Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges

Dr. Daniel Eisermann
Berlin, April 2020
Translation by Dr. Hans-Jakob Schindler

BERLIN RISK

COUNTER EXTREMISM PROJECT

Legal Notice

Berlin Risk was commissioned by the Counter Extremism Project (CEP) with the present study. Every effort has been made to verify the accuracy of the information contained in this report. All assessments are based on an analysis based on the current situation and may change in the future. No liability is assumed for the correctness of the findings or recommendations made, nor for any unforeseen changes that affect the evaluations and recommendations of the study. Berlin Risk also assumes no liability for any claims and damages that result from the unauthorized disclosure of information contained in the report. Berlin Risk Ltd. also does not take on claims any liability for any direct or indirect loss that may be related to the content of the study or related communication.

Berlin Risk

Berlin Risk is a consulting company that supports clients in assessing political risks and fulfilling compliance requirements. This includes business partner audits and issues related to fighting corruption, money laundering, fraud and preventing tax evasion. Customers include financial institutions, companies and investors as well as public institutions, law firms and non-governmental organizations.

Berlin Risk, which is represented in Berlin and Frankfurt am Main, is a member of the European consortium BCF Partners.

More information can be found here: www.berlinrisk.com

Counter Extremism Project (CEP)

The Counter Extremism Project (CEP) is a non-profit, non-partisan international organization that aims to counter the threat of extremist ideologies and to strengthen pluralistic-democratic forces. CEP deals with extremism in all forms – this includes Islamist extremism / terrorism as well as right-wing and leftwing extremism / terrorism. To this end, CEP exerts pressure on financial and material support networks of extremist and terrorist organizations through its own research and studies, works against extremist and terrorist narratives and their online recruitment tactics, develops good practices for the reintegration of extremists and terrorists, and promotes effective regulations and laws.

In addition to offices in the United States, CEP has offices and a separate legal entity as Counter Extremism Project Germany gGmbH in Berlin and maintains a presence in London and Brussels. CEP's activities are led by an international group of former politicians, senior government officials and diplomats. CEP supports policymakers to develop laws and regulations to effectively prevent and combat extremism and terrorism, particularly in the area of combating terrorist financing.

More information can be found here: www.counterextremism.com/german

Executive Summary

The rise of Bitcoin and other cryptocurrencies poses new challenges for the fight against money laundering and terrorist financing (AML/CFT). Cryptocurrencies provide their users with the opportunity to make global payments that are beyond the control of financial regulators and security authorities. In addition, there is a growing risk that terrorist financiers may evade state surveillance and tap into new sources of funding.

Recent evidence demonstrates that terrorist groups and their supporters have become increasingly familiar with the new technology. Terrorists use it to launder money or try to find new sources of finance, as a number of recent examples of fundraising by terrorist groups illustrate. We are still at an early stage of the development of this new threat, but the technical capabilities and capacities of terrorist groups close to ISIS or Hamas, for example, are progressing rapidly. For example, there have been several reported cases of terrorist groups using automatic address-generating software for cryptocurrency wallets to call for donations. None of these new addresses, which have not yet received payments, can be found on the blockchain.

Consequently, the long-held assumption that Bitcoin may not be suitable for illegal activities due to traceability or lack of liquidity is put into question. Various technical means are available to cryptocurrency users to conceal financial flows and protect against forensic analysis of the blockchain, such as the use of anonymizing services called ‘mixers’ or ‘tumblers’. Furthermore, cryptocurrencies known as Privacy Coins allow increased technical protection and encryption of the identity of the sender and the recipient of funds.

In mid-2019, governments agreed on a joint response at the level of the Financial Action Task Force (FATF), the international standard setter in the field. The new FATF recommendations are aimed at an effective regulation of crypto exchanges, the crucial interface between the sphere of cryptocurrencies and fiat currencies. AML/CFT standards that apply to traditional financial transactions should, as far as possible, also cover blockchain financial services. Ultimately, the plan is to put an end to anonymous crypto transactions. The Wire Transfer Rule, also called the ‘Travel Rule’, requires states to take precautions to ensure that Virtual Asset Service Providers (VASPs) monitor and share customer data among themselves and with the relevant government authorities.

At present, the crypto industry is faced with the task of finding technological solutions to operationalize these new compliance standards and establish appropriate Know Your Customer (KYC), due diligence and reporting procedures.

Both governments and companies have one year to comply with the new rules. In the European Union, the adoption of the new FATF recommendations coincided with the need to implement the latest EU anti-money laundering directive (AMLD5). In Germany, new legal rules on crypto assets came into force on 1 January 2020. Crypto companies are now obliged to fulfil KYC requirements and report suspicious transactions to the German financial intelligence unit (FIU). Germany and other countries seem to be on the

right track to prevent the practice of anonymous crypto transactions, which poses serious security risks. It should be noted, however, that a legal, and yet unregulated crypto payment system still exists. Additional regulation is required, in particular regarding the use of unhosted wallets.

The study makes a number of recommendations aimed at increasing the effectiveness of the agreed measures. Countries like Germany continue to face the difficult task of keeping pace with the high speed at which crypto technology is developing. It is therefore essential to increase the expertise and technical capabilities available to German regulatory authorities. The overlap of responsibilities between various German authorities in the area of AML/CFT should be reduced and ideally eliminated. The relevant functions, including prosecutorial responsibilities, expertise and capacity, should be pooled and integrated where possible.

Regulators must also pay attention to and demand more efforts from crypto companies in terms of regulatory compliance and testing of emerging industry procedures. Both sides should cooperate to find an appropriate way to comply with the new FATF rules. Finally, investigating authorities and VASPs should consult each other and develop typologies and indicators for terrorist financing methodologies and potential asset storage operations in the field of crypto transactions.

Recently, there have been first initiatives at the EU level to harmonize the entire crypto sector more effectively. Germany should actively participate in this, but in the meantime, it should not fail to catch up in the area of AML/CFT and develop its own structures and capacities with regard to cryptocurrencies without waiting for EU regulations to materialize.

1 Introduction

This study analyses the particular challenges associated with the global emergence of Bitcoin and other cryptocurrencies in the field of anti-money laundering and combatting the financing of terrorism (AML / CFT).[1] Financing of terrorism will be the focus of this report. Regular money laundering and financing of terrorism are regarded as one complex. However, financing of terrorism should be regarded as a separate phenomenon, which only for practical reasons is usually viewed as a phenomenon closely connected with money laundering.

In the broadest sense, financing of terrorism is understood to mean the provision or collection of financial resources that are, or are intended to be used in whole or in part for terrorist purposes.[2] This can include the support for individual terrorist perpetrators or groups, who often appear publicly and spread their extremist propaganda, as well as the financing of concrete attacks or the preparation for acts of violence and other crimes by terrorists. In contrast to money laundering, the financing of terrorism regularly involves smaller sums such as for example those required for the procurement of a murder weapon. This is one of the crucial differences to money laundering, which often involves significant amounts.

With regard to the analysis of the risks posed by cryptocurrencies – meaning cryptographically secure payment systems that are based on the blockchain technology[3] – this report will first clarify some basic elements and various features of the crypto-finance sector that are relevant to the topic addressed here. In a second step, the risk potential will be assessed, by analyzing to what extent Bitcoin and other cryptocurrencies actually have to be classified as risk factors in connection with the financing of terrorism. The report will then outline specific cases in which crypto assets have been used by terrorist groups and organizations. Furthermore, the report will also assess whether terrorists and their supporters have started to use this new technology to avoid government surveillance and to find new sources of finance.

In recent years, an internationally coordinated response has been agreed, particularly at the level of the European Union, the Financial Action Task Force (FATF) and the G7, to promote regulation of the crypto sector at various levels. These efforts will be examined here from a specific AML / CFT perspective. Which measures have been taken and what recommendations can be derived from these efforts for the government of Germany and the German crypto companies? The study concludes with a series of recommendations. These proposals aim to the increase the effectiveness of the planned regulatory steps aiming to combat money laundering and terrorist financing via the misuse of cryptocurrencies. Cryptocurrencies are a fascinating and controversial new sector in the

[1] This acronym denotes Anti-Money Laundering / Combating the Financing of Terrorism.
[2] The German criminal code includes a more detailed definition. For example: § 89c Financing of Terrorism, https://www.gesetze-im-internet.de/stgb/__89c.html
[3] For a more detailed definition of the term see below.

global financial industry. Germany and its partners are faced with the difficult task of keeping pace with the accelerating speed with which the technology underlying crypto assets is evolving.

2 Blockchain technology is transforming the financial industry

The development of cryptocurrencies began in 2008 with the release of the Bitcoin white paper.[4] More than a decade later, this technology is still at an early stage of its development. In comparison to the so-called fiat currencies,[5] the adoption rate and use of cryptocurrencies is still limited. As of early February 2020, some websites, including coinmarketcap.com, stated that the total capitalization of the around 2500 various crypto coins in existence amounts to around $270 billion. Most cryptocoins only service a small niche. The global market share of Bitcoin within this sector currently stands at more than 60 percent. The share of Bitcoins in all transactions that are suspected to have a criminal background is thought to be even higher. Experts estimate this to be up to 95 percent.[6]

Consequently, when this report refers to cryptocurrencies or crypto assets, it refers primarily to Bitcoin. The reasons why terrorists prefer Bitcoins will be outlined below. The new German regulations, in force since January 2020, use the term 'virtual currencies'. This term was defined in the latest EU update to the fourth EU Anti Money Laundering Directive (mostly referred to as the Fifth Anti Money Laundering Directive, AMLD5), which was transposed into national law in Germany.[7] This EU directive defines virtual currencies as "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange[8] and which can be transferred, stored and traded electronically."[9]

[4] Satoshi Nakamoto [pseudonym of Bitcoin-inventor]: Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf
[5] The term „fiat currencies" denotes government issued and controlled currencies that are not tied to the price of commodities, such as gold or silver. The term „fiat" is derived from the Latin term meaning „to be made" or „to occur".
[6] This data („95% of the cryptocurrency cases law enforcement investigates") is taken from a TV interview with Jonathan Levin, Co-founder of Chainalysis, one of the leading blockchain forensic companies (Bitcoin Accounts for 95% of Cryptocurrency Crime, Says Analyst, fortune.com, 24 April 2019) https://fortune.com/2019/04/24/bitcoin-cryptocurrency-crime/
[7] The changes that came into force in January 2020 primarily affect the Law on the Detection of Profits from Serious Crimes (Money Laundering Act) and the Banking Act.
[8] The amended German Banking Act adds here "or for investment purposes".
[9] Directive (EU) 208/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN

It is important to highlight that from a legal perspective cryptocurrencies are not currencies because they are not issued by a state or a central bank.[10] The Basel Committee on Banking Supervision emphasizes that virtual currencies do not reliably perform the standard functions of money as a medium of exchange or storage of value.[11] Politicians and regulators prefer to speak of crypto assets. This term subsumes not only cryptocurrencies, but also other digital tokens that can represent a wide variety of assets.

The term token refers to any digital token that represents a value or that allows the use of certain services. The term token is often used as a general category which also includes cryptocoins.[12] Digital tokens can basically represent any existing value, such as a property, shares and other securities (security tokens). They can also grant access to a specific software or to services (utility token). Incidentally, the Ethereum network, which is connected to Ether, the second largest cryptocurrency by market value, has dominated in the digital token segment. The programming options of Ethereum facilitate the so-called smart contracts. These are programs which enable automated contractual relationships and thus a detailed description and generation of tokens of all kinds.[13]

The trading of security tokens, which, like cryptocurrencies, can serve as an asset store, is obviously relevant for the fight against money laundering. Nevertheless, digital tokens are less the focus of this report. Instead, technical design differences between Bitcoin and other cryptocurrencies affect the fight against money laundering and terrorist financing. For the sake of clarity, the term cryptocurrencies will be used in this report. The decisive criterion is that these cryptocurrencies can be exchanged for fiat money on designated trading platforms. This node is the primary target of current government regulatory initiatives.

Bitcoin (this name refers to the unit of value as well as the protocol for the safe storage and transfer of bitcoins) and most other cryptocurrencies are based on blockchain technology. The blockchain functions as a decentralized and almost forgery-proof database that is managed over the Internet by a peer-to-peer network. Bitcoin users similar to users of most other cryptocurrencies use a private key that is only known to them in combination with a public key. For the public key, users can choose one or more pseudonyms to protect their privacy during the public transaction. As a result, transactions without financial intermediaries are possible. Transactions that have taken place can be tracked in a decentralized transaction book ("distributed ledger").[14] The blockchain is the best-known distributed ledger technology. To simplify matters, both

[10] In Germany, cryptocurrencies are legally treated as "intangible assets".
[11] Basel Committee on Banking Supervision: Statement on crypto-assets, 13. March 2019 https://www.bis.org/publ/bcbs_nl21.htm; The Basel Committee is comprised of representatives of central banks and financial supervisory authorities of the member states of the G-10.
[12] The term token is derived from the older physical token. These are f.ex. special coins or tokens for the use of public transport or tokens in casinos. The purpose of a token sale or the tokenization of an asset is to sent valuables over the Internet as efficiently as is the case with crypto money.
[13] Aaron Koenig: Die dezentrale Revolution. Wie Bitcoin und Blockchain Wirtschaft und Gesellschaft verändern, FinanzBuch Verlag, München 2019, page 99f.
[14] A distributed ledger ist he electronic equivalent to a distributed register.

terms are often used interchangeably.[15] All transactions for which a blockchain is designed are recorded chronologically and encrypted. After a verification process, new blocks of information are created that are successively inserted into the existing blockchain.

So far, cryptocurrencies have frequently demonstrated high fluctuations in value. After 2017, the 'Year of Bitcoin', the value of this leading cryptocurrency crashed, with most of its competitors, also known as altcoins, being hit even harder. Although Bitcoin's price subsequently recovered, it is often asked whether cryptocurrencies are not primarily a risky speculative object. On the other hand, there are advantages that crypto payments promise. It is an extremely innovative financial technology that enables cross-border transactions without delay. One of the attractive applications is the direct and almost cost-free transfer of currency equivalents to poorer countries, in which many recipients do not have access to the existing banking system. In general, opinions differ on the merits of this technology. In September 2017, the head of JPMorgan Jamie Dimon publicly called Bitcoin a "scam", but soon afterwards changed his mind. In February 2019, Dimon announced that the American bank wanted to be at the forefront of this development and introduce a digital coin linked to the US Dollar.[16]

2.1 The vision of "money without a state"

There is a large shadow hanging over this technology that cannot be overlooked. Cryptocurrencies enable their users to make payments outside the remit of financial regulators and security authorities. This creates a tension between the technical and functional design of virtual money and the basic principle of effective government regulation of financial transactions.

This tension is not surprising when one considers the political thrust that was the basis of the Bitcoin project. In 2015, the German Bitcoin activist Aaron Koenig published a book that focuses on the proximity of Bitcoin's approach, the idea of "money without a state", and to the Austrian School of Economics. The theoretical ideal of the Austrian School is aimed at maximum freedom for private property rights. Every government activity and control is mistrusted. This also extends to the area of finance. The Austrian School, for example, criticizes the move from a gold-backed currency towards state-controlled fiat currencies in Western countries. This development began in the 1930s. The decoupling of currencies from commodities enables governments and central banks to create practically unlimited amounts of money and public debt.[17] In the foreword to

[15] For example, Blockchain-Strategy of the Federal Government of Germany uses the terms Blockchain and Distributed-Ledger-Technology interchangeably, https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?__blob=publicationFile&v=3

[16] Matt Egan: Jamie Dimon hated bitcoin. Now JPMorgan is getting ahead of the crypto revolution, CNN, 15. February 2019 https://cnn.com/2019/02/15/investing/jpmorgan-bitcoin-crypto-jamie-dimon/index.html

[17] The Austrian school, which originally goes back to the border utility school founded by Carl Menger in the 1870s, experienced a wide variety of forms in Europe and the USA in the 20th century. The most famous representative is Friedrich August von Hayek (1899-1992).

Koenig's book to which the liberal politician Frank Schäffler (FDP) contributed, Friedrich August von Hayek, one of the prominent proponents of the Austrian School, and Bitcoin are characterized as "father and son". Bitcoin implemented Hayek's goal of free currency competition, including private currencies, in a way that even Hayek could not have imagined. [18]

Christoph Bergmann, who authored an insightful account of the history of Bitcoin, takes a similar stance. The unknown Bitcoin inventor created money that "surpasses the wildest dreams of the 'Austrians'."[19] Economists belonging to the Austrian School often were (or still are) supporters of a gold-backed currency. Mirroring the situation of a currency based on a limited commodity such as gold, the virtual money supply for Bitcoin-like cryptocurrencies is also limited. Another parallel in this regard are the so-called miners, who provide server capacity for the verification of past transactions and are rewarded for this service with newly 'mined' Bitcoins.

The libertarian ideas, to which supporters of the Austrian School often adhere to, are shared by many representatives of the Bitcoin and crypto community in North America and Europe. If liberals mostly have a differentiated understanding of the state, libertarians often adopt an almost anti-state attitude. In their view the role of state institutions, but also of established banks and centrally controlled corporations, should be pushed back as far as possible. In their world view, achieving the greatest possible individual freedom is the primary goal. This explicitly also includes the option to carry out financial transactions unimpeded by government control or the impact of central banks, both of which are seen as having a negative influence.

Of course, the cryptocurrency community is more diverse and many of its members have other political goals or are apolitical. Among them are investors or crypto companies that pursue commercial interests. Of course, there are also some Bitcoin skeptics even among economists, who belong to the tradition of the Austrian School. However, from the perspective of advocates of cryptocurrencies, they should not be understood solely as a technically sophisticated digital form of money. Rather, they should compete with state issued fiat currencies and end the dominance of fiat money. This is not only true for cryptocurrencies – similar ideas are also linked to other blockchain applications that are aimed at reducing the influence of governments. According to critics, Blockchain technology is actually "an ideology disguised as technology".[20]

Regardless of the latent political connotations, Western governments so far have largely observed and not obstructed the rise of cryptocurrencies. This may in part be based on

[18] Frank Schäffler, Vorwort, in: Aaron Koenig: BITCOIN – Geld ohne Staat: Die digitale Währung aus Sicht der Wiener Schule der Volkswirtschaft, FinanzBuch Verlag, München 2018 (4. Aufl.), pages 9-13. Schäffler refers to Hayek's book "Denationalization of Money", published in 1976.
[19] Christoph Bergmann: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, Moby Verlagshütte, Nersingen 2019 (2. Aufl.), page 145
[20] Michael Seemann: Digitaltechnologie Blockchain. Eine als Technik getarnte Ideologie, 15. March 2018 https://www.deutschlandfunkkultur.de/digitaltechnologie-blockchain-eine-als-technik-getarnte.1005.de.html?dram:article_id=413022

a limited recognition of the role and, to a certain extent, even fascination for this new technology. More importantly, the development of blockchain technology also raises hopes of opportunities for technical innovation and economic growth. The World Economic Forum estimates that it is possible that blockchains will store one tenth of the global gross domestic product by 2027.[21]

Consequently, the opportunities of a future "token economy" are at the center of the German Federal Government's blockchain strategy published in September 2019. However, also beyond Germany, politicians tend to focus not only on cryptocurrencies or crypto tokens, but "beyond Bitcoin" and advocate for other applications. According to its blockchain strategy, the German government aims to promote, among other things, a blockchain-based energy system connected with a public database or a blockchain-based verification of university certificates. Current efforts also concentrate on analyzing whether blockchain technology can be employed to increase transparency in supply and value chains. As far as cryptocurrencies are concerned, the German government wants to prevent stablecoins from developing into an alternative to government issued currency.[22] This also implicitly means that the government has a similar view towards other 'unstable' cryptocurrencies.

At the same time, it has been announced that the German regulatory system will be opened up for electronic securities, which will initially only apply to electronic bonds. A corresponding law should come into force by the end of the current legislative period. This approach is contrary to the rather hesitant attitude that prevails in Germany, Liechtenstein, which is known for its crypto-friendly stance, was the first European country to pass a blockchain law that came into force in early 2020. It remains to be seen whether this ambitious attempt to create a uniform legal basis for the token economy will be successful.[23]

Despite many interesting ideas and projects, cryptocurrencies have so far been the only commercially successful application of blockchain technology. Meanwhile, it is not only in Western countries that politicians and regulators are concerned by the fact that the anonymity of financial transactions is a guiding principle for most cryptocurrencies. Supporters of the crypto sector mostly neglect or deny the risks that the growth of potentially anonymous cryptocurrencies will inevitably open the door to more money laundering and terrorist financing. The crypto scene is mostly skeptical about regulation in the area of AML/CFT. Most of them suspect that these regulatory attempts by governments are indirect efforts to put an end to the development of cryptocoins altogether.

Among Bitcoin advocates, this argument is sometimes connected with the admission that cryptocurrencies are politically explosive. In his book on the history of Bitcoin,

[21] Margaret Leigh Sinrod: Still don't understand the blockchain? This explainer will help, 9. March 2018 https://www.weforum.org/agenda/2018/03/blockchain-bitcoin-explainer-shiller-roubini/
[22] Ibid., page 8
[23] Christopher Klee: Durchbruch im Crypto Country: Liechtenstein verabschiedet Blockchain Act, BTC-Echo, 3. October 2019 https://www.btc-echo.de/durchbruch-im-crypto-country-liechtenstein-verabschiedet-blockchain-act/

Christoph Bergmann admits that the Bitcoin scene had expected a worldwide Bitcoin ban for a long time, at least until around 2017. In the long term, with the growth of cryptocurrencies, governments risk losing control of financial flows worldwide. The opportunities for tax evasion would be radically simplified. Financial sanctions or orders to freeze money could in future come to nothing due to a lack of jurisdiction over the targeted accounts. Therefore, it is not surprising that in particular countries that are affected or threatened by sanctions such as Iran, North Korea and not least China[24] are particularly interested in blockchain technology. The supremacy of traditional financial institutions is challenged. Bergman poses the question as to what meaning rules against money laundering and terrorist financing still maintain, if financial intermediaries who currently implement these regulations are no longer necessary.[25] The obvious answer is that crypto exchanges and trading platforms must ultimately become partners for law enforcement – and must be obliged to make a similar contribution as that made by traditional financial institutions already.

2.2 The role of crypto exchanges and trading platforms

The basic effect of Bitcoin and other cryptocurrencies is to undermine the position of intermediaries, i.e. financial institutions, in payment transactions. However, the trading and handling of cryptocurrencies is still a challenge for users in a practical sense. Therefore, new specialized intermediaries have emerged. A paradox of the current development of cryptocurrencies is that, according to experts, 99 percent of crypto transactions continued to be processed via centralized crypto exchanges in 2018. The often-predicted trend towards decentralized exchanges, which better corresponds to the basic idea of blockchain technology, has not yet materialized. [26] The current market dominance of centralized trading platforms, where crypto money is typically also exchanged into fiat currencies, is an advantage for the developing regulatory framework.

The diverse variants of existing crypto exchanges and trading platforms can only be outlined briefly here. One difference between crypto exchanges and decentralized trading platforms is whether or not users control their private keys, as is the case with decentralized exchanges. Another important distinction is whether only cryptocurrencies can be traded, or whether the exchange between fiat currencies and crypto money is also possible. Such fiat-to-crypto exchanges are technically referred to as “fiat on-ramps”. In order to purchase cryptocurrencies, it is necessary for customers to use established payment methods, typically transfers from bank accounts or credit cards. For customers of such crypto exchanges, these interfaces pose a security risk because the private keys of the addresses to which Bitcoins are deposited are held by the operators of the exchange.

[24] Siehe z.B. die Meldung „China emittiert Blockchain-Anleihe“, Frankfurter Allgemeine Zeitung, 11. December 2019
[25] Bergmann: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, page 263ff.
[26] Nathan Sexer: State of Decentralized Exchanges, 2018 https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79

During the history of the development of cryptocurrencies many cases of hacked crypto exchanges occurred. Criminals have repeatedly managed to exploit security gaps and divert significant amounts of cryptocurrencies from customer accounts. For example, in August 2016, criminals stole almost 120,000 Bitcoins, worth $60 million from the Hong Kong-based Bitfinex exchange.[27] The perpetrators remain unknown. The first famous case concerned the Japanese Mt.Gox exchange, which handled the bulk of Bitcoin's global trading volume in early 2014. During this hack, which to date has not been resolved, a total of 740,000 Bitcoins disappeared. At the time, this constituted around 6 percent of all Bitcoins in existence, and the equivalent of more than a billion US Dollar in value, according to today's exchange rate.[28]

On the other hand, when it comes to combating money laundering and terrorist financing, Fiat on-ramps have the advantage of being subject to the same anti-money laundering rules that apply to financial institutions. Customers must be identified in accordance with the KYC requirements (Know your customer) by submitting documents, etc. This is not necessarily the case with crypto-only exchanges, where cryptocurrencies can be exchanged with one another.

So far, a "softer" practice has predominated at these crypto-only exchanges. Identity checks have not been carried out at all or at least more negligently than at fiat on-ramps. This opens up the possibility for criminals to carry out financial transactions in a non-regulated area. Therefore, the introduction of a new regulatory framework for the crypto sector, as decided in 2019, aims to create requirements for crypto exchanges and the associated crypto custody business (the new German technical term for this sector), that are fairly close to those of financial institutions. This will be discussed in more detail below.

It is clear that the fiat on-ramps are a logical starting point for regulatory interventions. Effective measures in the area of AML/CFT are easiest to carry out at the point where money is converted into cryptocurrencies and vice versa. But this seems to be a temporary snapshot. As the direct trade between cryptocurrencies develops and the use of cryptocurrencies as a means of payment also spreads to payments for goods and commodity trading, the centrality of the fiat-to-crypto exchanges in the sector will decline.

Another important distinction has to be made between traditional crypto exchanges and those decentralized exchanges or platforms where it is possible to trade cryptocurrencies directly between the sender and receiver, i.e. without the need of an intermediary. Here, there are then no central servers on which the cryptocurrencies are stored. Unwanted attacks are thus better prevented – but at the same time access is also more difficult for state authorities. Prices can be set between the sender and the recipient. However, trading still takes place under some supervision since these

[27] In his book Robert A. Küfner (Das Krypto-Jahrzehnt. Was seit dem ersten Bitcoin alles geschehen ist – und wie digitales Geld die Welt verändern wird, Börsenbuchverlag, Kulmbach 2018) documented various cases including Bitfinex (page 138).
[28] Andrew Norry: The History of the Mt Gox Hack: Bitcoin's Biggest Heist, blockonomi.com, 7.6.2019 https://blockonomi.com/mt-gox-hack/

platforms collect information about the identity of their client, the recipient of the transaction as well as type and scope of the transactions that are conducted. These decentralized crypto exchanges correspond more closely to the original design of Bitcoin and have long been considered as the future of trading in Bitcoin and other cryptocurrencies by the crypto community.[29]

Finally, there is over-the-counter OTC trading in cryptocurrencies, which is based on special software. Trading platforms are no longer involved in these transactions. So far, experts assume that peer-to-peer transfers only have a relatively small share of the total crypto payment traffic, which may change in the future. One of the peculiarities of such transactions is that they do not affect the exchange rate of the respective cryptocurrency. Huge assets can change hands in OTC trades. The trading partners remain largely anonymous or only identify themselves to each other. So far regulatory measures have failed at this point. A possible ban on practically anonymous OTC crypto trading does not seem practical. From today's perspective, it is difficult to see how regulators should best react to this trend.[30]

How opaque events on the cryptocurrency market are is demonstrated by a trade that occurred on 6 September 2019. This trade made international headlines. On that day, an unknown trader bought 94,504 Bitcoins worth around $1 billion. In terms of value, this is currently the largest transaction in the history of blockchain based currencies. Around 0.5 percent of all existing Bitcoins changed hands during this transaction. The details of the process remain in the dark. Experts suspect that this was an attempt to manipulate the exchange rate. The only piece of information analysts were able to obtain, was that a significant portion of the Bitcoins came from addresses registered with Huobi Global, a Singapore-based crypto exchange.[31]

In addition to crypto exchanges or trading platforms in countries where the crypto sector is currently less regulated, money launders and terrorist financiers also have additional opportunities to remain undetected. One risk area is the more than 5,000 Bitcoin ATMs, of which there are currently only very few in Germany. At these ATMs customers only have to identify themselves with their ID if they want to exchange more than 500 Euros.[32] Other weak points from an anti-money laundering perspective are prepaid debit cards and online gaming sites that accept Bitcoin or other cryptocurrencies as a form of payment. Finally, a group of new cryptocurrencies, so-called privacy coins, has emerged in recent years. These explicitly focus on the protection of privacy and hence on the anonymity of transactions.

---

[29] Phillip Horch: Dezentrale Börsen: Die Zukunft von Bitcoin, BTC-Echo, 29. September 2018 https://www.btc-echo.de/dezentrale-boersen-die-zukunft-von-bitcoin/
[30] Interview, September 2019.
[31] Anthony Cuthbertson: Billion worth of bitcoin and no one knows why, The Independent, 13.9.2019 https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-mystery-trade-cryptocurrency-market-transaction-blockchain-a9103611.html ; Daniel Eckert / Holger Zschäpitz: Wer steckt hinter dem Megatrade? Eine Milliardenorder für Bitcoin hat den Markt aufgeschreckt, Welt am Sonntag, 22. September 2019
[32] In May 2019 only four such ATMs were installed in Germany. Phillip Horch: BTC kaufen: Bitcoin-Automaten (ATM) jetzt auch in Deutschland, in: BTC Echo, 2. May 2019 https://www.btc-echo.de/btc-kaufen-bitcoin-automaten-atm-nun-auch-in-deutschland/

2.3 Pseudonymity and the possibility of blockchain analysis

One could counter criticisms concerning the various risks posed by Bitcoin and similar cryptocurrencies by arguing that the transactions carried out are not carried out in absolute anonymity. In principle, Bitcoin users make their financial operations transparent by using a public address. All transactions are documented in the blockchain. As a result, every transaction can be traced. This includes the number of coins that were bought or sold. The individual Bitcoins used remain identifiable in the Bitcoin wallet. Most of the time, different Bitcoins have to be combined, and there are 'coin splinters' in the virtual wallets, which can be recombined again in subsequent transactions.[33] However, all of this information cannot easily be attributed to a particular individual, especially since users can switch to using different pseudonyms or technology that constantly changes wallet addresses.

If it is possible at some point to prove the connection between a crypto wallet and a certain individual, then the case is different. Such a connection can be established if someone has made a payment address publicly known, for example on social media. In such a case essentially all Bitcoins and wallets that the person in question has ever used can be determined. If only one wallet is used, virtually all Bitcoin transactions that someone has carried out are exposed. Finally, a more comprehensive analysis can show the connections between different wallets. For several years, specialized companies have been established that analyze the Bitcoin blockchain, to forensically examine transactions carried out and determine the holders of the respective Bitcoin accounts. Government authorities in the United States and other countries are already using these specialized services to track money laundering. With regard to terrorist financing, researchers and investigators can learn more about funding methods and possibly the identity of members of a given terror network by tracking the respective crypto transactions.

Criminals are faced with the risk that technically savvy experts, whether they are employees of government agencies or those who work for analysis companies commissioned by governments, are able to remove the alleged anonymity of crypto transactions. The feasibility of such detection through blockchain analysis ultimately depends on the time and effort required for the investigators to carry out this forensic analysis. The scope of the information available for analysis could be increased if the exchange of user information is mandatory in order to make transactions.

However, even if a wallet is identified from which suspicious transactions are made from abroad, it is challenging to stop such cash flows, freeze or seize such crypto assets. As long as there are no worldwide rules for this, law enforcement agencies must submit a mutual legal assistance (MLA) request to the country concerned. This method is not an

[33] Bergmann: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, page 284ff.

adequate instrument to effectively combat terrorist financing, because MLA requests frequently take a significant amount of time to process.[34]

Although there is the possibility of a subsequent forensic analysis of the blockchain, Bitcoin users can take protective measures that hinder such an analysis. All users, including criminals, have technical instruments at their disposal to structure payment flows in Bitcoin and other cryptocurrencies in a highly complex and complicated manner.

However, anonymizing transactions requires some technical effort, such as the use of anonymization services called mixers or tumblers, or specialized software such as Darkwallet, which already includes such functions. [35] In order to disguise criminal proceeds in cryptocurrencies, for example in Bitcoins, individual amounts can be channeled through a sequence of addresses and then reassembled. At the end of the process apparently clean cryptocurrency amounts emerge. Different darknet addresses[36] can be used throughout the operation. After many detours, the amount in cryptocurrencies ends up on a regulated crypto exchange and can then be exchanged for fiat money.

Using a mixer is the equivalent to maintaining banking secrecy.[37] By using such a service, users can obscure their financial actions, which otherwise would be transparent to everyone (i.e., can be traced by a blockchain analysis). This makes sense for everyone who is concerned about their own security during crypto payments. It is important to highlight that cases of kidnappings and robberies have already been reported, which appear to be aimed specifically at people who are known to have Bitcoin. Many rich Bitcoiners, are reportedly now living in fear and are concerned about their personal security. [38] Even less wealthy Bitcoin users may feel similarly.

On the other hand, the use of mixers makes research and investigations significantly more complex and difficult when analyzing transactions with a potentially criminal background. Users, in their quest for more than pseudonymity, make it difficult for authorities to counter money laundering, financing of terrorism and tax fraud. This contradiction is a good example of how the development of cryptocurrencies presents the existing financial system with complex new problems for which there are currently no satisfactory solutions.

---

[34] Due to their complexity, the various details of MLA procedures cannot be elaborated in this report.
[35] Bundesministerium der Finanzen (Ed.): Erste Nationale Risikoanalyse. Bekämpfung von Geldwäsche und Terrorismusfinanzierung 2018/2019, page 127 https://www.nationale-risikoanalyse.de
[36] The term darknet denotes networks within the Internet which use access protocols that allow the user to remain anonymous, for example by concealing the true IP-address used for access.
[37] The author would like to thank Dr. Hans-Jakob Schindler (Counter Extremism Project) for this analysis.
[38] Some examples are outlined in the book by Bergmann: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, page 261f.

3 The use of cryptocurrencies by criminals and terrorist groups

The fight against money laundering and terrorist financing (AML / CTF) faces fundamental new challenges. Cryptocurrencies reduce the role of traditional financial intermediaries, especially banks, who observe customer-related due diligence obligations. Criminal users of cryptocurrencies are given an opportunity to act almost anonymously or by using false identities. The typical phases of money laundering also apply to cryptocurrencies. Assets of suspicious origins are fed into Bitcoin's financial system through exchanges, where the possibility of tracing such transactions is deliberately obfuscated; subsequently an exchange of these crypto assets into fiat money returns the funds to the legal money cycle.[39]

Consequently, cryptocurrencies have long been in the focus of security agencies. Since the development of Bitcoin, criminals have been interested in cryptocurrencies. Since then, transactions in cryptocurrencies have regularly been associated with latent proximity to criminal behavior and money laundering. In several cases, for example, kidnappers have requested payment of ransom in Bitcoin or other cryptocurrencies. There were also a number of scandals in which criminal hackers managed to exploit technical weaknesses and inadequate security measures on crypto exchanges and to steal large amounts of Bitcoin or other cryptocurrencies. Among other instances, the already mentioned case of the hack of Mt.Gox stock exchange in 2014, which law enforcement officers are investigating to date, has highlighted that operations on crypto exchanges need to be regulated more tightly.[40]

The OneCoin scandal is the biggest fraud case in connection with an alleged cryptocurrency. Ruja Ignatova, the Bulgarian inventor of OneCoin, is described as the main culprit in numerous media reports. By 2017, OneCoin is said to have raised more than $4 billion from investors worldwide. These investments are believed to have disappeared. This spectacular crime has connections to Germany, where Ignatova lived for a longer period, and to several other continents.[41] While Ignatova's whereabouts remain unclear, her brother Konstantin Ignatov, who was sought by police as an accomplice, was arrested in the United States in spring 2019. However, the OneCoin case does not concern a real cryptocurrency. OneCoin is not based on blockchain technology but is structurally a pyramid or Ponzi scheme.

[39] For an analysis of the current legal framework, see the recently published dissertation of Johanna Grzywotz: Virtuelle Kryptowährungen und Geldwäsche, Duncker & Humblot, Berlin 2019
[40] Andrew Norry: The History of the Mt Gox Hack: Bitcoin's Biggest Heist, blockonomi.com, 7. June 2019 https://blockonomi.com/mt-gox-hack/
[41] Milliarden-Betrug mit falscher Kryptowährung, FAZ, 17. November 2019 https://www.faz.net/aktuell/wirtschaft/die-macher-der-kryptowaehrung-onecoin-sollen-anleger-um-milliarden-betrogen-haben-16489799.html

3.1 Assessment of security experts

Cryptocurrencies present law enforcement with significant practical challenges. In 2018 the German Financial Intelligence Unit (FIU) received around 570 suspicious transaction reports related to cryptocurrencies.[42] These were filed mainly by the respective obliged entities within banks. In case of concrete suspicion of illegal behavior, cases involving cryptocurrencies have additional challenges in comparison to 'classic' transactions. For example, it is particularly challenging to determine the beneficial ownership of crypto assets or uncover the criminal background of a transaction. Furthermore, without knowing the private key, it is impossible to seize or freeze the assets deposited in a cryptocurrency wallet.

The investigative trail involving cryptocurrency transactions often leads to foreign trading platforms. The mostly cross-border nature of crypto transactions requires international legal aid procedures or international police cooperation to prosecute the suspected white-collar crime. Swiss government experts concluded that law enforcement agencies are often being surpassed by the pace of crypto transactions. In addition, there are difficulties connected to the question of which jurisdiction is responsible in a particular case.[43]

According to calculations by a study published in early 2018, by the London blockchain analysis company Elliptic, based on transaction data collected between 2013 and 2016, a significant part of Bitcoin-related money laundering activities focused on Europe.[44] Various forms of Bitcoin exchange services and exchange points (conversion services) were included in the data, as well as darknet activities, insofar as there was available information. In 2016, the last recorded year of the study, the share of suspicious activities in Europe was more than 56 percent (on average 37 percent over the entire period), while the rest was largely attributable to exchange services that could not be allocated geographically. In contrast, the corresponding suspicious activities in North America and Asia were significantly lower (7 and 3 percent). According to the authors, the reason for this astonishing finding can be attributed to the lack or ineffectiveness of regulation and supervision of cryptocurrency trading platforms in Europe.

[42] Financial Intelligence Unit: Jahresbericht 2018, page 36
https://www.zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/FIU/fiu_jahresbericht_2018.pdf?__blob=publicationFile&v=3
The role of the German FIU is discussed in more detail in section 5.
[43] Schweizerische Eidgenossenschaft (Ed.): National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding. Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), October 2018, page 35
https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf
[44] Yaya J. Fanusie / Tom Robinson: Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services, 12. January 2018 https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf

Elliptic also reported in September 2019 that Bitcoins worth $829 million (which is 0.5 percent of all Bitcoin transactions in 2019) is currently used on the dark web.[45] Finally, the U.S. company CipherTrace released a report projecting that in 2019 fraudsters and other crypto criminals turned over a combined equivalent of $4.3 billion.[46] Terrorism financiers probably only have an extremely small share of this volume. Although no exact data is available in this regard, it is important to keep in mind that terrorist attacks do not require vast amount of money to finance. Even very large attacks can be relatively inexpensive. The final report of the American government's special commission on the terrorist attacks of 11 September 2001 (The 9/11 Commission Report) found that the attack involving hijacked passenger planes targeting New York and Washington cost between $400,000 and $500,000 to plan and implement.[47]

Recently, a first case in Germany occurred, in which a terrorist act was linked to a crypto transaction. In October 2019, the Bavarian State Criminal Police Office subsequently classified the mass shooting on 22 July 2016, in which an 18-year-old student in a Munich shopping center killed nine people and injured five others, as right-wing motivated. For a long time, this attack was considered a 'mere' rampage by a disturbed teenager. Already in 2018, the Munich district court claimed that the perpetrator had acquired the weapon and ammunition via the Darknet and sentenced the respective arms dealer, who had confessed to the crime, to a prison sentence.[48] Shortly after the attack, media reports based on ongoing investigations, said that the student had announced under a pseudonym in a darknet forum that he would pay for the weapon with Bitcoin.[49] However, this case is only tangentially related to terrorist financing, because the perpetrator himself received no financial support for his crime.

Despite reports that terror groups are dealing with cryptocurrencies and although it can be proven that terror groups conducted first transactions using cryptocurrencies, the current prevailing opinion has been that the topic of cryptocurrencies is not yet relevant in connection with the fight against terrorism. Could this be an exaggerated threat and what is the evidence that cryptocurrencies are not very attractive to terrorists and their supporters? Are there any current trends and developments that question such an assessment?

---

[45] Elliptic: Bitcoin Money Laundering: How Criminals Use Crypto (And How MSBs Can Clean Up Their Act), 18. September 2019 https://www.elliptic.co/our-thinking/bitcoin-money-laundering
[46] Cryptocurrency Anti-Money Laundering Report, 2019 Q3, November 2019 https://ciphertrace.com/wp-content/uploads/2019/12/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q3-2.pdf
[47] 9/11 Commission Report (Executive Summary) https://govinfo.library.unt.edu/911/report/911Report_Exec.htm
[48] dpa-Meldung of 19. January 2018 („Sieben Jahre Haft für Waffenhändler vom Münchner Amoklauf") https://www.op-marburg.de/Mehr/Hessen/Sieben-Jahre-Haft-fuer-Waffenhaendler-vom-Muenchner-Amoklauf
[49] See in particular: Max Hoppenstedt: Der Fall „Maurächer" und die Darknet-Waffe des David S, vice.com, 26. May 2016 https://www.vice.com/de/article/wnxvvy/der-fall-mauraecher-und-die-darknet-waffe-des-david-s
9/11 Commission Report (Executive Summary) https://govinfo.library.unt.edu/911/report/911Report_Exec.htm

Only a few months ago, the German government published its first official assessment. In October 2019, the "First National Risk Analysis to Combat Money Laundering and Terrorist Financing" was published.[50] This report by the federal government is part of the risk-based approach, as required by the Fourth EU money laundering directive. In the report, the threat of money laundering and terrorist financing in Germany is classified as medium-high, which corresponds to the second highest risk level. In a short separate chapter, the report explicitly addresses the role of cryptocurrencies.[51] Since "simpler anonymous means of payment (such as primarily cash)" are said to enable money laundering with much less effort, the threat of money laundering using crypto assets is rated as medium-low in the report.

The specific risk of using cryptocurrencies for terrorist financing is currently rated as low in the report. This assessment is based on the argument that the use of cash compared to pseudonymous crypto assets does not allow tracking at all and that cash is easier to use. The Federal Government of Germany therefore assumes that cash couriers in particular are responsible for money transfers from terrorist organizations and that Hawala[52] and other money transfer service providers also play an important role. The report states that with regard to the financing of terrorism, government agencies have not yet obtained confirmed information as to whether cryptocurrencies are used "on a larger scale".

It is important to highlight that the report includes several caveats for its assessment. It states that the development should be closely monitored, as an increase in the risk potential cannot be ruled out. This concerns the exchange of cryptocurrencies with each other and in particular those cryptocurrencies that offer users the greatest possible anonymity. The report also states that privacy coins or "anonymous crypto assets", namely Monero, have become increasingly accepted in the darknet and could become an important alternative to Bitcoin.

The report outlines that a trend towards more anonymity can also be seen in older cryptocurrencies such as Bitcoin. The report states that cryptocurrencies have so far only been used for terrorist financing in a few isolated cases – apart from calls for donations for which there is a lack of knowledge regarding the amount of donations actually generated.[53] Finally, the report highlights that this risk assessment is also based on the fact that cryptocurrencies are currently used less as a means of payment, but rather as a speculative object, entailing the risk of high fluctuations in value. However, the report concedes that the spread of stablecoins, a category of cryptocurrencies

[50] Bundesministerium der Finanzen (Ed.): Erste Nationale Risikoanalyse. Bekämpfung von Geldwäsche und Terrorismusfinanzierung 2018/2019 https://www.nationale-risikoanalyse.de This report was compiled from data of 35 federal as well as state authorities since the end of 2017.
[51] Erste Nationale Risikoanalyse, pages 114-116
[52] Hawala is an informal payment method that is common in the Islamic world and involves cash transactions. For example, money is deposited in Germany and paid out abroad without physically being sent. Instead, traders at the locations of the sender and recipient settle balances that relate to various transactions. Hawala banking without prior approval by the German regulatory authority BaFin is prohibited in Germany. The Federal Government of Germany estimates that annually around $200 billion are transferred worldwide in this way. Erste Nationale Risikoanalyse, page 56
[53] Erste Nationale Risikoanalyse, page 115

designed to maintain a more stable value, could increase the risks of money laundering and terrorist financing.[54]

It seems reasonable to assume that the national risk assessment, in the absence of confirmed data, only analyses the treats emanating from cryptocurrencies very generally. However, the great dynamism inherent in this sector is recognized in the report. It is likely that the German government will assess the specific risks of cryptocurrencies in the context of the fight against money laundering in greater detail in the future.

It is revealing to compare these assessments with the National Risk Assessment published by Switzerland in 2018, which focuses on the "risk of money laundering and terrorist financing posed crypto assets and crowdfunding". At the beginning of the summary, the report states that "Swiss authorities have not identified a single case of terrorist financing using crypto assets or online crowdfunding and have recorded only a few cases of money laundering using these new technologies. Consequently, the real risk of money laundering and terrorist financing associated with them cannot be precisely assessed". Nevertheless, the National Risk Assessment comes to the conclusion that "that the risks posed by these technologies and the vulnerabilities of Switzerland in this area are considerable, whereby not only Switzerland but all countries are affected".[55]

The report further explains that the Swiss Financial Intelligence Unit (FIU) has already received information on suspected cases from a foreign partner agency. This involved bank transactions of fiat money from several countries, including Switzerland, which were credited to an account in the country whose FIU had triggered the alarm. The money received in the account was reportedly exchanged for Bitcoin and used to fund terrorist actions. The report argues that even the mere reporting of such a suspicion demonstrates the risks that cryptocurrencies pose for the financing of terrorism. In principle, this technology enables a fast and anonymous transfer of funds through which terrorist organizations could be supported.[56]

3.2 Cryptocurrencies and terrorist financing – an increasing risk

Current studies agree that there are only a small number of publicly documented and confirmed cases of terrorist financing using cryptocurrencies. Some important case studies will be outlined here. These demonstrate that both the technology underlying cryptocurrencies and the capabilities of terrorist groups are evolving. As was highlighted above, the situation in this field is very dynamic and the potential risks emanating from the misuse of cryptocurrencies are considerable.

[54] Erste Nationale Risikoanalyse, page 115
[55] National Risk Assessment (NRA): Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding, page 4
[56] National Risk Assessment (NRA): Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding, page 25

The way terrorist activities are funded differs from the objectives and methods of money launders and other criminals, who are primarily concerned with disguising financial transactions. Terrorists are also concerned with generating funding from criminal sources of income, including for example illegal drug and arms trades. In practice, experience has shown that the amounts of money in the area of terrorist financing "are very small and therefore easily fall through the regulatory grid". In addition, these funds often come from ostensive legal sources, such as wages or savings.[57]

Another peculiarity is that terrorists and their sympathizers are interested in fundraising in order to receive donations to support their respective organizations. Funds raised in this way or obtained from other sources can then be used to purchase material to support terrorist attacks and to provide other financial support for attacks. Operational support also includes the use of funds to support terrorist groups on an ongoing basis, including personnel costs, and funds for general security and communication.[58]

In the past strategies to combat terrorist financing (CTF) have proven to be effective. Therefore, it is easy to understand why cryptocurrencies are of interest to terrorist organizations. There are several reasons for this. Terrorist financiers require anonymity during their operations, furthermore they need uncomplicated handling and processing of transactions, relative security of the transactions and the quick execution of transfers. Finally, the increasing adoption rate of cryptocurrencies makes these assets interesting for terrorism financing. None of the existing cryptocurrencies fully perform all of these functions. If there was an almost perfect cryptocurrency, criminals would undoubtedly make intensive use of it. The known cases in connection with terrorist financing confirm that Bitcoin is clearly the primary cryptocurrency used in this regard.

Another challenge for regulators and financial authorities are the difficulties connected with attempts to seize, stop or freeze funds and financial flows in cryptocurrencies that are linked to the financing of terrorism. This is due to the lack of jurisdiction in many cases. As a result, terrorist financiers are unlikely to be prosecuted if they use this technology.

Terrorists initially approached the issue of cryptocurrencies with caution. In autumn 2015, Ghost Security (also GhostSec), an alleged anti-terrorist hacking initiative that emerged from the "Anonymous" network, warned that terrorist groups such as the Islamic State (ISIS) were interested in Bitcoin. The group claimed to have tracked down Bitcoin accounts that ISIS[59] uses to fund its operations. The report mentioned a total amount of $4.7 to $15.6 million in this regard. This would have constituted been between 1 to 3 percent of the total budget of the ISIS (estimated at $468 to $520 million annually

[57] Erste Nationale Risikoanalyse, pages 57, 61
[58] A summary of the methods and specifics of the financing of terrorism can be found here: Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston: Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats, RAND Corporation, Santa Monica 2019, page 7ff.
[59] The Arabic name of the Islamic State is ad-daula al-islāmīya (abbreviated Daesh). In Western media reports, the organization was mostly referred to as the Islamic State in Iraq and the Levant (ISIL), the Islamic State in Iraq and Syria (ISIS) or the Islamic State (IS). The last acronym predominates in German media reports.

by the U.S. Treasury Department at the time). However, the information given in the report was not supported by detailed evidence and was soon questioned by experts. It seems certain that early experiments by terrorist groups with Bitcoin took place in the darknet or inside private chat channels.

Following this initial study, further reports appeared highlighting the possible use of cryptocurrencies by terror groups. Shortly after the rise of ISIS in Syria and Iraq, supporters of the organization demonstrated an interest in financing opportunities using Bitcoin. In August 2015, an American teenager Ali Shukri Amin, was sentenced to a long prison term in Virginia. He had given recommendations to ISIS via Twitter on how the organization could be funded using Bitcoin.[60]

In practice, terror groups initially made some simple mistakes as demonstrated by the first concrete incident in 2016. At that time, a terror group named Ibn Taymiyya Media Center (ITMC), active in the Gaza Strip, publicly called for Bitcoin donations on Twitter and Telegram to support a financing campaign called Jahezona (Arabic for "equip us"). [61] ITMC is considered the media wing of the Mujahideen Shura Council (MSC), a collection of Salafist-jihadist groups in Gaza, that the American government has designated as a terrorist organization.[62] Although MSC mainly targets Israel, its leadership also supports IS. The Jahezona campaign, which had been running since 2015, regularly published graphics showing the weapons and ammunition needed by the group and the costs involved. In June 2016, the possibility of paying in Bitcoin was mentioned by the campaign for the first time. In addition, infographics with quick response codes (QR codes) appeared on Twitter, which referred to a Bitcoin address. Two transactions were received in early July 2016. The total amount of these two transactions was 0.929 Bitcoin (with a value of $540 at that time).

It cannot be ruled out that the organizers themselves carried out these transactions to test the Bitcoin address. Although the campaign was barely successful, it demonstrated that terrorists are experimenting with the new technology to open up new sources of finance. The critical mistake the activists made was to publicly provide a Bitcoin address and therefore, make themselves more transparent on the blockchain than was surely intended. Any group or individual that publicly refers to one or more wallet addresses is immediately open to increased scrutiny, as the connection between the group or the respective individual with the wallet address is a key piece of information. In such a case, security experts can understand that incoming transactions to these wallets are made by individuals attempting to send money to terrorists. Furthermore, through the transactions originating from a Bitcoin "donation account", it is possible to track the organization that receives money and forwards it to other addresses. However, despite

[60] financemagnates.com, 30 August 2015 https://www.financemagnates.com/cryptocurrency/news/teen-who-advised-on-funding-isis-with-bitcoin-gets-11-years-in-prison/
[61] Yaya Fanusie: The New Frontier in Terror Fundraising, in: Bitcoin, The Cipher Brief, 24 August 2016, https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin
[62] Office of Foreign Asset Control, Specially Designated National Update, 19.8.2014 https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20140819.aspx

this increased transparency, it remains impossible to stop this money or to determine the actual identity of the donor and recipient, without the use of specialized services.

A study commissioned by the European Parliament on cryptocurrencies and terrorist financing highlighted the case of al-Sadaqah, a jihadist organization active in Syria.[63] This group, which acts as a charity, launched a crowdfunding campaign at the end of 2017,, via al-Qaida related social media channels, and the messaging service Telegram. In the course of this, al-Sadaqah received 0.075 Bitcoin (at that time with a value of $803) into its Bitcoin account. The campaign initially called for supporters to anonymously and securely donate using Bitcoin. Several weeks later, once the campaign became publicly known, the organization announced on Twitter that privacy coins such as Monero and Dash could also be used to support the Mujahideen in Syria.[64]

Another case was reported at the end of 2017. Zoobia Shahnaz, a Pakistani-born American citizen, was charged with bank fraud and money laundering. According to the U.S. Department of Justice, Shahnaz, who later pleaded guilty, bought or exchanged around $62,000 in Bitcoin and other cryptocurrencies with more than a dozen fraudulent credit cards, and then began transferring funds to support ISIS.[65] Some experts see this case as an indication that terrorists and their supporters continue to be hesitant to use cryptocurrencies directly. In this case crypto transactions were utilized to conceal the criminal origin of the funds which were intended to be used to support terrorism

In the meantime, further cases in the Middle East demonstrated how the terrorists are learning. The research network Bellingcat reported that a Syrian jihadist group called Malhama Tactial, which operates in the region of Idlib, began publicly promoting Bitcoin donations in June 2018. However, it subsequently changed its approach to fundraising. Soon after the begin of its fundraising campaign tweets including the group's Bitcoin address were deleted. Instead, potential donors were asked to contact Malhama Tactical directly via direct message to obtain an address for donations. It remains to be seen whether this approach, which has since has also be used by other terrorist groups, is a particularly effective method of attracting donations.[66] However, the tracking of possible crypto transactions is made more difficult in this way. In order to investigate,

[63] Sadaqah means "charity" in Arabic and refers to the voluntary nature of the gift.
[64] Policy Department for Citizens' Rights and Constitutional Affairs: Virtual currencies and terrorist financing: assessing the risks and evaluating responses, May 2018, page 34. The authors of the study are Tom Keatinge, David Carlisle, and Florence Keen from the Royal United Services Institute,
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604970
[65] United States Department of Justice, 26 November 2018 https://www.justice.gov/usao-edny/pr/long-island-woman-pleads-guilty-providing-material-support-isis
[66] In general, the use of social media for terrorist financing through crowdfunding is increasingly playing a role. Tom Keatinge / Florence Keen: Social Media and Terrorist Financing. What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?, Global Research Network on Terrorism and Technology: Paper No. 10 (RUSI), London 2019
https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf

authorities would have to create their own fake accounts and establish direct contact with the respective terrorist group.[67]

Another important innovation was recently observed. In April 2019, it was reported that the Qassam Brigades, the military arm of Palestinian Hamas, had been calling on their supporters to donate in digital currency since January of the same year. The Qassam Brigades and Hamas are officially designated by the European Union as terrorist organizations.[68] Originally, donors were supposed to donate to a single Bitcoin address or wallet. However, as research by the analysis company Elliptic demonstrated, the financing website in question has been modified so that a new, unique Bitcoin donation address is automatically generated with each page view. None of these new individual addresses, which did not receive any amounts themselves, can be found on the blockchain. To put one of these newly generated addresses on the blockchain, the investigators would have to donate to Hamas themselves. In other words, every new donation belongs to a new wallet that only the donor has seen. This innovative fundraising campaign by Hamas is said to have raised $7,400 in donations during the first four months.[69]

At about the same time, it was found that ISIS was using the same address-generating software to advertise for Bitcoin donations through its media site al-Furqan. It is not certain which of the two organizations is originally responsible for this technological innovation. In August 2019, the New York Times also reported this new development, calling it alarming.[70] According to the article, American experts assume that the proceeds from such donation campaigns are likely to be in the range of several tens of thousands of US Dollars per campaign.

Much of the information concerning the increased use of cryptocurrencies by terrorists is included in a comprehensive report by the American terrorism expert Steven Stalynski.[71] The report connects this new trend with the removal of territorial control of IS in Syria and Iraq. The report argues that fugitive ISIS fighters no longer have access to a fixed and secured territory and therefore are more interested in crypto transactions than before.

---

[67] Brenna Smith: The Evolution Of Bitcoin In Terrorist Financing, 9 August 2019 https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/
[68] For the list of individuals, associations and bodies whose funds are frozen and against whom increased measures of police and judicial cooperation, are applied see the Council Decision (CFSP) 2019/1341 from 8 August 2019 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0025&from=de
[69] Reuters, 26.4.2019 https://uk.reuters.com/article/us-crypto-currencies-hamas/hamas-shifts-tactics-in-bitcoin-fundraising-highlighting-crypto-risks-research-idUKKCN1S20FA
[70] Nathaniel Popper: Terrorists Turn to Bitcoin for Funding, and They're Learning Fast, The New York Times, 18 August 2019 https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html
[71] Steven Stalinsky: The Coming Storm – Terrorists Using Cryptocurrency, 21 August 2019 https://www.memri.org/reports/coming-storm-%E2%80%93-terrorists-using-cryptocurrency Stalinsky is director of the Middle East Media Research Institute (MEMRI), which focuses on observing Islamic media in the Middle East. The Washington-based NGO is sometimes described as neoconservative and close to the Israeli government.

An Israeli analytics firm called Whitestream said it found evidence that the bombings on Easter Sunday 2019 in Sri Lanka, which killed 253 people and injured 485, were largely funded by Bitcoin transactions.[72] ISIS, which claimed responsibility for the attacks, apparently used the Canadian crypto exchange CoinPayments. Whitestream reported that balances in Bitcoin wallets, which according to the Israeli company are associated with ISIS, increased from $500,000 to $4.5 million just one day before the attacks. According to the experts at Whitestream, these balances fell to $500,000 immediately after the attacks.[73]

The Qassam Brigades and ISIS are unlikely the last terrorist organizations to use this technologically advanced form of fundraising. Hence the earlier assumption that Bitcoin is not suitable for illegal activities due to traceability of transactions and lack of liquidity should be seriously questioned. Rather, terrorist organizations have apparently found a way to anonymize their financing channels in these technologies. If they are also able to organize quick payouts or exchanges in fiat currencies, Bitcoin and other cryptocurrencies could become a second cornerstone of terrorist financing alongside cash.

Funds stored in cryptocurrencies are difficult to investigate as well, especially if these funds are only stored in wallets. It remains a challenge for security agencies to seize or freeze incriminated crypto assets. This asset class is therefore a potentially attractive method for terrorist organizations to store funds. This is particularly the case if the organization does not aim to generate profits but only intends to protect its funds from interference by government authorities. This is particularly the case for larger terrorist organizations, such as ISIS, Hezbollah or the Taliban, which regularly manage large budgets.

3.3 Messaging-services based on blockchain?

An important side-issue in this context are advanced messaging services that allegedly use advanced cryptography methods. The Counter Extremism Project (CEP) published a report in 2017 that demonstrates the increasing use of Telegram by various terrorist groups.[74] Telegram is a free, cloud-based instant messaging service. The development team of Telegram is apparently located in Dubai. The main founder of the company is the Internet billionaire Pavel Durov, who is sometimes referred to as the “Russian Mark Zuckerberg”. He also founded Russia’s most popular social network VK (vk.com). Durov was forced to emigrate from Russia. His stated goal was to build an app that allows

[72] Roy Katsiri: Bitcoin donations to ISIS soared day before Sri Lanka bombings, Globes (Israel), 2 May 2019 https://en.globes.co.il/en/article-exclusive-isis-funded-sri-lanka-bombings-with-bitcoin-donations-1001284276
[73] During the attacks in Sri Lanka on 21 April 2019, several churches and hotels were targeted by suicide bombers. The authorities in Sri Lanka announced that a local Islamist group and jihadists linked to international terrorism were responsible for the attacks. Bitcoin donations to ISIS soared day before Sri Lanka bombings, Globes (Israel), 2 May 2019 https://en.globes.co.il/en/article-exclusive-isis-funded-sri-lanka-bombings-with-bitcoin-donations-1001284276
[74] Counter Extremism Project (Ed.): Terrorists on Telegram, May 2017 https://www.counterextremism.com/terrorists-on-telegram

people to communicate without government agencies being able to intercept their communication. In fact, terrorists use this encrypted chat service, also for fundraising purposes. Finally, Telegram was one social media application through which IS material was distributed.

There has been an international backlash, which increased the pressure on Telegram operators to take action against the abuse of their services by terrorists, and to plan and implement new security measures. Furthermore, the United States Securities and Exchange Commission sued Telegram in October 2019, demanding that the platform postpone its blockchain project Telegram Open Network (TON). Durow and other officials have been ordered to testify in the United States. In the meantime, after pressure by Europol and European countries, Telegram and other internet companies have started to block numerous accounts of ISIS supporters. ISIS reacted defiantly and advised supporters to switch to other platforms. [75]

In December 2019, media reports appeared claiming that the ISIS is currently actively testing a blockchain-based messaging app that offers various advantages from the perspective of the terrorists, including an apparently secure and anonymous communication channel and a tamper-proof archive in which ISIS can save its propaganda videos. The messaging app is called BCM ("Because Communication Matters"). BCM is a company founded by David Xueling Li, a Chinese billionaire. The company is based in the British Virgin Islands. It remains to be seen whether the app can really be a replacement for Telegram from the perspective of ISIS. Interestingly, a key function of the BCM app, that other platforms do not offer, is an integrated wallet that enables the use of cryptocurrencies like Bitcoin and Ethereum. [76]

BCM also announced that it intends to build its own crypto exchange to simplify global anonymous crypto payments. This is concerning from a security perspective. However, some experts expressed doubts about BCM's announcements. Governments will also have sufficient time to take countermeasures, as was the case with Telegram. These developments concerning messaging services are a vivid example of how much attention the new technological trends require when terrorists increasingly begin to adopt cryptocurrencies and blockchain applications for their activities.

[75] Defiant Message From ISIS In Response To Campaign Against Its Presence On Telegram, Other Platforms, MEMRI, 2.December 2019 https://www.memri.org/reports/defiant-message-isis-response-campaign-against-its-presence-telegram-other-platforms
[76] The first media report, which triggered further reporting on this issue was David Gilbert: ISIS Is Experimenting with This New Blockchain Messaging App, vice.com, 13 December 2019, https://www.vice.com/en_us/article/v744yy/isis-is-experimenting-with-this-new-blockchain-messaging-app

4 Reaction by governments: coordinated regulatory approach

The emergence of Bitcoin and other cryptocurrencies is a worldwide phenomenon. Cryptocurrencies are not linked to certain jurisdictions like fiat money but exist as technology in global cyberspace. As has been pointed out above, cryptocoins with their significant development potential result in new and complex challenges for the fight against money laundering and terrorist financing (AML / CFT). These challenges are compounded by the speed of technological change. Not surprisingly, regulation of crypto payments is just beginning. It took some time before the first governments started to deal with this complicated matter. In many countries, there is a lack of experts at the government level with knowledge of this topic to develop the necessary expertise and understanding of the technical capabilities at their disposal.

A growing concern from the perspective of security agencies is that cryptocurrencies are an evolving technology and that they are already established in a certain niche of the financial sector. As a result, criminal actors and terrorist organizations such as ISIS have started to experiment with this new technology. They use this new technology for money laundering or to tap into new financial resources, as the recent examples of fundraising campaigns by terrorist groups demonstrate. At the same time, it is clear that these emerging risks are still at an early stage. Consequently, it is imperative that national security actors, such as financial regulatory authorities, law enforcement agencies or intelligence agencies, take on this new challenge. Ultimately, they must be enabled to use this new technology as intelligently as their opponents.

4.1 The new FATF recommendations (June 2019)

As far as possible, an effective response to these new challenges should be coordinated at an international level. It is not the first time that regulators in the AML / CFT area are facing problems that require global coordination and cooperation. The key standard-setter in this area is the Financial Action Task Force (FATF). The FATF is an intergovernmental body established by Western countries and based in Paris, which publishes and continuously updates recommendations and related interpretative notes aimed at regulating the fight against money laundering and terrorist financing.[77] Through its recommendations, the FATF has established worldwide standards and become a driver for further regulations in the AML/CFT sector. Although these recommendations are not legally binding, they are often incorporated into the legislation of many countries.

[77] The Financial Action Task Force (on Money Laundering), founded in 1989, is based at the OECD in Paris. The FATF is currently made up of 37 countries and two international organizations (the EU and the Gulf Cooperation Council). In addition to many mostly western countries, the members include China, which currently holds the presidency of the FATF with Xiangmin Liu, India and Russia.

Similar to the Financial Stability Board, [78] an organization responsible for monitoring financial stability risks, which is also currently paying more attention to the topic of crypto assets, the FATF regularly reports to the group of the 20 most important industrial and emerging markets (G20).

Crypto assets have been part of the FATF's recommendations for a number of years. At first, the institution was reluctant to regulate this new sector. Initially, the FATF only discussed a licensing requirement for Virtual Asset Service Providers (VASP). VASP are providers of services for virtual assets, including crypto exchanges. In October 2018, at the request of the G20 finance ministers, the FATF decided to include specific requirements for cryptocurrencies (virtual assets) in its future standards. [79] Shortly thereafter, the G20 countries announced at their summit in Buenos Aires that they would regulate cryptocurrencies in accordance with FATF standards. [80] At the same time, the ball was played back to the FATF with the request by the G20 to develop specific guidelines for such regulations. The FATF has since revised its recommendations accordingly [81] and on 21 June 2019 published detailed guidance for regulations concerning cryptocurrencies and related service providers. [82] Shortly afterwards, the heads of state and governments of the G20 confirmed at their Osaka summit that the FATF standards are applicable to cryptocurrencies and virtual asset service providers. At the same time, they held out the prospect of implementing new regulations in accordance with the revised and expanded FATF guidelines. [83]

At its core the aim is to implement a globally coordinated regulatory framework for crypto exchanges, the crucial interface between the sphere of the cryptocurrencies and fiat currencies. In essence, this means that in future the existing rules against money laundering and terrorist financing will also be applied to blockchain based financial services. The FATF has given governments one year to adopt these new recommendations. A first review is scheduled for June 2020. [84] The organization discussed this topic again at a plenary session in October 2019. At that time, the FATF member countries agreed on what steps the implementation of the new requirements would require. The FATF also decided that newly emerging virtual currencies such as

[78] The Financial Stability Board, which has existed in its current form since 2009, is located at the Bank for International Settlements (BIS) in Basel. As a standard setter in the field of cryptocurrencies, the organization deals with regulatory issues and financial stability risks that do not relate to the specific aspects of the fight against money laundering and terrorist financing.
[79] FATF: Regulation of virtual assets 19 October 2018 https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html
[80] G20 Leaders' Declaration: Building Consensus for Fair and Sustainable Development, 1 December 2018. see Nr. 25 http://www.g20.utoronto.ca/2018/2018-leaders-declaration.html
[81] FATF (Ed.): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations, Paris 2012-2019 www.fatf-gafi.org/recommendations.html
[82] FATF (Ed.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, June 2019 www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html
[83] G20 Osaka Leaders' Declaration, 29 June 2019, see Nr. 17 http://www.g20.utoronto.ca/2019/2019-g20-osaka-leaders-declaration.html
[84] FATF: Public Statement on Virtual Assets and Related Providers, 21 June 2019 http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html

stablecoins (clearly alluding to projects such as Libra[85]) would also be subject to these new regulations. [86] However, blockchain-based digital currencies developed by governments will apparently be treated differently by the FATF.

The implementation of the agreed new regulatory measures is currently ongoing. Although the FATF emphasizes, as is the case with all its recommendations, that the new crypto guidelines are not legally binding and do not override the responsibility of national authorities, governments have little choice. States failing to adopt the new regulatory framework risk being included on the FATF's "blacklist". In the worst case, countries that are judged negatively by the FATF risk losing access to the global financial system. [87] It remains to be seen to what extent all states and virtual asset providers, which will have to technically implement the new regulations, are able to keep to this ambitious schedule. Governments also retain a certain amount of room for interpretation when implementing the new guidelines.

What are the FATF's most important decisions? The amended FATF Recommendation 15 requires states to oblige crypto service providers (VASPs) operating in their jurisdiction to support the combating of money laundering and terrorist financing. VASP must be regulated and licensed accordingly and be subject to effective government supervision. An interpretive note, published at the same time by the FATF, [88] was explicitly mentioned in the G20 declaration. This interpretive note states that governments should require crypto service providers to collect information concerning the transactions they have processed. The relevant data must be exchanged with the service providers involved on the opposite side of a transaction. Customer data should be transmitted to the responsible authorities upon request.

Recommendation 16 (Wire Transfer Rule) further stipulates that governments should take precautions to ensure that banks and crypto service providers monitor information concerning the sender and recipient for possible missing information. The following information is required for each transaction: [89]

- name of the client
- account number of the client if such an account is used to process the transaction (e.g. the crypto wallet)[90]

[85] For a discussion concerning Libra, a virtual currency developed by Facebook and the issue of stablecoins see section 4.4 below.
[86] Outcomes FATF Plenary, 16-18 October 2019 https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2019.html
[87] The FATF „blacklist", officially called „high risk jurisdictions", currently includes North Korea and Iran. See FATF: Public Statement, 18 October 2019, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/public-statement-october-2019.html). In addition, the FATF maintains a list of jurisdictions with „strategic deficiencies", which consists of 12 countries. This list was last updated in October 2019, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/fatf-compliance-october-2019.html
[88] Interpretative Note to Recommendation 15, in: The FATF Recommendations, pages 70-71
[89] FATF (Ed.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, page 29 (Nr. 114)
[90] In the document referred to as "VA wallet"

- physical (geographical) address of the client or the national identification number or the customer identification number that uniquely identifies the client at the processing institution, or the date and place of birth
- name of the beneficiary
- beneficiary's account number if such an account is used to process the transaction (e.g. the crypto wallet)

Furthermore, crypto service providers have to develop adequate processes and procedures and ensure that their customers do not conduct illegal activities. The companies classified as crypto service providers will be subject to similar requirements as conventional banks and financial service providers in future. However, there are some open questions. So far, there is no system at the national or international level (such as Swift in interbank transactions), which can be used to reliably transmit identification data on payment transactions on the blockchain. Consequently, it is practically impossible for example to identify a beneficiary who uses a newly created, non-custodial Bitcoin wallet.

Crypto transactions that take place between wallets that are not subject to the supervision of the respective government are excluded from monitoring. Users of cryptocurrencies are not directly subject to regulation and therefore retain the option to use less regulated crypto exchanges or to carry out peer-to-peer transactions (with pure crypto-crypto payments) that are not recorded. In the worst case, the new rules will make peer-to-peer transfers via non-custodial wallets more attractive, which would make it significantly more difficult for authorities to track and control them. For example, a client could send cryptocurrencies from an exchange to a non-custodial wallet, for which only the user controls the private key. The crypto coins would then be sent from this wallet to another platform, with the result that none of the crypto service providers involved at the beginning or at end of the transaction would be able to oversee both sides of the transaction.

With regard to the exercise of customer-related due diligence ("Know your customer" or KYC procedures), the FATF has set a low threshold for crypto service providers. This is based on the assessment that crypto transactions are particularly vulnerable to their misuse in connection with money laundering and terrorist financing. Appropriate checks for occasional transactions should already be made from a minimum value of more than $1,000 or Euros.[91] In Germany, this threshold corresponds to the provisions of the Money Laundering Act that apply to the monitoring of money transfers. It is important to highlight that apparently most of the established crypto exchanges already carry out KYC checks, including identity checks of the clients (e.g. in order to compare the name with sanction lists), for incoming transactions starting at $1,000 or Euros. However, according to the new FATF rules, this would also be necessary for outgoing transactions

[91] Interpretative Note to Recommendation 15, in: The FATF Recommendations, page 71, Nr. 7a (Referencing recommendation 10 concerning Customer Due Diligence): „The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1.000“. In comparison the FATF recommends a threshold of $15.000 or Euro for transactions in fiat currencies.

in the future.[92] The FATF decided not to go into detail concerning attempts to circumvent these controls, for example, there are no provisions in the new regulation concerning the minimum time period within which transactions below the threshold must occur in order to trigger a review.[93]

On the other hand, the FATF encourages governments to review conspicuous crypto transactions in line with the risk-based approach, even if these transactions fall below the minimum threshold of $1,000 or Euros.[94] According to the FATF, triggering a review even below the minimum threshold is particularly advisable, as soon as suspicions of money laundering and terrorist financing exist. It is important to remember the recent fundraising campaigns by terrorist groups mentioned above, during which the total sum raised during the campaign consisted of numerous small donations.

It was clearly the realization that an effective regulatory framework for crypto-trading platforms was lacking (which was accompanied by increased money laundering activity in particular in Europe) that led the US government to push for stricter rules.[95] In essence, the expanded FATF recommendations are adopting the framework of crypto regulations that the U.S. Treasury Department, the Financial Crimes Enforcement Network (FinCEN) has developed. As early as 2013, FinCEN worked to expand the so-called travel rule enshrined in the Bank Secrecy Act to include crypto trading platforms.[96] The American Travel Rule, which previously referred to a threshold of $3,000, essentially corresponds to the FATF's Wire Transfer Rule with only a few minor differences.[97] In November 2019, Kenneth Blanco, FinCEN's director, confirmed that his government is demanding strict compliance with new and tighter requirements from crypto exchanges and wallet providers. Finally, there are ongoing efforts in the U.S. Congress to develop regulations for the entire cryptocurrency sector via the so-called

[92] Colin Harper: FATF Finalizes Crypto Guidelines, Recommends Exchanges Share Client Data, Bitcoin Magazine, 21 June 2019 https://bitcoinmagazine.com/articles/fatf-finalizes-crypto-guidelines-recommends-exchanges-share-client-data
[93] Nina-Luisa Siedler / Susi Förschler: FATF recommends regulating and monitoring Virtual Asset Service Providers, DWF Spotlight, 22 August 2019 https://www.dwf.law/Legal-Insights/2019/August/Regulation-of-virtual-asset-service-providers
[94] FATF (Ed.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, page 25 (Nr. 95)
[95] See: Yaya J. Fanusie and Tom Robinson: Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services, 12 January 2018 https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf
[96] The Travel Rule was first introduced by FinCEN in 1996 as part of the anti-money laundering standards that apply to all US financial institutions. Since March 2013, the scope of the regulation has been expanded to include crypto exchanges. See the current FinCEN guidance: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, 9 May 2019 https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf
[97] One difference is for example that data concerning the amount transferred (transmittal amount) is exchanged in the USA. A tabular comparison between the Travel Rule of the Bank Secrecy Act (USA) and the FATF recommendation can be found at CipherTrace: Cryptocurrency Anti-Money Laundering Report, 2019 Q3, November 2019, page 11 https://ciphertrace.com/wp-content/uploads/2019/12/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q3-2.pdf

"Crypto-Currency Act of 2020".[98] Until now, this sector has not been comprehensively regulated in the United States, apart from regulations concerning money laundering and financing of terrorism.

4.2 Increased requirements for compliance and technology

The 'Easy Guide' issued by the FATF to inform the public about the new regulations of the crypto sector, states that governments need to expand their knowledge concerning this new technology. The Guide also outlines that it is up to the crypto companies to inform themselves about the financial regulations that will apply to their activities in the future. The Easy Guide also clearly states that "It is up to the sector itself to develop the technology to meet the FATF's requirements, particularly when it comes to securely collecting and transmitting originator and beneficiary information."[99]

This means a significant change for the sector since the crypto industry only had few regulatory obligations in the past, compared to traditional financial institutions. Hardly any of the companies operating in the sector will be able to avoid hiring additional staff for compliance and to combat money laundering and terrorism financing. The new rules will apply to all companies that work with digital currencies and crypto tokens, including crypto exchanges, decentralized platforms, custodians (wallet providers), mixer services and crypto hedge funds. Every company must implement KYC rules that enable early detection of suspicious activities, such as for example potential terrorism financing and share the respective information with other service providers and government agencies.[100] Collected customer information must be stored for at least five years.[101] Finally, companies must ensure that they are able to intervene in an emergency, such as for example prevent transactions to incriminated wallets or freeze crypto accounts in cooperation with law enforcement agencies.[102]

As soon as it became apparent that the Wire Transfer Rule would be applied, the industry reacted with concern. As early as April 2019, when the FATF's key proposals became known, Jonathan Levin, a co-founder of the well-known consulting firm Chainalysis, expressed concerns. Levin said that crypto assets are basically designed in such a way that payments can be made without identifying the recipient. Funds could be transferred to a personal wallet that was unable to accept customer identification

[98] Jason Brett: Congress Considers Federal Crypto Regulators In New Cryptocurrency Act Of 2020, forbes.com, 19. December 2019 https://www.forbes.com/sites/jasonbrett/2019/12/19/congress-considers-federal-crypto-regulators-in-new-cryptocurrency-act-of-2020/#57eb0f4d5fcd
[99] FATF (Ed.): Virtual Assets: What, When and How? (Easy Guide to FATF Standards and Methodology), without date (December 2019) http://www.fatf-gafi.org/media/fatf/documents/bulletin/FATF-Booklet_VA.pdf
[100] The expansion of the obliged entities also increases the need to promote growth and further specialization of the relevant government agencies. These must be able to investigate and potentially prosecute complex crypto payment transactions.
[101] FATF (Ed.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, page 27 (Nr. 102)
[102] FATF (Ed.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, page 29 (Nr. 114)

data.[103] Therefore, the new regulatory steps could result in many platforms having to shut down, as there is currently no technology to transmit the relevant information. Levin further argued that restricting principally cooperative crypto exchanges could lead users to increasingly migrate to decentralized or peer-to-peer platforms. As a result, this would reduce the transparency from which the investigators had benefited so far.

There were also conciliatory voices. When viewed objectively, some fears appear exaggerated. The main incentive for Bitcoin users, for example, is not to evade government supervision, but to carry out transactions inexpensively and quickly. Phil Liu, chief legal officer of Arca, California crypto hedge fund, commented on the publication of the new FATF recommendations that crypto professionals like to make a big deal about giving customer data to the government. However, from his perspective there will "not be much disruption for legitimate users if the proposal is implemented".[104]

The economic concerns of the young industry, which includes numerous smaller companies and startups, are more than justified. The wave of regulation in the crypto sector is likely to drive up operational costs due to additional compliance measures and necessary technological upgrades. Thus, the thresholds for companies operating in the crypto sector will increase, and some business models will no longer be feasible in the future. Profit margins are likely to be narrower in many cases, and the crypto industry may experience business conditions, which until now have been prevalent only in traditional financial markets.

The main problem remains the technological implementation of the FATF's wire transfer rule. In November 2019, software developers from various companies came together with U.S. government experts at a conference organized by the analysis company CipherTrace. They concluded that the crypto industry was facing difficulties to fully comply with the demands of the FATF to fully implement all requirements by June 2020. Nevertheless, the conference participants concluded that crypto companies are on the right track to find at least preliminary solutions.[105] A month earlier, John Roth, chief compliance officer of the U.S. crypto exchange Bittrex, had sounded more negative. According to his knowledge, no one in the industry had complied with the Travel Rule so far. The great difficulty, he said, was that it was necessary to agree on a new industry wide technical standard. New and not yet tried-and-tested technical solutions would be required to cope with the speed and the high volume of data.[106]

---

[103] Nikhilesh De: 'Onerous' FATF Recommendations Harmful for Crypto Transparency: Chainalysis, 12 April 2019 https://www.coindesk.com/chainalysis-onerous-fatf-recommendations-harmful-for-crypto-transparency
[104] Cited in: Lukas Hofer: FATF veröffentlicht neue Krypto-Richtlinien – Bedrohung oder Chance?, ico.li (Liechtenstein), 24 June 2019 https://www.ico.li/de/fatf-veroffentlicht-neue-krypto-richtlinien/
[105] Valentina Kirilova: CipherTrace conference sheds light on FATF 'Travel Rule' for user info, LeapRate.com, 22 November 2019 https://www.leaprate.com/cryptocurrency/blockchain/ciphertrace-conference-sheds-light-on-fatf-travel-rule-for-user-info/
[106] Henry Linver: FATF AML Regulation: Can the Crypto Industry Adapt to the Travel Rule?, Cointelegraph, 10.October 2019 https://cointelegraph.com/news/fatf-aml-regulation-can-the-crypto-industry-adapt-to-the-travel-rule

CipherTrace published a report for the third quarter of 2019, which for the first time provides a look at the current KYC practices of crypto trading platforms around the world.[107] According to the report, identification and KYC checks leave much room for improvement and in general companies are poorly prepared for the adoption of the FATF rules. Two thirds of the 120 most important exchanges did not pursue a consistent KYC policy, let alone did they adhere to the soon to be binding wire transfer rule. If nothing changes as far as this alarming finding is concerned, the report opined that many exchanges will face consequences. Furthermore, a third of all platforms reportedly still allowed trading in privacy coins like Zcash and Monero. On the other hand, the majority of the exchanges had already started to remove privacy coins from their offerings. Privacy coins, including Monero, significantly hinder the tracing of transactions. As a result, crypto service providers can only partially comply with the wire transfer rule, which requires that crypto service providers must have access to the accounts and trading activity of their customers. Finally, the report concludes that it would be practically impossible for the exchanges to determine the origin of privacy coins that are transferred to customers' wallets held with the exchanges.

The European analysis house Crystal, which belongs to the Dutch blockchain company Bitfury, published a report in September 2019 on the historical financial flows of Bitcoins between global crypto exchanges. The report also dealt with the question of how the FATF rules will affect Bitcoin payments in the future. The researchers predicted that the number of exchanges for which it is not known where they are registered will decrease significantly as they will no longer be able to operate legally under the FATF rules without official registration and a license. The report forecasts optimistically that the Travel Rule (or Wire Transfer Rule) will undoubtedly make compliance with regulations more complicated for exchanges, but the risk of global criminal misuse of cryptocurrencies could also ultimately decrease considerably.[108]

4.3 Implementation of the Fifth EU Money Laundering Directive

In the European Union, the adoption of the new FATF recommendations coincided with the implementation of the latest EU money-laundering directive. In May 2018 the amending directive to the Fourth Anti-Money Laundering Directive was adopted, which is mostly referred to as the Fifth Anti-Money Laundering Directive (AMLD5).[109] The scope of the new directive is extended to platforms that exchange virtual currencies and wallet providers in order to make it easier to identify cryptocurrency users. The deadline for the

[107] Cryptocurrency Anti-Money Laundering Report, 2019 Q3, November 2019 https://ciphertrace.com/wp-content/uploads/2019/12/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q3-2.pdf
[108] Bitfury Crystal (Ed.): Report on International Bitcoin Flows 2013- 2019, September 2019 https://crystalblockchain.com/assets/reports/International%20Bitcoin%20Flows%20Report%20for%202013-2019%20-%20by%20Crystal%20Blockchain,%20Bitfury.pdf
[109] Directive (EU) 208/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN

directive's implementation into national law was 10 January 2020. Germany complied with this obligation on time so that the new national regulations, which mainly relate to changes in the German Money Laundering and Banking Acts came into force in early 2020.[110]

In two respects the tightening of due diligence in accordance with AMLD5 is particularly relevant for the fight against terrorism financing. Among other things, obliged entities are required to examine the background and purpose of all transactions that follow unusual transaction patterns and have no obvious economic or legal purpose. In order to decide whether these transactions or activities are suspicious, the obliged entities should better monitor existing business relationships. The new Article 18a also requires that additional information must be collected on transactions involving high-risk third countries.[111]

In the public discussion concerning the German implementation law for AMLD5, the topic of cryptocurrencies was only referred to in passing. Many of the new regulations affected other sectors such as the trading of precious metals, the acquisition of real estate (mandatory disclosure of beneficial owners) or stricter inspection requirements for notaries. The changes affecting the crypto sector primarily focused on one point. The crypto custody business (Kryptoverwahrgeschäft), which is the new German legal term for the sector, is now classified as a financial service.[112] Every form of trading in cryptocurrencies will be subject to prior authorization, and providers will in future be supervised by the Federal Financial Supervisory Authority (BaFin).[113] Even before the classification of virtual assets as a financial instrument, commercial trading in cryptocurrencies was subject to BaFin's prior approval. However, this administration practice had been questioned. In 2018, the Berlin Appellate Court had ruled that the unauthorized Bitcoin trading was not a criminal offense and that BaFin had overstretched its mandate.[114] The implementation of AMLD5 in Germany has now cleared up this ambiguity.

---

[110] Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie, 12 December 2019 https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Internationales_Finanzmarkt/2019-07-31-bekaempfung-geldwaesche.html

[111] For an overview of the changes and the development of the previous EU money laundering directives see the summary by Regula Heinzelmann: Die 5. EU-Geldwäscherichtlinie in der Umsetzung, haufe.de, 5 September 2018 https://www.haufe.de/compliance/recht-politik/geldwaescherichtlinie_230132_468208.html

[112] BaFin: Guidance notice – guidelines concerning the statutory definition of crypto custody business (section 1 (1a) sentence 2 no. 6 of the German Banking Act (Kreditwesengesetz – KWG), 2 March 2020 https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaeft_en.html

[113] BaFin has announced that in 2020 "Distributed Ledger Technologie (DLT) and the crypto assets based on it" will be a focus of its supervision activities. BaFin: Aufsichtsschwerpunkte 2020, Bonn und Frankfurt am Main, December 2019, page 9ff. https://www.bafin.de/SharedDocs/Downloads/DE/Broschuere/dl_Aufsichtsschwerpunkte2020.pdf?__blob=publicationFile&v=4

[114] Markus Frühauf: Regelungen bedrohen Bitcoin und Co., Frankfurter Allgemeine Zeitung, 24 July 2019 https://www.faz.net/aktuell/finanzen/digital-bezahlen/kampf-gegen-geldwaesche-regeln-fuer-geschaefte-mit-kryptowaehrung-16299333.html

Service providers based in Germany that exchange virtual currencies and fiat money, as well as wallet providers, are also included in the group of entities subject to money laundering obligations who have to exercise greater due diligence and report suspicious transactions. It should be noted that in August 2019 the German government reported that it was only aware of three companies in Germany that are active in the crypto custody business.[115] However, a significant increase is expected.

With the introduction of the new EU money laundering rules in conjunction with the FATF's travel rule, it seems that Europe, has adopted – with a delay of several years – the broad guidelines set out by American anti-money laundering regulations regarding cryptocurrencies. However, the U.S. system goes further than the new European regulations in one important aspect. In the United States, crypto-crypto payments are also subject to supervision, while the European Union – for the time being – does not intervene with regulations in this area of crypto transactions (i.e. cryptocurrency transactions without a direct link to fiat currencies).[116]

So far, the European Union has not aimed at developing a specific legal framework for cryptocurrencies. However, there is general agreement that national regulations in the crypto sector can only be a temporary solution. The Federal Government of Germany is currently signaling that it is waiting for the development of a new EU regulatory framework, in particular with regard to special crypto tokens such as security tokens or planned stablecoins such as Libra.[117] The Vice President of the European Commission, Valdis Dombrovskis announced a new legislative proposal in October 2019. However, no timeline for the development of this proposal is currently in place. This change in course was triggered by the broad public discussion about Facebook's planned stablecoin Libra. The Latvian EU commissioner had previously spoken out against the regulation of digital currencies. However, by now he agrees that a rethinking of the existing EU mechanisms to combat financial crime is needed.[118]

An EU panel of experts set up by the Commission to identify regulatory barriers to financial innovation submitted a report in December 2019, which also included a number of recommendations related to the crypto sector.[119] The report argues that ultimately, there is a need for extensive harmonization in this field. This harmonization should start with the risks arising from the lack of a common taxonomy regarding crypto assets and

[115] „Drei Betreiber im Kryptoverwahrgeschäft", 29 August 2019 https://www.bundestag.de/presse/hib/655760-655760
[116] Serhii Mokhniev: European AML Regulations Follow the US Path With a Six-Years' Delay, Cointelegraph, 30 November 2019 https://cointelegraph.com/news/european-aml-regulations-follow-the-us-path-with-a-six-years-delay
[117] Politik zu zaghaft. Gesetzentwurf für Blockchain verzögert sich, Frankfurter Allgemeine Zeitung, 15 November 2019
[118] Moritz Draht: EU-Kommissar Dombrovskis fordert eindeutige Gesetzgebung für Krypto-währungen, BIT-Echo, 9 October 2019 https://www.btc-echo.de/eu-kommissar-dombrovskis-fordert-eindeutige-gesetzgebung-fuer-kryptowaehrungen/
[119] Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG): Thirty Recommendations on Regulation, Innovation and Finance. Final Report to the European Commission, 13 December 2019, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf

the fragmented national approaches to classifying cryptocurrencies within the framework of EU regulations and the various national legislative systems that are a consequence of the missing common taxonomy. The requirements for customer-related due diligence (KYC processes) should, according to the recommendation of the report, be completely standardized, especially with regard to the provisions concerning the collection of customer data. For a uniform EU approach in the field of cryptocurrencies, the basic principle states that "activities that create the same risks should be governed by the same rules, thus avoiding fragmentation in this regard".[120]

It is probably no coincidence that the deputy head of the central bank of France, Denis Beau, in a recent speech on the role of cryptocurrencies in the payment system, formulated the same principle "same activities, same risks, same rules". It should be added that when risks are mentioned in this context, financial stability risks as well as the fight against money laundering and terrorism financing are included. In any case, further harmonization of EU money laundering rules seems very likely and necessary.

4.4 The political discussion concerning stablecoins

The international debate concerning cryptocurrencies has been significantly increased since the summer of 2019. At that time Facebook announced that it had launched its own blockchain-based cryptocurrency called Libra in partnership with a number of other companies.[121] Libra would achieve relative stability by connecting it to a currency basket. Therefore, Libra would avoid a major disadvantage of existing cryptocurrencies, i.e. their high volatility or large fluctuations in value. It is expected that such a user-friendly stablecoin with strong financial backing could develop into an attractive digital currency. In particular potential users in emerging and developing countries in particular could take a liking to a stable parallel currency that outperforms their own national fiat currencies. In contrast to leading cryptocurrencies such as Bitcoin or Ethereum, the members of the Swiss-based Libra Association would not operate the new digital currency as an open network. In comparison to for example Bitcoin, this would apparently have the technical advantage of increased transaction speed of the digital currency combined with low energy requirements.[122]

The project has currently stalled, and several participating companies have opted out. Due to the political resistance not only from the American government, the plans were weakened. Recently, there was only talk of a "global payment system" instead of a new currency. Most governments obviously want to prevent the loss of influence that would be caused by the weakening of existing government currencies. They also refer to the necessity to maintain control in order to ensure the stability of the international financial

[120] Thirty Recommendations on Regulation, Innovation and Finance, page 58
[121] Libra Whitepaper (deutsche Fassung) https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf
[122] Wolfgang Prinz: Die Idee hinter Libra ist wichtig für Deutschland, Frankfurter Allgemeine Zeitung, 7 December 2019 (updated online version fo 10 December 2019), https://www.faz.net/aktuell/finanzen/finanzmarkt/facebook-plant-eine-weltumspannende-digitale-waehrung-16522969.html

system. However, the general attraction of the idea behind Libra became clear when several governments announced that they would create their own state controlled digital currency. The German Finance Minister Olaf Scholz also spoke of Europe needing to advance the digital Euro in order to prevent leaving this sector to other states or private entities.[123] Preparations are most advanced in China. There, the government launched a pilot project for the world's first state digital currency.[124]

However, there are also doubts whether central banks are seriously interested in introducing their own cryptocurrencies. No preparatory work in this regard is currently planned at the European Central Bank.[125] It seems more likely that politicians are trying to motivate banks to improve inefficient and expensive cross-border payments by announcing the potential introduction of stablecoins. In any case, governments want to take the wind out of the Libra project's sails. Large banks such as JPMorgan and UBC have long announced plans for digital stablecoins. Furthermore, even before the announcement of Facebook, there were private stablecoins, including Tether, currently the fourth most common cryptocurrency, which also pursue the goal of value stability (e.g. by linking their coin to the U.S. Dollar or a basket of cryptocurrencies).[126]

As a precaution, the FATF already announced in October 2019 that stablecoins and their providers would also be subject to anti-money laundering standards.[127] Further efforts by the FATF on the topic are planned. Security aspects are hardly affected by the stablecoin discussion as long as the announced projects are still in the development phase and their final design remains open. In addition, it is hard to see why terrorists and other criminals should prefer to use a state-controlled cryptocurrency or a digital payment system (Libra) that is heavily influenced by governments. This would be different if countries like Iran or North Korea that are threatened by sanctions seriously considered the introduction of digital currencies. So far, the importance of the discussion concerning Libra or state digital currencies lies in the fact that the global community is gradually getting used to utilizing cryptocurrencies. Therefore, the rise of Libra or a digital Euro could also give Bitcoin and other cryptocurrencies a new boost. A wider adoption of cryptocurrencies in general could then in turn also increase their misuse by criminals or terror groups.

[123] Interview in Wirtschaftswoche, 3 October 2019 https://www.wiwo.de/politik/deutschland/finanzminister-scholz-sehr-sehr-kritisch-gegenueber-libra/25084172.html
[124] Mike Orcutt: Pilottest für Chinas staatliche Kryptowährung, Technology Review, 19 December 2019 https://www.heise.de/tr/artikel/Pilottest-fuer-Chinas-staatliche-Digitalwaehrung-4615207.html
[125] Martin Arnold: Central bank talk of launching cryptocurrencies is all bluff, Financial Times, 5 December 2019 https://www.ft.com/content/5988c3f4-15e6-11ea-9ee4-11f260415385
[126] Alex Anderson: Stablecoins for Beginners. What they are, how they work and where to buy them, Selbstverlag 2019 (Amazon Fulfillment, ISBN 9781077031005)
[127] Money laundering risks from "stablecoins" and other emerging assets, 18 October 2019 https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-virtual-assets-global-stablecoins.html

5 Next steps

Due to the rapid technical developments in the area of cryptocurrencies and the growing technical capabilities of various terrorist organizations, it can be expected that this form of terrorist financing will gain in importance in the short to medium term. Therefore, there is an urgent need to fully understand how terrorists can potentially misuse cryptocurrencies. A further question is how government and regulatory authorities can best respond to these developments.

In the past two years, global efforts to regulate the crypto financial sector have begun. These first regulatory steps became necessary due to the realization of the growing risks posed by financial flows involving cryptocurrencies for combating money laundering and terrorism financing. Not only in Europe, are these flows scarcely or not at all monitored. A first important step has been taken with the implementation of the FATF recommendations from June 2019. The agreed measures aim to treat crypto exchanges around the world analogously to traditional financial institutions. Germany and other countries are on the right track to prevent anonymous crypto transactions that have hitherto been tolerated but are dangerous due to their significant inherent security risks.

However, a major difficulty lies in the high speed with which the underlying technology is changing. It would be a delusion to believe that the current regulatory approach, which focuses on crypto exchanges and on the interfaces between fiat money and cryptocurrencies, offers a sufficient solution. Regulators will have to continue to follow the various technological developments. Differences between payments via banks and the crypto sector will remain. Therefore, governments should further develop and 'fine-tune' their regulatory approach in the coming years with the help also of private sector consultations involving crypto companies who are interested in adapting and maintaining their business model.

From the point of view of the German government, stakeholders and the crypto industry, a number of tasks are pending. Some issues related to cryptocurrencies continue to be neglected and some of the vulnerabilities that were already identified have not yet been addressed. The recommendations outlined below focus on these. It is also important to recognize that an innovative blockchain sector has emerged in Germany which can benefit from consistent regulation.

1. Germany should proceed in parallel - i.e. support further regulation of the crypto sector at the level of the European Union, while at the same time not being hesitant to adjust its national rules and regulations on AML / CFT issues if this becomes necessary.

Currently, among other issues, also as a result of the debate concerning state issued stablecoins, new initiatives at the EU level seem to be emerging. These aim to further harmonize the entire crypto sector. Experiences from dealing with cryptocurrencies and electronic wallets influence the discussion about new norms in the fight against money

laundering and terrorism financing. Therefore, it seems logical for German government stakeholders to support and participate in these European efforts and, for the time being, to refrain from pushing ahead with national rules, unless necessary. In the course of the online consultation on the development of the blockchain strategy of the Federal Government of Germany, very different opinions emerged among companies as to whether regulation at European or national level would be preferred.[128]

Finally, timing should be taken into account. In the context of the Libra discussion, Andreas Krautscheid, managing director of the German banking association, pointed out that it took almost eight years from the idea to the implementation of the new EU Payment Services Directive.[129] However, the eventual establishment of another EU authority should not be seen as an immediate and pressing concern, especially since it would be uncertain what mandate could be delegated to such a central body. Therefore, national approaches may be necessary in the meantime.

2. It is essential to increase the level of existing expertise of government agencies and to reduce the coexistence of parallel regulatory responsibilities in the fight against money laundering and terrorism financing, especially in the crypto sector.

The system responsible for combating money laundering and terrorist financing in Germany is not organized in a consistently effective and cost-efficient manner. Basically, there is a division of labor between the security and law enforcement authorities at the federal and state level. Criminal prosecution in the area of money laundering is largely the responsibility of the federal states. This means that in practical terms it is the responsibility of the relevant public prosecutor's office, which is supported by the police and customs authorities. As far as combating terrorism financing is concerned, the division of labor stipulates a cooperation between public prosecutors and security agencies of the federal and state governments.[130]

The central point for collecting and evaluating suspicious transaction reports in connection with money laundering or terrorist financing is the Financial Intelligence Unit (FIU), which is a separate body headquartered in Cologne that is embedded in the General Customs Directorate (under the authority of the German Finance Ministry).[131] Suspicious activity reports are received and investigated centrally by the FIU. The FIU has the responsibility to filter out important cases and pass them on to the responsible law enforcement authorities.[132]

---

[128] Online-Konsultation zur Erarbeitung der Blockchain-Strategie der Bundesregierung. Gesammelte Stellungnahmen, die zwischen dem 20. Februar und 30. März 2019 eingegangen sind (see for example pages 186, 212, 380, 814) https://www.blockchain-strategie.de
[129] Andreas Krautscheid: Interview with Wirtschaftswoche, 31 October 2019 https://bankenverband.de/newsroom/reden_und_interviews/interview-wiwo-ak-libra/
[130] The federal government's specialized public prosecutor's office for crimes related to terrorist financing is the Federal Attorney General at the Federal Court of Justice. Ultimately, the classification of the respective case determines whether federal or state authorities assume responsibility. See: Erste Nationale Risikoanalyse, page 52f.
[131] The official (less common) name is the Central Office for Financial Transaction Investigations.
[132] Erste Nationale Risikoanalyse, page 39ff.

Concerning the fight against terrorist financing, the FIU will immediately forward all reports that are relevant to terrorism to the Federal Office for the Protection of the Constitution (BfV). If necessary, the BfV will involve the relevant Office for the Protection of the Constitution (LfV) in the respective federal state. If a case involves issues of state security, the FIU forwards the result of its operational analysis to the relevant law enforcement agencies, such as the state protection department at the state criminal investigation offices or public prosecutor's office.[133]

Plans are currently underway to strengthen the FIU by increasing its access to relevant data in connection with money laundering and terrorism financing. However, the authority seems overburdened and has been heavily criticized. This criticism focused on failing to deal with suspicious transactions reports in a timely manner. According to media reports this mostly relates to a potentially problematic reorganization of the authority in summer 2017. Until then, the Federal Criminal Police Office had been responsible for the FIU. A total of 77,252 (2017: 59,845) suspicious activity reports were received in 2018. In August 2019, a backlog of more than 46,000 pending investigations was reported.[134]

As mentioned above, the FIU registered "around 570" suspicious transaction reports from obligated entities in 2018 that are related to cryptocurrencies. With the expansion of the circle of obliged entities as a result of the implementation of AMLD5 a significant increase of suspicious transaction reports related to this sector is likely and the authority itself is expecting this to occur.[135]

In addition to these major challenges, there is often a lack of competent interlocutors within government agencies who are familiar with crypto payment transactions and react to the respective suspicious activity reports. One expert at a crypto service provider in Germany highlighted that on the reporting form for suspicious transactions relating to cryptocurrencies there is currently only the option to indicate whether the respective transaction involves Bitcoin or another cryptocurrency.[136] Therefore, it must be assumed that most government investigators would not be able to effectively use information relating to one of the many other cryptocurrencies.

It is important to emphasize that the absence of qualified experts, relates to the entire blockchain industry. According to a company survey conducted in 2019, the industry expects that in the long term Germany will face a significant shortage of blockchain

[133] Erste Nationale Risikoanalyse, page 51
[134] This information was derived from the Federal Government of Germany's official answer to a written question from Markus Herbrand, member of the federal parliament (Bundestag) for the Free Democratic Party (FDP), see: Jan Willmroth: Der Stapel wächst, Süddeutsche Zeitung, 8 October 2019 https://www.sueddeutsche.de/wirtschaft/zoll-der-stapel-waechst-1.4631795
[135] Financial Intelligence Unit: Jahresbericht 2018, page 36 https://www.zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/FIU/fiu_jahresbericht_2018.pdf?__blob=publicationFile&v=3
[136] Interview, September 2019.

experts.[137] Therefore, it is not realistic to expect that it will be possible to place specialized investigators with knowledge of cryptocurrencies in every state criminal investigation office and every public prosecutor's office in the future. Therefore, it would make sense for the relevant authorities on the federal and state level to establish a joint pool of specialists, which among others law enforcement agencies can access.[138]

Such a central analysis center could be located at the FIU. Partners from the private sector could also be involved during the initial transitional period. Blockchain analysis tools have already been developed and are used in the commercial sector that enable precise monitoring of the cryptocurrency sector. Such technical capabilities should definitely become part of the toolbox of the financial supervisory authorities.

3. The authorities must require crypto providers to develop relevant compliance experiences and processes and review those. Both sides should cooperate in finding a suitable and cost-effective way to comply with the new FATF rules.

The mandatory implementation of the wire transfer rule by the relevant crypto companies until June 2020, and their monitoring by the supervisory authorities is a test of whether these new national regulations are working. There is a lot at stake for Germany, since the preparatory work for the upcoming mutual evaluation round of Germany by the FATF in December 2020 has begun. The main question will be whether the existing national regulations in the area of AML/CFT are also effectively implemented by law enforcement. [139] Therefore, German government stakeholders will also have to demonstrate that suspicious transaction reports relating to crypto transactions are effectively followed up in Germany.

However, also internationally the timely technical implementation of the Wire Transfer Rule presents challenges, as has already been explained above. A sustainable solution should in any case be cost-effective and thus prevent customers from migrating to a less regulated area, e.g. to use peer-to-peer networks.[140] Among other issues, specific attention should be paid to the quality requirements for technology enabling video and online identifications. Furthermore, it is necessary to develop a detailed definition of the

[137] Bitkom e.V. (Ed.): Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen. Studienbericht 2019, page 38 https://www.bitkom.org/Bitkom/Publikationen/Blockchain-Deutschland-Einsatz-Potenziale-Herausforderungen
[138] A comparison with the Central Office for Combating Internet and Computer Crime (ZIT), which was set up in 2010 as the Gießen branch of the public prosecutor's office in Frankfurt am Main, may be helpful in this regard. The ZIT is the first point of contact for the Federal Criminal Police Office for Internet crimes in the case of unresolved questions concerning local jurisdiction in Germany or in mass proceedings against a large number of suspects nationwide.https://staatsanwaltschaften.hessen.de/staatsanwaltschaften/gsta-frankfurt-am-main/aufgabengebiete/zentralstelle-zur-bekämpfung-der
[139] The last mutual evaluation took place in 2010. See: Bundesministeriums der Justiz und für Verbraucherschutz (Ed.): Kampf gegen Geldwäsche und Terrorfinanzierung. FATF Länderprüfung Deutschland 2020 – Informationen zum Ablauf der Prüfung https://www.bmjv.de/SharedDocs/Publikationen/DE/Geldwaesche.html
[140] Anton Moiseienko / Kayla Izenman: From Intention to Action. Next Steps in Preventing Criminal Abuse of Cryptocurrency, RUSI Occasional Paper, September 2019, page 25 https://rusi.org/publication/occasional-papers/intention-action-next-steps-preventing-criminal-abuse-cryptocurrency

heightened due diligence requirements for crypto business relationships that involve increased risks. The investigative authorities and crypto companies should cooperate to develop specific indicators concerning suspicious behavior and actions related to crypto transactions.

A positive signal is the announcement that all competent authorities in Germany will cooperate to develop updated typologies for the area of terrorism financing. The goal is to supply more and more specific information to the obliged entities.[141] In view of the peculiarities of terrorism financing, the role of the minimum threshold values for crypto transactions ($1,000 or Euros according to the requirements of the FATF) should not be seen as central. Terrorist groups and operations are often financed through a variety of transactions involving only small amounts.

Examples from the United States demonstrate that crypto companies are interested in a good relationship with law enforcement agencies. An employee at a decentralized trading platform indicated that there is hardly any government agency in the United States that does not feel responsible for crypto payment transactions or, in specific cases, requests cooperation. At the same time, he explained that American crypto exchanges are comfortable with regards to their confidential cooperation with state authorities. Information about transactions by suspects requested by authorities would be communicated, even if it was not always clear whether the (decentralized) exchanges were legally obliged to do so. He emphasized that companies are able set their own internal rules for this. Such self-regulation should be seen against the background that crypto providers also aim to develop a good reputation with government stakeholders to counteract calls for stricter regulation of crypto trading.[142]

4. The political goal of preventing anonymous transactions has not yet been achieved. Legal non-regulated crypto payments continue to exist. There is an additional need for regulating the use of non-custodial wallets.

The new FATF requirements focus on crypto payment transactions between intermediaries or customers who initiate transactions with wallets hosted on crypto exchanges. For other payment methods, which are likely to become more important, this regulatory framework is not sufficient. If many companies begin to accept cryptocurrency as a means of payment in the future, there should be a significant number of new risks and money laundering concerns. Regulatory gaps concerning non-custodial wallets also exist. The wire transfer rule takes effect only when the wallets on both sides of the transaction are hosted at an exchange. As soon as a customer sends e.g. Bitcoins to a non-custodial wallet (which is owned by an individual without a personal ID registered with an exchange), the transaction does not trigger the rule. Consequently, money can still be directed out of the regulated market.[143]

---

[141] Erste Nationale Risikoanalyse, page 61
[142] Interview, October 2019
[143] Yaya Fanusie: The Travel Rule Is Not Enough If Crypto Gets Adopted, forbes.com, 30 October 2019 https://www.forbes.com/sites/yayafanusie/2019/10/30/the-travel-rule-is-not-enough-if-crypto-gets-adopted/#6dbc7b0921e3 Fanusie refers to the American Travel Rule, which is in practical term includes the same provisions than the Wire Transfer Rule referred to here.

In some important respects, Switzerland has gone further than the FATF standards require. According to a statement published by the Swiss Financial Market Supervisory Authority (Finma) on 26 August 2019, institutions supervised by Finma "are only permitted to send cryptocurrencies or other tokens to external wallets belonging to their own customers whose identity has already been verified and are only allowed to receive cryptocurrencies or tokens from such customers. FINMA-supervised institutions are thus not permitted to receive tokens from customers of other institutions or to send tokens to such customers." [144] This practice, which is stricter than other similar national regulations, will apply as long as no reliable information can be transmitted within the respective payment system concerning the sender or recipient. It should be discussed whether this practice could not be adopted also by Germany.

Sooner or later the fate of so-called privacy coins like Monero seems to be sealed. In fact, it seems likely that the current regulatory development in this sector will result in a ban on payment transactions involving privacy coins at the crypto exchange level. This is due to the fact that the information required by the FATF cannot be collected by the exchanges for technical reasons if privacy coins are involved. Therefore, in the future it seems possible that this (almost) anonymous payment method will only be used in the unregulated peer-to-peer area. If all regulated crypto exchanges comply with the FATF guidelines, they can no longer offer privacy coins for trading. Thus, it will be very difficult to acquire or trade privacy coins or convert them into fiat currency in the future. If this becomes the case, the use of privacy coins could even be considered as a basis for initial suspicion concerning potential malign behavior.

Regulators will continue to face the difficult task of taking a balanced approach. In line with the security authorities, they are interested in ensuring that customers do not feel compelled to switch to relatively softly regulated crypto exchanges outside of Europe and North America. Criminals will look for and likely find ways to take advantage of new developments in this technology area and are likely to avoid the regulated sector altogether. Instead, governments should encourage the crypto industry to cooperate. Regulatory measures should avoid overburdening this young industry in order to prevent stifling innovation. In return, government agencies should expect crypto companies to be willing to make their necessary contribution to combating money laundering and terrorism financing.

[144] FINMA guidance: stringent approach to combating money laundering on the blockchain, 26 August 2019, https://finma.ch/en/news/2019/08/20190826-mm-kryptogwg/

6 Literature

The list includes a selection of the publications and media reports used for this report. It also includes resolutions and statements from international organizations and government agencies that refer to the existing or planned regulatory framework concerning crypto assets.

Basel Committee on Banking Supervision: Statement on crypto-assets, 13 March 2019
https://www.bis.org/publ/bcbs_nl21.htm

Basel Committee on Banking Supervision: Discussion paper. Designing a prudential treatment for crypto-assets. Issued for comment by 13 March 2020, December 2019
https://www.bis.org/bcbs/publ/d490.pdf

Beau, Denis: The role of cryptoassets in the payment system, Official Monetary and Financial Institutions Forum (OMFIF) Meeting, London, 15 October 2019
https://www.bis.org/review/r191015b.htm

Bergmann, Christoph: Bitcoin. Die verrückte Geschichte vom Aufstieg eines neuen Geldes, Moby Verlagshütte, Nersingen 2019 (second edition)

Bitfury Crystal (Ed.): Report on International Bitcoin Flows 2013-2019, September 2019
https://crystalblockchain.com/assets/reports/International%20Bitcoin%20Flows%20Report%20for%202013-2019%20-%20by%20Crystal%20Blockchain,%20Bitfury.pdf

Bitkom e.V. (Ed.): Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen. Studienbericht 2019
https://www.bitkom.org/Bitkom/Publikationen/Blockchain-Deutschland-Einsatz-Potenziale-Herausforderungen

Brett, Jason: Congress Considers Federal Crypto Regulators In New Cryptocurrency Act Of 2020, forbes.com, 19 December 2020
https://www.forbes.com/sites/jasonbrett/2019/12/19/congress-considers-federal-crypto-regulators-in-new-cryptocurrency-act-of-2020/#57eb0f4d5fcd

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (Ed.): Aufsichtsschwerpunkte 2020, Bonn und Frankfurt am Main, December 2019
https://www.bafin.de/SharedDocs/Downloads/DE/Broschuere/dl_Aufsichtsschwerpunkte2020.pdf?__blob=publicationFile&v=4

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (Ed.): Guidance notice – guidelines concerning the statutory definition of crypto custody business (section 1 (1a) sentence 2 no. 6 of the German Banking Act (Kreditwesengesetz – KWG), 2 March 2020 https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_krypto verwahrgeschaeft_en.html

Bundesministerium der Finanzen (Ed.): Erste Nationale Risikoanalyse. Bekämpfung von Geldwäsche und Terrorismusfinanzierung 2018/2019, October 2019 https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2019-10-19-erste-nationale-risikoanalyse_2018-2019.html

Bundesministerium der Justiz und für Verbraucherschutz (Ed.): Kampf gegen Geldwäsche und Terrorfinanzierung. FATF Länderprüfung Deutschland 2020. Informationen zum Ablauf der Prüfung, ohne Datum (November 2019) https://www.bmjv.de/SharedDocs/Publikationen/DE/Geldwaesche.html

Bundesministerium für Wirtschaft und Energie / Bundesministerium der Finanzen (Ed.): Blockchain-Strategie der Bundesregierung. Wir stellen die Weichen für die Token-Ökonomie, ohne Datum (September 2019) www.blockchain-strategie.de

Chainalysis: Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly, 17 January 2020 https://blog.chainalysis.com/reports/terrorism-financing-cryptocurrency-2019

Ciphertrace (Ed.): Cryptocurrency Anti-Money Laundering Report, 2019 Q3, November 2019 https://ciphertrace.com/wp-content/uploads/2019/12/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q3-2.pdf

Counter Extremism Project (Ed.): Terrorists on Telegram, May 2017 https://www.counterextremism.com/terrorists-on-telegram

Dion-Schwarz, Cynthia / Manheim, David / Johnston, Patrick B.: Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats, RAND Corporation, Santa Monica 2019 https://www.rand.org/pubs/research_reports/RR3026.html

Draht, Moritz: EU-Kommissar Dombrovskis fordert eindeutige Gesetzgebung für Kryptowährungen, BIT-Echo, 9 October 2019 https://www.btc-echo.de/eu-kommissar-dombrovskis-fordert-eindeutige-gesetzgebung-fuer-kryptowaehrungen/

Eidgenössische Finanzmarktaufsicht FINMA: Aufsichtsmitteilung: Konsequente Geldwäschereibekämpfung im Blockchain-Bereich, 26 August 2019 https://finma.ch/de/news/2019/08/20190826-mm-kryptogwg

Elliptic: Bitcoin Money Laundering: How Criminals Use Crypto (And How MSBs Can Clean Up Their Act), 18 September 2019
https://www.elliptic.co/our-thinking/bitcoin-money-laundering

Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG): Thirty Recommendations on Regulation, Innovation and Finance. Final Report to the European Commission, 13 December 2019
https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf**Fanusie, Yaya J.:** The New Frontier in Terror Fundraising, in: Bitcoin, The Cipher Brief, 24 August 2016
https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin

Fanusie, Yaya J. / Robinson, Tom: Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services, 12 January 2018
https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf

Fanusie, Yaya J.: The Travel Rule Is Not Enough If Crypto Gets Adopted, forbes.com, 30 October 2019
https://www.forbes.com/sites/yayafanusie/2019/10/30/the-travel-rule-is-not-enough-if-crypto-gets-adopted/#6dbc7b0921e3

Financial Action Task Force (FATF) (Ed.): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations, Paris 2019
www.fatf-gafi.org/recommendations.html

Financial Action Task Force (FATF) (Ed.): Money laundering risks from “stablecoins” and other emerging assets, 18 October 2019
https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-virtual-assets-global-stablecoins.html

Financial Action Task Force (FATF) (Ed.): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, June 2019
www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

Financial Action Task Force (FATF) (Ed.): Public Statement on Virtual Assets and Related Providers, 21 June 2019
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html

Financial Action Task Force (FATF) (Ed.): Virtual Assets: What, When and How? Easy Guide to FATF Standards and Methodology, December 2019
http://www.fatf-gafi.org/media/fatf/documents/bulletin/FATF-Booklet_VA.pdf

Financial Crimes Enforcement Network (FinCEN) (Ed.): FinCEN Guidance: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, 9 May 2019
https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

Financial Intelligence Unit (Ed.): Jahresbericht 2018, Köln, July 2019
https://www.zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/FIU/fiu_jahresbericht_2018.pdf?__blob=publicationFile&v=3

Gilbert, David: ISIS Is Experimenting with This New Blockchain Messaging App, vice.com, 13December 2019
https://www.vice.com/en_us/article/v744yy/isis-is-experimenting-with-this-new-blockchain-messaging-app

Grzywotz, Johanna: Virtuelle Kryptowährungen und Geldwäsche, Duncker & Humblot, Berlin 2019

Katsiri, Roy: Bitcoin donations to ISIS soared day before Sri Lanka bombings, Globes (Israel), 2 May 2019
https://en.globes.co.il/en/article-exclusive-isis-funded-sri-lanka-bombings-with-bitcoin-donations-1001284276

Keatinge, Tom / Keen, Florence: Social Media and Terrorist Financing. What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?, Global Research Network on Terrorism and Technology: Paper No. 10 (RUSI), London 2019
https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf

Kirilova, Valentina: CipherTrace conference sheds light on FATF 'Travel Rule' for user info, LeapRate.com, 22 November 2019
https://www.leaprate.com/cryptocurrency/blockchain/ciphertrace-conference-sheds-light-on-fatf-travel-rule-for-user-info/

Klee, Christopher: Durchbruch im Crypto Country: Liechtenstein verabschiedet Blockchain Act, BTC-Echo, 3 October 2019
https://www.btc-echo.de/durchbruch-im-crypto-country-liechtenstein-verabschiedet-blockchain-act/

Koenig, Aaron: Die dezentrale Revolution. Wie Bitcoin und Blockchain Wirtschaft und Gesellschaft verändern, FinanzBuch Verlag, München 2019

Küfner, Robert A.: Das Krypto-Jahrzehnt. Was seit dem ersten Bitcoin alles geschehen ist – und wie digitales Geld die Welt verändern wird, Börsenbuchverlag, Kulmbach 2018

Libra Whitepaper (deutsche Fassung)
https://libra.org/de-DE/white-paper

Linver, Henry: FATF AML Regulation: Can the Crypto Industry Adapt to the Travel Rule?, Cointelegraph.com, 10 October 2019
https://cointelegraph.com/news/fatf-aml-regulation-can-the-crypto-industry-adapt-to-the-travel-rule

Middle East Media Research Institute (MEMRI): Defiant Message From ISIS In Response To Campaign Against Its Presence On Telegram, Other Platforms, 2 December 2019
https://www.memri.org/reports/defiant-message-isis-response-campaign-against-its-presence-telegram-other-platforms

Moiseienko, Anton / Isenman, Kayla: From Intention to Action. Next Steps in Preventing Criminal Abuse of Cryptocurrency, RUSI Occasional Paper, September 2019
https://rusi.org/publication/occasional-papers/intention-action-next-steps-preventing-criminal-abuse-cryptocurrency

Mokhniev, Serhii: European AML Regulations Follow the US Path With a Six-Years' Delay, Cointelegraph, 30 November 2019
https://cointelegraph.com/news/european-aml-regulations-follow-the-us-path-with-a-six-years-delay

Policy Department for Citizens' Rights and Constitutional Affairs (Directorate General for Internal Policies of the Union) (Ed.): Virtual currencies and terrorist financing: assessing the risks and evaluating responses, May 2018
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604970

Popper, Nathaniel: Terrorists Turn to Bitcoin for Funding, and They're Learning Fast, The New York Times, 18 August 2019
https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html

Schweizerische Eidgenossenschaft (Ed.): National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding. Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), October 2018
https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf

Sexer, Nathan: State of Decentralized Exchanges, 2018
https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79

Smith, Brenna: The Evolution Of Bitcoin In Terrorist Financing, bellingcat.com, 9 August 2019
https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/

Stalinsky, Steven: The Coming Storm – Terrorists Using Cryptocurrency, Middle East Media Research Institute (MEMRI), 21 August 2019
https://www.memri.org/reports/coming-storm-%E2%80%93-terrorists-using-cryptocurrency

United States Department of Justice: Long Island Woman Pleads Guilty to Providing Material Support to ISIS, 26 November 2018
https://www.justice.gov/usao-edny/pr/long-island-woman-pleads-guilty-providing-material-support-isis

Wieczner, Jen: Bitcoin Accounts for 95% of Cryptocurrency Crime, Says Analyst. fortune.com, 24 April 2019
https://fortune.com/2019/04/24/bitcoin-cryptocurrency-crime/

Willmroth, Jan: Der Stapel wächst, Süddeutsche Zeitung, 8 October 2019
https://www.sueddeutsche.de/wirtschaft/zoll-der-stapel-waechst-1.4631795

Wilson, Tom & Williams, Dan: Hamas shifts tactics in bitcoin fundraising, highlighting crypto risks: research, Reuters, 26 April 2019
https://uk.reuters.com/article/us-crypto-currencies-hamas/hamas-shifts-tactics-in-bitcoin-fundraising-highlighting-crypto-risks-research-idUKKCN1S20FA

BERLIN RISK

COUNTER EXTREMISM PROJECT