COUNTER EXTREMISM PROJECT (CEP)

AND

BERLIN RISK

POLICY PAPER

FURTHER DEVELOPMENT OF EUROPEAN UNION REGULATORY FRAMEWORK

FOR CRYPTOCURRENCIES NECESSARY

TO MITIGATE RISKS OF TERRORISM FINANCING

COUNTER EXTREMISM PROJECT

BERLIN RISK

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 left-wing 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

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

AUTHORS:

Dr. Hans-Jakob Schindler, Senior Director CEP and former Coordinator ISIL, al-Qaida and Taliban Monitoring Team, United Nations Security Council

In cooperation with:

Jennifer Hanley-Giersch, Managing Partner Berlin Risk and founding board member of Association of Certified Anti-Money Laundering Specialists (ACAMS), Germany Chapter

Dr. Daniel Eisermann, Senior Partner Berlin Risk and member of the German Council on Foreign Relations

If you have any questions relating to this Policy Paper, please contact
Marco Macori, CEP Research Fellow: mmacori@counterextremism.com; Tel. +49 30 300 149 3369

Summary

During the last few years, cryptocurrencies have repeatedly been misused by terrorist groups as well as their members and supporters to finance their activities. Both extremist Islamist as well as extremist right-wing organizations have demonstrated an interest in adopting this new technology, attempted to solicit funds, and in one case, apparently financed a terrorist attack using this asset class. The ability to keep the identity of sender and receiver of cryptocurrencies anonymous presents a core challenge for countering the financing of terrorism (CFT) in this regard.

Regulators both via the Financial Action Task Force (FATF) as well as the European Union (EU) have reacted to this emerging threat, highlighting the various risk factors and providing guidance both to national regulators as well as industry participants. With the Fight Anti Money Laundering Directive (AMLD5), the EU decided that virtual asset service providers would now be included as obliged entities and adhere to the reporting requirements of financial institutions. This is a first important step. However, further EU regulatory action is required in order to further mitigate CFT risks in connection with cryptocurrencies.

These should concentrate on **four main areas:**

a) **Conceptualizing crypto assets as a distinct regulatory sector** to avoid only regulating the use of this new asset class in certain sectors, and therefore potentially creating regulatory loopholes for other sectors who have already or are likely to adopt this technology in the future.

b) **Increasing cooperation between European Financial Intelligence Units**, since cryptocurrencies are specifically engineered to facilitate cross-border transactions. This could be done by building on the European Banking Authority's (EBA) already existing mandate and the development of a European Financial Intelligence Unit (FIU) Dashboard through which the exchange of investigative information and technical capabilities and capacities would be facilitated.

c) **Regulating crypto-to-crypto exchange**, since the AMLD5 currently focuses only on the exchange between fiat and cryptocurrencies. Maintaining only one single regulatory hurdle against the illicit misuse of cryptocurrencies seems insufficient, given rising adoption rates of cryptocurrencies overall.

d) **Responding to the challenges posed by privacy coins, non-custodial wallets and exchanges**, which offer enhanced protection of user data and remove the intermediary. Such technologies present serious challenges for CFT. Unless and until new investigative technological tools that are effective and efficient for general market monitoring have been developed, it seems necessary to prohibit the use of privacy coins, non-custodial wallets and exchanges within the jurisdiction of the EU. This would enable law enforcement authorities to focus their specialized investigative and legal tools on a smaller set of individuals who insist on continuing to use this technology.

1. Developing threat of terrorism financing using cryptocurrencies

Over the past years, there have been numerous cases – from extremist Islamist to extremist right-wing – of attempts to solicit funds in cryptocurrencies.[1] In the case of the 2019 bombing in Sri Lanka for example, cryptocurrencies were used to finance a complex terrorist attack.[2] Furthermore both in 2015 and 2017, ISIL members were arrested and convicted in the United States for attempting to support the terrorist group in adopting this technology and attempting to solicit funds in cryptocurrency,[3] demonstrating the interest of this global terror network in this new asset class.

In February 2020, the Counter Extremism Project (CEP) and Berlin Risk completed an in-depth report, analysing this emerging threat, highlighting global and European regulatory developments and making a range of recommendations for the German government.[4] Therefore, while this type of asset may not yet be the major terrorist financing tool within the European Union, cryptocurrencies offer several advantages for individuals and groups engaged in illicit behaviour, including the financing of terrorist organisations.[5]

One of the main challenges for CFT is the enhanced ability to keep the identity of cryptocurrency users confidential. Terrorist financing frequently involves small sums to finance terror cells or individual attacks. Consequently, verifying the identity of the sender as well as that of the receiver and their potential connection to terrorist groups is essential to CFT. The ability to anonymize transactions using cryptocurrencies is seen by many as a necessary tool to guarantee user privacy since transactions are publicly recorded on the blockchain.[6] However, the use of so-called mixing services and tumblers that break up individual transactions and re-assemble them in a different form[7] weakens the argument that the public record of the transactions in the blockchain is a sufficient tool used to mitigate the risk of illicit misuse.

Another risk factor is the ability to transact from one cryptocurrency to another. If this type of transactions remains unregulated, the regulated fiat-to-cryptocurrency and crypto-to-fiat

[1] Yaya Fanusie, "Hamas Military Wing Crowdfunding Bitcoin," *Forbes*, 4 February 2019, https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#5327df034d7f; "Far-Right European Terrorist Group Crowdfunding Cryptocurrency," *Counter Extremism Project*, 28 August 2018, https://www.counterextremism.com/blog/far-right-european-terrorist-group-crowdfunding-cryptocurrency.
[2] Yashu Gola, "Breaking: ISIS Used Bitcoin to Fund Horrific Sri Lanka Easter Bombings, Research Claims," *CCN MArkets*, 2 May 2019, https://www.ccn.com/isis-bitcoin-fund-sri-lanka-easter-bombings/.
[3] Nikita Malik, "How Criminals And Terrorists Use Cryptocurrency: And How To Stop It," *Forbes*, 31 August 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#21a6f8493990.
[4] Dr. Daniel Eisermann, "Kryptowährungen als Risiko für die öffentliche Sicherheit und Terrorismusbekämpfung. Gefahrenanalyse und Probleme der Regulierung." CEP and Berlin Risk, February 2020.
[5] 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.
[6] "Protect your privacy," *Bitcoin.org*, https://bitcoin.org/en/protect-your-privacy.
[7] Osato Avan-Nomayo, "Cryptocurrency Mixers and Why Governments May Want to Shut Them Down," *Cointelegraph*, 28 May 2019, https://cointelegraph.com/news/cryptocurrency-mixers-and-why-governments-may-want-to-shut-them-down.

currency exchanges will be the only hurdle against illicit misuse. Given the complexity of challenges and the significant risk linked to CFT, a single hurdle is not sufficient. As the adoption rate of this asset class is generally expected to increase globally through the introduction of further stable coins, the threat posed will naturally increase also.[8]

2. Current regulatory responses and emerging challenges

Regulators both on the global as well as on the EU level have responded to this situation.[9] The FATF published guidance in 2019[10] and the EU focused on elements of the new technology that offer services to users, in particular providers of custodial wallets and custodial exchanges. With the AMLD5, the EU decided[11] that virtual asset service providers would be included amongst the list of those entities obliged to adhere to the reporting requirements of financial institutions.[12] This is an important first step as these service providers now have to implement and maintain effective compliance, due diligence and Know Your Customer (KYC) procedures. Although this is a fairly new provision, online service providers as well as regulators will have to ensure that the appropriate mechanisms for customer identification and verification are set. In addition, regulators and prosecutors will need to have sufficient expertise, including technical capabilities and capacities, to handle the new reports being filed by this industry.

However, further regulation on the EU level will be necessary. Uneven regulatory frameworks within the EU would entail the risk that any regulatory differences could be exploited by terrorist groups. For example, Hamas has already exploited such a situation in one of its crowdfunding campaigns. The group moved its campaign away from a regulated U.S.-based exchange to another jurisdiction with a less stringent regulatory framework.[13]

[8] Ana Alexandre, "Report: Stablecoins See Significant Growth in Adoption Over Recent Months". Cointelegraph, 10 December 2018, https://cointelegraph.com/news/report-stablecoins-see-significant-growth-in-adoption-over-recent-months.
[9] Already in 2014 the European Banking Authority (EBA) classified the terrorism financing risks associated with cyrptocurrencies as high. See: European Banking Authority. "EBA Opinion on 'virtual currencies' EBA/Op/2014/08", 4 July 2014, page 22, https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1.
[10] "Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers," *Financial Action Task Force*, June 2019, http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.
[11] AMLD5 had to be transposed into national law by all members of the EU by 10 January 2020.
[12] "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU," *Official Journal of the European Union,* 30 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN.
[13] Brenna Smith, "The Evolution Of Bitcoin In Terrorist Financing," *Bellingcat*, 9 August 2019, https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/.

3. Necessary additional regulatory steps

3.1 Conceptualizing crypto assets as a distinct regulatory sector

In February 2020, the European Supervisory Authorities (ESAs) published a revised draft of its "Risk Factors Guidelines".[14] These guidelines aim to inform the financial industry and support their development of measures to mitigate the risk of the misuse of the financial sector for money laundering and terrorism financing.[15] Therefore, these guidelines are also significant for national authorities in their design of national legal and regulatory frameworks. Continuing to address the newer developments in the cryptocurrency sector within the revised guidelines will be an important step.

The current draft of the guidelines addresses cryptocurrencies only in connection within two sectors – retail banks[16] and crowdfunding platforms.[17] Of course, the risk of the misuse of retail banking by terrorist financiers has been documented for almost two decades.[18] Furthermore, fundraising is one of the major terrorism financing tools, and consequently, crowdfunding platforms face an increased risk that their services will be misused.[19]

However, the application of cryptocurrencies and their related technology is not limited to these two sectors. For example, several real estate companies in the United States accept bitcoins as payment.[20] Regulating the use of cryptocurrencies for each sector only after the adoption of this asset class in the respective sector, is a retroactive approach and not an effective risk mitigating mechanism. The definition of cryptocurrencies and crypto assets as a separate regulatory sector within the Risk Factors Guidelines would allow for overall regulation of this

[14] European Banking Authority (EBA), European Security and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA), Joint Committee of the European Supervisory Authorities, "Consultation Paper", 5 February 2020, https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2020/Draft%20Guidelines%20under%20Articles%2017%20and%2018%284%29%20of%20Directive%20%28EU%29%202015/849%20on%20customer/JC%202019%2087%20CP%20on%20draft%20GL%20on%20MLTF%20risk%20factors.pdf.

[15] European Banking Authority (EBA), "Guidelines on risk factors and simplified and enhanced customer due diligence", https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence.

[16] European Banking Authority (EBA), European Security and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA), Joint Committee of the European Supervisory Authorities, "Consultation Paper", 5 February 2020, page 80f.

[17] European Banking Authority (EBA), European Security and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA), Joint Committee of the European Supervisory Authorities, "Consultation Paper", 5 February 2020, page 126f.

[18] See for example: Financial Action Task Force (FATF), "Guidance for Financial Institutions in Detecting Terrorism Financing", 24 April 2002, https://www.fatf-gafi.org/media/fatf/documents/Guidance%20for%20financial%20institutions%20in%20detecting%20terrorist%20financing.pdf.

[19] CEP will be highlighting deficiencies concerning CFT in the Terms of Service of crowdfunding platforms in the forthcoming CEP Policy Paper "Social Media and Financing of Terrorism"; *see also*: Tom Keating, Florence Keen, "Social Media and Terrorist Financing: What are the Vulnerabilities and How Could Public and Private Sector Collaborate Better?" Royal United Services Institute, 2019, https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.

[20] Xcel Pay, "Real Estate Companies that Accept Bitcoin", 13 June 2019, https://medium.com/@xcelpay2018/real-estate-companies-that-accept-bitcoin-25f3d7eb0c7a.

asset class, irrespective of individual sectors, and thus prevent the emergence of regulatory loopholes when new sectors adopt this technology.

3.2 Increasing cooperation between European Financial Intelligence Units

The basic approach of cryptocurrencies is their extraterritorial character, removed from centralized controls and regulatory frameworks.[21] Therefore, the involvement of multiple jurisdictions within transactions is not the exception but the rule. Consequently, purely national oversight within the EU is unlikely to be a sufficient approach in the prevention of their misuse of the financing of terrorism. In July 2019 the European Commission highlighted the need to reinforce cooperation between European FIUs to counter the challenge terrorism financing.[22]

Countering the misuse of cryptocurrencies is going to require a stronger pooling of resources, technical capabilities and expertise as well as a quick and efficient exchange of relevant information between European FIUs. To this end, faster and more efficient information exchange mechanisms should be developed. Given the technological challenges that emerging technologies like cryptocurrencies present, designating specialized FIUs with enhanced technical capabilities, such as blockchain analysis tools,[23] may be an effective step to manage limited resources in mitigating these developing risks in CFT.

For this purpose, the mandate of the EBA "to lead, coordinate and monitor the AML/CFT efforts of all EU financial services providers and competent authorities"[24] could be built upon. Already the EBA is planning to create a new AML/CFT database and to foster cooperation between "AML/CFT competent authorities, and between AML/CFT competent authorities and prudential authorities".[25] In this context, the EBA could lead in developing a European FIU Dashboard for cryptocurrency investigations. Such a European FIU Dashboard could then be accessed via a secure application programming interface (API) by the respective competent authorities. The European FIU Dashboard could allow FIUs to securely exchange information relevant to cryptocurrency investigation as well as house and provide access to specialized technical investigative tools for the participating competent authorities.

---

[21] Dr. Daniel Eisermann, "Kryptowährungen als Risiko für die öffentliche Sicherheit und Terrorismusbekämpfung. Gefahrenanalyse und Probleme der Regulierung." CEP and Berlin Risk, February 2020, page 11ff.
[22] European Commission, "Fight against money laundering and terrorist financing: Commission assesses risks and calls for better implementation of the rules", 24 July 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4452.
[23] Kieran Smith, "Blockchain analysis leads to darknet takedown", BraveNewCoin, 25 October 2019, https://bravenewcoin.com/insights/blockchain-analysis-leads-to-darknet-takedown.
[24] European Banking Authority (EBA), "Anti-money laundering and countering the financing of terrorism", February 2020, page 2, https://eba.europa.eu/sites/default/documents/files/document_library/News%20and%20Press/Press%20Room/Press%20Releases/2020/EBA%20acts%20to%20improve%20AML/CFT%20supervision%20in%20Europe/AML%20CFT%20Factsheet.pdf.
[25] European Banking Authority (EBA), "Anti-money laundering and countering the financing of terrorism", February 2020, page 8.

3.3 Regulating crypto to crypto exchange

Although, the AMLD5 has taken a first step by bringing cryptocurrencies (referred to as virtual assets) into the regulatory framework's scope, the directive merely regulates "providers engaged in exchange services between virtual currencies and fiat currencies".[26] While this is a first significant step, it does not regulate providers when they are engaged in exchanging one cryptocurrency into a different cryptocurrency.

If this type of transaction remains unregulated, only the regulated fiat-to-cryptocurrency and crypto-to-fiat currency exchanges will be a hurdle against illicit misuse. Maintaining only one single regulatory hurdle against the illicit misuse of cryptocurrencies seems insufficient, given rising adoption rates of cryptocurrencies. This could become a serious threat if the adoption rate of this asset class increases globally through the introduction of additional so-called stable coins.[27]

This will also mean that other economic sectors will begin to adopt crypto transactions and accept cryptocurrencies as tender, increasing the likelihood for crypto-to-crypto exchanges.[28] Consequently, adding such exchanges to the regulatory framework seems to be a necessary next step in order to ensure that even if illicit behavior is not detected during the initial exchange from fiat to cryptocurrencies, further monitoring is possible and that the risk of detection remains high at all stages.

3.4 Responding to the challenges posed by privacy coins, as well as non-custodial wallets and exchanges

Finally, the technical development of this asset class continues at great speed, demonstrating the need to ideally address emerging CFT risks imminently. Privacy coins like Monero offer even more enhanced protection of user privacy.[29] There is already one documented case of a terrorist group in Syria publicly announcing its intention to use the privacy coins Monero, Dash and Verge to finance its activities.[30] Therefore, a regulatory decision concerning the particular

[26] Amendment to Directive (EU) 2015/849 (1) point (3) of Article 2(1), adding point (g) "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU," Official Journal of the European Union, 30 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN.
[27] Ana Alexandre, "Report: Stablecoins See Significant Growth in Adoption Over Recent Months". Cointelegraph, 10 December 2018, https://cointelegraph.com/news/report-stablecoins-see-significant-growth-in-adoption-over-recent-months.
[28] For example, already online retailers for luxury cars, such as BitCars (https://bitcars.eu), but also sectors in problematic jurisdictions, such as travel agencies in the Islamic Republic of Iran, are adopting this asset class as tender; *see also*: BTC Manager, "Iran's Tourism Sector Recognizes Cryptos as Legal Tender", 23 March 2019, https://btcmanager.com/irans-tourism-sector-recognizes-cryptos-legal-tender/?q=/irans-tourism-sector-recognizes-cryptos-legal-tender/&.
[29] "Monero: A Reasonably Private Digital Currency," *Monero*, https://www.getmonero.org.
[30] Policy Department for Citizens' Rights and Constitutional Affairs: Virtual currencies and terrorist financing: assessing the risks and evaluating responses, Mai 2018, page 34,

sub-set of cryptocurrencies has to be made. Given the increased protection of customer data, including by providers of intermediary services such as exchanges, general regulatory action seems to be a significant challenge since regular customer due diligence operations are impossible to conduct for such transactions. Consequently, only the development of enhanced monitoring tools that enable competent authorities to decipher privacy coin transactions may be able to help mitigate the risks. Until and unless such technology is available,[31] the use of such cryptocurrencies should not be legally allowed within the jurisdiction of the EU, enabling competent law enforcement authorities to investigate such transactions with their increased legal and investigative toolsets.

A similar regulatory challenge presents the use of non-custodial or decentralized wallets[32] and exchanges,[33] which allow a pure peer-to-peer (P2P) transactions without the provision of an intermediary. The lack of an intermediary in the preparation and facilitation of such transactions means that the current regulatory framework, which shares the burden of risk mitigation between financial intermediaries and FIUs and consequently avoids putting all transactions under general suspicion, will not be possible.[34]

Consequently, only two approaches seem technically possible. On the one hand, FIUs could be enabled to monitor all such transactions directly through public-private partnerships. Companies specialized in the development of tools built specifically to investigate financial crime through cryptocurrencies have emerged in recent years.[35] However, given that such monitoring requires both technical expertise as well as potentially significant financial resources, this does not seem to be a feasible way to proceed for general market monitoring and supervision purposes, given limited resources. This is particularly the case if – as is generally expected – the global adoption rate of cryptocurrencies is going to increase with the introduction of stable coins, such as Facebook's Libra.[36]

---

https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

[31] Some have therefore argued that the upper layer of the regulatory framework should link into the lower anonymised layer of cryptocurrency transactions and that "the investigation would thus happen at the upper layer, and where the regulatory infrastructure in a country would define that all transactions would be logged from an anonymised identity to a real identity". Simon Dyson, William J Buchanan, Liam Bell, "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime", 29 July 2019, https://arxiv.org/pdf/1907.12221.pdf.

[32] Jamie Redman, "The Difference Between Custodial and Noncustodial Cryptocurrency Services," *Bitcoin.com*, 29 November 2018, https://news.bitcoin.com/the-difference-between-custodial-and-noncustodial-cryptocurrency-services/.

[33] Andrew Gillick, "The importance of non-custodial decentralized exchange," *Brave New Coin*, 17 January 2019, https://bravenewcoin.com/insights/the-importance-of-building-a-non-custodial-decentralized-exchange.

[34] Some have therefore argued for Simon Dyson, William J Buchanan, Liam Bell, "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime", 29 July 2019, https://arxiv.org/pdf/1907.12221.pdf.

[35] Jennifer Hanley-Giersch, "Regulating a Game Changer - Europe's Approach to Cryptocurrencies" ACAMS Today, 26 June 2018, https://www.acamstoday.org/regulating-a-game-changer-europes-approach-to-cryptocurrencies/.

[36] See for example: Arthur Linuma, "Facebook's Libra: Potential To Increase Demand For Bitcoin", Forbes Agency Council, 17 July 2019,

A second potential approach would be to prohibit the use of such technology within the jurisdiction of the EU. Although this would not likely eliminate the use of such technology, in particular by nefarious actors, it would most likely sufficiently limit the technology's use so that competent law enforcement authorities could concentrate their resources and legal toolsets on investigating those that insist on using this technology for their transactions. If only a limited amount of cases needs to be investigated, the use of public-private partnerships could avoid straining the limited resources available to competent law enforcement authorities.

https://www.forbes.com/sites/forbesagencycouncil/2019/07/17/facebooks-libra-potential-to-increase-demand-for-bitcoin/.