FRIEDRICH NAUMANN FOUNDATION For Freedom.

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

DARK CRYPTO

The Use of Cryptocurrency for Illegal Purposes

Johannes Rieckmann, Tim Stuchtey

ANALYSIS

Imprint

Publisher
Friedrich Naumann Foundation For Freedom
Truman-Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit
/stiftungfuerdiefreiheit

Author
Dr. Johannes Rieckmann, Senior Research Fellow,
Brandenburg Institute for Society and Security (BIGS)
Dr. Tim Stuchtey, Executive Director,
Brandenburg Institute for Society and Security (BIGS)

Editorial
World Order and Globalization Hub, Washington D.C.
Globale Themes Division, Berlin

Contact
Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Date
April 2023

Notes on using this publication
This publication is an information offer of the Friedrich Naumann Foundation for Freedom. It is available free of charge and not intended for sale. It may not be used by parties or election workers for the purpose of election advertising during election campaigns (federal, state or local government elections, or European Parliament elections).

Content

EXECUTIVE SUMMARY **4**

1. INTRODUCTION **5**

2. THE *BLOCKCHAIN* AND CRYPTOCURRENCIES **6**

2.1. The *Blockchain* Technology 6

2.2. Cryptocurrencies 6

2.3. Transparency 8

3. OBFUSCATION TECHNIQUES **9**

3.1. Mixers and Tumblers 9

3.2. Privacy Coins 10

3.3. Crypto Exchanges 10

4. USES FOR ILLEGAL PURPOSES **12**

4.1. Forms of Illegal Transactions with Cryptocurrency 12

4.2. Extremism and Terrorist Financing 13

4.3. Money Laundering 14

4.4. State-Sponsored Actors, National Security 14

5. APPROACHES IN FIGHTING MONEY LAUNDERING **16**

5.1. Regulation 16

5.1.1. National 16

5.1.2. International und Supranational 17

5.2. Sanctions 17

5.3. Investigation and Prosecution 18

6. RECOMMENDATIONS FOR ACTION **19**

7. FUTURE OUTLOOK **20**

LIST OF ABBREVIATIONS **21**

LIST OF REFERENCES **21**

Executive Summary

Blockchain technology and the cryptocurrencies based on it offer considerable innovation potential for the economy and society as a whole. But cryptocurrencies have also become the payment method of choice for certain criminal activities. In this study, economists Johannes Rieckmann and Tim Stuchtey of the BIGS (Brandenburgisches Institut für Gesellschaft und Sicherheit – Brandenburg Institute for Society and Security) provide an overview of illegal uses of cryptocurrencies. They explain various methods to obfuscate and anonymize transactions using crypto mixers as well as the differences between classical cryptocurrencies, such as Bitcoin and Ether on the one hand and anonymized cryptocurrencies on the other hand, which make it almost impossible to track transactions. They reveal for which crimes cryptocurrencies are misused, both within the *blockchain* and at the intersections between the analog and digital world. They analyze existing and planned approaches for regulation and action.

The authors recommend actions, based on their analysis and expert interviews, as to how the misuse of cryptocurrencies for illegal purposes can be prevented without disproportionately limiting the technology's potential to innovate. Cryptocurrencies and their marketplaces, which so far have been largely unregulated compared with the traditional financial sector, will henceforth have to comply with rules that allow de-anonymizing transactions when required by a court order. These rules must be transparent to users so that they do not lose confidence in a currency and its marketplaces. At the same time, a well-regulated market can significantly expand the options available to use cryptocurrencies legally.

Plans by the German federal government to consolidate investigative functions in a Federal Financial Criminal Investigation Office appear to be reasonable to curb crime, money laundering, terrorist financing and the avoidance of sanctions, due in part to the dearth of investigators with the necessary expertise. In this context, it is necessary to find a reasonable balance. A central point of contact for all issues related to law enforcement can also give a location an attractive advantage to for innovative companies with legal business models.

1. Introduction

The topic of monetary and currency theory – which most people would consider rather boring – has become more fascinating with the emergence of cryptocurrencies. The fact that there is very little government regulation so far makes cryptocurrencies particularly fascinating for libertarians. People with strong capital market orientation are captivated by often rapid price increases and the associated stories of people who have acquired substantial wealth within a very short time. Skeptics of these new currencies, in turn, are intrigued that such assets, due to their extreme price fluctuations, can vanish just as quickly as they were created, and some may even feel a certain Schadenfreude. Business founders and innovators with mathematical acumen are fascinated by potential applications of the *blockchain* technology that underpins cryptocurrencies. Meanwhile, the dark side associated with the new currencies fascinates nearly everyone. The lack of regulation and elusive nature of cryptocurrency transactions have made them the currencies of choice for many criminals, especially in the area of cybercrime.

This policy paper seeks to clarify

- → why cryptocurrencies are so popular particularly in the area of illegal trade,
- → how extensively cryptocurrencies are used,
- → why it is important to differentiate between different cryptocurrencies,
- → what opportunities or obstacles this presents for the fight against crime and
- → whether this necessitates regulatory measures.

This paper intends to serve as a guide and thematic introduction for readers who are interested in the technology's development and application in payment transactions from a regulatory perspective. Our focus is not on aspects of energy, environmental, industrial, or monetary policy (which are also relevant), but on security-related aspects.

The following will briefly discuss the mechanisms of cryptocurrencies in their various current forms, with particular emphasis on obfuscation procedures. We will continue to focus on the use of cryptocurrencies by criminals for crimes, illegal transactions, financing of terrorist activities, and its use by state-sponsored actors. We will present national, European, and international approaches to control illegal use as well as the challenges associated with their technological development.

2. The Blockchain and Cryptocurrencies

Digital currencies, blockchain, crypto money – what is this all about? It all starts with the most famous digital currency today: Bitcoin. This is a non-governmental form of payment which, similar to cash payments in the physical world, allows transactions to be made in the digital space between individual actors without having to use intermediaries such as banks or payment service providers. The so-called blockchain, the innovative technology underlying Bitcoin and all subsequent cryptocurrencies, was launched in 2008 by a programmer under the pseudonym Satoshi Nakamoto when he published a white paper.[1] The technical concept was innovative because, for one, despite the absence of a central issuing and managing body for the digital currency, it ensured that each unit of money can only be used once by the same player for a transaction and thus changes owner, i.e. cannot be copied. Secondly, it created an incentive system for administering and updating transactions: "for the purpose of preserving and maintaining a database in a decentralized network".[2]

Cryptocurrencies derive their name from the encryption technology used. Encryption, together with redundant documentation of transactions, ensures tamper-proof security throughout the network. It also ensures that each participant's money can only be used by that person – or, more specifically, by the owner of the private key – together with the public key for a transaction.[3]

2.1. The Blockchain Technology

Transactions are combined into blocks in regular time intervals, and the blocks are arranged in a chain. This blockchain is a continuous sequence of summaries of electronic signatures. The process called mining creates an economic incentive to participate in the large-scale, decentralized review process by rewarding participants with newly created money, the so-called *block reward*.[4]

All other participants can check and verify the calculation result during the mining process.[5] The updated *blockchain*, which is validated by a *consensus mechanism* (a well-known example is *proof-of-work*) – namely the above-mentioned verification of past transactions – is documented decentrally and redundantly in a kind of distributed ledger, which is intended to make manipulation difficult to the point of impossibility.[6]

Each network participant has the same information. Therefore, the Bitcoin *blockchain* is a publicly accessible database of past transactions, which is continuously and jointly maintained and verified.

2.2 Cryptocurrencies

It is controversial whether so-called cryptocurrencies can actually be called money. Money issued by central banks (so-called fiat money[7]) is characterized by the fact that it fulfills three basic functions:[8] It serves as a medium of exchange, as a unit of account, and as a store of value. Which of these functions the various types of cryptocurrencies fulfill is briefly outlined below.

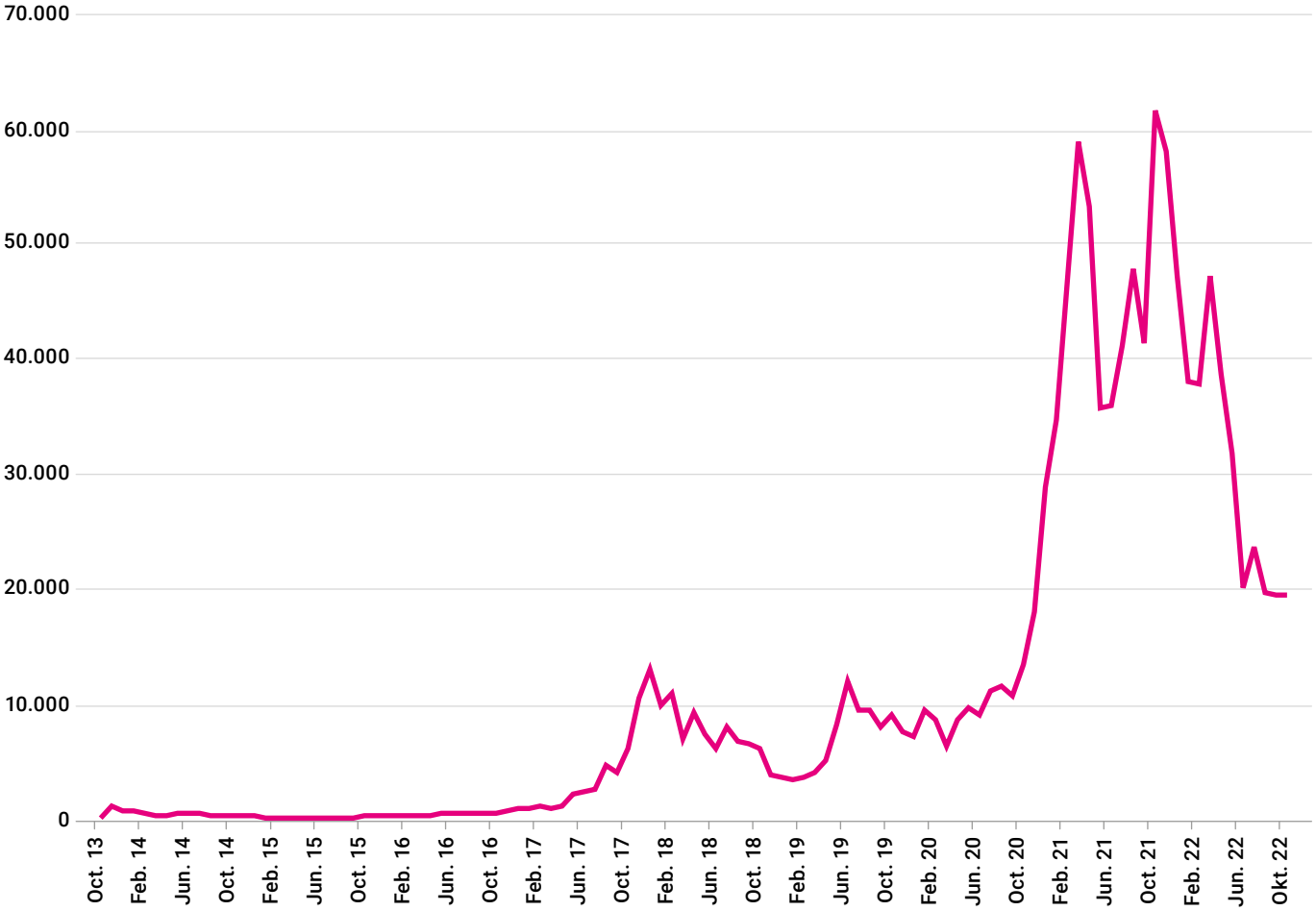
An important difference between cryptocurrency and fiat money, certainly significant in terms of its potential use for illegal purposes, is that electronic payment transactions can be handled independently of and without any intermediaries.[9] As we describe below, however, the cryptocurrency universe now also includes optional intermediaries, who, among other things, offer services such as managing depositories (so-called wallets) or concealing transaction routes. By eliminating a central issuing authority (in the case of fiat money, a central bank) and financial institutions acting as intermediaries (in the case of fiat money, the commercial banks), cryptocurrencies are in fact taking the fundamental concept of the Austrian School of Economics[10] to the next level. One of the resulting challenges is the elimination of documentation, control and possibly reporting abilities common in the banking world, which were developed to institute procedures for customer identification (Know-Your-Customer, KYC) as well as suspicious activity reports (SAR) to identify money laundering.

Bitcoin attempts to ensure value stability by, for example, limiting the money supply. However, this is not the case, as demonstrated in the following graph (Fig. 1), which shows Bitcoin's considerable price fluctuations. Therefore, it must be concluded that Bitcoin does not fulfil the function of a store of value. In addition, it has only a limited function as a medium of monetary exchange and unit of account.[11]

Despite Bitcoin's high fluctuations and low acceptance as a medium of exchange, Bitcoin had an early reputation as a currency

1 Hilgers, Sven & Greilich, K. (2021), p. 10.
2 Ibid., p. 10.
3 Ibid., p. 11.
4 Antonopoulos, A. M. (2017), p. 5.
5 For a more detailed explanation of the organization, functioning, and incentive mechanisms of the Bitcoin blockchain please refer to Hilgers, S. & Greilich, K. (2021), p.11 f.
6 The proof-of-work process to achieve consensus on the unified database content and to simultaneously create new bitcoins through mining is very energy-intensive, even as verification of successful mining is easy. This ensures that it becomes unattractive for miners to sneak in counterfeit transactions because the effort, the probability of detection and the risk of losing the spoils on the spot are very high. A more energy-efficient mechanism is the proof-of-stake process, in which network participants who are randomly selected to verify the transactions receive compensation for their expenses, in a sense a form of interest on the currency. The consensus mechanism of the Ethereum blockchain was changed from proof-of-work to proof-of-stake on September 15, 2022.
7 This is the cash and book money used in everyday life, which is based on the Latin word fiat (translation: „Let it be done").
8 Anderegg, R. (2014), p. 19.
9 As with (electronic) cryptocurrency transactions, cash transactions usually take place without intermediaries. This raises the question of what should be considered the closest equivalent to cryptocurrency transactions when designing regulation – cash payments or electronic transfers of fiat money.
10 The Austrian School of Economics was founded in the 19th century by Carl Menger and was considerably shaped by Ludwig von Mises and Friedrich August von Hayek. It is critical of government regulation and central management of economic processes. See also Menger, C. (1884), von Mises, L. (1949) and Hayek, F. A. (2022).
11 Hilgers, Sven & Greilich, K. (2021), p. 13.

Figure 1 | Bitcoin Value Development since 2013



Bitcoin price chart in U.S. dollars (USD), daily prices, October 2013 to October 2022.

Source: CoinGecko

for criminals, even though its technical setup provides perfect transparency into all executed transactions. Section 3.4 will explain this in more detail.

The creation of an additional programmable cryptocurrency – initially called colored coins – in 2011 provided an additional ability to add further information to individual monetary units.[12] Since then, actual "software programs can run within the decentralized system"[13] and can document contracts – so-called smart contracts – in a tamper-proof manner.[14] But this category of cryptocurrencies only fulfills the above-mentioned monetary functions to a limited extent, apart from being a medium of exchange. In addition, it causes further complexity depending on the type of smart contract. A prominent representative of this category is the Ethereum blockchain.

The concept of stablecoins attempts to address the problem of extreme fluctuations in value and the resulting limited usefulness of cryptocurrency as unit of account and store of value. It does so by pegging its value to that of a fiat currency (typically the US dollar), a raw material such as oil or gold, real estate, or to that of other cryptocurrencies. Pegging is done by means of collateralization, for instance by depositing a corresponding quantity of the reference currency, or through an

12 Hilgers, Sven & Greilich, K. (2021), p. 13.
13 Ibid., p. 13.
14 In this case, eliminating intermediaries could be equivalent, for example, to buying real estate without hiring a notary and entering the purchase in the land register. The additional information that can be documented on the blockchain also enables the creation of new assets, known as non-fungible tokens (NFT), due to their non-uniformity.

algorithm which adjusts supply to demand by tying it to the value of a fiat currency, for example (without actually storing it as a collateral).[15] Digital payments remain tamper-proof and fast, whereas the currency volatility is reduced compared to Bitcoin.

The collateralization of *stablecoins* must be centrally managed to keep its value in line with that of the currency in circulation. Because a purchase or sale also entails a corresponding counter-transaction with the underlying collateral, they are by nature not anonymous. One representative of *stablecoin* with fiat money as collateral is Tether.

Due to their relatively stable value, it can be said that *stablecoins* have the properties of a unit of account and a store of value. However, strong fluctuations in other cryptocurrencies have shown that *stablecoins* can also be affected, over and above the impact of inflation on fiat currencies.

The central banks of several countries are already engaged in the examination and preparation stages of developing and introducing digital currencies. These so-called *Central Bank Digital Currencies* (CBDC) aim to fulfill all three monetary functions and be a complement to cash. The effects of a national cryptocurrency – in this case centrally managed – on privacy and the commission and prosecution of crimes are still unclear and will, among other things, be heavily dependent on the respective design and political guidelines.

2.3. Transparency

Since their inception, cryptocurrencies have had a reputation for being complicated and suitable only for technology-savvy users, while also for serving mainly illegal purposes. As Bitcoin was used shortly after its creation by extortionists for ransom demands, for transactions between criminals and for payments on Darknet platforms, the general public soon got the impression that cryptocurrency transactions are not only fast and imperceptible beyond the Internet, but above all also completely anonymous.

However, this is not at all the case for Bitcoin – and for most other cryptocurrencies created after it. In fact, the entire transaction history can be viewed by the public using *Blockchain Explorers*,[16] although it is not necessarily very clear. Instead of anonymity, Bitcoin offers only pseudonymity: The wallet, identified by a combination of numbers and letters (which is not meaningful in itself), in which the transferred money is located at the time of consideration, is freely known. In other words, the wallet can be identified, and associated transactions can be observed. However, as long as no real or legal person reveals herself or himself as an owner, he or she remains an eminence grise – similar to a book author using a pseudonym.

It is difficult for criminals to maintain their pseudonymity at the so-called *off-ramp*, the point of converting cryptocurrency into fiat money, goods or services in the analog world. This is because at this point the owner of the wallet must expose their identity or that of a person appointed by them. This is why the *off-ramp* is also a point where law enforcement agencies start their investigations. Therefore, criminals often use complex cover-up and money-laundering procedures before and after this point to prevent discovery, seizure and prosecution.

However, it is conceivable to use payments within the *blockchain* for criminal services that cannot be assigned to the payer in the analog world. This could be, for example, payment on a *Darkweb* platform for a service provider offering *crime-as-a-service* (CaaS). In this case, the cryptocurrency has already served the first criminal as a means to an end, whereas the challenge of further use is passed on to the second criminal, in a sense, while maintaining his own pseudonym.

15 Reaume, A. (2022).
16 Stevens, R. (2022).

3. Obfuscation Techniques

Similar to cash, there are users who value the anonymity of their transaction. They may have a legitimate interest such as privacy, but also an illegal interest, for instance to conceal crimes, launder money, circumvent sanctions or raise funds for terrorist organizations. It is therefore necessary to examine whether such illegal activities can be reduced by market intervention. As in the use and regulation of cash, there is a tension between competing priorities when weighing the trade-offs.

Various obfuscation procedures are used to anonymize transactions, which make it time-consuming and almost impossible, though technically possible, to track the path taken by the money. One frequently used method is *layering*, i.e. making transactions artificially complex to make it more difficult to trace funds. A systematic difference to the fiat world, is the possibility of conducting a large number of transactions in very small parts, and very quickly. This makes tracking more difficult and simplifies circumventing any thresholds that might trigger suspected money laundering reports. This is usually done using so-called mixers and tumblers.

In this paper we only consider ways to obfuscate transactions before the *off-ramp* (i.e. on the blockchain), since those after the off-ramp are not different from conventional methods known from the world of fiat currencies.

3.1. Mixers and Tumblers

Specialized service platforms offer one possibility to anonymize transactions: they are called mixers (sometimes tumblers). They mix one user's money with another user's and then return the sum – possibly minus a service fee.[17] However, payouts are done from other wallets, so that there is no logical connection (on-chain link) to the deposit. This deliberate decoupling makes it almost impossible, without access to the internal information of the mixer, to trace the path taken by the transaction. To further complicate mapping the transaction to a user, payouts are often split up at random in various amounts and at various times. At times, payouts are sent to various other wallets of the depositor.

However, the various types of mixers share a systematic vulnerability: mixing and decoupling funds no longer works when individual users deposit very large amounts, as a large part of these amounts is returned to them.

Since 2020, the use of mixers initially increased considerably and has now stabilized at a high level.[18] A significant proportion of the increase is due to transactions from wallets whose connection to illegal activities[19] has been well documented.[20] Their share alone in all transactions moving into mixers, as observed by Chainalysis, a company specializing in blockchain analysis, amounted to 23 percent at the end of the reporting period on 14 July 2022[21].

In most countries, mixers are not prohibited. However, their operators are sometimes subject to legal requirements, just like traditional financial service providers, but they usually do not comply with them. Recently, regulators and law enforcement agencies have taken several steps against mixers, see Section 5.2 (Sanctions).

The activities and users of mixers are not only interesting to law enforcement and financial authorities. They also play a role in foreign and security policy. For example, some cybercriminal groups are affiliated with state intelligence services on the one hand, and with Darknet marketplaces such as Hydra on the other, and these in turn are connected to mixers. It is probable that hacker attacks for information gathering, influencing, or destabilizing purposes are ordered, paid for, and concealed in this way. Other hacker attacks most likely serve to attain money in the form of cryptocurrency for the purpose of circumventing sanctions and raising funds,[22] including for nuclear programs.[23] A basic distinction is made between centralized and decentralized mixers.

In the case of **centralized mixers** (also called *custodial* mixers), the service is provided by a platform that charges a service fee. Some mixers vary the amount of this fee from transaction to transaction to disguise the use of their service. However, the user must trust the platform and its willingness to repay, as he must temporarily cede control over his money

17 Typically, this fee is one to three percent of the transaction total (Allison, I., 2015).

18 Chainalysis (2022a).

19 According to the definition used by Chainalysis, this includes Terrorism financing, theft, scams, sanctions, extortion software (ransomware), administrators of cybercriminal networks, fraudulent online trading, trading in the Darknet, and child pornography. The most significant volume moving to mixers is from perpetrators associated with sanctions and ransomware (Chainalysis, 2022a, Figure: Quarterly value sent to mixers from illicit addresses by category). Especially the Russia-based Darknet marketplace Hydra as well as the North Korean hacker group Lazarus and the mixer Blender.io, which was itself sanctioned, have already sent large amounts of money to mixers this year.

20 Chainalysis (2022a).

21 Ibid.

22 In the year 2022 alone, the North Korean hacker group Lazarus is believed to have stolen over USD1 billion worth of cryptocurrency, with the main target being decentralized, blockchain-based financial markets (Decentralized Finance, DeFi). In addition to a variety of minor thefts, Lazarus is behind spectacular cases such as the 2022 theft of USD600 million from an online gaming platform (Berwick, A. & Wilson, T., 2022a) and the attempt to steal almost a billion dollars from the Bank of Bangladesh in 2016.

23 United Nations Security Council, (2019), p. 49.

to the platform. In addition, the platform must, at least until the conclusion of the payout, document which amounts have been deposited and paid out, when and in which wallets, so that the money can be returned, and fees can be charged. If law enforcement authorities gain access to this data, for example by seizing servers, the transaction can be de-anonymized. In addition, there is at least theoretically the possibility that governmental investigators might have set a trap, also known as honeypot.

As an alternative to mixers, **decentralized** (or *non-custodial*) **mixers** are used to reduce the risk of de-anonymization and possibly to address mistrust toward any intermediaries. They do not need a platform as a central intermediary and are software-based, partly also integrated in wallets. They are also subdivided into different kinds. In a **peer-to-peer mixer**, the funds are pooled without an intermediary, mixed and then paid out again. **CoinJoin mixers**, also known as privacy wallets, allow user groups to mix their assets and have them returned in a series of transactions without using a central server and without having to cede control over the funds to others. This variant has gaining popularity among criminal users for years.[24] **Smart Contract mixers** confirm the authorship of a transaction's sender using an encrypted receipt. Later, the sender can use this receipt to send another transaction to the mixer from another wallet and thus transfer money to that other wallet. In contrast to centralized mixers, there is no documentation of the transaction history that could become known if the servers were seized. Nor can a legal or natural person acting as an intermediary be held legally responsible or be sanctioned.

3.2. Privacy Coins

In addition to classic cryptocurrencies, such as the intrinsically transparent Bitcoin and Co., there are cryptocurrencies that already have anonymization technology built into their code. This group is referred to as *privacy coins*, sometimes also known as *dark coins,*[25] or *Anonymity Enhanced Cryptocurrency* (AEC). Two well-known representatives are Monero and Zcash.

With **Monero**, the anonymization technology cannot be disabled. It uses one-time addresses as well as grouping with older transactions and a technique that conceals the amount. With **Zcash** it is at least possible to make the existence of a transaction transparent. So-called zero-knowledge proofs – mathematical verifications of a computation – can confirm a transaction without disclosing the wallets or transaction volumes. The cryptocurrency **Polkadot** acquires the property of a privacy coin only when combined with the so-called Phala network.[26]

Of course, there may be legitimate reasons for using *privacy coins*.[27] Nevertheless, criminals have clearly have utilized these coins as well. Since these cryptocurrencies make tracking transactions virtually impossible, various nations (e.g. Japan) have completely banned their use out of concern about the use by organized crime.[28] In Australia and South Korea, privacy coins may not be traded through trading platforms that allow the exchange of one cryptocurrency currency into another or into fiat money (so-called *cryptocurrency exchanges*). Countries are also reacting on a technical level: for example, in 2020, the *Internal Revenue Service* (IRS) offered a $625,000 prize for deciphering Monero transactions.[29] This endeavor must have been a success, because in the meantime patents on this subject have been submitted.[30]

Bitcoins were originally the opposite of privacy coins, as their transactions are completely public and transparent. Since the Taproot update in November 2021, "private Lightning Network transactions"[31] have been possible with advanced features that look like ordinary transactions. However, they are not as opaque as *privacy coins*.

3.3. Crypto Exchanges

Cryptocurrencies are traded on cryptocurrency exchanges where they can be exchanged for other cryptocurrencies or fiat currencies. Exchanges can be centralized (*custodial*, with *hosted wallets*) and decentralized (non-custodial with self-custody wallets). The former maintain the private key and have control over users' money (and can therefore freeze suspicious deposits) as well as the responsibility for protecting it against theft by hackers. The latter let users keep control over their deposits and do not assume any responsibility to protect them.[32]

In the fight against crime and money laundering, decentralized crypto exchanges are a challenge because trading is organized via software code (smart contracts) and no central authority carries out KYC protocols. However, even centralized crypto exchanges can hamper or prevent effective investigations and prosecution if they do not cooperate, do not use,

24 Robinson, T (2020).
25 Until 2015 the privacy coin Dash was called Darkcoin.

26 Bylund, A. (2022).
27 Ibid.
28 Seth, S. (2019).
29 SAM.gov (2020).
30 Sinclair, S. (2020).
31 Hertig, A. (2021).
32 But this is no longer a deterrent to many users, as decentralized exchanges have become much more user-friendly over the last three years.

or comply with KYC protocols and therefore do not know their users. One striking example is the Binance crypto exchange, which initially did not carry out any identity checks. Internal comments by founder Zhao in 2017 raised the question whether this was done deliberately to gain market share.[33] It was sufficient to enter any e-mail address to create a wallet.[34] The company delayed introducing identification functions and their implementation seemed to be deficient at times.[35] Not until August 2021 did Binance require new customers to present a picture ID, after England[36] and Japan banned their business.[37] Binance deals, among others, in *privacy coins* such as Monero, and in the past has been heavily frequented by users of the Darknet platform Hydra.[38] Binance was also used to launder funds from large-scale theft and fraud cases (such as an investment fraud that hurt many retirees in Germany).[39]

33 "Do everything to increase our market share, and nothing else," see Berwick, A. & Wilson, T. (2022a).
34 Ibid.
35 Reuters reports that in one case, for example, Binance accepted three identical copies of a restaurant bill as proof of identity (ibid.).
36 Reynolds, K. (2021).
37 Crawley, J. (2021).
38 Berwick, A. & Wilson, T. (2022a).
39 Ibid.

4. Uses for Illegal Purposes

Blockchain-based technology and its applications are increasingly intertwined with financial markets. As technology matures and despite high price fluctuations, cryptocurrencies are increasingly accepted and seem to develop into an independent asset class for risk-seeking investors. Analysts expect this trend, coupled with increased monitoring of illegal transactions, to result in a reduction of their relative share despite the absolute growth of illegal transactions. According to current estimates, illegal transactions account for only 0.15 percent of all cryptocurrency transactions.[40]

4.1. Forms of Illegal Transactions with Cryptocurrency

When discussing the use of cryptocurrencies for illegal purposes, one can generally differentiate between "*crypto-native crime*," which is carried out on the blockchain itself (such as hacker attacks to steal cryptocurrency)[41] and "off-chain crime" (in this case the blockchain only acts as a medium of payment for illegal crimes, e.g. to pay ransom money or a drug delivery). The following are brief descriptions of various areas of criminal use.

Cryptocurrencies were used for payment purposes on marketplaces in the *Darknet* as early as the beginning of cryptocurrency. Silk Road marked the beginning in 2011, and in 2015 Hydra became another very well-known platform.

Since then, small-time criminals and also their customers have used cryptocurrency for transactions. As in organized and serious crime, they do not completely replace fiat currencies,[42] but nowadays almost all areas of profitable crime[43] have contact with cryptocurrency.

There can be **fraud** with the cryptocurrency itself or it can be used merely as a medium of payment. For example, especially in 2019, fraud was a focus area of cryptocurrency-related crime, and it continues to play an important role.[44] It affects investors and users who are misled by means of various scams into making payments. One example are snowball systems, where a deliberate hype is created around a currency that is said to be gaining a great deal of value. Initial investors receive distributions of money from investors who follow them and who may have even been recruited directly by them. After some time, these systems collapse, revenues are absorbed by the initiators, and most investors lose the capital they invested. Until that point, Messenger apps, such as Telegram, are used to keep investors on board. Another criminal application are fraudulent merchant sites on the Internet, so-called fraud shops.[45]

Ransomware attacks are hacker attacks in which victims' sensitive data is encrypted and sometimes stolen. The data may be returned after payment of a ransom or not at all.[46] The attackers usually require ransom payments in the form of cryptocurrency.

The above-mentioned crypto exchanges are subject to repeated **thefts** and 2021 was a record year in that respect.[47] This also applies to the area of *decentralized finance* (DeFi) with its decentralized platforms, which many users consider safe because of the absence of custodial intermediaries and the *blockchain's* transparency. In fact, the irreversible nature of *blockchains* creates considerable difficulties in recovering any ransom money or even freezing it without central intermediaries.

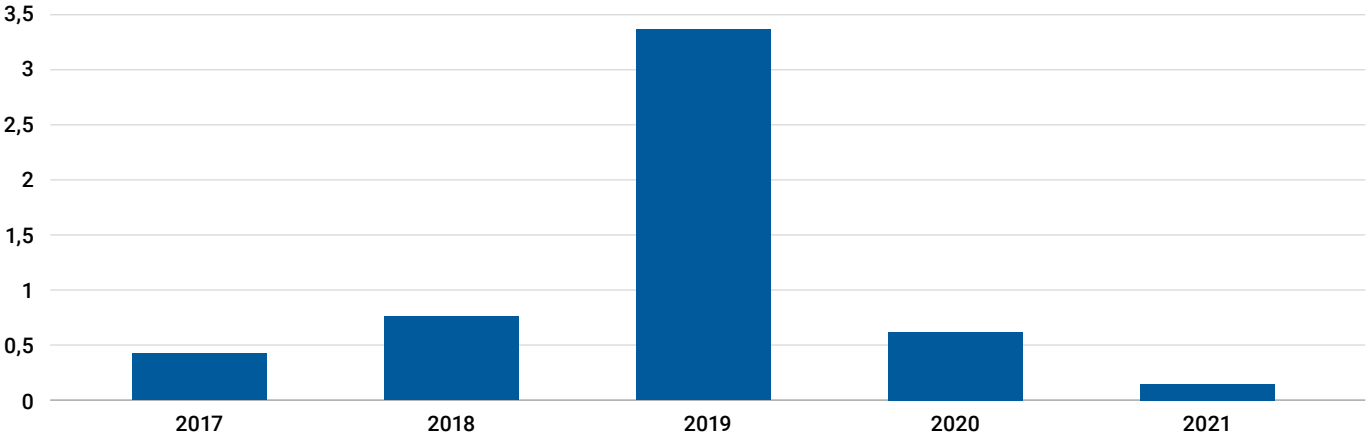
The area of crypto exchanges and *cross-chain bridges* – bridges to convert currencies of incompatible *blockchains* – always poses a risk due to complex and partly incomplete coding done by dynamically developing start-up companies and FinTechs.[48]

Typical schemes are so-called code exploits that take advantage of bugs in computer code .[49] When developers deliberately build such errors into the program to be used as back doors, they are called a *rug pull* (also called: *exit scam*). They are not easy to distinguish from other forms of fraud due to the pseudonymous nature of the transactions. With *admin key exploits*, developers deliberately install back doors that allow updates to *smart contracts* or the management of reserves, but those back doors can be misused when discovered by criminals.

The exploitation of programming vulnerabilities in so-called *economic exploits* is different. In this method, developers use unexpected properties, mainly in combinable *tokens*, in order to enable, for example, sudden short-term value manipulation

40 Chainalysis (2022b), Chainalysis (2022c), p.4.
41 Owners of cryptocurrency are not only found on the criminal side, but are often victims, for example of theft in connection with hacking or fraud in connection with scamming.
42 Europol (2021), p.2.
43 According to an expert from the German Federal Office of Criminal Investigations, in a background conversation on August 08, 2022, the increased use of cryptocurrencies by criminals coincided with the discussion of the topic in broad media coverage and social media. There had been, said the expert, a particularly strong increase over the last three years. In addition to organized money laundering and cybercrime, drug dealers in street trading can now get paid in cryptocurrency.
44 Chainalysis (2022d).
45 Collins, J. (2022), p. 18.
46 Chainalysis (2022d).
47 Ibid.
48 Elliptic (2021), p. 15.
49 Elliptic (2021), p. 17 f.

Figure 2 | Share of illegal use in crypto transactions 2017-2021 (in percent)



Source: Chainanalysis 2022c

and arbitrage transactions. The *blockchain* analytics company Elliptic explains and gives examples of these various schemes in their DeFi report.[50]

Non-fungible tokens (NFT) allow forms of market manipulation to the detriment of other participants.[51] One example is a form of sham trading, so-called *wash trading*.[52] In this form of market manipulation, the perpetrator is both the seller and the buyer side but is pretending to trade with other participants. This creates the impression of high demand and trading frequency for the token, which some trading platforms reward financially using special incentive systems, so-called *native tokens*. These, in turn, can be used by the perpetrator (*staking*) to generate even more trade volume. The price of the original token is artificially inflated. On the one hand, the perpetrator obtains the rewards granted by the platform operator, on the other hand he tricks other market participants into believing the excessive liquidity of the token he holds (and sells it at an inflated price, if necessary). However, this scheme is only worthwhile if the revenue exceeds the fees charged by the platform operator per transaction (*gas fees*).[53]

4.2. Extremism and Terrorist Financing

A particularly serious area – though not quantitatively significant – in which cryptocurrencies can be used for criminal purposes is the financing of terrorist groups.[54] Terror organizations have repeatedly called for donations. In view of what has been identified in recent years on the Bitcoin *blockchain*, it can be assumed that – compared with other areas – the amounts collected are smaller than a few thousand Euros each. No major increases in transaction volumes were observed on the Bitcoin *blockchain* following requests for donations, and there have been no major seizures since 2020. Europol also describes the number of cases involving cryptocurrencies for the financing of terrorism as manageable.[55] However, it typically does not require large sums of money to carry out attacks when weapons, explosives, vehicles or travel need to be financed.

Cryptocurrencies are used by terrorist organizations for crowdfunding and fundraising as well as for (sometimes legal) online shops. Since 2017, extremist online shops have barely used traditional payment service providers such as PayPal, Klarna or Mastercard, but have switched to cryptocurrency. There are significant developments in the choice of preferred cryptocurrency by extremists and terrorists, who use Bitcoin much less today than they did three years ago.[56] Now they prefer *privacy coins* like Monero, Zcash and Dash. Because of their properties, *blockchain* analysts cannot monitor them – at least not to the same extent as Bitcoins, Ether, and other established cryptocurrencies.

According to Chainalysis, at least ten terrorist organizations have used or attempted to use cryptocurrencies for their funding in recent years, including al-Qaida, the so-called Islamic State, and Hamas.[57] They ask for donations in classic social media such as Facebook and through channels in messenger services such as Telegram.[58] In the past, even software used

50 Elliptic (2021), p. 18 f.
51 In contrast to the blockchain units of the respective cryptocurrency, an NFT is unique, not interchangeable or divisible. It stands for a digital or even physical object. For example, it could be a plot in a virtual world or a work of art.
52 Similar forms of market manipulation are called painting the tape and churning.
53 Chainalysis (2022e).
54 Eisermann, D. & Schindler, H.-J. (2020).
55 Europol (2021), p.2.
56 In a background conversation on August 22, 2022, an experienced diplomat and adviser in the foreign and security environment pointed out that these trends have been observed mainly in the areas of right-wing extremism and Islamism. According to the expert, no such trends were observed in the ransomware realm because those demanding ransom money are targeting companies, institutions, and persons not otherwise familiar with such transactions. The value of ransom demands in Bitcoin is easier to assess, and there is more widespread knowledge about the technical implementation of transactions in Bitcoin than in more exotic and recent cryptocurrencies.
57 Chainalysis (2022) The 2022 Crypto Crime Report, p. 92 ff.
58 Ibid., p.93.

to automatically generate wallet addresses has been used for fund-raising calls.[59]

However, provided that the currencies used are not *privacy coins*, the funds can often be seized in good time before they can be exchanged into fiat currencies on crypto exchanges. This was achieved in Israel, for example, with deposits in Bitcoin, Ether, Tether, XRP, and other currencies.[60]

Although the main sources of income of terrorist organizations are diverse and are more likely to be *off-chain* (drug trafficking, extraction of raw materials, extortion, human trafficking, etc.), it is much easier to monitor and freeze transactions on *blockchains* than to interfere in areas of cultivation, extraction sites, etc. This approach should therefore be used more intensively than previously.

4.3. Money Laundering

Cryptocurrencies have been of interest to money launderers from the very beginning, despite the technically almost complete, clear, and transparent documentation of the transaction history in the various *blockchains*. Last year, an estimated USD8.6 billion was laundered using cryptocurrencies, 30% more than in the previous year.[61] At first, the reason may have been the pseudonymisation as well as the apparent complexity of the new technology. In addition, *layering* – used in analog money laundering as well – can be multiplied much more easily in digital and encrypted transaction traffic, and transactions can be branched. Investigating agencies were not yet up to the task due to a lack of qualified personnel and technical capabilities.

As with any new technology adopted by criminals, a race between the two sides is developing as cryptocurrencies become more widespread. Since then, partnerships between investigative agencies and specialized companies have made it possible – though with considerable effort – to use the "*follow the money*" strategy to track many cryptocurrencies.

The functionalities of *privacy coins* and mixers take the technical challenge for investigative agencies to a new level. The de facto anonymization that these tools currently offer ensures that money launderers enjoy a period of immunity from prosecution – unless legally usable data is collected later and documented within the limitation periods. This tide will likely turn again with the arrival of quantum computers, but legislators, executive and judicial authorities should be interested in this topic early on.

4.4. State-Sponsored Actors, National Security

The situation is more difficult if the criminals are so-called state-sponsored actors. Even if investigative agencies can more successfully trace hacker attacks and track transactions in the future by using quantum computers or other advanced capabilities and resources, they often reach their limits when perpetrators or servers with data relevant to investigations are located in sovereign states that do not cooperate with the German authorities.

Such states may be interested in, among other things, instrumentalizing hackers who are not in public service, particularly competent and who rent out their services to the highest bidder. These states can then use these hackers for geopolitical purposes, either for destabilization and hybrid warfare or espionage. The states want to pay these hackers in a secure and deniable manner.

States that are themselves subject to sanctions may have two additional motives: On the one hand, they may want to carry out transactions with embargo-breaking trading partners, either when their banks are excluded from the international financial system (such as the SWIFT system)[62] or if, despite the possibility of regular transactions, they wish to make a transaction as opaque as possible.

On the other hand, states may be motivated by trying to procure financial resources for themselves, if they cannot access their treasury because they do not have enough foreign exchange reserves or because they need to cover expenses from non-controllable budgets.

Both the undiscovered breach of embargoes by concealing trade and service-related transactions, facilitated by the use of cryptocurrency-based concealment procedures, and covert fundraising for such transactions can pose challenges for national and international security. These funds can be finance the continuation and expansion of nuclear weapons programs.

The assumption that cryptocurrencies could be used in significant volumes by states or state-sponsored actors to circumvent sanctions or to obtain financial resources, has not been sufficiently verified up until now. At least beyond *privacy coins* and mixers, there are only limited indications that Russian oligarchs, who are subject to sanctions, would be moving large sums of money.[63] Moreover, there were no significant

59 Eisermann, D. & Schindler, H.-J. (2020) p. 4.
60 Ibid., p. 94.
61 BBC (2022).

62 SWIFT stands for the Belgium-based Society for Worldwide Interbank Financial Telecommunications. An exclusion makes foreign trade transactions considerably more difficult. At the moment, against the backdrop of the Ukrainian conflict, Russian banks are excluded from the SWIFT system. Due to their nuclear weapons programs, Iranian banks have been excluded since 2018 (and from 2012 to 2016) and North Korean banks since 2017.
63 Nestler, F. (2022).

developments in cryptocurrency values associated with the Russian attack on Ukraine.[64] And while Iran is indirectly promoting intensive *mining* of cryptocurrencies in the country by subsidizing electricity, the volume is not sufficient to stabilize the country's economy.[65]

It should not be forgotten that cryptocurrencies, precisely because they do not use intermediaries, create a way of supporting dissidents in totalitarian states by, for example, helping them to secure their assets when they are on the run. This may be the reason why the People's Republic of China has banned all cryptocurrency transactions in the past year[66] and is working on developing the renminbi as a "further building block in the digital surveillance state".[67]

64 This assessment was made in an informal meeting on August 22, 2022, by Dr. Hans-Jakob Schindler, Senior Director Counter Extremism Project and an expert in sanctions and the fight against terrorist financing.
65 Ibid.
66 Wurzel, S. (2021).
67 Hilgers, S. & Greilich, K. (2021), p. 22.

5. Approaches in Fighting Money Laundering

For years, money laundering related to cryptocurrencies has been a major challenge for regulators, government agencies, and financial sector companies. Relevant laws and regulations have been enacted on a national, supranational, and international level, the most important of which are briefly outlined below. In addition, there are promising developments in the area of investigation and prosecution, which up until now have reached their limits when confronted with mixers, privacy coins and decentralized crypto exchanges.

5.1. Regulation

Regulation is done through laws and regulations directed at natural and legal persons. However, in the absence of intermediaries such as banks, crypto exchange operators – as is often the case in *blockchain*-based transactions – regulation can at best outlaw the use of the technology or certain applications (such as decentralized mixers without a customer database and KYC protocols, decentralized crypto exchanges, or *privacy coins*). Thus, there is a tension between classic financial regulation and technology-related regulation, where new ways and creative approaches are needed.

Currently, efforts to regulate cryptocurrencies are focused on the high energy requirements of the *proof-of-work* process (which is not a subject of this overview) and on combating money laundering and terrorist financing.

One topic common to all regulatory efforts is the obligation to establish and comply with *Know-Your-Customer* (KYC) protocols, i.e. the verification of new customer credentials, including the collection of personal identification and business data.

One regulatory challenge can arise from the geographical location of actors and thus the limits of jurisdiction. In 2020, for example, more than half of all crypto exchanges were registered in the Republic of Seychelles.[68]

The following section discusses the currently most important regulatory aspects, particularly in Germany, the European Union, and the United States.

5.1.1. National

In the **United States**, crypto exchanges are regulated by the *Bank Secrecy Act* (BSA, 1970), which mandates registering operators with the *Financial Crimes Enforcement Network* (FinCEN)[69] and implementing anti-money laundering (AML) controls. Another relevant piece of regulation is the *National Defense Authorization Act* (NDAA) of 2021, which integrates the *Anti-Money Laundering Act* of 2020 and reforms *counter-terrorist financing* (CTF). Moreover, financial institutions in the USA must comply with the *Travel Rule* issued by *the Financial Action Task Force* (FATF, see below).

Beyond that, regulation remains patchwork – the *US Securities and Exchange Commission* (SEC) considers cryptocurrencies as securities, with corresponding regulations for wallets and crypto exchanges. The US regulator for futures and options markets (*Commodities Futures Trading Commission*, CFTC), on the other hand, considers Bitcoins to be a commodity which may be publicly traded, including their derivatives.[70]

The U.S. Treasury is working on regulating so-called *unhosted wallets* that can be kept offline and are therefore difficult to control. Currently under discussion are reporting requirements for transactions over USD 10,000 per day[71] and a requirement for banks to collect information on the parties involved above a threshold of more than USD 3,000.[72]

Under **Germany's** Kreditwesengesetz (KWG - German Banking Act), providers of cryptocurrency services must have a crypto custody license, which they can request from the Federal Financial Supervisory Authority (BaFin).[73] This regulation

68 Ciphertrace (2020).

69 FinCEN is a bureau of the U.S. Department of the Treasury that combats domestic and international money laundering, terrorism financing and other financial crimes by collecting and analyzing information about financial transactions.
70 Complyadvantage.com (2022).
71 Thomas, D. & Rossow, A. (2022).
72 Ibid.
73 Huemer, S. (2022).

applies both to the safekeeping business as well as other "services with crypto values".[74] In addition, the Geldwäschegesetz (GWG – German Anti-Money Laundering Act), which defines the obligated parties in §2, is significant for the on- and *off-ramp*.[75]

5.1.2. International and Supranational

The multinational organization FATF makes recommendations for curbing money laundering, financing of terrorism, and proliferation of weapons of mass destruction. In 2019, the FATF updated their Recommendation 16, known as the **Travel Rule**, by adding that virtual asset providers should exchange the user data of beneficiaries and originators with each other when conducting transfers and share this information with law enforcement authorities upon request (**Crypto Travel Rule**).

There is no specific regulatory framework at European Union level, but two regulatory initiatives are underway: Markets in Crypto-Assets Regulation (**MiCa**) and the **Transfer of Funds Regulation** cover crypto-related services.[76] The question of jurisdiction has been the subject of dispute over the past few months, as there are currently no clear rules on the circumstances under which the European Securities and Markets Authority or national authorities of the member states are responsible. The *European Securities and Markets Authority* (ESMA), which will maintain and publish a blacklist of cryptocurrency service providers without authorization, will now be responsible for leading the implementation of the planned MiCa.[77] The regulation of NFT and *decentralized finance* (DeFi) remains open for the time being.

The current agreement on money transfer regulation[78] extends the scope of existing rules to crypto values and stipulates that "crypto platforms will have to collect information about senders and recipients when conducting transactions"[79] and will have to share this information with authorities in the context of money laundering or terrorism investigations. This is expected to apply regardless of the amount, whereas a threshold of EUR 1000 is being considered for *unhosted wallets*. The aim is to manage the "risks of money laundering and terrorist financing" through the "traceability of crypto-asset value transfers."[80] However, direct transfers between holders of platform-independent crypto wallets or deposits" remain unaffected.[81]

The current fifth **European Anti-Money Laundering Directive**[82] requires "crypto exchanges to verify the identity of their own customers."[83] An EU anti-money laundering authority is currently in the planning stage, which would be able to take control in the event of a substantial risk of money laundering.[84]

5.2. Sanctions

Sanctions are another crucial tool for curbing criminal uses of cryptocurrencies. Sanctions were imposed on the hacker group Lazarus in 2019[85] the Bitcoin mixers Helix and CoinNinja in 2020[86] and Bitcoin Fog on the basis of registration and licensing regulations in 2021.[87] Also in 2021, crypto broker Suex, based in Moscow and St. Petersburg, was sanctioned for its links to ransomware extortionists, fraud and darknet platforms.[88] In 2022, mixers were sanctioned for the first time. The first was the centralized, *custodial* mixer Blender.io.[89] A short time later, the *non-custodial* Ethereum mixer Tornado Cash was sanctioned.[90] The U.S. *Office of Foreign Assets Control* (OFAC) added it to its SDN List,[91] specifying 38 crypto addresses.[92] As with Blender.io, there was a connection to the North Korean hacker group Lazarus,[93] and stolen crypto values were laundered on a large scale. This move, in turn, mobilized critics and led to a lawsuit by the largest US crypto-exchange platform, since the target of the sanction, for the first time, was not a natural or legal person, but rather software.[94]

However, according to a think tank employee specializing in cryptocurrencies, sanctioning software code and protocols – which ultimately amounts to a ban on the use of software by citizens and businesses in the sanctioning nation – is a less direct strategy than sanctioning natural or legal persons

74 Federal government of Germany (2022), p. 2 f.
75 In connection with reporting obligations, cryptocurrencies' high level of volatility makes defining value thresholds problematic.
76 European Council (2022a).
77 Institutional-money.com (2022).
78 European Council (2022b).
79 Mussler, W. (2022).
80 European Council (2022b).
81 Mussler, W. (2022).
82 European Union (2020).
83 Huemer, S. (2022) Neue Regeln für den Bitcoin.
84 Mussler, W. (2022) Kryptotransfers auf der Spur.
85 Berwick, A. & Wilson, T. (2022a).
86 Authority implementing the measure: FinCEN (Financial Crimes Enforcement Network, USA).
87 Authority implementing the measure: DoJ (Department of Justice, USA).
88 Chainalysis (2021).
89 U.S. Department of Treasury (2022).
90 Authority implementing the measure: OFAC (U.S. Treasury's Office of Foreign Assets Control, USA).
91 Specially Designated Nationals And Blocked Persons List.
92 Authority implementing the measure: OFAC
93 The Lazarus group, which is alleged to be acting on behalf of the North Korean intelligence agency bureau 121, is also behind the theft of USD5.4 million on a Slovak crypto exchange (Berwick, A. & Wilson, T. (2022a).
94 Newmyer, T. (2022).

for whom such a measure entails economic disadvantages.[95] This strategy must be considered untested at this stage because it is the first and only such sanction of its kind that has been imposed. Time will tell whether it proves its worth. This strategy is also complicated to enforce. First, there may not be a single living person responsible for the day-to-day operation of the protocol. Secondly, there is a delicate prospect of dealing with a large number of non-criminal users who often interact with the protocol anonymously.

The aim of sanctions is mostly to obstruct the *off-ramp* by isolating sanctioned entities from compliant financial services providers. For example, U.S. citizens and companies are no longer allowed to have business relationships with sanctioned entities when they are listed on the SDN list.

5.3. Investigation and Prosecution

New forms of crime and transactions caused great difficulties for investigators in the early years of illicit cryptocurrency uses, but considerable progress has been made. Particularly in the United States, agencies such as the *Federal Bureau of Investigation* (FBI) and the *Internal Revenue Service – Criminal Investigation* (IRS-CI) unit have established extensive skill sets. Systematic cooperation with companies specializing in *blockchain* analysis has also proven to be effective. These companies are all located in the USA.[96]

Another target of investigation are the favorable conditions for crime: for example, U.S. federal investigators have asked the world's largest exchange platform, Binance, to release extensive information regarding internal communications and audit procedures. Binance is associated with a lack of, and later lenient, KYC protocols as well as large-scale money laundering.[97]

In Germany, the Federal Criminal Investigation Office is increasing its expertise. However, organizational obstacles remain, such as adapting to the international nature of the crime and the lack of clear jurisdiction between the German agencies.[98] Investigations are carried out not only by Internal Affairs, but also Finance. According to the German Federal Government's response to a parliamentary question from the Parliamentary Group Die Linke, the *Financial Intelligence Unit* (FIU), which is part of the German Customs Office, received nearly ten times more suspected money-laundering reports on cryptocurrency in 2021 than in 2018.[99]

The Federal Ministry of Finance envisions the FIU to be integrated into an independent agency, the "Federal Investigation Office for Financial Crimes." In this new Federal Agency, competences would be bundled in four pillars: Firstly, an area of investigation with genuine investigative powers; secondly, the control and enforcement of sanctions. Thirdly, the anti-money laundering unit FIU would be integrated into the new Federal Agency. The fourth pillar is a central body for supervision in the non-financial sector tasked with coordinating state-level responsibilities and defining standards.[100] The creation of this central federal agency should also significantly strengthen the ability to identify illegal activities using cryptocurrency.

There are also promising developments in the private and technical sector. One such development could be called "Compliance Plus." Innovative start-ups develop compliance strategies and advise companies in the financial sector on implementation.[101] In addition to list-based controls, customer interviews, and checking off checkpoints, which rarely lead to timely detection of violations, proactive procedures are used. FinTech companies, in particular, are able to identify dubious patterns of behavior and fake identities at an early stage, thanks to their connection to the Internet using openly available parts of social media and other sources.[102] Another benefit could come from advances in quantum computing in conjunction with the complete documentation in the *blockchains*. This could allow, at a later stage, identifying forensic timelines and subsequently using available computer resources to clear up past obfuscations.

95 This point was raised by Yaya J. Fanusie, Adjunct Senior Fellow at the Center for a New American Security, in a background conversation on August 30, 2022.
96 The best-known are Chainalysis, CipherTrace, Elliptic and TRM Labs, as well as Tracer from Coinbase.
97 Berwick, A. & Wilson, T. (2022b).
98 Source: Background conversation with Saleh Altuntas on August 8, 2022.
99 Federal government of Germany (2022), p. 5.
100 Bundesfinanzministerium (German Federal Ministry of Finance) (2022).
101 One example is the German consulting firm BerFin.
102 Source: Background conversation with Dr. Hans-Jakob Schindler, Senior Director Counter Extremism Project, on August 22, 2022.

6. Recommendations for Action

Regulation to Shape the Market:

The regulation of markets is intended to ensure their efficiency in allocating scarce resources. One essential element of efficient market operation is that market participants need to be **confident** that transactions are carried out in a fair and legal manner. Protecting consumers and capital market investors is a valuable asset. This is particularly true for markets with considerable information asymmetries. At the same time, they must not be used as a fig leaf for excessive restriction of consumer freedom.

As in the traditional financial sector, profit-oriented companies in the cryptocurrency sector may deliberately accept **compliance** penalties to some degree for business reasons. Good implementation and enforcement of regulations must motivate the sector to comply as much as possible.

Another aspect of efficient **financial markets** is financial stability. The 2008 financial crisis showed that capital markets, from a certain size onwards, need regulation and monitoring to avoid creating cascading risks for the entire financial system. Nations regulate markets to prevent **tax evasion**, money laundering, illegal trade, and terrorist financing.

Regulation Hopping:

Legislators and regulators are in a dilemma. On the one hand, the widespread use of cryptocurrencies for illegal transactions necessitates strict regulation of this market. On the other hand, it is precisely this regulation and the associated costs that lead such platforms and companies to locate their headquarters outside of the regulatory sphere and thus to completely evade regulation (so-called *regulatory arbitrage*). For example, Hong Kong was a popular location prior to the containment of cryptocurrency activities. Today, the Seychelles are one of the preferred countries for business domiciles.[103]

The US approach of banning its citizens and US companies from using such institutions in this case is a tool, but it is unlikely to deter people with sufficient criminal energy from using them. Such an approach can only be effective, especially for smaller countries, if it is possible to enforce a largely uniform regulation of crypto markets internationally. It is advisable for the US and the European Union to make regulation of cryptocurrencies and their marketplaces the subject of the Joint Trade and *Technology Council* (TTC). This is the appropriate forum to come up with and subsequently jointly implement coordinated regulatory policies for the two dominant economic areas.

Pooling of Expertise:

It is obvious, once again, that it is important in the digital world to pool expertise and skills in one place in what is an otherwise federally structured nation. This is absolutely necessary, not least of all because there is not enough human capital with the necessary qualifications in the labor market. The Federal Ministry of Finance's approach to create a Federal Investigation Office for Financial Crimes is therefore promising and should be implemented consistently.

A single point of contact may also motivate *blockchain* analysts to take up business in Germany instead of the US, as they recognize the demand in Germany. *Blockchain* experts would find it easier to establish their enterprises in Germany.

Areas of Technical Risk:

Mixers, *privacy coins* and decentralized crypto exchanges as well as *unhosted wallets* currently allow for largely unobserved transactions. To comply with the European Union's requirements for transparency, they must either be outlawed or investigative capabilities (including those of the public sector) must be considerably strengthened. It appears questionable whether the second approach can be implemented at all without (undesirable) extensive monitoring of Internet traffic.

One challenge will be the Metaverse on which NFTs will be traded in the future. This creates unregulated trading venues used exclusively for cryptocurrency values. Such venues pose a significant potential risk of money laundering.

Terrorist Financing:

Although no large transactions have been observed in the recent past, the financing of terrorism is of considerable import-

103 Source: Background conversation with Salih Altuntas on August 8, 2022.

ance because of its impact and must be vehemently stopped and combated.

Although the main sources of revenue for terrorist organizations are primarily *off-chain*, intervention on the *blockchain* level should be used more vigorously than in the past.

KYC:

Central crypto exchanges and other crypto service providers must be required to effectively comply with KYC protocols. They must share customer data with investigating authorities upon a court order.

A Balanced Approach:

Despite recent sharp price fluctuations experienced by leading cryptocurrencies, the proportion of those who use cryptocurrencies and blockchain technology for innovative and legal purposes is rising. The blockchain analysis firm Chainalysis reports the **proportion of illegal transactions** as only **0.15 percent**.[104] As important as it is to prevent or at least trace illegal transactions, the innovation potential of *blockchain* technology and the currencies based on it must not be unreasonably curtailed. It is for good reasons that cash is not banned just because it is used to pay for illegal transactions. And this despite the fact that cash's share is likely to be well above 0.15 percent. The same can be said about the *blockchain* that has been said about the internet and many other innovations: **an innovation is probably not very innovative if it is not used by criminals.**

Regulators should keep this in mind during considerations of legal interest and cost-benefit analysis – provided that price volatility does not cause legal market participants to leave the market in view of incalculable financial risks and business disadvantages, resulting in an increase of the relative share of dishonest users who remain due to the potential for concealment. Not least of all, an innovation-friendly business climate should be maintained within the regulator's jurisdiction.

Displacing financial service providers and platform providers through excessive regulation and control beyond this area of jurisdiction can also be counterproductive if, for example, companies react by moving their headquarters to offshore locations and law enforcement agencies no longer have access. On the other hand, lawless or de facto protected spaces for criminals must not be tolerated since the limitless nature of the internet would result in a high concentration of crime. The public would perceive this as government failure and legal cryptocurrency services would be negatively affected.

7. Future Outlook

There can be no doubt that cryptocurrencies will be more regulated in the future – at least those that, because of their market capitalization, are somewhat relevant to the stability of financial markets. If this reduces the volatility of crypto markets, it will increase their attractiveness.

Nations will push for taxation on profits and certain transactions. That alone requires deanonymization. Cryptocurrencies that feature anonymity as their central characteristic will be particularly targeted by regulators and investigating authorities.

The best way to make crypto money an efficient means of payment and capital investment is to create a digital currency tied to an issuer who is subject to the rules of a liberal constitutional state, who ensures monetary stability and puts transparent and high constitutional hurdles ahead of the deanonymization of a transaction. A cryptocurrency conceived in this way has considerable potential to become the tender of choice for legal transactions in economic competition. This would be a positive trend for cryptocurrencies, financial markets, and efforts to combat cross-border organized crime.

104 Chainalysis (2022b), p.4.

List of Abbreviations

AEC *Anonymity Enhanced Cryptocurrency*

AML *Anti-Money Laundering*

BKA Bundeskriminalamt *(German Federal Criminal Investigation Office)*

BSA *Bank Secrecy Act*

CBDC *Central Bank Digital Currencies*

CFTC *Commodities Futures Trading Commission*

CTF *Counter-Terrorist Financing*

DeFi *Decentralized Finance*

ESMA *European Securities and Markets Authority*

FATF *Financial Action Task Force*

FBI *Federal Bureau of Investigation*

FinCEN *Financial Crimes Enforcement Network*

FIU *Financial Intelligence Unit*

GWG Geldwäschegesetz *(German Money Laundering Act)*

IRS-CI *Internal Revenue Service – Criminal Investigation*

KWG Kreditwesengesetz *(German Banking Act)*

KYC *Know-Your-Customer*

MiCa *Markets in Crypto-Assets Regulation*

NDAA *National Defense Authorization Act*

NFT *Non-Fungible Tokens*

OFAC *U.S. Treasury's Office of Foreign Assets Control*

SDN *Specially Designated Nationals And Blocked Persons List*

SEC *U.S. Securities and Exchange Commission*

SWIFT *Society for Worldwide Interbank Financial Telecommunication*

USD U.S. Dollar

List of References

Allison, I. (2015). Bitcoin tumbler: The business of covering tracks in the world of cryptocurrency laundering. https://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480, last accessed in September 2022.

Anderegg, R. (2014). Grundzüge der Geldtheorie und Geldpolitik [Principles of Monetary Theory and Policy]. In Grundzüge der Geldtheorie und Geldpolitik. Oldenbourg Wissenschaftsverlag, p.19.

Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the open blockchain. Second edition. Sebastopol, CA: O'Reilly.

BBC (2022) Crypto money laundering rises 30%, report finds. https://www.bbc.com/news/technology-60072195, last accessed in September 2022.

Berwick, A. & Wilson, T. (2022a) How crypto giant Binance became a hub for hackers, fraudsters and drug traffickers. A Reuters Special Report. https://www.reuters.com/investigates/special-report/fintech-crypto-binance-dirtymoney/, last accessed in September 2022.

Berwick, A. & Wilson, T. (2022b) Exclusive: U.S. sought records on Binance CEO for crypto money laundering probe. https://www.reuters.com/technology/exclusive-us-sought-records-binance-ceo-crypto-money-laundering-probe-2022-09-01/, last accessed September 2022.

Bundesfinanzministerium (German Federal Ministry of Finance) (2022). Finanzkriminalität schlagkräftig bekämpfen [Fighting finance crime effectively]: Press statement by Christian Lindner. https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Video-Textfassungen/2022/textfassung-2022-08-24-finanzkriminalitaet-bekaempfen.html, last accessed in September 2022.

Bundesregierung [German Federal Government] (2022). The German Federal Government's response to the parliamentary question posed by Members Christian Görke, Dr. Gesine Lötzsch, Klaus Ernst, other Members of Parliament and the parliamentary group DIE LINKE. Printed Matter 20/2531.

Bylund, A. (2022) What Are Privacy Coins? https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/privacy-coins/, last accessed in September 2022.

Chainalysis (2021) Chainalysis in Action: OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over $160 million from Ransomware Attackers, Scammers, and Darknet Markets. https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021/, last accessed in September 2022.

Chainalysis (2022a) Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cybercriminals Contributing Significant Volume. https://blog.chainalysis.com/reports/crypto-mixer-criminal-volume-2022/, last viewed September 2022.

Chainalysis (2022b). Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity, https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/, last accessed in September 2022

Chainalysis (2022c) The 2022 Crypto Crime Report.

Chainalysis (2022d) Webcast: Crypto Crime in 2022: Everything You Need to Know Part 2. https://go.chainalysis.com/2022-crypto-crime-part-2.html, last accessed in September 2022.

Chainalysis (2022e) Theft, Money Laundering, and NFT Market Manipulation Underline Import of Safety and Compliance in Web3. https://blog.chainalysis.com/reports/chainalysis-web3-report-preview-safety-compliance-defi/, last accessed in September 2022.

Collins, J. (2022) Crypto, crime and control. Cryptocurrencies as an enabler of organized crime. https://globalinitiative.net/wp-content/uploads/2022/06/GITOC-Crypto-crime-and-control-Cryptocurrencies-as-an-enabler-of-organized-crime.pdf, last accessed in September 2022.

Complyadvantage.com (2022). Cryptocurrency Regulations Around The World. https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/#:~:text=Cryptocurrency%20exchanges%20are%20legal%20in,submit%20reports%20to%20the%20authorities, last accessed in September 2022.

Crawley, J. (2021) Japan's Financial Services Regulator Issues Binance Warning. https://www.coindesk.com/markets/2021/06/25/japans-financial-services-regulator-issues-binance-warning/, last accessed in September 2022.

Ciphertrace (2020) 2020 Geographic Risk Report: VASP KYC by Jurisdiction. https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/, last accessed in September 2022.

Eisermann, D. & Schindler, H.-J. (2020) Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges. https://www.counterextremism.com/sites/default/files/Cryptocurrencies%20as%20Threats%20to%20Public%20Security%20and%20Counter-Terrorism_ENG%20Translation_April%202020.pdf, last accessed in September 2022.

Elliptic (2021) DeFi: Risk, Regulation, and the Rise of DeCrime. https://www.elliptic.co/resources/defi-risk-regulation-and-the-rise-of-decrime, last accessed in September 2022.

European Council (2022a) Digital finance: agreement reached on European crypto-assets regulation (MiCA). Press release. https://www.consilium.europa.eu/de/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/, last accessed in September 2022.

European Council (2022b) Anti-money laundering: Provisional agreement reached on transparency of crypto asset transfers. Press release. https://www.consilium.europa.eu/de/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/, last accessed in September 2022.

European Union (2020) Directive (EU) 2018/843. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843, last accessed in September 2022.

Europol (2021), Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf, last accessed in September 2022.

Hayek, F. A. (2022). Law, Legislation, and Liberty: A New Statement of the Liberal Principles of Justice and Political Economy (Vol. 19). Routledge, first edition: 1973.

Hertig, A. (2021) Taproot, Bitcoin's Long-Anticipated Upgrade, Has Activated https://www.coindesk.com/tech/2021/11/13/taproot-bitcoins-long-anticipated-upgrade-activates-this-weekend/, last accessed in September 2022.

Hilgers, S. & Greilich, K. (2021) Four waves of digital currencies and the future of money. Policy Paper. Friedrich Naumann Foundation for Freedom, Potsdam.

Huemer, S. (2022) Neue Regeln für den Bitcoin [New rules for Bitcoin]. https://zeitung.faz.net/fas/wert-wohnen/2022-04-24/da7430e0bb876ac575e8baf1c672d39e/?popup=user.lf-ns, last accessed in September 2022.

Institutional-money.com (2022) Krypto-Einigung der EU bringt Schwarze Liste, Offenlegungszwang [EU crypto agreement brings blacklist, disclosure requirement]. https://www.institutional-money.com/news/regulierung/headline/krypto-einigung-der-eu-bringt-schwarze-liste-offenlegungszwang-216879/, last accessed in September 2022.

Menger, C. (1884). IV. Untersuchungen über die Methode der Sozialwissenschaften und der politischen Ökonomie insbesondere [Studies on the method of social sciences and political economics in particular]. Jahrbücher für Nationalökonomie und Statistik, 42(1), 353-370.

Mussler, W. (2022) Kryptotransfers auf der Spur [Tracking crypto transfers]. https://www.faz.net/aktuell/finanzen/eu-legt-in-geldtransfer-verordnung-erstmals-regeln-fuer-kryptotransfers-fest-18140664.html?premium=0xdb587ed22210c97da66f86d74aedebf4&GEPC=s5, last accessed in September 2022.

Nestler, F. (2022). Die zwei Seiten von Kryptowährungen [The two sides of cryptocurrency]. https://zeitung.faz.net/faz/finanzen/2022-03-12/e8e10fc85ea38439e177f2dc68655ca2/?GEPC=s9, last accessed in September 2022.

Newmyer, T. (2022) Crypto exchange targets Treasury sanctions in national security clash. https://www.washingtonpost.com/business/2022/09/08/coinbase-treasury-sanctions-mixers-/, last accessed in September 2022.

Reaume, A. (2022) Stablecoin: What It Is & List Of Top Stablecoins. https://seekingalpha.com/article/4468065-what-are-stablecoins?source=acquisition_campaign_google&internal_promotion=true, last accessed in September 2022.

Reynolds, K. (2021) Binance Isn't Allowed to Be Operating in the UK, Watchdog Warns. https://www.coindesk.com/policy/2021/06/27/binance-isnt-allowed-to-be-operating-in-the-uk-watchdog-warns/, last accessed in September 2022.

Robinson, T. (2020). „Crime Proceeds Being Laundered in Privacy Wallets." https://www.elliptic.co/blog/13-bitcoin-crime-laundered-through-privacy-wallet, last accessed in September 2022.

SAM.gov (2020). https://sam.gov opp/3b7875d5236b47f6a77f64c19251af60/view?index=opp, last accessed in August 2022.

Seth, S. (2019) Japan's FSA Bans Private Cryptocurrencies. https://www.investopedia.com/news/japans-fsa-bans-private-cryptocurrencies/#:~:text=Japan%20Imposes%20Ban%20on%20Private,of%20anonymity%2C%20according%20to%20CoinDesk., last accessed in September 2022.

Sinclair, S. (2020) CipherTrace Says Homeland Security Work Gave Rise to Monero-Tracking Patent Filings. https://www.coindesk.com/tech/2020/11/23/ciphertrace-says-homeland-security-work-gave-rise-to-monero-tracking-patent-filings/, last accessed in September 2022.

Stevens, R. (2022) What Are Privacy Coins and Are They Legal? https://www.coindesk.com/learn/what-are-privacy-coins-and-are-they-legal/, last accessed in September 2022.

Thomas, D. & Rossow, A. (2022) U.S. Treasury Department on Track to Regulate Unhosted Wallets. https://beincrypto.com/u-s-treasury-department-on-track-to-regulate-unhosted-wallets/, last accessed in September 2022.

United Nations Security Council, "S/2019/171: Report of the Panel of Experts established pursuant to resolution 1874 (2009)," Tech. Rep., 2019, p. 49.

U.S. Department of Treasury (2022) U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats. https://home.treasury.gov/news/press-releases/jy0768, last accessed in September 2022.

von Mises, L. (1949). Human Action – A Treatise on Economics.

Wurzel, S. (2021) China verbietet Kryptogeld-Handel [China prohibits cryptographic money trading]. https://www.tagesschau.de/wirtschaft/finanzen/china-kryptowaehrungen-101.html, last accessed in September 2022.