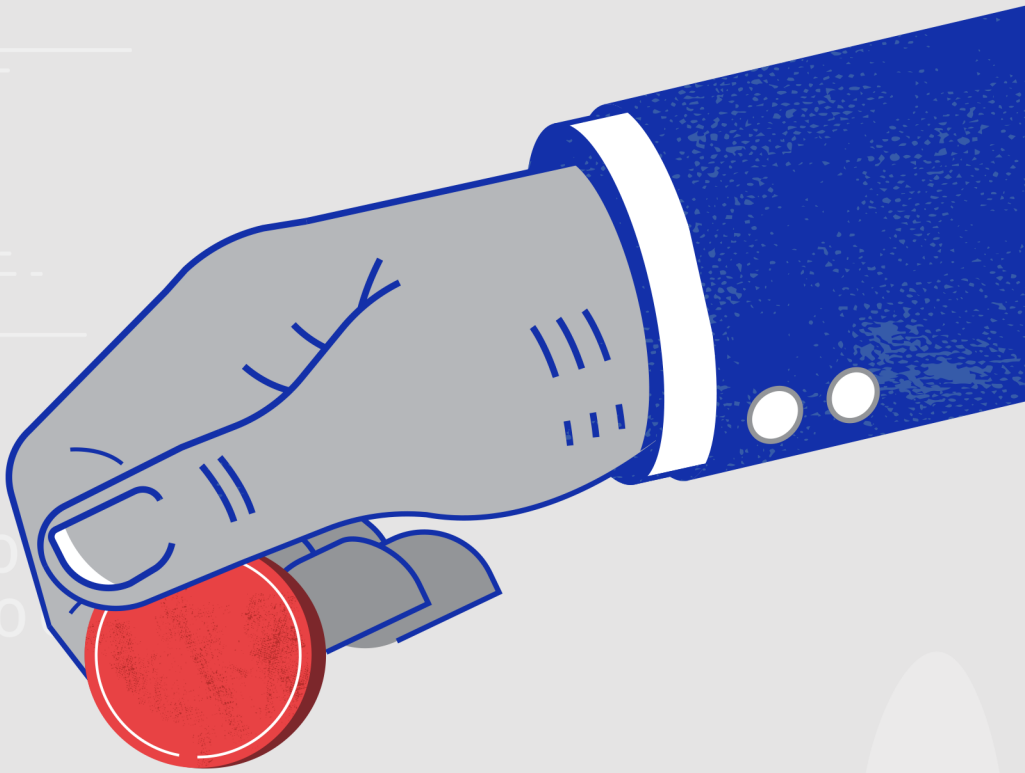
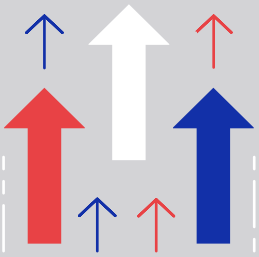
EUROPOL



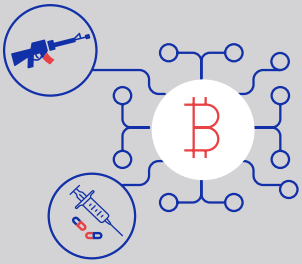
EUROPOL SPOTLIGHT

CRYPTOCURRENCIES: TRACING THE EVOLUTION OF CRIMINAL FINANCES

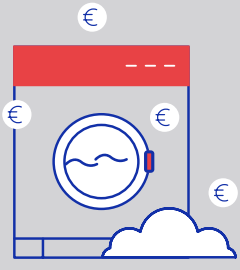
KEY FINDINGS



The use of cryptocurrency as part of criminal schemes is increasing and the uptake of this payment medium accelerating. However, the overall number and 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. A range of constraints are related to the use of cryptocurrencies, with high volatility likely a major factor in criminals' reluctance to use cryptocurrencies for long term investments.



Recent years have seen cryptocurrency increasingly used as part of criminal activities and to launder criminal proceeds. Criminals have also become more sophisticated in their use of cryptocurrencies. In addition to using cryptocurrencies to obfuscate money flows as part of increasingly complex money laundering schemes, cryptocurrencies are increasingly used by criminals as a means of payment or as an investment fraud currency. The number of cases involving cryptocurrencies for the financing of terrorism remains limited.



The criminal use of cryptocurrency is no longer primarily confined to cybercrime activities, but now relates to all types of crime that require the transmission of monetary value. However, the scale and share of the illicit use of cryptocurrencies as part of criminal activities is difficult to estimate. Criminals and criminal networks involved in serious and organised crime also continue to rely on traditional fiat money and transactions to a large degree, in addition to emerging value transfer opportunities.

3

Money laundering networks specialised in large-scale money laundering as-a-service have adopted cryptocurrencies and are offering their services to other criminals.

The illicit use of cryptocurrencies is predominantly associated with money laundering purposes, the (online) trade of illicit goods and services, and fraud. Fraud is the most frequently identified predicate offence in the illegal use of cryptocurrencies. Cryptocurrencies continue to be used as part of exchanges within the growing number of for-profit schemes relating to child sexual abuse material (CSAM).

The regulations governing the use of cryptocurrencies and the associated anti-money laundering (AML) frameworks are becoming more effective. Improved regulation of the cryptocurrency environment now requires service providers and platforms to capture more information on users and transactions, which has improved the law enforcement response to the criminal use of cryptocurrencies.

Introduction

The scale of the illicit use of cryptocurrencies as part of criminal activities is difficult to estimate. However, this Intelligence Notification provides an overview of the illicit use of cryptocurrencies, including those services that facilitate their illicit use, illustrating relevant modi operandi using case examples.

The note is based on operational information contributed to Europol, data collected for the EU Serious and Organised Crime Threat Assessment (SOCTA) 2021[1], and on reports from the private sector, academia and other relevant open sources.

Cryptocurrencies are a technical and financial innovation that hold high potential for the global economy. At the same time, they are also used for criminal purposes in the absence of effective regulation.

The use of this virtual currency for criminal activities and laundering of profits has grown over the past years in terms of volume and sophistication.[2] Tools facilitating the use of cryptocurrencies are now widely available, and services dedicated to the channelling of criminal profits are well-established. As a consequence, 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.

The private sector[3] reports that the unlawful use of cryptocurrencies accounts for a small part of their overall use, accounting for the 0.34% of transactions.[4] In contrast, research from academia[5] estimated a

1 Europol (2021), European Union Serious and Organised Crime Threat Assessment 2021 - A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021

2 Europol (2020), Internet Organised Crime Threat Assessment 2020, accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

3 Chainalysis (2021), The 2021 Crypto Crime report, https://go.chainalysis.com/2021-Crypto-Crime-Report.html

4 In its annual report, the cryptocurrency tracing company Chainalysis estimates that illicit activities represent the 0.34% of all cryptocurrency activities, or USD 10 billion in transaction volume in 2020. This estimation is lower than the previous year's assessment where the illicit use of cryptocurrencies accounted for the 2.1% of transaction volume in 2019. Estimations from Chainalysis are based on their own attribution datasets where transactions are tagged as illicit whenever linked to clearly illicit activities, such as the ones from and to dark web marketplaces and ransomware clusters. It is important to highlight that these figures are affected by a significant intelligence gap related to a lower level of detection of some criminal activities, including frauds and money laundering.

5 S. Foley, J. Karlsen and T. Putnis (2019), Sex, Drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? accessible at https://www.uts.edu.au/about/uts-business-school/our-

much higher volume, reporting that about 23% of transactions are associated with criminal activities.[6] The significant difference in estimation might be partially due to the different approaches and methodologies in the transaction analysis. Research agrees that the proportion of cryptocurrency use associated with illicit activities compared to legitimate use decreased overtime while the absolute amount has continued to increase. The illicit use of cryptocurrencies is predominantly associated with money laundering purposes, the (online) trade of illicit goods and services, and fraud.

The cryptocurrency landscape

In 2009, Bitcoin emerged as the first decentralised virtual currency. While existing virtual currencies had centralised entities as intermediaries, this new currency became popular because of the absence of third parties in the transactions. Its use of online technologies combined with cryptography resulted in a completely new transfer system where a secure payment could be sent directly without the use of an intermediary, such as a central bank or public authority. Due to its dependence on cryptography, this type of currency is commonly referred to as cryptocurrency.

Cryptocurrencies have since then developed into a widespread means of payment, of investment and transfer of funds. The inception of an innovative payment system that allows reliable, irreversible, end-to-end transactions in real time and on a global scale has caused regulatory concerns. The revolutionary nature of this type of currency did not allow an immediate legislative and enforcement response. AML (Anti-Money Laundering) and KYC (Know-Your-Customer) processes were not originally designed to cater for cryptocurrencies. However, some more recent AML legislation is starting to account for the cryptocurrency landscape.

Criminals, in particular cybercriminals, took advantage of the favourable environment and started using cryptocurrencies for trading on the dark web and as part of fraud and extortion schemes. Bitcoins have always been traceable and are not completely anonymous. In order to make use of their profits, criminals started to use services such as exchanges to cash out cryptocurrencies and convert them into fiat currencies. Improved

research/research-impact/sex-drugs-and-bitcoin

6 The research group analysed a blockchain dataset containing almost 220 million Bitcoin transactions for the period 2009-2017. The study resulted in an estimation of the value of illicit Bitcoin transaction at around USD 72 billion per year.

regulation of the cryptocurrency environment now requires service providers and platforms to capture more information on users and transactions, which has improved the law enforcement response to the criminal use of cryptocurrencies.[7]

Blockchain explained

Blockchain can be defined as a transactional database. It is a particular type or subset of so-called distributed ledger technology (DLT). DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers called nodes. Blockchain is a mechanism that employs an encryption method known as cryptography and uses specific mathematical algorithms to create and verify a continuously growing data structure – to which data can only be added and from which existing data cannot be removed.[8]

A public/permissionless blockchain is accessible by everyone, without any approval. There is no central owner of the network and software, and identical copies of the ledger are distributed to all the nodes in the network. The majority of cryptocurrencies currently in circulation, including Bitcoin, is based on permissionless blockchains. Permissioned blockchain is coordinated by a central entity and transaction validators (i.e. nodes) have to be pre-approved to be able to join the network. This type of blockchain can also be public, allowing anyone to view the ledger that can only be updated by authorised participants.[9]

Market overview

The cryptocurrency market has diversified considerably over recent years. Bitcoin now shares the market with plenty of other coins, also known as altcoins. However, it still remains the most valuable coin, dominating the market with 44% of the market share.

The proliferation of altcoins includes the emergence of privacy coins that have a specific focus on encryption and offer a higher level of anonymity by using an obfuscated public ledger. Monero is one of the predominant

7 US Department of Justice (2020), Cryptocurrency Enforcement Framework, accessible at https://www.justice.gov/archives/ag/page/file/1326061/download

8 European Parliament (2018), Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion, accessible at https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1

9 European Parliament (2018), Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion, accessible at https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1

privacy coins and is frequently used by criminals.[10] It allows anonymous transactions by hiding both sending and receiving addresses[11] as well as the amounts of transactions using different techniques and technologies. While Monero has gained great popularity in the past years, it is still far from overtaking Bitcoin. Dash and Zcash are other examples of commonly used privacy coins.

Many exchanges have now delisted privacy coins following guidance from regulators.[12] Nevertheless, these coins have not become as popular as expected, probably because they are not as liquid[13] as Bitcoin and other altcoins and thus more impractical. Bitcoins are in fact widely accepted and easy to exchange to other coins and currencies. However, the scale of the use of privacy coins is hard to estimate due to their enhanced anonymity features.

Services, facilitators and obfuscation methods

Often illicit funds do not flow straight from wallet to wallet. They instead travel through a multi-step process involving different financial entities, many of which are novel and are not yet part of standardised, regulated financial payment markets. Obfuscation methods and other countermeasures continue to be developed and used by criminals.

Exchanges and trade mechanisms

Cryptocurrency exchanges are online financial service providers that allow users to purchase and convert cryptocurrencies into other coins or fiat currency against the payment of a certain fee.[14] They can accept a wide range of payment options such as other coins and fiat currencies through wire transfers, credit cards or online service providers (OSPs). Some exchanges only accept payments in cryptocurrencies.

In the EU, these services operate as legitimate businesses and are obligated to fulfil due diligence requirements. They fall into the same regulatory framework as banks and other financial services and are

10 Trendmicro (2019), Evasive threats, pervasive effects, accessible at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

11 European Parliament (2018), Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion, accessible at https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1

12 Institute for Security and Technology (2021), Combating Ransomware, accessible at https://securityandtechnology.org/ransomwaretaskforce/report/

13 Liquidity refers to the ease of conversion into other coins and currencies.

14 Transaction fees are on average between 0.1% and 0.5% of the transaction value.

required to identify their users and report suspicious activities to Financial Intelligence Units (FIUs).

CASE EXAMPLE

Exchanges and money laundering

BTC-e, a widely used cryptocurrency exchange operated by a Russian national, was founded in 2011 and seized in 2017 for facilitating financial transactions related to cybercrime, corruption and drug trafficking. Investigations revealed that over the course of its operations BTC-e processed more than USD 4 billion worth of cryptocurrencies.

Source: US Department of Justice 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

Criminals now increasingly add steps to their laundering processes and rely on unlicensed exchanges. These exchanges often impose loose KYC requirements and allow illicit cryptocurrency trades by exchanging funds across various markets.[15] Some exchanges have been accused of facilitating money laundering activities and illicit transactions using fake and stolen identities.[16]

Nested services operate within legal exchanges and mask illicit activity within the overall pool of transactions. They use the liquidity and access to trading pairs of larger services by setting up accounts on big exchanges for their businesses. Common examples of nested services include over-the-counter (OTC)[17] and swapping services, described later in this chapter.

Exchanges are not the only way to trade cryptocurrencies for fiat currency or vice versa. Several options for direct trade from buyer to seller are available to users and are safe options to obfuscate financial operations.

15 Todayheadline.com (2021), The rise of crypto laundries How criminals cash out of Bitcoin?, accessible at https://todayheadline.co/the-rise-of-crypto-laundries-how-criminals-cash-out-of-bitcoin/

16 US Department of Justice News2017, 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, accessible at https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.

17 All trades conducted directly between two parties without the intervention of exchange is known as over-the-counter (OTC) trading.

9

P2P trading refers to the direct trade of cryptocurrencies between counterparts without the use of an intermediary. P2P trading lowers the tracing risks by skipping the identification process required by the exchange, but entails high risks when it comes to fraud, as transactions are not protected. Users who want to buy or sell cryptocurrencies get directly in touch to proceed on the transaction on mutually agreed terms, rather than the terms decided by the exchange. Direct contact among users can in fact result in one of the parties breaking the deal by not paying the agreed sum. Several platforms facilitate P2P trading, finding the best match between seller and buyer, protecting users and transactions with an escrow service that limits the fraud risk.

While P2P platforms are generally used for smaller trades, in recent years OTC cryptocurrency trading has gained popularity for larger transactions. OTC trading is another method of direct exchange between a buyer and a seller outside of an open exchange, covering transactions that are crypto-to-crypto, crypto-to-fiat, fiat-to-crypto or crypto-to-other goods. Parties do not need to apply the market price to their transactions and can determine the pricing bilaterally. Since transactions happen outside exchanges, even major transactions do not affect the cryptocurrency market. This process can involve a buyer and a seller in a local setting (e.g. a restaurant or a hotel) or established platforms and services. Many exchanges have opened OTC desks to assist users in placing large purchases or sales of cryptocurrencies. This established trading setting should comply with AML regulations and generally involves wire transfers via bank accounts. There are also independent professional OTC brokers who facilitate contacts between parties, taking a percentage of the transaction in return.

Services and main obfuscation methods

Crypto-swapping services facilitate a quick conversion of one coin into another by placing orders on behalf of users. These transactions are difficult to trace when well-known coins are exchanged into less known ones or privacy coins, enhancing anonymity. Many of these services use lenient or non-existent KYC procedures. In some cases, they even advertise their non-compliance.

The popularity of cryptocurrencies has also led to the creation of instruments that facilitate and expedite their use in daily life, as well as offering opportunities to launder criminal profits. Users can spend their virtual assets in most locations by using crypto debit cards. The quick exchange of cryptocurrency for cash fiat currency and vice versa is facilitated by the use of Bitcoin ATMs (BATMs). Users can send cryptocurrencies to a specific address

generated by the BATM and receive cash in return, or insert cash in the physical device in exchange for cryptocurrencies.

Decentralised Finance ("DeFi") is another important element in the cryptocurrency market. Whereas traditional exchanges are focussed on turning fiat currencies into cryptocurrencies, decentralised exchanges are focussed on turning cryptocurrencies into other coins and currencies. Most of the time users obtain cryptocurrencies via centralised exchanges, but this may change in the future to DeFi.

Other than trading systems, some other services and methods are often used to enhance cryptocurrencies' anonymity. The use of cryptocurrency mixers (or tumblers) is a common obfuscation technique for criminals who want to conceal illicit transactions. These services enhance transaction privacy by breaking the links between the original and the final address using several intermediary wallets, charging a transaction fee.

Non-fungible tokens (NFTs) allow specific individual items to be sold and traded on the blockchain. NFTs are basically digital high-value goods that use blockchain to record their ownership. Like Ethereum or Bitcoin, NFTs are a store of value but unlike these coins, these digital goods can have a high value.

Another popular obfuscation technique used to conceal criminal profits is channelling them into cryptocurrency gambling platforms.

Opportunities and threats for criminal actors

Pseudo-anonymity and decentralisation provide a favourable environment for criminals. It is important to highlight that cryptocurrencies are not anonymous. Every single transaction is logged in the blockchain, which is a ledger of all transactions distributed to all users in the network. Most blockchains are publicly available, making transactions traceable. However, a number of services and techniques can enhance anonymity and hinder law enforcement investigations. Privacy coins may also hide (parts) of their blockchain. The decentralisation of this financial system provides additional opportunities because it circumvents the verification role of a traditional central authority, as well as geographical constraints. This not only enables extremely quick international transactions, but offers also the possibility to exploit regulatory gaps between jurisdictions.

Nonetheless, the criminal use of cryptocurrencies entails a number of risks. Unlike many fiat currencies, cryptocurrencies are subject to a high

level of volatility. Criminal networks might be reluctant to entrust funds to unpredictable currencies in contrast to the stability offered by conventional cash flows.

Crypto-wallets are susceptible to theft via hacking. Cryptocurrency theft can be carried out in several ways. In some cases, hackers have exploited vulnerabilities in ledgers and stolen coins worth hundreds of millions of euros.[18]

The criminal use of cryptocurrencies

Cryptocurrencies have been adopted as part of money laundering schemes and are particularly associated with several predicate offences including fraud and drug trafficking. They are also widely used as a means of payment for illegal goods and services offered online and offline.

Money laundering is the main criminal activity associated with the illicit use of cryptocurrencies. The growing popularity and adoption of cryptocurrencies have led to their increasing use in money laundering schemes. Other criminal activities that show an intensive use of cryptocurrencies are related to the use of cryptocurrencies as a payment method for illicit goods and services, fraudulent cryptocurrency investments and cybercrime. In all instances, criminals want to obfuscate the source of the illicit assets with cryptocurrencies. A number of indicators show how criminals involved in frauds strongly rely on the use of cryptocurrencies.

Cryptocurrencies are also the means of payment of choice for criminal commodities and services, such as drugs or child sexual abuse material (CSAM) purchased online. This applies in particular to listings on dark web marketplaces where they are the main means of payment. Different types of malware target cryptocurrencies for theft as well as for the mining of coins in the network of unaware victims. Extortion schemes carried on by cybercriminals make extensive use of cryptocurrencies. Digital services and infrastructure abused for criminal purposes like servers, virtual private networks (VPNs) and hosting services are mostly purchased in cryptocurrency.

18 BBC News (2021), Hackers steal $600m in major cryptocurrency heist, accessible at https://www.bbc.com/news/business-58163917

Money laundering

Virtually all kinds of criminal profits are laundered using cryptocurrencies. These activities range from the laundering of proceeds already in digital form, such as the payment of ransoms or criminal infrastructures, to a transformation of huge amounts of cash into virtual assets. Examples of cryptocurrency usage in money laundering schemes include the purchase of cryptocurrencies by criminal networks using illicit proceeds and the use of cryptocurrencies to transfer funds.

The use of cryptocurrencies in money laundering schemes has been increasing, and many criminal networks relied on cryptocurrencies as a payment medium during the COVID-19 pandemic.[19]

Money laundering networks specialised in large-scale money laundering as a service have adopted cryptocurrencies and are offering their services to other criminal actors.[20] These networks can already rely on established infrastructure such as numerous bank accounts as well as in-depth knowledge of the banking system and use of FinTech.[21] Money laundering networks provide their services to other criminal networks, which may include the acquisition or trade of cryptocurrencies, the legalisation of criminal assets and the final cash out in the accounts of criminals. Professional money laundering networks are a significant threat and enable other criminal networks to operate. Marketplaces on the dark web advertise money laundering cryptocurrency service providers. They also offer information on how criminals can cash out cryptocurrencies, such as by exchanging Bitcoin for gift vouchers or prepaid debit cards.[22]

Predicate offences

The use of cryptocurrency in money laundering involves the profits of both online and offline criminal activities. They are in fact frequently reported in the context of drug trafficking, fraud and cybercrime.[23] Cybercrime proceeds

19 Europol (2021), European Union Serious and Organised Crime Threat Assessment 2021 - A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, accessible at https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

20 Europol (2021), European Union Serious and Organised Crime Threat Assessment 2021 - A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, accessible at https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

21 FinTech stands for financial technology. It includes any technology that is used to streamline, disrupt and digitalise financial services.

22 Todayheadline.com, 2021, The rise of crypto laundries How criminals cash out of Bitcoin?, accessible at https://todayheadline.co/the-rise-of-crypto-laundries-how-criminals-cash-out-of-bitcoin/

23 Europol (2021), European Union Serious and Organised Crime Threat Assessment 2021 - A corrupting

primarily concern funds coming from online frauds, ransomware and dark web marketplaces. The highest volume of illicit transactions is associated with these criminal activities.[24]

Fraud

Fraud is the most frequently identified predicate offence for the illegal use of cryptocurrencies, accounting for more than half of identified criminal transactions.[25] Criminals involved in fraud either make use of professional (crypto) money laundering services or set up their own money laundering schemes.

CASE EXAMPLE

Fraudulent cryptocurrency investment

Belgian and Swiss law enforcement authorities dismantled a criminal network running a worldwide Ponzi scheme using pyramid selling of the cryptocurrency "VITAE". Its members are for the most part Belgian nationals who were making use of a company under Swiss jurisdiction. This criminal network was using the social reward website 'Vitae.co' and website 'Vitaetoken.io' to trick people into investing into a Ponzi scheme. A social reward website is similar to a social network, but to activate their account clients paid a monthly fee (USD 200). However, the recruitment of three people would cover the fee (pyramid system). It is believed that some 223 000 individuals from 177 countries have fallen victim to this scheme.

The case is an example of an exit scam. It involves enhancing the trust in a specific cryptocurrency. This leads people to invest in the coin or depositing it on a specific platform. The criminal network then either gets away (or 'exits') with a large part of the cryptocurrency and converts it to other currencies before the price bubble is burst, or they artificially inflate the value by disinformation in order to sell a large part of the cryptocurrency and realize a huge capital gain. The criminal organisation owned a large part of the cryptocurrency. A total of EUR 1.1 million in cash was seized, alongside EUR 1.5 million worth in cryptocurrencies.

Source: Europol 2021, Europol helps Belgian and Swiss authorities unravel Vitae Ponzi Scheme.

influence: the infiltration and undermining of Europe's economy and society by organised crime, accessible at https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

24 Chainalysis (2021), The 2021 Crypto Crime report, accessible at https://go.chainalysis.com/2021-Crypto-Crime-Report.html

25 The annual report on the criminal use of cryptocurrency conducted by Chainalysis reports that frauds represent the 54% of illicit activities detected in 2020, accounting for USD 2.6 billion. [Chainalysis (2021), The 2021 Crypto Crime report]

Criminals involved in investment fraud are particularly adept at using cryptocurrencies to channel illicit proceeds. Cryptocurrency investment fraud schemes have been identified in several EU Member States.[26]

Fraudsters create websites devoted to cryptocurrency investments or advertise lucrative investments and encourage investors to create accounts on online trading platforms. Alternatively, operators from established call-centres offer opportunities requiring small initial investments that end in high profits. The victims have the impression to be able to monitor their investments thanks to internet platforms. However, the whole process is a deception. Brokers try to obtain information about the victims using social engineering techniques, while gaining their trust with simulated trading activities.

CASE EXAMPLE

Fraudulent trading scheme

A criminal network created several different trading online platforms advertising substantial profits from investments in high-risk options and cryptocurrencies. The criminal group ran at least four such professional-looking trading platforms, luring victims through advertisements on social media and search engines. The members of the criminal group were posing as experienced brokers when contacting the victims via the call centre they had set up. The suspects were using manipulated software to show the gains from the investments and to motivate the victims to invest even more.

The fraud scheme, organised mainly by Israeli nationals, was disseminated via call centres, ran from Bulgaria and North-Macedonia. In total, the criminal network defrauded victims across Europe of an estimated EUR 30 million.

Source: Europol 2021, Trading scheme resulting in €30 million in losses uncovered

On some occasions, fraudsters collect capital to initiate a new profitable cryptocurrency which does not really exist. Pyramid schemes are a frequently used method of attracting investors with promises of high returns. The increase in value promised to investors is just an illusion, and

26 Europol (2021), European Union Serious and Organised Crime Threat Assessment 2021 - A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, accessible at https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

any disbursements to investors are merely funds transferred from investors further down the pyramid. Members are encouraged to bring others into the fold in exchange for a commission.

Drug trafficking

Cryptocurrencies are increasingly used to launder the proceeds of drug trafficking. In recent years, EU law enforcement authorities carried out several investigations into the laundering of drug trafficking proceeds using cryptocurrencies. These large-scale laundering activities normally involve specialised criminal networks that provide professional crypto money laundering services.

Cybercriminals

Cybercriminals make extensive use of cryptocurrencies that consequently have to be laundered, invested or cashed out. Proceeds from cybercrime activities normally do not require a conversion as they are often already in cryptocurrencies. Cybercriminals extensively use obfuscation techniques and services to hinder transactions traceability.

CASE EXAMPLE

Money laundering network for cybercriminals

A complex investigation involving 20 countries resulted in the dismantling of a criminal network laundering tens of millions of euros in stolen funds that was advertising its services in online forums. Against the payment of a transaction fee (up to the 50% of the transaction), the network opened and maintained hundreds of corporate and personal bank accounts worldwide to receive and transfer money from cybercriminals who stole it from accounts of victims. Laundered funds were then returned to their cybercriminal clientele.

Source: Europol 2020, 20 arrests in QQAAZZ multi-million money laundering case

Means of payment

Cryptocurrencies are also used to send payments to suppliers or to accept payments for the purchase of illicit goods online. The use of cryptocurrencies as a payment method for illicit activities, although limited in comparison to global illicit finance handled in fiat currency, is growing.[27] The purchase of illicit goods and services concerns mainly online trading, particularly on dark web marketplaces. Cryptocurrencies are also used to extract ransomware payments from victims as well as to pay for intangible goods and services including for child sexual abuse material (CSAM).

Means of payment in dark web marketplaces

Cryptocurrencies have been the standard means of payment for users of dark web platforms since the onset of the first major marketplace in 2011, Silk Road. The volume of transactions for 2020 related to dark web market places is estimated to be EUR 1.5 billion (USD 1.7 billion) worth of cryptocurrency activity.[28] Criminals' need to use their illicit profits and overcome the traceability of cryptocurrencies through the logs in public ledgers popularised the use of obfuscation techniques.

Just like companies, each dark web marketplace accepts selected coins. Despite the proliferation of altcoins, Bitcoin remains the prevalent coin accepted by dark web marketplaces. However, a number of marketplaces accept altcoins too, especially Monero and Ethereum.[29]

While the total value of the cryptocurrencies used to trade illicit commodities and services on dark web marketplaces is hard to assess, the analysis of crypto transactions of the largest active marketplace (Hydra) can provide an indication. Since its inception in 2015, the Russian-language marketplace became very popular among criminals and is mostly known for offering large quantities of illicit drugs through a wide range of sellers, as well as other goods and services. Its reliability and safety features saw the marketplace flourish over the years, reaching an annual revenue of more than EUR 1.18

27 Chainalysis (2021), The 2021 Crypto Crime report, accessible at https://go.chainalysis.com/2021-Crypto-Crime-Report.html

28 Chainalysis (2021), The 2021 Crypto Crime report, accessible at https://go.chainalysis.com/2021-Crypto-Crime-Report.html

29 An analysis of 581.871 listings scraped from 8 leading dark web marketplaces reports that 98% of cryptocurrencies mentions are about Bitcoin, Monero and Ethereum. [RAND Europe (2020), Exploring the use of Zcash cryptocurrency for illicit or criminal purposes]

billion (USD 1.33 billion) in 2020 alone.[30] It is estimated that Hydra accounts for around 75% of the dark web market revenue worldwide.[31]

CASE EXAMPLE

Criminal services online

A blockchain analysis carried out by Europol enabled the identification and arrest of a man hiring a hitman. The suspect had transferred the equivalent of EUR 10 000 in Bitcoins to a hitman enlisted on a specialised site, to kill his ex-girlfriend.

Source: Europol 2021, Dark web hitman identified through crypto-analysis

Ransomware payments

The evolution of ransomware as a lucrative criminal business has been closely tied to the rise of Bitcoin and other cryptocurrencies.[32] Ransomware consists of the deployment of a malware that encrypts computer systems and/or data followed by the demand of a ransom in exchange of the decryption key. An increasing number of cases involves as well the exfiltration and retention of data used to blackmail the victims (often referred to as double-extortion). The fear of disclosure of sensitive data, reputational damage and potential sanctions prompts businesses and individuals to pay the ransom and avoid reporting, making this extortion process extremely profitable. As attacks become more targeted and sophisticated, the average amount of ransom demanded keeps rising.[33] The demanded ransom is moreover adjusted to what criminals expect victims are able to pay.

Almost all ransomware payments are made in cryptocurrencies, usually Bitcoins.[34] Normally the victim is asked to pay a ransom request in Bitcoin in order to have their system decrypted. The positive response to this demand entails the withdrawal from a financial institution of fiat currency to purchase

30 Flashpoint and Chainalysis (2021), Hydra: Where the crypto money laundering trail goes dark; accessible at https://www.flashpoint-intel.com/blog/chainalysis-hydra-cryptocurrency-research/

31 Chainalysis (2021), The 2021 Crypto Crime report, accessible at https://go.chainalysis.com/2021-Crypto-Crime-Report.html

32 Institute for Security and Technology (2021), Combating Ransomware, accessible at https://securityandtechnology.org/ransomwaretaskforce/report/

33 Europol (2020), Internet Organised Crime Threat Assessment 2020, accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

34 Custers, B.H.M., Oerlemans, J.J., Pool, R. (2020) Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies, accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694282

the requested cryptocurrencies. The amount is then transferred to the wallet address provided by the criminal actor.

CASE EXAMPLE

Ransomware proceeds

Hackers behind the WannaCry ransomware in 2017 started withdrawing money from the three Bitcoin wallets associated to their criminal activity only three months after the attacks. They then sent the funds to the exchange Shapeshift.io, in order to convert Bitcoins in Monero and hinder traceability.

Source: Guardian 2017, WannaCry: hackers withdraw £108,000 of Bitcoin ransom

The trade in child sexual abuse material (CSAM)

The monetisation of child sexual abuse material (CSAM) is a growing threat. An estimation of the yearly revenue of CSAM sites shows that the annual revenue has more than tripled in the period 2017-2020.[35] While the trade in CSAM accounts for a very limited portion of the volume of funds transferred in regard to illicit activities, it poses a high threat due to its potential impact.

CSAM is mainly commercialised through dedicated marketplaces and forums on the dark web. Nearly all major dark web marketplaces explicitly forbids its sale. Most of the transactions use cryptocurrencies as means of payment.

35 Chainalysis (2021), The 2021 Crypto Crime report, accessible at https://go.chainalysis.com/2021-Crypto-Crime-Report.html

19 Conclusions

As with most technological innovations, cryptocurrencies were initially misused by cybercriminals, before expanding to other types of criminal actor.

At the beginning, cybercriminals used to feel safe by simply processing their illicit transactions in Bitcoins. Soon after, it became clear that Bitcoin was far from being anonymous and untraceable, when blockchain analysis resulted in several successful law enforcement investigations. Consequently, the criminal use of cryptocurrencies had to be linked to the use of services that would enhance anonymity.

Most relevant cases involve the laundering of criminal proceeds. The development of specialised cryptocurrency money laundering services has inevitably lowered the bar of technical knowledge required, contributing to the widespread use of these techniques by many criminal actors and networks.

Cryptocurrency remains appealing for criminals, primarily due to its pseudo-anonymous nature and the ease and speed with which funds can be sent anywhere in the world. However, the use of cryptocurrencies for illicit activities seems to comprise only a small part of the overall cryptocurrency economy, and it appears to be comparatively smaller than the amount of illicit funds involved in traditional finance.[36]

36 Chainalysis (2021), The 2021 Crypto Crime report, accessible at https://go.chainalysis.com/2021-Crypto-Crime-Report.html

Headquartered in The Hague, the Netherlands, Europol supports the 27 EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. We also work with many non-EU partner states and international organisations. From its various threat assessments to its intelligence-gathering and operational activities, Europol has the tools and resources it needs to do its part in making Europe safer.

EUROPOL SPOTLIGHT - CRYPTOCURRENCIES: TRACING THE EVOLUTION OF CRIMINAL FINANCES

PDF | ISBN 978-92-95220-37-9 | ISSN 2600-2760 | DOI: 10.2813/75468 | QL-AN-21-004-EN-N

Luxembourg: Publications Office of the European Union, 2021

Cite this publication: Europol (2021), Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu