development and use of innovative technologies to track funds held in cryptocurrencies. In this regard, cryptocurrency exchanges and other virtual asset service providers have the potential to support law enforcement investigations by sharing information, technical capabilities as well as tools for data analysis and live monitoring. For example, they can establish dedicated departments to coordinate requests from the national authorities, restrict access to assets for criminals or block suspected criminal assets.

International development organisations, law enforcement agencies and NGOs can play a role in proactively seeking to build mechanisms for cooperation and information sharing, using existing public-private partnerships as a platform for exchanging information and building trust (Basel Institute on Governance, Europol, Interpol 2021). The takedown of the "Welcome to Video" child exploitation site and multiple international arrests, which involved over 1.3 million Bitcoin addresses and thousands of Bitcoin payments, highlights the successful outcome of cooperation between the public and private sector, as the US Department of Justice used Chainalysis products in its investigation (Larkin 2022).

References

Almasi, P., Aberg, S.,Whitten, R., Merchant, F. and Parsefar, Y. 2023. "Crypto and Russia Sanctions: A Primer and Survival Guide For Crypto Companies."

Alarabiya News. 2022. Bitcoin shows that the get-rich-quick dream never dies.

Albrecht, C., K.M. Duffin, S. Hawkins and V.M. Morales Rocha. 2019. "The use of cryptocurrencies in the money laundering process." Journal of Money Laundering Control 22 (2).

Alper, T. 2022. S Korean gov't worker 'embezzled public funds and escaped with $2.8m in crypto.

ACFE.2022. Occupational Fraud: A report to the nations.

Bains, P., Arif, I., Melo, F. and Sugimoto, N. 2022. Regulating the crypto ecosystem: The case of unbacked crypto assets. Washington DC: Fintech/IMF.

Basel Institute on Governance. 2022. Seizing the opportunity: 5 reccomendations for crypto assets-related crimes and money laundering. Basel Institute on Governance.

Basel Institute on Governance, Europol, Interpol. 2021. Combating virtual assetsbased money laundering and crypto enabled crime: 2021 Recommendations of the Tripartite Working Group on Criminal. Basel Institute on Governance, Europol, Interpol.

Bele, Julija Lapuh. 2021. "Cryptocurrencies as facilitators of cybercrime." SHS Web of Conferences 111 (01005).

Better Business Bureau. 2022. Cryptocurrency Scams Study. Better Business Bureau,.

Campanelli, A. 2017. Cryptocurrencies: Instruments for payments or corruption? FCPA.

Chainalysis. 2022. The 2022 Crypto Crime Report. 3.

Chohan, Usman W., SSRN. 2017. "A History of Bitcoin." SSRN Electronic Journal.

Choo, Renee. 2021. Bitcoin's impacts on climate and the environment. Columbia Climate School .

Christos, Porios, and Schneier Bruce. 2022. "How to decarbonize crypto." The Atlantic.

Cox, Chelsey. 2022. Treasury warns against Russia's efforts to evade sanctions with cryptocurrencies. CNBC.

Elliptic. (2022). NFT and Financial Crime: Money Laundering, Market Manipulation, Scams & Sanctions Risks in NFTs. Elliptic.

European Parliment Think Tank. 2022. Markets in crypto-assets (MiCA).

European Union Agency for Criminal Justice Cooperation. 2022. Controlled deliveries .

Europol. 2022. Cryptocurrencies: Tracing the evolution of criminal finances. Europol.

FATF. 2021. Updated guidance for a risk based approach: Virtual assets and virtual asset recovery. Paris: FATF.

FATF. 2014. Virtual currencies: Key definitions and potential AML/CFT risks. FATF/OECD.

Holtmeier, M. and Sandner, P. 2019. "The impact of cryptocurrencies on developing countries." Frankfurt School, Blockchain Center.

Ibrahimi, Adrianit, and Besa Arif. 2022. "Corruption and cryptocurrency: Blockchains as corruption tools." Academicus International

Scientific Journal 13 (26): 93-103. doi:10.7336/academicus.2022.26.06.

Kutera, M. 2022. "Cryptocurrencies as a subject of financial fraud." Journal of Entrepreneurship, Management, and Innovation, 18 (4

KYC360. 2020. On the periphery: Financial crime risks in cryptocurrency mining

Larkin, Aiden. 2022. "CEO of asset reality." Crypto asset recovery Q&A part 1 – Scope, laws and cooperation. Basel Institute on Governance. Basel.

Lawrence, Dennis. 2015. Bitcoin and the future of bribery. ACFE.

Marwa, Alnasaa, Gueorguiev, Jiro Nikolay and Eslem Honda. 2022. Crypto, corruption, and capital: Cross country correlation. IMF.

OECD. 2017. Toolkit on illicit financial flows: Annotations. OECD.

OECD. 2019. Cryptocurrencies: Opportunities, risks and challanges for anticorruption compliance systems. Warsaw School of Economics.

Oswego State Univeristy of New York. 2022. The Basics about Cryptocurrency.

Out-law Analysis. 2022. Cryptocurrency money laundering on DeFi skyrockets.

Phadtare, Mahdura. 2022. Bitcoin: How to use bitcoin mining to launder money.

Pierangelo, De Pace, and Rao Jayant. 2023. "Comovement and instability in cryptocurrency markets." International Review of Economics and Finance 83: 173-200.

Oettler, Mario. 2021. Anonymity vs pseudonymity. Blockchain Academy Mittweida.

Spencer, Hsu. 2022. US issues charges in first criminal cryptocurrency sanctions case. The Washington Post.

Transparency International Russia (TI Russia).2023. From Moscow city with crypto: A step-by-step guide to receiving cash from russia anonymously in London

UNCTAD. 2022. "UN Conference on Trade and Development."

UNODC. 2020. Conceptual framework for the statistical measurement of illicit financial flows.

United States Attorney's Office. 2017. Russian national and Bitcoin exchange charged in 21-count indictment for operating alleged international money laundering scheme and allegedly laundering funds from hack of Mt. Gox.

United States Attorney's Office. 2022. Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme.

University of Luxembourg. 2015. Mutual legal assistance in the digital age: Problems, challenges, solutions for criminal justice.

US Department of Justice. 2016. Founder of Liberty Reserve pleads guilty to laundering more than $250 million through his digital currency business.

US Department of Justice, US Attorney's Office,. 2022. Two Chinese intelligence officers charged with obstruction of justice in scheme to bribe US government employee and steal documents related.

DISCLAIMER
All views in this text are the author(s)' and may differ from the U4 partner agencies' policies.

PARTNER AGENCIES
GIZ/BMZ (Germany), Global Affairs Canada, Ministry for Foreign Affairs of Finland, Danida (Denmark), Sida (Sweden), SDC (Switzerland), Norad (Norway), UK Aid/FCDO.

ABOUT U4
The U4 anti-corruption helpdesk is a free research service exclusively for staff from U4 partner agencies. This service is a collaboration between U4 and Transparency International (TI) in Berlin, Germany. Researchers at TI run the helpdesk.

The U4 Anti-Corruption Resource Centre shares research and evidence to help international development actors get sustainable results. The centre is part of Chr. Michelsen Institute (CMI) in Bergen, Norway – a research institute on global development and human rights.

www.U4.no
U4@cmi.no

KEYWORDS
cryptocurrencies – organised crime – money-laundering