



# D2.1

## Report on Terrorist financing threats and trends

**Lead Beneficiary:** Crime & Tech

**Dissemination  
Level:** Public

**Date:** 31/01/2022

**GA Number:** 101036276



The CTC project has received funding from the ISFP programme under  
Grant Agreement No 101036276.

(This page is intentionally left blank)

## Project Information

<b>Grant Agreement Number</b>	101036276
<b>Acronym</b>	CTC
<b>Name</b>	Cut The Cord
<b>Topic</b>	ISFP-2020-AG-TERFIN TERFIN
<b>Free keywords</b>	CTF, LEAs, Cryptocurrencies, New Payment Systems, FinTech
<b>Start Date</b>	01/11/2021
<b>Duration</b>	24 Months
<b>Coordinator</b>	KEMEA

## Document Information

<b>Work Package</b>	<b>WP2:</b> Identification of Terrorist Financing trends, risks, and end users' requirements
<b>Deliverable</b>	<b>D2.1</b> Report on Terrorist financing threats and trends
<b>Date</b>	31/01/2022
<b>Type</b>	Report
<b>Dissemination Level</b>	Public
<b>Lead Beneficiary</b>	Crime & Tech
<b>Main Author(s)</b>	<b>Maria Jofre</b> (Crime&Tech) <b>Alberto Aziani</b> (Crime&Tech)
<b>Contributors</b>	<b>Mirko Nazzari</b> (Crime&Tech) <b>Mariarena Koulouri</b> (KEMEA) <b>Dimitris Kavallieros</b> (CERTH)
<b>Document Reviewers</b>	<b>Marco Crabu</b> (ABI Lab) <b>Emiliano Anzellotti</b> (ABI Lab) <b>Vassileios Roussakis</b> (HP) <b>Giorgos-Eythimios Giataganas</b> (HP) <b>Georgios Pistolas</b> (HP)
<b>Security Reviewer</b>	<b>Panos Mertis</b> (KEMEA)
<b>Ethics Reviewer</b>	<b>Georgia Melenikou</b> (KEMEA)

## Revision History

Version	Date	Author(s)	Comments
0.1	22/12/2021	Maria Jofre (C&T) Alberto Aziani (C&T)	First draft for review
0.2	26/01/2022	Maria Jofre (C&T) Alberto Aziani (C&T)	Second draft for final review
0.3	28/01/2022	Marco Crabu – Emiliano Anzellotti (ABI Lab)	Review of the Document
0.4	28/01/2022	Vassileios Roussakis (Hellenic Police)	Review of the Document
0.5	30/01/2022	Efstathios Skarlatos (KEMEA)	Consolidated Review

## Disclaimer

The contents of this deliverable are the sole responsibility of the author(s) and do not necessarily reflect the opinion of the European Union.

## Copyright

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation, or both. Reproduction is authorised provided the source is acknowledged.

## Abbreviations

ATM	Automated Teller Machine
CDD	Customer Due Diligence
CTF	Counter-Terrorist Financing
DLT	Distributed Ledger Technology
DPoS	Delegated Proof of Stake
EBA	European Banking Authority
EC	European Commission
EU	European Union
FATF	Financial Action Task Force
FIU	Fiscal Investigation Unit
FBI	Federal Bureau of Investigation
I2P	Invisible Internet Project
IP	Internet Protocol
KYC	Know Your Customer
ML	Money Laundering
MSB	Money-Services Businesses
NFT	Non-Fungible Token
P2P	Peer-to-Peer
STR	Suspicious Transaction Report
TF	Terrorist Financing
TOR	The Onion Router
UK	United Kingdom
UN	United Nations
US	United States of America

# Table of Contents

Executive summary.....	7
1 Introduction.....	9
2 Terrorist financing threats.....	10
2.1 Payment systems.....	10
2.1.1 Traditional payment systems.....	10
2.1.2 Cryptocurrencies.....	11
2.1.3 Non-fungible Tokens (NFTs).....	14
2.1.4 Other New Payment Systems.....	14
2.2 Obfuscation techniques.....	15
2.2.1 Crowdfunding and fundraising initiatives.....	15
2.2.2 Mixers.....	16
2.2.3 Chain-hopping.....	17
2.2.4 Digital wallets.....	17
2.2.5 Metaverse.....	18
2.3 Internet-based communication platforms and social media.....	19
3 Terrorist financing trends.....	20
3.1 Increasing use of crypto assets.....	20
3.2 Increasing use of FinTech-based obfuscation techniques.....	21
3.3 Increasing reliance on self-sustainment.....	22
3.3.1 Fundraising campaigns.....	22
3.3.2 Online crimes and frauds.....	23
4 European and international standards.....	23
4.1 The European Parliament and the Council.....	23
4.2 MONEYVAL.....	24
4.3 European Banking Authority.....	24
4.4 FATF.....	24
4.5 European Securities and Markets Authority (ESMA).....	25
4.6 The World Bank.....	25
5 Conclusions.....	25
5.1 Summary of findings.....	25
5.2 Policy implications.....	26
References.....	27

## Executive summary

In the last decade, a considerable body of evidence has emerged suggesting that **terrorists and terrorism supporters are increasingly making use of FinTech and emerging technologies**. In line with this, it can be observed that terrorist organizations are currently altering their financing techniques and that several emerging threats and resulting trends are becoming known with severe impacts to the EU economies.

Still today, terrorism rely on **traditional payment systems** that include cash smuggling, money-service businesses, formal banking system, false trace invoicing, acquisition of high-value commodities, and the well-known Hawala system. However, terrorist organizations are increasingly making **use of cryptocurrencies**, most of which pose serious terrorism financing (TF)-related threats due to their pseudonymity, potential high negotiability, and capacity to be transacted and withdrawn in real-time. **Bitcoin is the preferred cryptocurrency** for TF purposes. Nonetheless, **alternative cryptocurrencies** have emerged due to their potential for improved anonymity and high-volume transactions. Moreover, alternative crypto-based payment methods have also gained popularity, including **crypto debit and credit cards**, as well as **Bitcoin ATMs and local trade**. Aside cryptocurrencies, terrorism financiers exploit other financial technologies, as is the case of **mobile phone-based money transfers** and **alternative digital payment systems** (e.g., PayPal, other “Peer to Peer” (P2P) transfer payments, etc.). Finally, due to the increasing popularity of Non-Fungible Tokens (NFTs), their use for TF practices is expected to become more frequent soon.

In addition to the use of payment systems, terrorists make use of several **obfuscation techniques** to decrease the risk of being detected. One of the most popular techniques relates to **crowdfunding and fundraising initiatives** (where platforms carry out limited or no due diligence on project owners and their projects), mainly due to the little attention law enforcement pays to them and considering that not all investment-based crowdfunding platforms have the same regulatory status.

With respect to crypto assets, the use of **mixers and shared digital wallets** is prominent as to prevent tracing the source of a transaction. **Chain-hopping**, which moves money from one cryptocurrency to another using exchange services remains popular. Lastly, some indications have been found on the possible use of **gambling in the Metaverse** as a way to hide the origin of capitals used to fund terrorism.

In addition, **internet-based platforms and social media** have emerged as key technologies for terrorism and TF, including **Telegram, Wickr, Facebook, Twitter, YouTube, video games, personal blogs and chat rooms**. These instruments allow terrorists to exploit the digital multiplier effects and reach a vast audience with their messages.

Additionally, the crypto galaxy is set in an uneven regulatory framework around the globe that creates additional problems. Cryptocurrencies are traded virtually, and users can move wallets and use exchanges in several jurisdictions. Therefore, while regulators and investigators may become aware of attempts to finance terrorism, they are unable to stop the transaction or freeze the assets due to the lack of jurisdictional authority.

TF-trends are, therefore, arising in relation to these emerging threats. First, the increasing **availability of crypto assets** as payment systems. Second, the increasing **exploitation of FinTech-based**

**obfuscations techniques** specifically designed for crypto assets. The last dynamic gives account of terrorists' greater **reliance on self-financing activities**, including fundraising campaigns as well as online crimes and fraud. The three factors are interconnected and influence each other reciprocally.

To combat the advancing threats and emerging trends of TF, law enforcement agencies and competent authorities need to be able to **understand emerging technologies**, improve the **mapping of anomalous schemes**, and **assess relevant recurrent patterns**. This will support law enforcement detection capabilities and further enhance TF counteracting strategies.



# 1 Introduction

In the last years, the Terrorist Financing (TF) has experienced a rapid transformation towards the use of technology-based methods and systems, such as cryptocurrencies. This process is intended to enhance anonymity of TF-related transactions and it is favoured by the growing diffusion of these technologies. In response to this, recent development in **legislation have aimed to strengthen anti-money laundering (AML) and countering the financing of terrorism (CTF) framework** in relation with the new technologies, both at European and global level. However, **research and knowledge regarding the emerging use of technologies enabling TF and the associated threats and risks posed by them are still limited.**

While terrorist events may be limited in number, they have an enormous impact from a social, economic, safety, and security perspective. In order to build capacity of the CTF end-users and to design timely prevention actions against funding of terrorism, a **detailed monitoring and analysis of financial transactions through new technologies is required.** Counteracting strategies must aim at early detection of trends and methodologies of modern TF. Therefore, special attention should be placed to understand the risks posed by new payment methods and to assess associated threats and trends.

Consequently, WP2, in the framework of the CTC Project, has the objective of understanding, identifying and assessing the spectrum of threats and risks related to emerging TF trends. Task T2.1, in particular, aims at **identifying new threats and trends on the modus operandi employed by terrorist organizations so as to finance their related criminal activities.**

**The present document is an operational report on new TF threats and trends that focuses mainly –but not only– on the rapid growth of the FinTech industry and the new emerging technologies,** such as crypto assets, new payments systems, obfuscation methods, and social media and other internet-based communication technologies. The assessment is performed based on the review of intelligence from public and private sector, police and judicial reports, institutional publication and press releases, EU legislation, academic literature, civil society reports, and media articles.

The report is structured as follow: Chapter 2 provides a review of most relevant TF threats, including traditional and new payment systems, obfuscation techniques, as well as internet-based communication platforms and social media. Chapter 3 presents TF trends associated to emerging threats. Chapter 4 highlights both international and European legal regime that has emerged to combat TF activities that focus on emerging technologies. The concluding Chapter 5 advances some policy implications that can be derived from the analysis conducted so far. The list of references provides exact indication of all the documents cited in this report.

## 2 Terrorist financing threats

Understanding and assessing how terrorism is being financed today is essential to define timely, effective, and efficient CTF strategies.

In this respect, it is relevant to investigate the threats posed by both **traditional payment systems** and specific **FinTechs** (i.e., cryptocurrencies and new payment systems). For each of these different payment systems, terrorists and terrorist financiers may use different **obfuscation techniques** (e.g., mixer services, fake charitable crowdfunding initiatives, money mules) to further hide the illegal nature of their transactions.

Finally, threats related to terrorism and TF activities emerge also in relation to the use of **communication platforms and social media**.

### 2.1 Payment systems

Terrorism financiers require to conceal the true nature of their financial transactions so to elude controls from law enforcement authorities and private obliged entities. At the same time, terrorist organizations might be in need to move the funds across borders to use and distribute them as they please. The combination of these pressing needs lead terrorism related actors to adopt payment methods that present high levels of privacy and anonymity. This applies to both traditional payment methods and FinTech systems.

#### 2.1.1 Traditional payment systems

Still today, terrorist organizations rely on what might be considered traditional payment systems to collect, move and disguise funds intended to finance terrorist activities. The most relevant consist of:

- **Cash smuggling** is known to be one of the most widely used methods for TF (Freeman and Ruehsen 2013), which is simply the cross-border smuggling of cash through couriers.
- **Money-service businesses (MSBs)** include currency dealers or exchangers; check cashers; issuers of traveller's checks, money orders or stored value cards; and money transmitters, among others. MSBs are generally subject to the same regulations as banks and other obliged entities, as well as regulatory audits. However, they often do not apply rigorous know your customer (KYC) procedures, thus potentially attracting terrorism financiers (Freeman and Ruehsen 2013; Winer 2008).
- **Formal banking institutions** can engage with terrorism-related funds in a variety of ways. It may be the case that a bank does not perform the required KYC procedures. Terrorist financiers may cooperate with bank employees to transfer their funds to terrorist organizations, or use money mule accounts without creating suspicious or alert the bank security checks and without being intercepted by supervisors and competent authorities. Finally, there may be circumstances where a bank fully complies with customer due diligence (CDD) requirements, but still fails to detect TF transactions, as it occurred in the case of the 9/11 hijacker accounts (Freeman and Ruehsen 2013).

- **False trade invoicing** is one of the oldest methods of transferring values overseas. It is accomplished by over and under representing the price of a good or service in order to transfer money between colluding importers and exporters (Zdanowicz 2009).
- **Acquisition of high-value commodities** as gold, diamonds, and other high-value commodities are anonymous and are capable of readily holding and transferring stored value (Freeman and Ruehsen 2013; Winer 2008).
- **Hawala system**, aside digital and internet-based FinTechs, is a funding method that attracts particular attention in the context of jihadist organizations to transfer Islamic money (Levy and Yusuf 2021). Hawalas, and other similar service providers, arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a prolonged period. What makes them distinct from other money transmitters is their use of **non-bank settlement methods/ Informal Value Transfer Systems** (FATF 2013).

#### *Traditional payment systems and TF today*

- US-based Da'esh supporters tended to avoid using banking institutions to move funds, but to use **money or value transfer services** (Vidino, Lewis, and Mines 2020).
- A central figure of the jihadist movement in the Netherlands and leading member of the so-called Hofstad network,<sup>1</sup> was arrested on charges including TF. He was alleged of receiving money from various people to help women and children in the Syria/Iraq conflict area. The money would then be transferred to these women via **hawala banking**, which is illegal in the Netherlands (Europol 2021a).
- The Spanish National Police, supported by Europol, arrested a man suspected of transferring money between several European and Arabian countries via the **hawala informal money transfer system** with the aim of reintroducing foreign terrorist fighters in Europe (Europol 2020).

## 2.1.2 Cryptocurrencies

Cryptocurrencies are decentralized convertible virtual currencies that are protected by cryptography and that rely on public and private keys to transfer value from one person (individual or entity) to another. Terrorist organizations are increasingly making **use of cryptocurrencies**, as Bitcoin or others, to support their activities (Dion-Schwarz, Manheim, and Johnston 2019).<sup>2</sup>




#### **Threat**


Most of cryptocurrencies pose TF-related threats because of their **pseudonymity**, their **elusiveness and high negotiability**, and their capacity to be transacted and withdrawn in **real-time** (Kim-Kwang 2015).

<sup>1</sup> Also known as Hofstadgroep, it used to be included in the EU terrorist list (EU 2011).




<sup>2</sup> Decentralised Virtual Currencies (a.k.a. cryptocurrencies) are math-based, decentralised convertible virtual currencies that must be cryptographically designed each time it is transferred. In turn, a virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value but does not have legal tender status in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency (FATF 2014).

 <p><b>Temporal Dynamic</b></p>	<p>The cryptocurrency market is <b>constantly evolving</b> due to increasing <b>popularity and product innovations</b> (UK Gambling Commission 2021). The evolving nature of contemporary cryptocurrency market is <i>per se</i> a threat to CTF policies as it makes harder to enforcement agencies and obliged entities to cope with an always emerging environment.</p>
 <p><b>Exemplificative Evidence</b></p>	<p>The recent seizures of cryptocurrencies from al-Qaida,<sup>3</sup> Da'esh,<sup>4</sup> and the al-Qassam Brigades, Hamas'<sup>5</sup> military wing, by the US Department of Justice demonstrate how terrorist groups use cryptocurrencies to finance their activities (US Department of Justice 2020b).</p>

In this scene and as cryptocurrencies offer major potential for the global economy both from technical and financial point of view, Europol (Europol, 2022) has undertaken an analysis of the criminal use of cryptocurrencies to support law enforcement and its response to changing trends in this area. The resultant report contains core definitions, case examples, and details of the challenges authorities face in combating the illicit use of cryptocurrency. Among cryptocurrencies, Bitcoin is by far the most popular alternative in regard both licit and illicit transactions (ACAMS 2021; Europol 2021b; Majumder, Routh, and Singha 2019; McKendry 2015; Nauert 2015; US Department of Justice 2015; Yuniar 2017).

 <p><b>Threat</b></p>	<p><b>Bitcoin is the preferred cryptocurrency</b> for terrorism financing (TF) purposes, as well as for Dark Web users.</p>
--	---

In the last few years, alternative crypto-based payment methods have also gained popularity, including **crypto debit cards**, **Bitcoin ATMs** and **local trade** (Europol 2021b).


 <p><b>Threat</b></p>	<p>Most of <b>Bitcoin ATMs</b> are <b>not subject to an adequate KYC process</b>. Users do not even need a digital wallet as Bitcoin ATMs autonomously create them, providing users with printouts of wallet addresses and private keys.</p>
 <p><b>Practical Functioning</b></p>	<p>Bitcoin ATMs enable people to buy and sell bitcoin as well as other cryptocurrencies <b>directly from an exchange</b>, using <b>bank cards</b> or even <b>cash</b>. In addition, terrorists employ <b>money mules</b> to make small to large deposits at different times and locations into the same addresses.</p>
 <p><b>Exemplificative Evidence</b></p>	<p>Evidence is emerging that Bitcoin ATMs are frequently used to send funds to 'high-risk exchanges': almost 88% of US Bitcoin ATMs transactions in 2019 sent funds to <b>offshore jurisdictions</b> (Schlabach 2020).</p>

<sup>3</sup> Targeted by UN international sanctions (United Nations Security Council 2021).

<sup>4</sup> Also known as IS or ISIL, acronym of Islamic State in Iraq and the Levant; included in the EU terrorist list (EU 2021).

<sup>5</sup> Included in the EU terrorist list (EU 2021).

Lately, alternative cryptocurrencies to Bitcoins have emerged.

 <b>Threat</b>	<p><b>Cryptocurrencies</b> other than Bitcoin pose a threat due to their potential for <b>improved anonymity and high-volume transactions</b> (Dion-Schwarz, Manheim, and Johnston 2019).</p>
--	---

Some of the most used cryptocurrencies are:

- **Binance Coin** (BNB) is one of the two cryptocurrencies developed and launched by Binance, the other being Binance Smart Chain (BSC). As July 2021, Binance was the largest cryptocurrency exchange in terms of daily trading volume of cryptocurrencies (Peters 2021). Binance was founded in China in 2017 and it is currently registered in the Cayman Islands.
- **Dash** (DAO) is a cryptocurrency that allows the user to choose whether or not their transactions are anonymous and private using its PrivateSend feature. This allows users who would like to remain within their countries' regulatory standards to do so. The feature works by obscuring the origins of your funds. Choosing to use the PrivateSend feature will slightly raise the fee for the transaction. Dash achieves this through a mixing protocol utilising a decentralized network of servers called master nodes (Seth 2021).
- **EOS** public chain supports millions of processing speeds per second and is currently the fastest blockchain: EOS, based on the DPoS protocol, produces a block every 0.5 seconds (Song et al. 2021).
- **Ethereum** is historically the second most popular cryptocurrency after Bitcoin. In 2016, Ethereum was divided into Ethereum classic (ETC) and Ethereum (ETH) (Majumder, Routh, and Singha 2019).
- **Horizen** (ZEN) uses a series of protocols (e.g., domain fronting, distributed publishing, client-to-node encryption, and end-to-end encryption) to ensure the privacy and safety of its users. In this respect, Horizen technologies allow users to customise the level of transparency for their digital assets and communications.
- **Monero** (XMR) is hard to trace because it uses ring signatures and stealth addresses, which help to hide the identities of both the sender and the receiver. Additionally, Ring Confidential Transactions (RingCT) helps to conceal also the transaction amount, providing additional privacy (Seth 2021). As result, observers cannot decipher addresses trading XMR, transaction amounts, address balances or transaction histories (Majumder, Routh, and Singha 2019).
- **Ripple** (XRP) is a real-time gross settlement system, currency exchange and remittance network (Ahmad 2022). Ripple claims to allow 'secure, instantly and nearly free global financial transactions of any size with no chargebacks'. The ledger employs the native cryptocurrency known as XRP (Dcointrade, 2021).
- **Tez** (XTZ) is the native cryptocurrency for a decentralized open-source blockchain that can execute peer-to-peer (P2P) transactions named Tezos.
- **Verge** (XVG) is based on the existing and tested technology of The Onion Router (TOR) and the Invisible Internet Project (I2P) to protect users' identities, instead of relying on cryptographic techniques. TOR bounces a user's communications over a distributed network of relays and tunnels run by volunteers spread across the globe, thereby hiding the users' identities. On the other hand, I2P encrypts user data before sending it through an anonymous, P2P and volunteer-




run globally distributed network. In this manner, I2P allows to hide the locations and IP addresses of the transacting participants (Seth 2021).

- **Zcash** (ZEC) is another cryptocurrency that offers a higher degree of privacy than Bitcoin and other cryptocurrencies. In addition, Zcash can be used and transferred offline. This feature can make its tracking even more difficult for law enforcement (Dion-Schwarz, Manheim, and Johnston 2019).

Over the years, other cryptocurrencies have been proposed, including **Hawk**, **Omni Layer (MasterCoin)** and **BlackCoin**, which would allow fully private contracts and transactions on the Ethereum blockchain (Dion-Schwarz, Manheim, and Johnston 2019), as well as the so-called **Privacy Coins**, which are characterized by blockchains that have native privacy features, such as ring signature, zero knowledge proof and Mumblewimble protocols, among others. New analytical tools are being developed all the time, therefore in the future computers may become powerful enough to crack modern encryption methods. Nonetheless, under current encryption methods, Privacy Coins have proven resilient.

### 2.1.3 Non-fungible Tokens (NFTs)

NFT is a unit of data stored on the blockchain, which can be **(i)** sold and transferred, and **(ii)** associated with a particular digital or physical asset or a license. As such, NFTs are becoming an increasingly popular way to buy and sell **digital artwork** as well as the rights to other **intellectual property**.

 <p><b>Threat</b></p>	<p>The relative <b>anonymity enjoyed by NFTs</b>, thanks to blockchain technology, favours their possible use for TF. Moreover, NFTs are currently <b>not regulated</b> as most of NFT marketplaces do not perform any KYC process. In addition, NFTs are bought and sold using <b>cryptocurrencies</b>, adding further complexity to the task of tracing these transactions.</p>
 <p><b>Temporal Dynamic</b></p>	<p>The market for NFT is <b>particularly large</b>—NFT Market Surpassed \$40 Billion in 2021—and <b>rapidly growing</b> (Bloomberg 2022).</p>
 <p><b>Practical Functioning</b></p>	<p>Terrorists could generate an anonymous NFT, sell it to their lenders on the blockchain, then make the profit from the sale of the artwork and use it for terrorism-related activities.</p> <p>Alternatively, the scheme may be centred on <b>money-laundering (ML)</b>. In this case, terrorists could generate anonymous NFTs, list them for sale on a marketplace, purchase them from themselves with another anonymous digital wallets, and declare the money as legitimate funds from the sale of the artwork.</p>

### 2.1.4 Other New Payment Systems

Aside cryptocurrencies, TF schemes exploit other financial technologies.



New Technologies	Exemplificative evidence
Mobile phone money-transfer systems	<ul style="list-style-type: none"> <li>Swedish competent authorities noted the use of <b>Swish</b>, a Swedish payment service that allows the users to transfer money directly to other users and companies by using their <b>phone numbers</b> (Europol 2021a).</li> <li>The increasing use of mobile phone money transfer by al-Shabaab<sup>6</sup> has facilitated informal remittance. This is particularly characteristic in Somalia, where <b>mobile money has superseded the use of cash</b> (Levy and Yusuf 2021).</li> </ul>
Alternative digital payment systems	<ul style="list-style-type: none"> <li>Islamic militants based in the Middle East used Bitcoin and online-payment services such as <b>PayPal</b> and other “Peer to Peer” (P2P) transfer payments, to fund terrorist activities in Indonesia, largely in Java (Yuniar 2017).</li> <li>A foreign Fiscal Investigation Unit (FIU) communicated to the Belgian FIU that they received a suspicious transaction report (STR) concerning a national from a European country selling precursors that can be combined to make explosives. The goods were sold to customers in Eastern Europe. The criminals planned to collect the proceeds of their sales through an <b>Internet payment service provider</b> and consequently to launder these proceeds, also using the same service provider (FATF 2008).</li> </ul>

## 2.2 Obfuscation techniques

Beside the use of payment systems characterized by pseudonymity, anonymity and, in general, a high level of privacy, terrorists make use of several obfuscation techniques to decrease their risk of being detected by law enforcement authorities. Among them, are relevant the organization of **fake charitable crowdfunding initiative**, and **fraudulent front websites and transactions**.




In addition to these obfuscation strategies, which may rely on the use of cryptocurrencies as not, obfuscation techniques specifically intended for transaction in cryptocurrencies have been developed. Indeed, transactions of (most) cryptocurrencies can be traced as the blockchain stores a record of both the source and destination addresses of every transaction.

Therefore, terrorists employ a series of **obfuscation techniques to increase their degree of financial privacy**, thus mitigating their exposure to enforcement interventions. Critically, and in contrast to typical uses of obfuscation techniques in the financial sector, in cryptocurrencies, obfuscation is not aimed against the system designer but is instead enabled by design (Narayanan and Möser 2017). In this respect, of importance is the use of **mixer services** and **chain-hopping** techniques.

### 2.2.1 Crowdfunding and fundraising initiatives



Terrorist organizations can use several online channels to solicit funds, such as explicit as well as **fraudulent crowdfunding and fundraising initiatives**.

<sup>6</sup> Targeted by UN international sanctions (United Nations Security Council 2021).


 <p><b>Threat</b></p>	<p>TF schemes based on crowdfunding and fundraising exploit the fact that <b>often regulators have been paying marginal attention</b> to these initiatives in comparison to other TF mechanism (Levy and Yusuf 2021; Maremont and Steward 2017).</p>
 <p><b>Exemplificative Evidence</b></p>	<ul style="list-style-type: none"> <li>Through the years, using a variety of social media sites, Da’esh has conducted online fundraising through the <b>disguise of charitable non-profit organizations</b> (Kancherla, 2020).</li> <li>The vast majority of US-based Da’esh supporters raised a <b>small amount of money</b>, no higher than a few thousand dollars, and often through simple tactics, relying on <b>personal savings</b> or by means of simple <b>fundraising activities</b> (Vidino, Lewis, and Mines 2020).</li> </ul>
 <p><b>Reaction to Enforcement</b></p>	<p>Methods and locations of fundraising activities are not static. On the contrary, they <b>react to enforcement pressure</b>: after the successful seizure of Hamas fundraising sites by the US Department of Justice, FBI and other authorities, the group is <b>shifting its cryptocurrency fundraising away from the US platform</b> and developed new techniques for obfuscating transactions in other regions (TRM 2021).</p>

### 2.2.2 Mixers

A mixer, also known as ‘tumbler’, is a software service that divides funds into smaller sets and subsequently mix them with other transactions.




 <p><b>Threat</b></p>	<p>Mixing is a <b>cooperative</b> obfuscation method to prevent tracing, by making it <b>difficult to identify the source of a transaction</b>.</p>
 <p><b>Practical Functioning</b></p>	<p>People pool together their cryptocurrencies. Each individual then takes back coins of the same value but from a different source (or sources) than the ones they brought to the mixer (Elliptic 2018). To do this, users in the mixer group may provide <b>tumbling services</b>, which consists of <b>reshuffling cryptocurrencies into hundreds of transactions</b> and <b>interpolating transactions with other users</b> to decrease or eliminate traceability (Amiram, Jorgensen, and Rabetti 2020).</p> <p>Moreover, cryptocurrencies mixers can disguise the true nature of transactions through implementing a <b>time delay</b> of the transaction to the blockchain and enter illegitimate transactions into the blockchain with a legitimate one in a single transaction (ShenTu and Yu 2015a; 2015b). Finally, in addition to mixing, mixer services can also <b>fragment the wallet into small crypto-wallets</b>, in order to also mask the original amount of the paid sum.</p>



 <p><b>Exemplificative Evidence</b></p>	<p><b>Silk Road</b> represents the first use of a Bitcoin mixer, which served to disguise the illegal origin of bitcoins through a series of ‘dummy transactions’ on the blockchain network. Thenceforth, tumblers/mixers started to play a crucial role in the crypto laundering process (Fanusie and Robinson 2018).</p>
--	--

### 2.2.3 Chain-hopping


An obfuscation method that is gaining popularity is the so-called chain-hopping.



 <p><b>Threat</b></p>	<p>Crypto-to-crypto exchanges through a process known as chain-hopping are open to abuse because they:</p> <ol style="list-style-type: none"> <li>1) create money trails that are <b>harder to track</b>, and</li> <li>2) can also <b>convert traceable cryptocurrency</b> such as Bitcoin into privacy coins that are currently exceedingly difficult to trace (RUSI 2018).</li> </ol>
 <p><b>Practical Functioning</b></p>	<p>Money is moved <b>from one cryptocurrency into another</b> employing <b>digital currency exchange services</b> (e.g., Binance, Huobi, OKEx, SimpleSwap) - the less-regulated the better.</p>
 <p><b>Exemplificative Evidence</b></p>	<p>Hamas supporters started experimenting with mixers and tumblers, then migrated to <b>chain-hopping</b>, where they repeatedly switch from one cryptocurrency to another within an exchange, taking it to a place with no visibility (ACAMS 2021).</p>

### 2.2.4 Digital wallets

Regardless of the cryptocurrency of adoption, the acquisition of a digital cryptocurrency wallet, also referred to as e-wallet, is the first step in the exploitation of cryptocurrencies for TF purposes (Teichmann, 2018).



Within the macro-class of the digital wallets, so-called ‘Dark Wallets’ deserve specific attention as obfuscation technique. FATF (2014, 6) defines dark wallets as: ‘a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymizer (mixer); decentralized trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralized market places similar to Silk Road’. The use of dark wallets for TF purposes has been documented in the last years (Kancherla 2020; Valeri 2018; Weimann 2016).

 <p><b>Threat</b></p>	<p>Shared digital wallets can being designed as to <b>camouflage illegal transactions within licit transactions</b> (Brantly 2014).</p>
--	---

 <p><b>Practical Functioning</b></p>	<p>A <b>cryptocurrency wallet</b> is a device, physical medium, program, or a service that <b>stores the public and/or private keys for cryptocurrency transactions</b>. In addition to this basic function, a cryptocurrency wallet often also offers the functionality of encrypting and/or signing information.</p>
 <p><b>Exemplificative Evidence</b></p>	<ul style="list-style-type: none"> <li>▪ Hamas posted a request for overseas supporters to donate bitcoins to a <b>single digital wallet</b> that the group had opened with <b>Coinbase</b>. Federal prosecutors in Washington DC, announced that they had seized control of 150 <b>digital wallet</b> accounts tied to Hamas (ACAMS 2021; Al Jazeera 2021).</li> <li>▪ Da’esh militants’ suggestions on using <b>Dark Wallet</b>, a new Bitcoin wallet that keeps the user of Bitcoins anonymous (US Department of Justice 2015).</li> </ul>

### 2.2.5 Metaverse

Technically, a Metaverse is a 3D space that allows the socialization, learning, and collaboration of a network of connected users.

 <p><b>Threat</b></p>	<p>There is negligible means of monitoring financial activity, <b>limited CDD</b> and <b>scant rules for KYC processes</b> in the Metaverse.</p>
 <p><b>Practical Functioning</b></p>	<p>An individual connected to a terrorist group may open numerous separate <b>virtual accounts</b> in the Metaverse, all using <b>fictional IDs</b>. The accounts are then funded with TF proceeds. The terrorists can then make purchases in the Internet to and from themselves using those same accounts as purchasing assets from other residents. Subsequently, proceeds can be moved to an account that they maintain. Finally, the funds can be withdrawn either from the <b>bank</b> or using an <b>ATM</b>.</p> <p>In a simpler scheme, terrorist financiers may use their actual <b>credit or debit card</b> to purchase online virtual money in the Metaverse and then <b>redeem those credits</b> for actual money with another individual acting in the Metaverse in <b>another country</b> and in that country <b>currency</b>.</p> <p>This could be considered as the virtual counterpart of the Hawala system.</p>

In addition to the general exploitation of laundering schemes centred on the exploitation of financial transaction in the Metaverse, new threats might be posed by specific services offered in the Metaverse that in consideration of their specificities might attract TF thus deserve to be monitored in the future. Among these services, **is gambling in the Metaverse**.

<p><b>Traditional gambling</b></p>
<ul style="list-style-type: none"> <li>▪ <b>Terrorism financiers used not to rely much on gambling or casinos</b> (Maitland Irwin, Kim-Kwang, and Lin 2012). The tight controls and regulations of gambling and casinos may explain their traditional low levels of use for ML purposes (Unger et al. 2006).</li> </ul>
<p><b>Gambling in the Metaverse</b></p>

- In the Metaverse, it becomes possible to gamble on any casino site in the world without having to worry about common issues like: whether the casino site will accept players from a specific country; whether the site will be able to process deposits/withdrawals directly from and to a local bank; whether an individual will be charged high fees for being an international player (Guardian Nigeria 2021).

## 2.3 Internet-based communication platforms and social media

Illegal markets have expanded to different **encrypted communication channels** due to increased legal action taken by law enforcement. These include channels like **Telegram** and **Wickr** (Europol, 2021b). Terrorists also make use of encrypted communication services for confident chats (Szydelski, 2021).

Similarly, **internet-based platforms and social media** have emerged as a key technologies for terrorism and TF (Kwon, Chadha, and Pellizzaro 2017; Rudner 2017). These instruments, indeed, allow terrorists to exploit the **digital multiplier effects** and **reach a vast audience** with their messages.

The use of both internet-based communication platforms and social media have multiple purposes among which: the recruitment of new members, sharing propaganda, disseminating their ideology, and technical knowledge related to terrorist activities.

Purpose for using technology	Exemplificative evidence
Recruiting new members	<ul style="list-style-type: none"> <li>▪ Da'esh radicals in Syria have used <b>Telegram Messenger</b>, an encrypted messaging app, and <b>Facebook</b> to recruit members in Malaysia and Indonesia (Purnell and Woro Yuniar 2016).</li> <li>▪ Da'esh continues to use social media to send their violent and hateful message around the world to <b>radicalize, recruit</b> and <b>incite</b> youth and others to support their cause (US Department of Justice 2015).</li> </ul>
Fundraising	<ul style="list-style-type: none"> <li>▪ Hamas initially tested cryptocurrency fundraising by soliciting Bitcoin donations on its <b>Telegram channel</b> before shifting to <b>direct fundraising on its website</b> (ACAMS 2021).</li> <li>▪ Internationally, foreign fighters actively used social media networks to collect money to support Da'esh (Europol 2021a).</li> <li>▪ Perpetrators inspired by Da'esh have raised funds through social media-based fundraising campaigns (Maremont and Steward 2017).</li> <li>▪ Hamas posted a request on an <b>encrypted communications platform</b> for overseas supporters to donate cryptocurrencies (ACAMS 2021).</li> <li>▪ <b>Twitter account</b> as a pro-Da'esh platform to conduct conversations regarding ways to develop financial support for Da'esh using on-line currencies and ways to establish a <b>secure donation system</b>. The account boasted over 4,000 followers (US Department of Justice 2015).</li> </ul>

	<ul style="list-style-type: none"> <li>In the period 2015-2018, ITMC, the media wing of Shura Council in the Environs of Jerusalem,<sup>7</sup> also involved in Da'esh propaganda, launched a social media campaign to promote a <b>crypto fundraising</b>. The campaign was spread through <b>Twitter</b>, <b>YouTube</b> and <b>Telegram</b>. The social campaign, that explicitly aimed at <b>raising funds to buy weapons</b>, received transactions amounting to thousands of dollars, reaching picks of sums equivalent to \$289,000 and \$123,000 (Barone 2018).</li> </ul>
<p>Spreading propaganda messages</p>	<ul style="list-style-type: none"> <li><b>Video games communication applications</b> used to share right-wing terrorist and extremist propaganda, especially among young people. Right-wing extremists continued to use a variety of online platforms, from <b>static websites</b> to <b>social media</b> and <b>messenger services</b> (Europol 2021a).</li> </ul>
<p>Disseminating technical knowledge</p>	<ul style="list-style-type: none"> <li>Establishment of <b>personal blogs</b> for publishing highly technical articles and <b>how-to guides</b> detailing the use of security measures in online communications, including <b>encryption and anonymity software, tools and techniques</b>, as well as the use of the virtual currencies to anonymously fund Da'esh (US Department of Justice 2015).</li> <li>Da'esh militants are believed to have received <b>bomb-making lessons</b>, among other instructions (Purnell and Woro Yuniar 2016).</li> </ul>

### 3 Terrorist financing trends


Terrorist organizations are altering their financing techniques to cope with the mutations of the international political scenario and the increase in controls and intelligence of Governments and international financial system, and to exploit emerging opportunities provided by innovative technologies in the fields of finance and communication.

In relation to emerging threats, it is therefore possible to identify emerging trends in TF. These **trends are connected to**:


- 1) The **increasing availability of crypto assets** as payment systems because of the privacy provided by these instruments – the *pull* factor.
- 2) The **exploitation of obfuscation techniques** specifically designed for cryptocurrencies.
- 3) A greater reliance of terrorist organizations on **self-financement** schemes – the *push* factor.

The three factors are interconnected and influence each other reciprocally. At the same time, all trends are also linked to the ever-increasing availability of and by new communication instruments.



#### 3.1 Increasing use of crypto assets

 <p><b>Trend</b></p>	<p>One of the most significant emerging trends in TF is the <b>ever-increasing use of cryptocurrencies</b>.</p>
---	---

<sup>7</sup> Included in the US Foreign Terrorist Organizations list (US Bureau of Counterterrorism 2022).



 <p><b>Exemplificative Evidence</b></p>	<ul style="list-style-type: none"> <li>▪ The terrorist organization Al-Shabaab originally relied on international, also called external or cross-border, funding by means of donations from diaspora communities and charcoal exports. Nowadays, it <b>migrated to internal revenue</b> sources not only by means of port fees, racketeering and piracy, but also through <b>cryptocurrency donations</b> (Levy and Yusuf 2021).</li> <li>▪ Da'esh attempted creating its <b>own money</b>, minting gold, silver and bronze caliphate coins, <b>selling them for bitcoin cryptocurrency</b>, and encouraging supporters to use these coins or cryptocurrency to <b>avoid strengthening Western currencies</b> (Levy and Yusuf 2021).</li> </ul>
--	---

The challenge posed by virtual assets extends beyond Bitcoin as many new cryptocurrencies have emerged recently, including alternative currencies such as **MasterCoin, BlackCoin** and **Monero**, which are promoted as **more private** and secure than Bitcoin (Dion-Schwarz, Manheim, and Johnston 2019; Europol 2021b). Evidence of actual use of NFTs for TF purposes is still limited. Nonetheless, the rapid expansion of their markets together with their intrinsic characteristics, and limited transparency of their market suggest their use in the TF domain might soon become relevant.

 <p><b>Trend</b></p>	<p>Aside the general increase in the use of cryptocurrencies, <b>the increase in the use of cryptocurrencies other than Bitcoin</b> is, <i>per se</i>, an emerging trend.</p>
 <p><b>Exemplificative Evidence</b></p>	<p>In 2021, the Israeli National Bureau of Counterterrorism Finance seized several cryptocurrency addresses controlled by agents of Hamas containing, among others, <b>Bitcoin, Doge and Tron</b> (TRM 2021).</p>



### 3.2 Increasing use of FinTech-based obfuscation techniques

While criminals and terrorists still make most payments in Bitcoin, recipients are increasingly converting them to Monero and other privacy coins by using swapping services, mixers, tumblers and CoinJoins (Europol 2021b).



 <p><b>Trend</b></p>	<p>Connected to the increasing use of cryptocurrencies, is the <b>growing exploitation of obfuscation techniques specifically designed for crypto assets</b> (i.e., shared digital wallets, mixers, chain-hooping).</p>
 <p><b>Exemplificative Evidence</b></p>	<p>In 2019, Izz ad-Din al-Qassam Brigades, one of Hamas's armed groups, conducted three crypto-fund raisings which lasted 9 months in total. In the three funding rounds, fund camouflage methods have improved exponentially, ranging from an almost <b>direct currency shift to the creation of a new crypto-wallet with each new donation</b>. The campaign received more than a hundred donations, totalling tens of thousands of dollars.</p>

### 3.3 Increasing reliance on self-sustainment


The increasing reliance on FinTechs to manage activities finalized at TF relates to the so-called **New Economy of Terrorism**. Since the first decade of the 2000s, terrorist organizations have been evolving from relying on external sponsorship, often from states, using (online or offline) prepaid cards or vouchers-coupons with customer due diligence exemptions (EU, 2019), to developing **self-sufficient funding mechanisms** by taking advantage of areas of weak government (Napoleoni 2010).

 <b>Trend</b>	Predatory funding practices, including <b>ransom and extortion</b> .
 <b>Exemplificative Evidence</b>	<ul style="list-style-type: none"> <li>▪ Al-Shabaab developed its own sources of funding and become increasingly independent from external sponsorship through the use of predatory practices, such as <b>ransom, extortion, and territorial conquest</b> (Levy and Yusuf 2021).</li> <li>▪ In August 2015, an Illinois Internet retailer was targeted by a <b>ransomware</b> attack under the username of Albanian Hacker, who demanded the payment of two Bitcoin, which had a value of \$500 at the time, to remove the viruses from the company’s computers. While seizing control of computers, Albanian Hacker generated a list used as one of the first kill lists issued by the Da’esh (Johnson 2016).</li> </ul>

There is always the element of cost efficiency.

 <b>Trend</b>	Self-sufficiency as a result of <b>reduction of costs</b> .
 <b>Exemplificative Evidence</b>	<ul style="list-style-type: none"> <li>▪ There is a shift in Da’esh’s tactics towards <b>inexpensive attacks</b>, which has advocated <b>lone offender and small group attacks</b> that can be carried out quickly, with minimal funding and preparation.</li> <li>▪ As support, Da’esh has published <b>how-to guides</b> offering advice on carrying out attacks with <b>low-tech, low-cost weapons</b> such as improvised explosive devices, vehicles, knives and arson (US Department of Justice 2020a).</li> </ul>

#### 3.3.1 Fundraising campaigns

 <b>Trend</b>	Increasing reliance on funds collected through <b>disguised and manifest fundraising campaigns</b> .
---	--



Especially since the beginning of the long-lasting war in Syria, jihadist terrorist groups have changed their narrative. In particular, they started to present themselves as organizations motivated by humanitarian goals, who struggle against war criminals oppressing innocent communities. This change in strategy allows terrorist organizations and their sympathizers to diversify their affiliates, by exposing



the atrocities and injustices caused by wars globally through the Internet and by overlapping them with issues exclusively related to violent extremism or radicalization.

From the TF standpoint, this branch of the jihadist communication strategy, which is carried out on the web and addresses a global audience, is resulting in a growing number of apparently **decentralized crowdfunding campaigns**, which are carried out by individuals or small groups. **Often these campaigns accept cryptocurrencies**, especially Bitcoins (Barone 2018).

### 3.3.2 Online crimes and frauds

 <p><b>Trend</b></p>	<p>The TF through online crimes and frauds (e.g., fraudulent front websites) is <b>increasing</b> in parallel with the general increase in these illegal activities (i.e., not TF-related).</p>
 <p><b>Exemplificative Evidence</b></p>	<ul style="list-style-type: none"> <li>▪ One operative from Da’esh was discovered gathering funds through <b>fraudulent eBay transactions</b> (Levy and Yusuf 2021; Maremont and Steward 2017).</li> <li>▪ Perpetrators inspired by Da’esh have gotten <b>small amounts</b> through low-level fraud such as <b>check scams</b> and <b>online lending fraud</b> (Maremont and Steward 2017).</li> <li>▪ A supporter of Da’esh engaged in a scheme to <b>defraud several financial institutions</b>. The scheme allowed the militant to access over \$85,000 in illicit proceeds. She further wired these funds to various individuals and <b>opaque companies overseas</b>, located in Pakistan, China, and Turkey, that were associated with Da’esh (US Department of Justice 2020a).</li> </ul>

## 4 European and international standards

An **international legal regime has emerged to combat TF activities resulting in an increase of AML/CTF efforts focused on FinTechs**, virtual currencies, communication technologies and other emerging trends, including European Union, MONEYVAL (Council of Europe), the European Banking Authority, Financial Action Task Force (FATF), European Securities and Markets Authority (ESMA) and the World Bank, among others.

### 4.1 The European Parliament and the Council

The EU Anti-Money Laundering Directives (AMLD) of the European Parliament and of the Council made relevant amendments on its statutes regarding the prevention of the use of the financial system and emerging trends for the purposes of ML or TF. After 3AMLD, EU launched three directives within the space of two and a half years. The last three directives are complementary, as the fifth directive (5AMLD 2018), amends the fourth (4AMLD 2015), and the sixth directive (6AMLD 2018) compliments the fifth one. The 5AMLD was created following the terror attacks in France and Belgium. What stood out about 5AMLD was that cryptocurrency exchanges are now considered ‘obliged persons’ and therefore required to comply with the AML/CFT requirements. The 6AMLD has made requirements more onerous for obligated entities, such as cryptocurrency exchanges and wallets. They also urged

Member States to combat risks associated to virtual currencies and other anonymous technologies, and to take measures to ensure transparency of owners (EU 2018a; 2018b).

On 24 September 2020, the European Commission (EC) adopted a broad new digital finance package aimed at transforming and promoting the European economy in the coming decades. The package aims to improve the competitiveness of the EU FinTech sector and technologies mitigating risks, and ensuring the financial stability of the European economy by reducing regulatory fragmentation on this matter. The regulatory fragmentation indeed gives rise to regulatory arbitrage and may distort competition in the single market. This would make it harder for service providers of cryptocurrencies to expand their operations cross-border. The new regulatory framework includes a comprehensive new legislative proposal on cryptocurrencies, the so-called Markets in Crypto-assets (MiCA). MiCA was designed to simplify distributed ledger technology (DLT) and virtual asset regulation in the EU while protecting customers and investors (Vermaak, 2020). The initiative aims also to support innovation and fair competition by creating a framework for the issuance, and provision of services related to crypto asset as well as address financial stability and monetary policy risks that could arise from a wide use of crypto assets and DLT-based solutions in financial markets (EU, 2021).

## 4.2 MONEYVAL

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, Council of Europe (MONEYVAL) recognized in its 2020 report that there is a broad-based effort among European jurisdictions to mitigate risks from virtual currencies and new technology, and that some states, including Albania, Germany, North Macedonia, Poland, Romania, Russian Federation and Serbia, have adjusted their new national AML/CFT strategies accordingly. Furthermore, new domestic legislations were adopted in some countries to regulate ML/TF risks stemming from innovative technologies, initiatives that are encouraged to other jurisdictions (MONEYVAL 2020).

## 4.3 European Banking Authority

The European Banking Authority (EBA) recently issued a report on the risks of ML and TF affecting the EU's financial sector in relation to virtual currencies and to the services provided through FinTech and RegTech firms, among others. EBA acknowledged that risks arising from virtual currencies, crypto-assets and FinTech products have increased due to a constant growth on the virtual currency market within the European financial sector and further recommended the EU Commission to consider the recent revisions to the FATF standards and guidance regarding virtual assets and virtual currency systems. The EBA also proposed to competent authorities to familiarise with the technological developments deployed by FinTech and RegTech firms as to mitigate associated risks (EBA 2021).

## 4.4 FATF<sup>8</sup>

The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal

---

<sup>8</sup> <https://www.fatf-gafi.org/>



activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

In June 2014, FATF issued a report on virtual currencies as to define a common set of terms reflecting how emerging technologies operate as to enable government officials, law enforcement and private sector entities to assess the potential AML/CTF risks that these technologies entail (FATF 2014). In 2015, a guidance for a risk-based approach using virtual currencies was further published to support competent authorities to adapt risk assessment activities in the virtual currency context, identify the entities involved in virtual currency payment products and services (VCPSS) and clarify the application of the relevant FATF Recommendations to convertible virtual currency exchangers (FATF 2015). Later, the FATF adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving virtual assets and highlighted the need for countries, virtual asset service providers (VASPs) and other entities involved in virtual assets activities, to understand the ML/TF risks associated with their activities and take appropriate mitigating measures to address them (FATF 2019). In October 2021, the FATF updated its 2019 Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs), focusing on rapidly emerging areas of development including the following: NFTs, P2P transactions and decentralized protocols, stablecoins, ‘travel-rule’ for data sharing, inter-agency information sharing and cooperation (FATF 2021).

## 4.5 European Securities and Markets Authority (ESMA)

In 2015, the European Securities and Markets Authority (ESMA) highlighted the risk posed by investment-based crowdfunding platforms: They could be misused for terrorist financing, in particular ‘where platforms carry out limited or no due diligence on project owners and their projects.’ (<https://www.esma.europa.eu/document/questions-and-answers-investment-based-crowdfunding-money-launderingterrorist-financing>).

## 4.6 The World Bank

The World Bank has issued a report on recent developments of financial services that support economic development but also provide opportunities for crimes, such as TF. The report explores four innovations, including value cards, mobile financial services, online banking and payments, and digital currencies, outlining how they work, assessing their risks and identifying ways in which governments and providers are attempting to reduce their attractiveness for TF (Zerzan, 2010). Through this report, the World Bank acknowledged that understanding these risks is critical to ensure integrity in the market and to create an environment friendly to business and empowering to the poor.

# 5 Conclusions

## 5.1 Summary of findings

Identified TF threats from emerging technologies relate to three main categories. The first threat category is associated with the use of FinTech payment methods, including Bitcoins and other cryptocurrencies, mobile phone money-transfer and alternative digital payment systems. Nowadays,

terrorist financiers exploit these system aside traditional payment systems, such as cash smuggling, formal banking institutions, false trade invoicing and the Hawala system. The second category of threats relates to more complex obfuscation techniques, such as crowdfunding, mixers and tumblers, chain-hopping, shared digital wallets and Metaverse. Lastly, a third category of threat was established regarding internet-based communication platforms and social media, which could further relate to a variety of TF purposes, including recruiting new members, fundraising, spreading propaganda messages and disseminating technical knowledge. The TF trends that associate with the previously identified emerging threats are the augmented use of crypto assets, mainly Bitcoin and other cryptocurrencies; the increase in the exploitation of FinTech-based obfuscation methods, such as shared digital wallets, mixers and chain-hopping; the continuing increase of the relevance of self-financing schemes. The principal sub-trends characterizing the reliance on self-financing schemes are the collection of funds through disguised fundraising campaigns and online fraudulent activities.

## 5.2 Policy implications

The set of tools available for making international transactions is constantly changing and evolving. As a result, the methods used by the financiers of terrorism to raise and move capital internationally are also updated and differentiated implying a real need for LEAs and experts to be continuously informed about the recent trends. To develop more effective regulations and strategies to combat the TF, more studies on the mode of operation of the financiers of terrorism, their use of FinTechs and the links between digital transactions and the offline world are necessary. Such studies must increase the understanding of the contemporary mechanisms of TF not only from a theoretical point of view, but also and above all from an empirical point of view. In this respect, it is essential to establish the relevance of the different mechanisms in terms of their frequency and ideally of impact on society.

Although further investigation is necessary in many aspects of the TF, the evidence gathered to produce this report and the study of the analyses of TF and technologies already available make possible to formulate some policy implications. To mitigate the risk of terrorism, it is crucial to **improve the mapping of anomalous schemes and automatically detect recurrent patterns in the financial system**. This exercise has to embrace both traditional pay-systems as new payment systems and cryptocurrencies. On this respect, while most cryptocurrencies characterize for their pseudonymity, blockchain technologies, on which cryptocurrencies rely on, can be also designed for auditing and tracking of funds, while, simultaneously preserving users' privacy.

Related to the tracing of digital transactions and the automatized detection of suspicious behaviours is the need for expanding the **use of KYC procedures in the realm of crypto assets and digital economy** in general. Indeed, to reduce the risk for TF crypto assets and digital payment systems need to be brought into the regulated financial markets. The necessity to introduce effective KYC procedures is particularly pressing with respect to NFTs market places and in the Metaverse. In fact, in both environments, anonymity of economic agents is still high. Finally, as it is in the fight against other crimes, also with respect to TF conducted through FinTechs, **law enforcement cooperation in cybersecurity domains and the control of cryptocurrency markets** will be fundamental to reach enforcement effectiveness. Being the digital integrated at the global level, the cooperation among enforcement agencies across countries will be crucial for the deanonymization and tracking of funds as well as to counter offline activities that both proceed and follows TF.

## References

- ACAMS. 2021. ‘Changes in Bank Regulations, Financial Compliance Regulations, Regulation Banks, Money Laundering Cases, Anti Money Laundering, Money Laundering Training’. 2021. <https://www.moneylaundering.com/news/cryptocurrency-laundering-grows-in-sophistication-expands-beyond-dark-web/>.
- Ahmad, Nadia. 2022. ‘Ripple (XRP): What Is It, History and How to Buy’. *SmartAssets* (blog). 2022. <https://smartasset.com/financial-advisor/ripple-xrp>.
- Al Jazeera. 2021. ‘Israel Says It Is Targeting Hamas’s Cryptocurrency Accounts’, 2021. <https://www.aljazeera.com/news/2021/7/9/israel-says-it-is-targeting-hamas-cryptocurrency-accounts>.
- Amiram, Dan, Bjorn Jorgensen, and Daniel Rabetti. 2020. ‘Coins for Bombs: Increased Transparency of the Global Financial System - Evidence from Terrorist Attacks Financing Detection in Blockchain-Based Currencies’. SSRN Scholarly Paper ID 3616207. Rochester, NY: Social Science Research Network. <https://doi.org/10.2139/ssrn.3616207>.
- Barone, Daniela Maria. 2018. ‘Jihadists’ Use of Cryptocurrencies: Undetectable Ways to Finance Terrorism’. *Siurezza, Terrorismo e Società* 8 (2): 17–60.
- Bloomberg. 2022. ‘NFT Market Surpassed \$40 Billion in 2021, New Estimate Shows’, 6 January 2022. <https://www.bloomberg.com/news/articles/2022-01-06/nft-market-surpassed-40-billion-in-2021-new-estimate-shows>.
- Brantly, Aaron. 2014. ‘Financing Terror Bit by Bit’. *CTC Sentinel* 7 (10): 1–20.
- Dcointrade. 2021. ‘RIPPLE(RXP) - DcoinTrade’. 2021. <https://www.dcointrade.com/currency/xrp>.
- Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston. 2019. ‘Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats’. RAND Corporation. [https://www.rand.org/pubs/research\\_reports/RR3026.html](https://www.rand.org/pubs/research_reports/RR3026.html).
- EBA. 2021. ‘The EBA Highlights Key Money Laundering and Terrorist Financing Risks across the EU’. European Banking Authority. 3 March 2021. <https://www.eba.europa.eu/eba-highlights-key-money-laundering-and-terrorist-financing-risks-across-eu>.
- Elliptic. 2018. ‘What Are Bitcoin Mixers & Are They Compliant With AML Standards?’ 2018. <https://www.elliptic.co/blog/bitcoin-mixers-assessing-risk-bitcoin-transactions>.
- EU. 2011. *Council Decision 2011/70/CFSP of 31 January 2011 Updating the List of Persons, Groups and Entities Subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the Application of Specific Measures to Combat Terrorism*. Vol. OJ L 28. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R0138&qid=1642694616307&from=EN>.
- EU. 2018. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law (6AMLD) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN>.
- EU. 2018a. *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 (Text with EEA Relevance)*. Vol. OJ L 156 (5AMLD). <https://eur-lex.europa.eu/eli/dir/2018/843/oj/eng>.
- EU. 2018b. *Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on Combating Money Laundering by Criminal Law*. Vol. OJ L 284 (6AMLD). [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2018.284.01.0022.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.284.01.0022.01.ENG).
- EU, 2019. Commission Staff Working Document, Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. [https://ec.europa.eu/info/sites/default/files/supranational\\_risk\\_assessment\\_of\\_the\\_money\\_laundering\\_and\\_terrorist\\_financing\\_risks\\_affecting\\_the\\_union\\_-\\_annex.pdf](https://ec.europa.eu/info/sites/default/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union_-_annex.pdf).

- EU. 2021. *Council Implementing Regulation (EU) 2021/1188 of 19 July 2021 Implementing Article 2(3) of Regulation (EC) No 2580/2001 on Specific Restrictive Measures Directed against Certain Persons and Entities with a View to Combating Terrorism, and Repealing Implementing Regulation (EU) 2021/138*. OJ L 258. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R0138&qid=1642694616307&from=EN>.
- EU. 2021a. ‘European Union Terrorism Situation and Trend Report 2021 (TESAT)’. <https://doi.org/10.2813/677724>.
- EU. 2021b. ‘Internet Organised Crime Threat Assessment (IOCTA) 2021’. *Europol*. <https://doi.org/10.2813/113799>.
- Europol. 2020. ‘Individual Arrested in Madrid for Transferring Money to Syria to Fund the Return of Foreign Terrorist Fighters to Europe’. *Europol*, 2020. <https://www.europol.europa.eu/media-press/newsroom/news/individual-arrested-in-madrid-for-transferring-money-to-syria-to-fund-return-of-foreign-terrorist-fighters-to-europe>.
- Europol (2022), Cryptocurrencies: Tracing the Evolution of Criminal Finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.
- Fanusie, Y.J., and T. Robinson. 2018. ‘Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services’. Foundation for Defense of Democracies and Elliptic. [https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/MEMO\\_Bitcoin\\_Laundering.pdf](https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/MEMO_Bitcoin_Laundering.pdf).
- FATF. 2008. ‘Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems’. Paris: Financial Action Task Force. <https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf>.
- FATF. 2013. ‘The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing’. Paris: Financial Action Task Force. <https://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf>.
- FATF. 2014. ‘Virtual Currencies: Key Definitions and Potential AML/CFT Risks’. <https://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>.
- FATF. 2015. ‘Guidance for a Risk-Based Approach to Virtual Currencies’. <https://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html>.
- FATF . 2019. ‘Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>.
- FATF. 2021. ‘Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’. Paris: Financial Action Task Force. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>.
- Freeman, Michael, and Moyara Ruehsen. 2013. ‘Terrorism Financing Methods: An Overview’. *Perspectives on Terrorism* 7 (4): 5–26.
- Guardian Nigeria. 2021. ‘How Will the Metaverse Impact Online Gambling?’ *The Guardian Nigeria*, 26 December 2021. <https://guardian.ng/sport/other/how-will-the-metaverse-impact-online-gambling/>.
- Johnson, Tim. 2016. ‘The Computer Hacker Who Helped Feed An Islamic State Death List’. *Task & Purpose* (blog). 22 July 2016. <https://taskandpurpose.com/news/computer-hacker-helped-feed-islamic-state-death-list/>.
- Kancherla, Jayanth. 2020. ‘Terrorism Financing: Al-Qaeda and ISIS’. SSRN Scholarly Paper ID 3750495. Rochester, NY: Social Science Research Network. <https://doi.org/10.2139/ssrn.3750495>.
- Kim-Kwang, Raymond Choo. 2015. ‘Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?’ In *Handbook of Digital Currency*, edited by David Lee Kuo Chuen, 283–307. San Diego: Academic Press. <https://doi.org/10.1016/B978-0-12-802117-0.00015-1>.
- Kwon, K. Hazel, Monica Chadha, and Kirstin Pellizzaro. 2017. ‘Proximity and Terrorism News in Social Media: A Construal-Level Theoretical Approach to Networked Framing of Terrorism in Twitter’. *Mass Communication and Society* 20 (6): 869–94. <https://doi.org/10.1080/15205436.2017.1369545>.



- Levy, Ido, and Abdi Yusuf. 2021. 'How Do Terrorist Organizations Make Money? Terrorist Funding and Innovation in the Case of al-Shabaab'. *Studies in Conflict & Terrorism* 44 (12): 1167–89. <https://doi.org/10.1080/1057610X.2019.1628622>.
- Maitland Irwin, Angela Samantha, Raymond Choo Kim-Kwang, and Liu Lin. 2012. 'An Analysis of Money Laundering and Terrorism Financing Typologies'. *Journal of Money Laundering Control* 15 (1): 85–111. <https://doi.org/10.1108/13685201211194745>.
- Majumder, Amit, Megnath Routh, and Dipayan Singha. 2019. 'A Conceptual Study on the Emergence of Cryptocurrency Economy and Its Nexus with Terrorism Financing'. In *The Impact of Global Terrorism on Economic and Political Development*, edited by Ramesh Chandra Das, 125–38. Emerald Publishing Limited. <https://doi.org/10.1108/978-1-78769-919-920191012>.
- Maremont, Mark, and Christopher S. Steward. 2017. 'FBI Says ISIS Used eBay to Send Terror Cash to U.S.' *Wall Street Journal*, 11 August 2017, sec. US. <https://www.wsj.com/articles/fbi-says-isis-used-ebay-to-send-terror-cash-to-u-s-1502410868>.
- McKendry, Ian. 2015. 'ISIL May Be Using Bitcoin, Fincen's Calvery Says'. *American Banker*, 16 November 2015. <https://www.americanbanker.com/news/isil-may-be-using-bitcoin-fincens-calvery-says>.
- MONEYVAL. 2020. 'Annual Report for 2020'. Committee of Experts on the Evaluation of anti-money laundering measures and the financing of terrorism (MONEYVAL).
- Napoleoni, Loretta. 2010. *Terrorism and the Economy: How the War on Terror Is Bankrupting the World*. <https://www.penguinrandomhouse.com/books/214120/terrorism-and-the-economy-by-loretta-napoleoni/>.
- Narayanan, Arvind, and Malte Möser. 2017. 'Obfuscation in Bitcoin: Techniques and Politics'. *ArXiv:1706.05432 [Cs]*, June. <http://arxiv.org/abs/1706.05432>.
- Nauert, Heather. 2015. 'ISIS Parks Its Cash in Bitcoin, Experts Say'. *BGR*, 26 November 2015. <https://bgr.com/general/isis-parks-its-cash-in-bitcoin-experts-say/>.
- Peters, Katelyn. 2021. 'What Is the Binance Exchange?' *Cryptocurrency* (blog). 8 July 2021. <https://www.investopedia.com/terms/b/binance-exchange.asp>.
- Purnell, Newley, and Resty Woro Yuniar. 2016. 'Islamic State Eludes Southeast Asian Authorities With Telegram App'. *Wall Street Journal*, 19 January 2016, sec. Tech. <https://www.wsj.com/articles/islamic-state-eludes-southeast-asian-authorities-with-telegram-app-1453173661>.
- Rudner, Martin. 2017. "'Electronic Jihad': The Internet as Al Qaeda's Catalyst for Global Terror". *Studies in Conflict & Terrorism* 40 (1): 10–23. <https://doi.org/10.1080/1057610X.2016.1157403>.
- RUSI. 2018. 'From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime'. <https://rusi.org/explore-our-research/publications/occasional-papers/money-mules-chain-hopping-targeting-finances-cybercrime>.
- Schlabach, Adam. 2020. 'Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report - CipherTrace'. *CipherTrace* (blog). 2020. <https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/>.
- Seth, Shobhit. 2021. 'The 6 Most Private Cryptocurrencies'. *Cryptocurrency* (blog). 4 July 2021. <https://www.investopedia.com/tech/five-most-private-cryptocurrencies/>.
- ShenTu, QingChun, and JianPing Yu. 2015a. 'Transaction Remote Release (TRR): A New Anonymization Technology for Bitcoin'. *ArXiv:1509.06160 [Cs]*, September. <http://arxiv.org/abs/1509.06160>.
- ShenTu, QingChun, and JianPing Yu. 2015ab 'A Blind-Mixing Scheme for Bitcoin Based on an Elliptic Curve Cryptography Blind Digital Signature Algorithm'. *ArXiv:1510.05833 [Cs]*, October. <http://arxiv.org/abs/1510.05833>.
- Song, Wanshui, Wenyin Zhang, Linbo Zhai, Luanqi Liu, Jiuru Wang, Shanyun Huang, and Bei Li. 2021. 'EOS.IO Blockchain Data Analysis'. *The Journal of Supercomputing*, October. <https://doi.org/10.1007/s11227-021-04090-y>.
- Szydelski, Jakub. 2021. 'Terrorists' Activities on-Line during Covid-19 Pandemic - the European Perspective'. *European Journal of Geopolitics* 9: 19–35.

- Teichmann, Fabian Maximilian Johannes. 2018. 'Financing Terrorism through Cryptocurrencies – a Danger for Europe?' *Journal of Money Laundering Control* 21 (4): 513–19. <https://doi.org/10.1108/JMLC-06-2017-0024>.
- TRM. 2021. ' Hamas and Cryptocurrency: The Evolution of Terror Financing and the Global Effort to Stop It | TRM Insights'. 2021. <https://www.trmlabs.com/post/hamas-cryptocurrency-financing-campaign-a-continuing-evolution>.
- UK Gambling Commission. 2021. 'Emerging Money Laundering and Terrorist Financing Risks'. Gambling Commission. 2021. <https://www.gamblingcommission.gov.uk/licensees-and-businesses/guide/emerging-anti-money-laundering-risks>.
- Unger, Brigitte, Melissa Siegel, Joras Ferwerda, Wouter de Kruijf, Madalina Busoioic, and Kristen Wokke. 2006. 'The Amounts and the Effects of Money Laundering. Report for the Ministry of Finance'. [https://www.maurizioturco.it/bddb/2006\\_02\\_16\\_the\\_amounts\\_and\\_.pdf](https://www.maurizioturco.it/bddb/2006_02_16_the_amounts_and_.pdf).
- United Nations Security Council. 2021. 'Subsidiary Organs of the United Nations Security Council. 2021 Fact Sheet'. United Nations Security Council. [https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/subsidiary\\_organs\\_factsheets.pdf](https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/subsidiary_organs_factsheets.pdf).
- US Bureau of Counterterrorism. 2022. 'Foreign Terrorist Organizations Designated by the Secretary of State in Accordance with Section 219 of the Immigration and Nationality Act (INA), as Amended'. US Department of State. <https://www.state.gov/foreign-terrorist-organizations/>.
- US Department of Justice. 2015. 'United States v Ali Shukri Amin'.
- US Department of Justice. 2020a. 'United States v Zoobia Shahnaz'.
- US Department of Justice. 2020b. 'Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts'. The United States Department of Justice. <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>.
- Valeri, Robin Maria. 2018. 'From Declarations to Deeds: Terrorist Propaganda and the Spread of Hate and Terrorism Through Cyberspace'. In *Terrorism in America*. Routledge.
- Vermaak, Werner. 2020. 'MiCA: A Guide to the EU's Proposed Markets in Crypto-Assets Regulation'. *Sygn* (blog). 6 October 2020. <https://www.sygn.io/blog/what-is-mica-markets-in-crypto-assets-eu-regulation-guide/>.
- Vidino, Lorenzo, Jon Lewis, and Andrew Mines. 2020. 'Dollars for Daesh: Analyzing the Finances of American ISIS Supporters'. George Washington University. <https://doi.org/10.4079/poe.09.2020.00>.
- Weimann, Gabriel. 2016. 'Going Dark: Terrorism on the Dark Web'. *Studies in Conflict & Terrorism* 39 (3): 195–206. <https://doi.org/10.1080/1057610X.2015.1119546>.
- Winer, Jonathan M. 2008. 'Countering Terrorist Finance: A Work, Mostly in Progress'. *The ANNALS of the American Academy of Political and Social Science* 618 (1): 112–32. <https://doi.org/10.1177/0002716208317696>.
- Yuniar, Resty Woro. 2017. 'Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says'. *Wall Street Journal*, 10 January 2017, sec. World. <https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198>.
- Zdanowicz, John S. 2009. 'Trade-Based Money Laundering and Terrorist Financing'. *Review of Law & Economics* 5 (2): 855–78. <https://doi.org/10.2202/1555-5879.1419>.
- Zerzan, Andrew. 2010. *New Technologies, New Risks? Innovation and Countering the Financing of Terrorism*. World Bank Working Paper, no. 174. Washington, D.C: World Bank.