STUDY

For the TERR committee

European Parliament

Virtual currencies and terrorist financing: assessing the risks and evaluating responses

Counter-Terrorism

Policy Department for Citizens' Rights and Constitutional Affairs

Directorate General for Internal Policies of the Union

PE 604.970- May 2018

EN

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

COUNTER-TERRORISM

Virtual currencies and terrorist financing: assessing the risks and evaluating responses

STUDY

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the TERR Committee, explores the terrorist financing (TF) risks of virtual currencies (VCs), including cryptocurrencies such as Bitcoin. It describes the features of VCs that present TF risks, and reviews the open source literature on terrorist use of virtual currencies to understand the current state and likely future manifestation of the risk. It then reviews the regulatory and law enforcement response in the EU and beyond, assessing the effectiveness of measures taken to date. Finally, it provides recommendations for EU policymakers and other relevant stakeholders for ensuring the TF risks of VCs are adequately mitigated.

ABOUT THE PUBLICATION

This research paper was requested by the European Parliament's Special Committee on Terrorism and was commissioned, overseen and published by the Policy Department for Citizens' Rights and Constitutional Affairs.

Policy Departments provide independent expertise, both in-house and externally, to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU external and internal policies.

To contact the Policy Department for Citizens' Rights and Constitutional Affairs or to subscribe to its newsletter please write to: poldep-citizens@europarl.europa.eu

RESPONSIBLE RESEARCH ADMINISTRATOR

Kristiina MILT
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@europarl.europa.eu

AUTHORS

Tom KEATINGE, Director of the Centre for Financial Crime and Security Studies, Royal United Services Institute (coordinator)
David CARLISLE, Centre for Financial Crime and Security Studies, Royal United Services Institute, etc.
Florence KEEN, Centre for Financial Crime and Security Studies, Royal United Services Institute, etc.

LINGUISTIC VERSION

Original: EN

Manuscript completed in May 2018

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

AMLD	Anti-Money Laundering Directive
5AMLD	EU Fifth Anti-Money Laundering Directive
AML/CFT	Anti-money laundering and countering the financing of terrorism
CDD	Customer due diligence
Dapps	Decentralised applications
DDoS	Distributed denial of service attack
DEX	Decentralised exchange
DLT	Distributed ledger technology
EBA	European Banking Authority
FATF	Financial Action Task Force
FCA	UK Financial Conduct Authority
FinCEN	US Financial Crimes Enforcement Network
FINMA	Swiss Financial Market Supervisory Authority
FIUs	Financial intelligence units
FSA	Financial Services Agency of Japan
FSRBs	FATF-Style Regional Bodies
G7	Group of Seven
G20	Group of Twenty
GDPR	General Data Protection Regulation
GFSC	Gibraltar Financial Services Commission
IOCTA	Internet Organised Crime Threat Assessment
ISIS	Islamic State of Iraq and Syria
ITMC	Ibn Taymiyya Media Center

JMLIT	Joint Money Laundering Intelligence Task Force
KYC	Know Your Customer
MSB	Money service business
MSC	Mujahideen Shura Council in the Environs of Jerusalem
OCGs	Organised crime groups
LEAs	Law enforcement agencies
P2P	Peer-to-peer
PPP	Public-private partnership
RBA	Risk-based approach
STR	Suspicious Transaction Report
SNRA	Supra-National Risk Assessment
SPLC	Southern Poverty Law Center
TF	Terrorist financing
VC	Virtual currency

LIST OF TABLES

LIST OF MAPS

LIST OF FIGURES

FIGURE 8

EXECUTIVE SUMMARY

Virtual currencies (VCs) - which include cryptocurrencies such as Bitcoin, as well as a range of other digital value-transfer methods – are innovative new technologies that enable digital transactions and the delivery of financial products and services in new online networks, environments and marketplaces. Consequently, some observers view VCs as important for furthering competition in payments services, expanding financial inclusion and enabling greater efficiency and speed in cross-border value transfer.

Like other financial products and services, VCs have features that present risks for facilitating criminality, including money laundering and terrorist financing (TF). The borderless, peer-to-peer (P2P) nature of certain VCs offers the prospect for terrorist actors to transfer funds outside the regulated sector and beyond the purview of anti-money laundering and countering the financing of terrorism (AML/CFT) authorities. VCs also feature varying levels of anonymity and pseudonymity, which can enable the concealment of illicit activity.

Instances of VCs' illicit use in cybercrime and in encrypted Dark Web marketplaces are well-documented. However, there are still only a small number of publicly-documented and confirmed cases of TF involving VCs. In their current form and at current levels of adoption, VCs may not present terrorist actors with substantial advantages over other methods of funding and financing they already utilise.

Nonetheless, the public record demonstrates that religiously and politically-inspired extremist actors have utilised VCs, if in relatively low-volume and unsystematic fashion, and may be seeking to expand their use. The prospect exists for TF through VCs to mature and to grow, even if the precise nature, scale and scope of this risk remains difficult to anticipate.

In the near-term, terrorist use of VCs is most likely to involve occasional use for specific and limited purposes, including:

- raising funds or procuring illicit items on the Dark Web;
- soliciting donations in crowdfunding campaigns conducted on social media and encrypted messaging platforms; and
- transmitting funds internationally among members of terrorist networks using P2P value transfers.

Several developments could elevate and shape the nature of these risks over time, especially:

- the proliferation of VCs featuring high levels of privacy and anonymity;
- terrorists' broader adoption and utilisation of encryption technology, social media and other online platforms;
- the nexus between terrorist actors and other criminal activity; and
- the general pace and shape of VC innovation and adoption more broadly.

The prospect for sustained, larger-scale TF to emerge through developments such as the convergence of terrorism with cybercriminality presents a possible long-term risk of concern. This study considers these near-and long-term risks in detail.

The EU regards mitigating the TF risks associated with VCs as a significant security priority. The EU's recently adopted Fifth Anti-Money Laundering Directive (5AMLD) requires that Member States bring VC exchange platforms and custodial wallet providers within the scope of their AML/CFT regulation. This marks an important step in bringing transparency to VC

networks across the EU and is consistent with guidance issued by the Financial Action Task Force (FATF). But the passage of 5AMLD is only a first step. To ensure its effectiveness:

- Member States should clarify the scope and purpose of regulation once transposed locally and must undertake meaningful enforcement.
- The EU should play a leadership role in advocating for a coordinated AML/CFT global regulatory framework towards VCs, building on efforts it has undertaken at the Group of Twenty (G20).
- The EU-wide VC sector can play a role by forming credible self-regulatory bodies to help the sector build resiliency against a range of illicit threats, including TF.

Furthermore, it is important that the EU sustains a regulatory framework that remains relevant. As regulators' understanding of the risks and benefits of VCs and related innovations evolves, new regulatory approaches may be needed. To this end:

- The EU should convene an expert working group to assess whether further measures may be required to supplement 5AMLD.
- This should include exploring how future regulatory regimes can respond to the emergence of increasingly complex P2P, decentralised financial products and ecosystems.
- The EU should consider regulating the exchange of VCs for other VCs, as the current scope of 5AMLD covers only the exchange of VCs for fiat currency – a factor which may limit 5AMLD's ability to address the full range of risks.

EU law enforcement agencies (LEAs) have demonstrated significant recent progress in tracing illicit activity involving VCs and disrupting related criminal activity. However, VCs demand that LEAs develop new skills and acquire new resources. Important technical and skills gaps remain across the EU. To fill these:

- The EU should prioritise formal, strategic and sustained law enforcement training to enhance the capacity of LEA's for investigating illicit activity involving VCs.
- Member States should ensure LEAs are appropriately staffed with dedicated technical experts and that they are able to access to essential resources, such as forensic tools for analysis of illicit activity on cryptocurrency 'blockchains'.
- A priority for the EU should be to develop a comprehensive intelligence framework for assessing VCs' use across a range of risks, including TF, cybercrime and other illicit finance activity.
- To this end, Member States should develop interagency VC intelligence task forces staffed with dedicated experts focused on developing a coherent local picture of VC risks.

To further these aims, robust information sharing on the illicit use of VCs is essential. As VC exchanges and custodial wallet providers are brought within the scope of AML/CFT requirements under 5AMLD, public sector agencies should engage and share information with them. Formal public-private partnerships (PPPs) can facilitate these contacts and interactions.

Aim

This study examines the TF risks from VCs and considers the efficacy and relevance of related public policy responses. Whilst it refers to instances of VCs' use in other forms of illicit activity, such as cybercrime and general money laundering, this study's focus is primarily on TF. It does not attempt to provide a comprehensive review of the general illicit uses of VCs, which has been addressed in other studies. It's discussion of regulatory matters focuses on AML/CFT regulation and does not attempt to address comprehensively the full range of consumer protection or other regulatory regimes that may apply to VCs.

This study is drawn from a review of open-source literature, including official public-sector reports, academic studies, analysis of social media information and press reporting. One limitation of its methodology is that its assessments of TF risks are based on publicly available information and do not draw on confidential sources. Research for this paper has also included interviews with 21 subject matter experts, including individuals from Europol, Member State LEAs, regulatory bodies and FIUs, as well as representatives from academia and the VC industry. It is organised as follows:

Chapter 1 – Virtual Currencies: Definitions, Characteristics and Uses describes the types of VCs that exist, their technical features and uses, both licit and illicit.

Chapter 2 – Background on Counter-Terrorist Financing Efforts and Virtual Currencies provides an overview of international responses to TF that have emerged over the past two decades and describes how in recent years these responses have evolved to meet the challenges posed by a range of new technologies, including VCs.

Chapter 3 – Assessing Terrorist Financing Risks and Trends Involving Virtual Currencies provides a review of existing literature on terrorist use of VCs, and considers how broader developments in the technology and in terrorist behaviour could influence the nature and scale of VCs' possible use in TF over time.

Chapter 4 – Legal and Regulatory Mechanisms summarises recent regulatory measures in place globally, but focuses on the implications of 5AMLD and related measures across the EU. It explains the rationale for the design of these mechanisms and considers their effectiveness, noting areas of priority for regulators as they seek to balance the aims of mitigating risks whilst fostering innovation.

Chapter 5 – Cooperation and Partnership Across the EU describes efforts by EU law enforcement to act against the illicit use of VCs, and considers the efficacy of this response. It also explores the potential for further efforts to develop enhanced intelligence by improving information sharing and coordination across the public sector, as well as between the public and private sectors.

Chapter 6 – Policy Recommendations provides a summary set of recommendations for key stakeholders across the EU.

1. VIRTUAL CURRENCIES: DEFINITIONS, CHARACTERISTICS AND USES

KEY FINDINGS

- The FATF has distinguished between two types of VCs: decentralised (cryptocurrencies) and centralised VCs.
- Cryptocurrencies are P2P value transfer networks that, whilst not used widely in commercial and retail transactions, are used for speculative purposes and in decentralised applications (Dapps).
- The 'blockchain' innovation of Bitcoin has sparked tremendous interest across industries such as finance, trade, medicine and others as a method of enabling secure and disintermediated data transfer and storage.
- Centralised VCs feature in alternative payments platforms and gaming environments. Cryptocurrencies and centralised VCs can be exchange across a growing number of online platforms.
- In recent years, VCs have featured in online criminal payments and particularly in large-scale cybercrime and on the Dark Web.

1.1. Types of VCs, Their Features and Uses

1.1.1. Basic Definitions

There is no single global definition of the term 'virtual currency'. Indeed, the French and German finance ministries have suggested that use of the term 'currency' when describing these technologies is misleading, and that new terminology, such as 'crypto-assets', may prove appropriate.[1]

However, to provide for a common regulatory approach through 5AMLD, the EU has adopted a definition of VCs derived from the FATF's guidance. 5AMLD regards VCs as, 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.'[2]In its 2014 report *Virtual Currencies: Key Definitions and Potential AML/CFT risks*[3], the FATF defined two forms of VCs: decentralised VCs, and centralised VCs. Whilst 5AMLD does not distinguish between these types, the taxonomy provides a useful framework for understanding the gradation in the range of risks VCs may pose. The following sections describe these types and provide examples of their use, both licit and illicit.

[1]Letter from France and Germany to the G20 Ministers, 7 February 2018, https://www.politico.eu/wp- content/uploads/2018/02/G20-Letter-on-crypto-assets-tokens.pdf.

[2] European Parliament, Position of the European Parliament adopted at first reading on 19 April 2018 with a view to the adoption of Directive (EU) …/… of the European Parliament and of the Council 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*, Article 3 new point 18 of the Directive (EU) 2015/849, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2018-0178.

[3] Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FATF Report, June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

1.1.2. Decentralised VCs (Cryptocurrencies)

Decentralised VCs do not require a central issuer or authority to enable agreement on the validity of transactions within a network, or to generate and issue new units. The term 'decentralised VC' is generally synonymous with the popular term 'cryptocurrency', originally used to refer to Bitcoin.

Cryptocurrencies are open-source, P2P value transfer networks that rely on cryptographic proof to validate transactions and provide consensus about network activity without reliance on a trusted third-party, such as a bank or other financial institution. Cryptocurrencies function as a form of 'digital cash' by enabling P2P, direct transfers between two parties, much as two people could exchange physical fiat currency, but without the same limitations of space and distance.

Launched in 2009, Bitcoin was the first cryptocurrency and marked a significant innovation over earlier attempts to establish digital cash systems, which had always required the presence of a central issuing party to govern network activities and mint new coins. Bitcoin's founding was routed in the libertarian-leanings of the 'cypherpunk' community of cryptographers, who believed that the creation of decentralised, alternative payment systems impervious to the control of governments or banks is essential to the development of true financial freedom.[4] Satoshi Nakamoto, the pseudonymous creator of Bitcoin, suggested that the development of a P2P payment network would reduce reliance on the highly intermediated mainstream financial system, which features third parties such as banks and credit card issuers who can charge fees and rent-seek from inefficiencies.[5]

Developing a decentralised payment system required overcoming technical hurdles. Foremost among these was ensuring reliability of transactions and creating disincentives to sabotage a network without a single arbiter. Central to resolving this dilemma is 'mining,' which in Bitcoin is the process of incentivising participants in the network to supply computing power to arrive at consensus about network activities. The mining process prevents 'double spending' of any single coin, ensuring that a coin is not in effect counterfeited and repeatedly spent by the same party. Once confirmed, P2P transactions are recorded on the blockchain, Bitcoin's ledger of transactions, which provides a complete, chronological record of network activities and is maintained in identical copies on numerous computers across the network (and is therefore referred to as 'distributed ledger technology', or DLT). The Bitcoin blockchain serves as a reliable and secure record of transactions, as its contents are distributed across various nodes and are not maintained in on a single server or location; altering its contents or tampering with the network would require harnessing prohibitively enormous computing power.

For many observers, it is this innovation – the creation of a shared database that contains a reliable and secure record of all network activity and is assembled through a mechanism of distributed consensus – that marks Bitcoin's primary technological contribution. Enormous attention is being given to the potential applications of DLT. In industries as diverse as trade finance, energy, food distribution, wholesale banking, and humanitarian aid disbursement, practitioners are interested to understand and explore how disintermediated, secure databases may enhance processes and systems that are presently fragmented and lacking in transparency. Central governments, including some across the EU, have also begun to discuss the possibility of issuing central bank digital currencies, which could draw on DLT

[4] Lopp, Jameson, 'Bitcoin and the Rise of the Cypherpunks,' *CoinDesk*, 9 April 2016, https://www.coindesk.com/the-rise-of-the-cypherpunks/.
[5] Nakamoto, Satoshi, 'Bitcoin: A Peer-to-Peer Electronic Cash System', https://bitcoin.org/bitcoin.pdf.

innovations.[6] In April 2018, the European Commission's Digital Single Market initiative announced the launch of the My Health My Data project, which aims to reduce the vulnerability of medical records to security breaches by creating a DLT platform to enable 'data to be stored and transmitted safely and effectively.'[7]

Sceptics suggest that much of the current enthusiasm around DLT is misplaced and that most proposed use cases remain unproven, or worse, wasteful.[8] Whether and just how successfully DLT and related innovations will take shape beyond Bitcoin remains unclear; regardless, Nakamoto's innovation has inspired enormous discussion and debate about the direction of technological innovation.

The exact scale, nature and extent of cryptocurrency adoption and usage globally is difficult to characterise with precision. A 2017 study by researchers from Cambridge University suggested that the number of individual cryptocurrency users is between approximately three and six million users, with as many as 11.5 million cryptocurrency wallets in active use.[9]

A cryptocurrency wallet represents users 'private keys', which are in essence passwords used to sign transactions associated with a user's public cryptocurrency addresses that appear on the blockchain. The person in possession of private keys is the effective owner of the associated cryptocurrency. Private keys can either be recalled by memory or written down. However, maintaining security of private keys is a priority for cryptocurrency users, as the theft or loss of those keys results in the user losing access to their cryptocurrency. Numerous wallet services are available assist in private key management, including:

- **hardware wallets:** these allow users to store keys offline on physical devices like USB sticks that are easily portable;
- **software wallets:** these downloaded applications can be maintained on a desktop or mobile device and allow storage of private keys securely on the device;
- **hosted/custodial wallets:** these are maintained on the Web and offered through the websites of third-party service providers, such as cryptocurrency exchanges; these hosted wallet services are 'custodial' in that the wallet provider retains access to the user's private keys;
- **hybrid wallets:** these are also hosted on the webpage of a third-party service, but unlike custodial wallets, hybrid wallet providers do not have access to the user's private keys;
- **multi-signature wallets:** these provide enhanced security by requiring that multiple keys are used to authorise a transaction, reducing the risk of theft if a single private key is compromised.

Since early 2017, the proliferation in the number of cryptocurrencies and volumes and values traded has been substantial. It is possible that the number of individual users has grown significantly since the time the Cambridge study was conducted: information gathered by Japanese regulators in early 2018 suggests that there may be as many as 3.5 million cryptocurrency users in Japan alone.[10] Estimates suggest that at minimum 1500

[6] Bank for International Settlements, *Central Bank Digital Currencies*, study by the Committee on Payments and Market Infrastructures and the Markets Committee, March 2018, https://www.bis.org/cpmi/publ/d174.pdf.
[7] European Commission, 'Blockchain to enable medical data to be stored and transmitted safely and effectively,' Projects Story, 10 April 2018, https://ec.europa.eu/digital-single-market/en/news/blockchain-enable-medical-data-be-stored-and-transmitted-safely-and-effectively.
[8] Kaminska, Izabella, 'Growing scepticism challenges the blockchain hype,' *Financial Times*, 20 June 2017, https://www.ft.com/content/b5b1a5f2-5030-11e7-bfb8-997009366969.
[9] Hileman, Garrick and Rauchs, Michael, *Global Cryptocurrency Benchmarking Study,* Cambridge Centre for Alternative Finance and University of Cambridge Judge Business School, 2017, p.10, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf.
[10] Zhao, Wolfie, 'Japan Could Have More than 3 Million Crypto Trades,' CoinDesk, 10 April 2018, https://www.coindesk.com/3-5-million-traders-japan-releases-domestic-cryptocurrency-statistics/.

cryptocurrencies (or 'alt-coins', as cryptocurrencies other than Bitcoin are known) have been created, with as much as half of this this number having been developed since early 2017.[11] As of May 2018, the total US dollar value of cryptocurrencies is approximately USD 450 billion, a fifteen-fold increase over the previous year.[12] Bitcoin has historically dominated among cryptocurrencies, accounting for approximately 35 % of the current total value in May 2018; however, its market share has declined substantially, from nearly 80 % in early 2017, owing to the growth in the number and usage of alt-coins. Particularly relevant to study are recent innovations in privacy-focused alt-coins, or those cryptocurrencies that preserve high levels of anonymity. These are described further in Chapter 3. Table 1 in Annex II provides a list of major cryptocurrencies and their values.

In practice, cryptocurrencies have thus far failed to achieve Satoshi Nakamoto's promise of cheaper, faster micro-payments that can rival the incumbent payments infrastructure. As the number of Bitcoin users has grown, transaction speeds have slowed substantially owing to network congestion. In some cases, transaction confirmation times have risen to as much as 16 hours.[13] Due to limits on the scale of the blockchain, Bitcoin processes approximately seven transactions per second, versus credit card providers such as Visa, which can process up to 24,000 transactions per second.[14] Bitcoin also is not widely used as a form of payment for goods and services in developed economies. In developing countries, the picture is somewhat different, as Bitcoin adoption has been notable in countries such as Venezuela, where local currencies are volatile and access to reliable financial services is lacking.[15] This has led some observers to suggest that cryptocurrencies could further financial inclusion, or the extension of financial services to underserved populations. However, cryptocurrency usage is only a very small component of payment systems in the developing world and in remittance markets.[16]

Nonetheless, the range of cryptocurrency products and services is growing. Bitcoin ATMs, which permit users to deposit cash and receive Bitcoin into their online wallet, have grown in number substantially. There are at least several hundred Bitcoin ATMs located across Europe, with Austria and the UK each having more than 100.[17] Pre-paid cryptocurrency cards have emerged as well, allowing users to load their card with Bitcoin to spend at retailers, making Bitcoin easily portable and readily convertible using a VISA card. In February 2018, a bank in Liechtenstein, Bank Frick, announced that its customers can now invest directly in cryptocurrencies.[18]

[11] See figures from CoinMarketCap, https://coinmarketcap.com/.
[12] Ibid.
[13] Buchko, Stephen, 'How Long do Bitcoin Transactions Take?' *CoinCentral,* 12 December 2017, https://coincentral. com/ how-long-do-bitcoin-transfers-take/.
[14] Howmuch.net, 'Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?', https://howmuch.net/articles/crypto-transaction-speeds-compared
[15] Voge, Cady, 'Where Could Bitcoin Succeed as a Currency? In a Failed State,' *Wired*, 22 March 2018, https://www.wired. com/story/where-could-bitcoin-succeed-as-a-currency-in-a-failed-state/.
[16] Varruciu, Massimiliano, 'Bitcoin and remittance, where are we?' *Fintastico*, 6 July 2017, https://www.fintastico.com/blog/bitcoin-and-remittance-where-are-we/.
[17] CoinATM Radar, 'Bitcoin ATMs in Austria,' https://coinatmradar.com/countries/.
[18] Bank Frick, 'Bank Frick allows direct investments in leading cryptocurrencies,' Bank Frick website, 28 February 2018, https://www.bankfrick.li/en/about-bank-frick/news/bank-frick-allows-direct-investments-in-leading-cryptocurrencies.

Map 1:Map of Bitcoin ATMs in Austria by Number and Location

Source: Website of CoinATM Radar. The circles indicate the number of Bitcoin ATMs in certain regions of Austria, indicating, for example, that 40 Bitcoin ATMs are present in the region of Vienna and 36 in the region of Graz.

Another related development is the emergence of decentralised applications (Dapps), or open-source software programmes that use cryptocurrencies as a form of settlement. Like Bitcoin, Dapps do not feature a central authority but are open to all users and rely on incentivising mechanisms to ensure consensus about updates to network activity. Some observers see Dapps as important developments for enabling secure and open applications across the Internet that can replace reliance on the large corporations that currently develop and provide most online services - just as Bitcoin was designed to provide an alternative to the heavily intermediated payments system with a secure and open P2P payments network.[19] Dapps have been developed that enable cryptocurrencies to be used for a range of purposes including in prediction markets (for example, using the Augur platform[20]), in markets for digital file storage (for example, using Filecoin[21]) and in markets for enabling shared computing power arrangements (for example, using the Golem platform[22]).

However, most cryptocurrency usage today is speculative: users purchase cryptocurrencies with fiat currencies such as the euro, generally on large cryptocurrency exchanges, seeking to profit from fluctuations in value. A substantial volume of global Bitcoin trading has recently shifted to Malta[23], which has created a permissive regulatory environment for cryptocurrency companies, as described in Chapter 4. This speculative use has also accelerated with development of Initial Coin Offerings (ICOs), or fundraising mechanisms created using new tokens as an alternative to venture capital fundraising (and often built as Dapps on platforms such as Ethereum), a phenomenon that has generated both interest and controversy. This trend has led to the introduction of the term 'crypto-assets' to replace 'cryptocurrencies' in some quarters, including at the G20 and the FATF, reflecting the technology's function as instruments for fuelling digital speculation for use in specific Dapps that generally fail to fulfil the full range of functions expected of 'money'.

One realm in which cryptocurrencies have been used as a form of payment is for illicit purposes. Since 2014, Europol's *Internet Organised Crime Threat Assessment* (IOCTA)

[19] FundYourselfNow, '2018 The Year of Dapps,' *Medium*, 15 January 2018, https://medium.com/the-mission/2018-the-year-of-dapps-dbe108860bcb.
[20] Augur website, http://www.augur.net/.
[21] Filecoin website, https://filecoin.io/.
[22] Golem website, https://golem.network/.
[23] Katz Lily, 'Most Cryptocurrency Trading is Moving to Malta, at Least Legally,' *Bloomberg*, 25 April 2018, https://www.bloomberg.com/news/articles/2018-04-25/most-cryptocurrency-trading-is-moving-to-malta-at-least-legally?&utm_source=Newsletter&utm_medium=email&utm_content=Nasdaq%3A+the+next+killer+crypto+exchange%3F&utm_campaign=Weekly+Brief+5%2F2.

reports have demonstrated how cryptocurrencies act as an enabler of cybercrime.

According to Europol's 2017 IOCTA, cryptocurrencies are the currency of choice as payment for cyber-related extortion, such as ransomware and distributed denial of service (DDoS) attacks.[24] Ransomware attacks, which involve hackers encrypting victims' files or data and demanding a payment in exchange for returning access to the files or data, have grown increasingly ambitious and lucrative in scope, with single strains of ransomware yielding as much as USD 2 million for the cybercrime groups executing them.[25]

Cybertheft of cryptocurrency is also on the rise. A study by Chainalysis, a firm that analyses the blockchain, found that hacks targeting Bitcoin exchanges may have accounted for as much as USD 75 million in Bitcoin theft in 2017 alone.[26]

Another lucrative form of cybercrime is 'crypto-jacking', a process whereby the victim unknowingly has software installed onto their browser to mine cryptocurrency on the hacker's behalf. According to Check Point's 2017 Global Threat Index, 55 % of businesses worldwide have been affected by crypto-jacking malware, citing 'Coinhive', 'Rig ek' and 'Cryptoloot' as the 'three most wanted' strains.[27] The UK's National Cyber Security Centre and National Crime Agency have indicated that crypto-jacking is likely to become a major threat in 2018-19.[28]

Cryptocurrencies also feature as the preferred form of payment on the Dark Web, or that portion of the Web that relies on encrypted services, such as the Tor protocol, to shield users' identifying information and communications. Dark Web marketplaces, which are described in further detail in Chapter 3, are synonymous with the sale and purchase of illicit materials such as arms, drugs, counterfeit currency, fake passports, stolen credit cards details, as well as the provision of 'crime as a service', such has hacking for hire. These marketplaces work like Amazon or eBay, allowing users to 'peer review' illicit products and services which in turn leads to better quality products - at lower prices.[29]

There is also evidence suggesting cryptocurrencies are increasingly used in money laundering schemes by organised criminal groups (OCGs). Rob Wainwright, the former director of Europol, has stated that cryptocurrencies comprise approximately EUR 3 – 4 billion, or three to four percent, of illicit proceeds laundered through Europe annually.[30] Press reporting suggests that Colombian drug trafficking OCGs have taken advantage of the unregulated status of Bitcoin ATMs in Europe to launder the proceeds of narcotics sales from Europe to

[24] Europol, *Internet Organised Crime Threat Assessment (IOCTA 2017),* The Hague, 2017, p.11 ,https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017; DDoS attacks describe a process whereby hackers send multiple data requests from multiple sources in order to overload a website, mostly through a 'botnet' which are PCs that are compromised by malware, in order to send requests to the website without the users knowledge. This will eventually lead to an error message on the website, stating that the server is no longer responding.

[25] 'True scale of Bitcoin extortion revealed,' MIT Technology Review, 19 April 2018, https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/.

[26] Chainalysis, 'Report: The Changing Nature of Cryptocrime,' Chainalysis blog, 18 January 2018, https://blog.chainalysis.com/crypto-crime/.

[27] CheckPoint Software Technologies, 'December's Most Wanted Malware: Crypto-Miners Affect 55% of Businesses Worldwide,' 15 January 2018, https://globenewswire.com/news-release/2018/01/15/1289323/0/en/December-s-Most-Wanted-Malware-Crypto-Miners-Affect-55-of-Businesses-Worldwide.html.

[28] National Cyber Security Centre and the National Crime Agency, *The cyber threat to UK business*, London, 2017-2018 Report, p.25, https://www.ncsc.gov.uk/file/3077/download?token=Z5h53HP-.

[29] Glenny, Misha, 'Partners in crime: Why mafia groups and cybercriminals are joining forces,' World Economic Forum, 10 April 2018, https://www.weforum.org/agenda/2018/04/partners-in-crime-why-mafia-groups-and-cybercriminals-are-joining-forces.

[30] Silva, Shiroma, 'Criminals hide "billions" in crypto-cash – Europol,' *BBC News*, 12 February 2018, http://www.bbc.co.uk/news/technology-43025787.

Colombia.[31] Law enforcement across Europe indicate that they are identifying an increasing number of money laundering cases involving the use of cryptocurrencies[32], some of which are documented in Table 2 in Annex III.

Whatever their range of potential use cases, or whether they succeed as 'money', cryptocurrencies look poised to influence discussions of financial innovation for some time.

1.1.3. Centralised VCs

Unlike cryptocurrencies, centralised VCs feature an administrator to issue new units and to record information about network activities. Centralised VCs typically function as a unit of account and means of settlement in concentrated online environments, such as in alternative payment settlement networks, and in gaming.

Examples of alternative payment networks include WebMoney, a Russia-based payments services platform, and Perfect Money, a payments service platform based in Panama. These platforms issue their own VCs, which users can obtain in exchange for fiat currency and use to settle on-platform payments with other users. Many of these services also offer platforms for crowdfunding, merchant payments, budget planning and other integrated functions that enable them to be used as concentrated financial ecosystems for a wide range of uses.

As with cryptocurrencies, the exact scale and usage of centralised VCs is difficult to determine with accuracy. However, experts generally agree they are used on a scale far greater than cryptocurrencies, given their sheer number and reach. Platforms such as WebMoney and Perfect Money feature widely in the use of remittances, e-commerce purchases and in P2P payments on their platforms. WebMoney claims to have as many as 36 million users.[33]

Services such as WebMoney and Perfect Money have featured widely in cybercrime and money laundering activity.[34] Europol's IOCTA reports suggests centralised VC services are utilised in online criminal-to-criminal payments, but have been usurped by Bitcoin has the preferred method of transfer between online criminal actors.[35]

Developers of gaming services have also introduced VCs to enable commerce in the digital environments they have created. An example is Linden Dollars, which are used in the game Second Life. Whilst 5AMLD states that currencies used exclusively for use in gaming environments do not fall within in its scope, there are a growing number of gaming-based VCs that can be converted for fiat currency, and some jurisdictions regulate gaming-based VC exchange services. For example, in the US, Linden Labs, the developer of Linden Dollars, is registered as a money service business (MSB).[36]

Whilst technologically distinct, cryptocurrencies and centralised VCs are in practice exchangeable. Bitcoin can be used on platforms such as Perfect Money and WebMoney, and certain cryptocurrency exchanges are offering users the ability to purchase cryptocurrencies with centralised VC units.[37] Cryptocurrencies can be traded for gaming-based VCs as well.

---

[31] Couvée, Koos, 'European Traffickers Pay Colombian Cartels Through Bitcoin ATMs : Europol Official,' *ACAMS moneylaundering.com*, 28 February 2018, https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/.

[32] Authors' interviews with subject matter experts.

[33] WebMoney, 'About the System,' WebMoney website, https://www.wmtransfer.com/eng/information/short/index.shtml.

[34] 'The Secrets of Online Money Laundering,' MIT Technology Review, 18 October 2013, https://www.technologyreview.com/s/520501/the-secrets-of-online-money-laundering/.

[35] Europol, *Internet Organised Crime Threat Assessment (IOCTA 2016)*, The Hague, 2016, p. 24, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

[36] Grimes Law, 'Money Transmitter Licensing,' http://www.grimeslawaz.com/money-transmitter-licensing/.

[37] 'Cryptocurrency exchange EXMO adds WebMoney for Payments,' *CryptoNinjas*, 22 March 2017, https://www.cryptoninjas.net/2017/03/22/cryptocurrency-exchange-emxo-adds-webmoney-for-payments/.

This ability to operate across a diverse range of online environments has implications for illicit finance. One recent study suggests that cybercriminals are laundering funds by converting cryptocurrencies into gaming currencies, and then back to cryptocurrencies again to frustrate efforts at detection.[38]

[38] Town, Sam, 'Bitcoin vs. WoW Gold: Why Aren't Cryptos Treated Like In-Game Currencies?' *Cryptoslat*e, 19 March 2018, https://cryptoslate.com/crypto-in-game-currencies/.

2. BACKGROUND ON AML/CFT EFFORTS AND VIRTUAL CURRENCIES

KEY FINDINGS

- Since the establishment of the FATF in 1989, the international community has aimed to maintain a robust and coordinated framework for the prevention of illicit finance.
- The FATF and EU are committed to assessing and monitoring the TF risks around VCs, and to ensuring their members have appropriate mitigating measures in place. These measures, including the EU's 5AMLD, have focused on regulating certain third-party VC service providers, especially VC exchange platforms.
- However, many jurisdictions have yet to clarify their regulatory position on VCs, resulting in an incoherent international framework. A more coherent and coordinated international regulatory response is needed.

In 1989, the international community elevated the prevention of illicit finance and the protection of the integrity of the international financial system as major security priorities through the creation of the FATF. Founded by finance ministers of the Group of Seven (G7) countries, the FATF is the international standard-setting body for matters related to the prevention of money laundering, TF and the financing of proliferation of weapons of mass destruction.[39] It has since grown to include 37 full members, including the European Commission, which represents the interests of the EU at the FATF. The FATF standards have also been adopted by nine FATF-style Regional Bodies (FSRBs), including MONEYVAL, the Council of Europe's monitoring body that monitors compliance with the FATF standards across 47 European members.

In total 190 countries comprise the FATF network of full and affiliated members. This comprehensive, coordinated approach is central to making the international financial system more resilient against illicit actors and threats. A focus of the FATF's mission is enabling this coordination and identifying emerging systemic risks that could undermine the integrity and effectiveness of this framework.

In its first decade of existence, the FATF focused exclusively on the development and implementation of AML efforts; CFT-specific measures had yet to be adopted. Those AML priorities are reflected in the FATF's Forty Recommendations, first issued in 1990.[40] The Forty Recommendations, which were subsequently updated in 1996, form the bedrock of the international AML regime. They require that countries have in place arrangements such as legal provisions for criminalising money laundering and prohibitions on the use of anonymous accounts. FATF members must also require that financial institutions conduct customer due diligence (CDD) and file suspicious transaction reports (STRs)[41].

However, the events of 9/11 elevated TF as an international security priority and led the FATF to introduce measures and arrangements required to combat TF effectively. In 2001, the FATF expanded the original Forty Recommendations to include nine further CFT-specific

[39] Financial Action Task Force, 'Who we are,' website of the FATF, http://www.fatf-gafi.org/about/.
[40] Financial Action Task Force, *The Forty Recommendations of the Financial Action Task Force*, 1990, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF Recommendations 1990.pdf.
[41] This report uses the term 'STR', which used by Europol and many Member States. However, some jurisdictions use terms such as 'Suspicious Activity Reports' or 'Suspicious Matter Reports'.

recommendations.[42] These include measures related to the criminalisation of terrorist financing and the confiscation of terrorist assets.

The Nine Special Recommendations also set out that countries should provide for the regulation of alternative remittance systems, such as hawala networks and other informal value transfer mechanisms that sit outside the formal, regulated financial system – a priority that carries relevance for the FATF's later focus on the digital ecosystems that VCs enable.

The EU has demonstrated its commitment to ensuring that the FATF's standards are reflected in EU-wide requirements and that Member States transpose these locally. It has done so through the adoption of, to date, five AML Directives (AMLDs), with the first of these adopted in 1991 to implement the original Forty FATF Recommendations. Subsequent AMLDs have been adopted to ensure that EU Member States' AML/CFT frameworks align with the updated FATF Recommendations, and to ensure harmonised EU-wide AML/CFT approaches.

2.1. New Payment Methods, FinTech and CFT Efforts

2.1.1. The FATF and New Technologies

As the FATF developed its AML/CFT Recommendations during the 1990s and early 2000s, technological innovation impacting the financial sector, and society more broadly, sped forward at a tremendous pace. The development and widespread adoption of the Internet, the World Wide Web, personal computers, mobile devices, and related platforms and services, has had a vast impact on the pace and nature of social interactions, including on commerce and financial transactions.

In 2006, the FATF set out to understand these developments when it published a report on new payment methods.[43] The study suggests that the ability of new financial innovations, such as pre-paid cards and online and mobile payment platforms, to enable rapid cross-border payments presents elevated TF risks. The FATF followed this assessment with a more detailed study in 2010,[44] which suggests that FATF members were encountering a growing number of cases involving the illicit use of new payment methods, and points to a more detailed picture of risks. It notes the ability of new technologies to enable remote, non-face-to-face access, which affords users anonymity. Importantly, the FATF's 2010 report stresses that implementing CDD measures at the point where users access new technologies can mitigate the associated TF risks.

2.1.2. The FATF and VCs

In June 2014, the FATF took up the specific topic of VCs when it published *Virtual Currencies: Key Definitions and Potential AML/CFT risks*.[45] It suggests that VCs' global accessibility allows them 'to exist in a digital universe outside the reach of any particular country.'[46] It describes

[42] Financial Action Task Force, *The FATF IX Special Recommendations,* FATF Standards*,* Paris, 20 October 2001 http://www.fatf-gafi.org/publications/fatfrecommendations/documents/ixspecialrecommendations.html.
[43] Financial Action Task Force, *Report on New Payment Methods*, FATF Report, Paris, 13 October 2006,http://www.fatf-gafi.org/media/fatf/documents/reports/Report on New Payment Methods.pdf.
[44] Financial Action Task Force, *Money Laundering Using New Payment Methods*, FATF Report, Paris, October 2010, http://www.fatf-gafi.org/media/fatf/documents/reports/ML using New Payment Methods.pdf.
[45] Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FATF Report, Paris, June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
[46] Ibid, p. 10.

cryptocurrencies as being 'particularly vulnerable'[47] to anonymity risks because customer identification features such as name and address are not attached to a user's Bitcoin address, and because the system has no central service provider that has oversight of transactions and can be held accountable. According to the FATF's assessment, suspicious activity may therefore not only be more difficult to detect, but the source of payments may be obfuscated in contrast to traditional credit or debit cards, or payment systems such as PayPal and Western Union.

The FATF's 2014 report was published shortly after two highly-publicised law enforcement cases involving VCs made headlines. The first of these was the case of the Silk Road, an illicit marketplace operating on the Dark Web. Founded in 2011, the Silk Road acted as a marketplace for narcotics and other illicit items, and relied on Bitcoin as its primary means of payment. In 2014 US law enforcement arrested the Silk Road's founder and seized the website and associated Bitcoin.[48] The case highlighted the ability of new decentralised technologies to enable the flourishing of a new variety of illicit marketplace.

The second case related to Liberty Reserve, a centralised VC platform subject to US law enforcement action in 2013. Liberty Reserve was a Costa Rica-based online money remittance service that used its own VC, known as Liberty Dollars, to settle transactions among users, who could retain their anonymity on the platform. Liberty Road was itself a criminal enterprise that facilitated transactions by illicit actors including fraudsters, cybercriminals and narcotics traffickers. According to the US government, Liberty Reserve facilitated as much as USD 8 billion in illicit transactions.[49] The case demonstrated how a centralised VC platform could be exploited – or even designed – to conceal transactions among criminals on a large scale.

In June 2015, the FATF provided a more detailed report, *Guidance for a Risk-Based Approach: Virtual Currencies*[50], which offers practical guidance for countries on how to manage the money laundering and TF risks associated with VCs. It includes two general principles of note.

First, it suggests that a risk-based approach (RBA) to the management of VCs is possible, and that by assessing the risks associated with VCs countries can apply the FATF Recommendations to mitigate those risks.

Second, it suggests that the risks of VCs are highest where they are convertible for other units of value, and that the focus of countries' risk-based AML/CFT measures should be on points of intersection, or gateways, between VC networks and fiat currency. This recommendation was suggested on the basis that criminals will generally seek to 'cash out' from VCs to fiat currencies, and that points of exchange between VCs and fiat currency therefore present the greatest need for transparency and oversight among participants in VC ecosystems. As Chapter 4 of this study describes, these principles are reflected in the approach to regulation of VC service providers that the EU and other jurisdictions have adopted since the FATF issued its guidance in 2015.

[47] Ibid, p. 9.
[48] Greenberg, Andy, 'End of the Silk Road : FBI Says It's Busted the Web's Biggest Anonymous Druge Market,' *Forbes*, 2 October 2013, https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/ - 1190f0dc5b4f.
[49] United States Department of Justice, 'Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of Dollars,' Justice News, 6 May 2016, https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars.
[50] Financial Action Task Force, *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF Guidance, Paris, June 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

The FATF has also aimed to understand the potential scale and nature of TF-specific risks related to VCs. Its *Emerging Terrorist Financing Risks* report, published in 2015, notes that LEAs are increasingly concerned about the use of VCs by terrorist organisations, with evidence of websites connected to terrorist organisations seeking Bitcoin donations or providing instructions of how to purchase weapons using Bitcoin. [51] A January 2018 report by the FATF on TF for recruitment purposes highlights an instance in which an ISIS propaganda website, whose owner is unidentified, was used to solicit donations in Bitcoin, some of which was used to pay for the site's web-hosting services.[52] Some similar cases are examined in Chapter 3. However, the FATF's reports do not suggest that its membership has identified widespread use of VCs in TF, but rather see it as an emerging TF issue.

Recently, the FATF has broadened its efforts to assess and promote the management of the risks of new financial technology (FinTech) writ large. During 2017 and 2018, it engaged the FinTech and regulatory technology (RegTech) sectors through its FinTech and RegTech Initiative.[53] The FATF makes clear that it endorses responsible financial innovation, including involving VCs, that is aligned with the FATF standards. It is also interested in understanding the potential of new RegTech innovations to improve the implementation of AML/CFT measures. Related to this latter goal, of significant interest is the potential for the forensic analysis of cryptocurrency 'blockchains' to improve the intelligence picture of financial crime – a topic this paper explores in further detail in Chapters 3 and 5.

At its Plenary meeting in February 2018, and amid a substantial growth in the value and usage of cryptocurrencies over the previous year, the FATF announced it would review its earlier guidance on VCs.[54] This announcement recognises that in the three short years since the FATF had released its guidance, VCs, and particularly cryptocurrencies, have evolved with incredible speed. New innovations such as ICOs and various experiments in the use of DLT have expanded the understanding about the range of applications that VCs have inspired.

As of this study's publication date, the shape or scope any further FATF guidance might take remains unclear; however, the FATF continues to regard management of the money laundering and TF risks from VCs as an international policy priority. At the March 2018 meeting of the G20, finance ministers reinforced this view by committing to pursuing global implementation of the FATF's guidance on VCs.

2.1.3. The EU Response

With the FATF's approach in mind, the EU has set out to support these efforts.

VCs were first addressed at the EU level in detail when the European Central Bank (ECB) published a report on VCs in October 2012.[55] Responding to the emergence of Bitcoin, the ECB stated that the degrees of anonymity afforded by VCs can present TF risks. It suggests that whilst regulation of VC service providers would not offer a full remedy to these risks,

[51] Financial Action Task Force, *Emerging Terrorist Finance Risks*, FATF Report, October 2015, p.36, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.
[52] Financial Action Task Force, *Financing of Terrorism for Recruitment Purposes*, FATF Report, January 2018, p.20, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.
[53] Financial Action Task Force, 'FATF FinTech and RegTech Initiative,' website of the FATF, http://www.fatf-gafi.org/fintech-regtech/?hf=10&b=0&s=desc(fatf_releasedate).
[54] Financial Action Task Force, *FATF Report to G20 Finance Ministers and Central Bank Governors*, Paris, March 2018; see http://www.fatf-gafi.org/media/fatf/documents/FATF-G20-FM-CBG-March-2018.pdf.
[55] European Central Bank *Virtual Currency Schemes*, Frankfurt, October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

regulation 'would at least reduce the incentive for terrorists, criminals and money launderers to make use of these [VC] schemes for illegal purposes.'[56]

In December 2013, the European Banking Authority (EBA) issued a consumer warning on VCs, highlighting that the potential for VCs to be used in criminality could place consumer funds at risk of law enforcement action.[57] In July 2014, the EBA issued a formal opinion on VCs, which states that VCs present high risks to the financial integrity of the EU due to potential for money laundering and TF. To mitigate these risks, the EBA recommended that VC exchanges be brought within the scope of the EU's AMLDs.[58]

Some Member States took the early initiative to understand the risks around VCs and to identify appropriate policy responses. In June 2014, France published the findings of a VC Working Group it had formed the previous year. The report echoes the EBA's call to establish a regulatory framework for managing the related financial crime risks.[59]

Similarly, in March 2015, the UK published the results of a public consultation on VCs.[60] It indicates that the UK seeks 'to support the research, development and application of new technology, to promote competition and innovation in payment systems,' but also 'to limit any opportunities for criminals or terrorists'.[61] (A listing of relevant FATF and EU guidance, regulatory instruments and Member State assessments related to VCs appears in Annex I.)

In November 2015, shortly after the FATF issued its guidance, the Islamic State of Iraq and Syria (ISIS) carried out a terrorist attack in Paris.[62] In February 2016, the European Commission responded by declaring its intention to amend the earlier Fourth AMLD to address a range of TF risks.[63] (These amendments are referred to collectively as 5AMLD.) In its February 2016 statement, the Commission indicated it would include in 5AMLD measures to address the risks posed by VCs, consistent with the FATF's guidance and the EBA's earlier recommendations. The Commission put these suggestions forward in a formal draft proposal in July 2016. In December 2017, the Parliament and the Council agreed the compromise text of 5AMLD, which reflects the Commission's original aims as set out in its February 2016

[56] Ibid., p. 27.
[57] European Banking Authority 'Warning to Consumers on Cryptocurrencies,' 12 December 2013, https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf.
[58] European Banking Authority, *EBA Opinion on Virtual Currencies*, *4 July 2014,* *https*://www.eba.europa.eu/ documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.
[59] Ministere des Finances et des Comptes Publics, *Regulating Virtual Currencies: Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering*, Virtual Currencies Working Group Report, June 2014, https://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf.
[60] HM Treasury, *Digital currencies : response to the call for information*, London, March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf.
[61] Ibid, p. 3.
[62] Shortly after the Paris attacks, press reports surfaced suggesting that the perpetrators purchased weapons from the Dark Web, which some observers have inferred to suggest Bitcoin may have been involved in the procurement of weapons in the attack. We note, however, that other reports have challenged these allegations as unsubstantiated and suggest that certain facts may have been misreported. EU law enforcement and intelligence agencies have not publicly confirmed reports that the Paris attackers purchased firearms on the Dark Web or otherwise provided any public indication VCs played a role in the Paris attacks. Our research has not identified any further evidence to suggest they may have played such a role. Consequently, we regard the suggestion that VCs played a role in those attacks as unconfirmed. A further general discussion of the Dark Web, the role VCs play in Dark Web markets and the implications for TF appears in Chapter 3.
[63] European Commission, *Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight against Terrorist Financing*, Strasbourg, 2 February 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1455113825366&uri=CELEX:52016DC0050.

statement. On 19 April 2018, Parliament adopted 5AMLD by a vote of 574 to 13,[64] and on 14 May 2018 the Council of the EU adopted 5AMLD as well.[65]

It is important to note that the inclusion of VCs in 5AMLD was not in response to actual indication of their use in Europe for TF purposes, but rather general concern about the potential for TF risks to emerge. In its January 2016 report, *Changes in the modus operandi of Islamic State terrorist attacks*, Europol indicates that, 'Despite third party reporting suggesting the use of anonymous currencies like Bitcoin by terrorists to finance their activities, this has not been confirmed by law enforcement.'[66]

More recently, the European Commission's *Supra-National Risk Assessment* (SNRA) published in June 2017[67] finds that VCs pose a 'significant risk' because they are not yet regulated in the EU. However, in describing the level of threat, the SNRA noted that whilst VCs have gained in general popularity, evidence of their expansion amongst terrorist organisations has not matched the pace of adoption amongst cybercriminals, with known cases of TF involving VCs remaining low.[68]

Nonetheless, the Commission included VCs in 5AMLD out of a perceived need to ensure TF risks associated with VCs do not grow. The preamble to 5AMLD notes that because VC exchange platforms and custodial wallet providers have not been regulated to date, they have been 'under no Union obligation to identify suspicious activity. Therefore, terrorist groups may be able to transfer money into the Union financial system or within virtual currency networks by concealing transfers or benefiting from a certain degree of anonymity on those platforms.'[69] The Commission therefore regarded it as appropriate to require that Member States regulate VC service providers. Chapter 4 of this report considers the implications of 5AMLD in detail.

Like the FATF, the EU's aims to promote responsible innovation whilst managing risks. In discussing the need to regulate VCs, 5AMLD's preamble highlights the importance of a 'balanced and proportional approach, safeguarding technical advances . . . in the field of alternative finance and social entrepreneurship.'[70] The European Parliament's May 2016 resolution on VCs notes that the DLT underpinning cryptocurrencies is set to have a 'transformational capacity not only in the area of VCs but in fintech more broadly speaking, where clearing and settlement might be one obvious application, as well as others beyond finance, especially with regard to proof of identity and property.''[71] The resolution stresses

[64] European Parliament, 'Anti-money laundering : MEPs vote to shed light on the true owners of companies,' press release,' 19 April 2018, http://www.europarl.europa.eu/news/en/press-room/20180411IPR01527/anti-money-laundering-meps-vote-to-shed-light-on-the-true-owners-of-companies.

[65] Council of the EU, 'Money laundering and terrorist financing: new rules adopted,' press release, 14 May 2018, http://www.consilium.europa.eu/en/press/press-releases/2018/05/14/money-laundering-and-terrorist-financing-new-rules-adopted/.

[66] Europol, *Changes in the modus operandi of Islamic State terrorist attacks,* Europol, The Hague*, January 2016,* p. 7.

[67] European Commission, Report from the Commission to the European Parliament and to the Council on the as - sessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Brussels, 26 June 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0241.

[68] Ibid., p. 87.

[69] Position of the European Parliament adopted at first reading on 19 April 2018 with a view to the adoption of Directive (EU) …/… of the European Parliament and of the Council 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*, Recital 8.

[70] Ibid.

[71] European Parliament Resolution on Virtual Currencies, 26 May 2016, http://www.europarl.europa.eu/ sides /getDoc .do? type=TA&reference=P8-TA-2016-0228&language=EN&ring=A8-2016-0168

the importance of having in place a regulatory framework that is both risk-based and innovation-friendly.

In February 2018, the EU signalled its formal intent to pursue innovation through the development of DLT when it announced the EU Blockchain Observatory and Forum, with the aim of providing for an EU-wide approach to assessing and testing the potential for DLT in a range of applications.[72] In March 2018 the Commission announced a broader FinTech Action Plan, with the goal of making EU a global leader in FinTech services.[73] In a letter to G20 Ministers that same month, the French and German finance ministers note their countries' interest in pursuing 'sustainable innovation' though DLT and related developments.[74]

However, in the same letter, France and Germany stress that preventing the use of VCs in criminal activity 'will require a coordinated international effort' and 'a common approach in the field of anti-money laundering and counter-terrorism financing.'[75]

As Chapter 4 will show, in the nearly three years since the FATF issued its guidance, many jurisdictions have yet to bring regulation to the VC sector. This incoherent and uncoordinated landscape threatens to undermine the FATF's efforts to establish a coherent international AML/CFT approach – a substantial problem when dealing with technologies with global, borderless reach.

[72] European Commission, 'European Commission launches the EU Blockchain Observatory and Forum,' press release, 1 February 2018, https://ec.europa.eu/digital-single-market/en/news/european-commission-launches-eu-blockchain-observatory-and-forum.
[73] European Commission, 'FinTech: Commission takes action for a more competitive and innovative financial market,' press release, 8 March 2018, http://europa.eu/rapid/press-release_IP-18-1403_en.htm.
[74] Letter from France and Germany to the G20 Ministers.
[75] Ibid.

3. ASSESSING THE TERRORIST FINANCING RISKS OF VIRTUAL CURRENCIES

KEY FINDINGS

- A small number of cases suggest some jihadist and right-wing extremists are utilising cryptocurrencies. They are likely attracted by cryptocurrencies' perceived anonymity and P2P, decentralised nature.
- However, VCs currently do not provide substantial benefits for a wide range of terrorist and extremist actors over other established TF methods.
- In practice, Bitcoin is not truly anonymous, and cryptocurrency networks feature centralised 'chokepoints' in the form of exchanges. As such, the utility of VCs to terrorists is presently limited, but further technological innovations could change this.
- The most significant near-term risks relate to the potential for VCs to be used in paying for illicit items on the Dark Web, raising funds through online crowdfunding efforts and moving funds internationally using P2P transfers.
- Longer-term risks include the prospect of the convergence of terrorism with cybercrime, or terrorist actors exploiting advanced VC-related applications.

3.1. TF Risks in Context

As noted in Chapter 1, the use of VCs in cybercrime and in money laundering typologies is well-documented. However, VCs feature in only a small number of confirmed cases of TF.

If other illicit actors use VCs at a significant scale, why is the same not true of terrorists?

Press reporting, and much academic study, often describes the prospects of terrorist use of VCs in generic terms. However, terrorist actors are complex, representing a wide range of ideologies, motivations, capabilities, tactics and behaviours. They also vary widely in structure. Examples of the range of terrorist actors include:

- **lone actors**, who are generally inspired by, but may lack formal connections to, a central terrorist group;
- **small-cells and facilitation networks**, which may be either inspired by, or connected to, a main group;
- **command and control organisations** without a single established base (such as Al-Qaeda); and
- **territory controlling groups** (such as ISIS or Al-Shabaab).

With respect to methods of TF, these can take several forms, including:

- **raising** funds, for example through donations, or through criminal activity;
- **moving** funds, for example by transferring funds through banks from Europe to countries near theatres of combat, or simply by carrying cash; and
- **storing** funds, for example by maintaining reserves of cash that can later be spent on attacks, military operations, travel or other facilitation activity.

Considering these nuances, it is important to ask how various terrorist actors may seek to exploit VCs for specific purposes, rather than treating them as a uniform block. For example:

- Do VCs provide specific benefits to lone or small cell actors versus other funding methods they use at present? How might this change with time?
- Are VCs a useful or necessary funding method for large groups that aim to hold territory?

With respect to lone actor and small cells, the financial resources needed to commit an attack are often quite low. For example, in the 2016 Bastille Day attack in Nice, France, the attacker only required sufficient funds to hire a truck. A British husband and wife who were convicted of planning an unsuccessful bomb plot in 2015 raised £14,000 through payday loans and the wife's salary.[76] The pre-emptive identification of such individuals by financial institutions presents an enormous challenge, if not a near impossible one.

VCs therefore may not present lone actors and small cells with substantial advantages that can already be funded simply and readily using conventional methods, such as cash or credit cards, and through self-funding. Indeed, VCs are neither a necessary nor practical way to pay for vehicle hire in Europe. The present limited opportunities for their everyday, practical use may limit VCs' utility for most terrorist actors.

However, VCs may prove occasionally attractive to certain lone actors and small cells operating online. In June 2015, a Virginia teenager, Ali Shukri Amin, was convicted in the US of providing material support to ISIS over social media.[77] Amin admitted to using Twitter to advise others on how Bitcoin could be used to mask the provision of funds in support of ISIS. Whilst Amin does not appear to have been successful in raising Bitcoin for ISIS, his case provides a warning: he is reflective of a younger demographic of jihadis who have grown up with the Internet and may be comfortable using new financial technologies.

When it comes to funding the ongoing operations of larger groups, such as al-Qaeda and ISIS, VCs are unlikely to be necessary or useful to them for many of their ongoing operations. ISIS's financing of its activities in Syria and Iraq, for example, has drawn primarily from the enforced taxation of individuals and businesses under its control.[78] What's more, the present characteristics of many VCs – especially volatility and challenges of usability – would likely make them unreliable methods of transferring or moving funds in meaningful volumes. In February 2018, terrorism analyst Michael S. Smith II of the US national security consultancy Kronos Advisory, noted that that the al-Qaeda online publication al-Haqiqa featured an article on the uses of Bitcoin, including discussion of whether Bitcoin is allowed by sharia law and concluding that, 'We see lots of possibilities for the use of cryptocurrencies for our purposes, but we also see lots of obstacles.'[79]

Rather than looking to VCs as methods of ongoing, sustained finance, terrorist groups may therefore find greater utility in them for occasional and ad hoc international P2P transfers among members of a group as a method of moving funds, or for use in targeted crowdfunding campaigns designed to raise funds online. Terrorist crowdfunding efforts may be used for a wide variety of purposes, such as procuring weapons, facilitating travel, paying for

[76] Barret, David and Whitehead, Tom, 'Middle Class Daughter of Magistrate Who Turned to Suicide Bomb Plotter', *The Telegraph*, 20 December 2015; Bowcott, Owen, 'Couple Found Guilty of 7/7 Anniversary London Bomb Plot', *The Guardia*n, 29 December 2015.
[77] United States Department of Justice, 'Virginia Teen Pleads Guilty to Providing Material Support to ISIS,' Justice News, 11 June, 2015, https://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil.
[78] Geneva Centre for Security Policy, 'GCSP Discusses ISIS Funding with CNN Money,' 11 December 2015, https://www.gcsp.ch/News-Knowledge/Global-insight/GCSP-discusses-ISIS-funding-with-CNN-Money.
[79] See: https://twitter.com/MichaelSSmithII/status/959293289823285248

propaganda campaigns or procuring everyday supplies and services. They often operate under a pretext of soliciting donations for humanitarian activity or other noble cause.

Yaya Fanusie of the Foundation for Defence of Democracies suggests jihadist facilitation networks are innovating their financing methods by soliciting cryptocurrencies to raise funds, if only thus far in experimental fashion. Fanusie identified a campaign of this sort in July 2016 run by the Ibn Taymiyya Media Center (ITMC), which is the online media unit of the Mujahideen Shura Council in the Environs of Jerusalem (MSC), a network of Salafi-jihadist groups in the Gaza strip.[80] The US State Department has designated the MSC as a foreign terrorist organisation for targeting Israel and pledging support to the Islamic State.[81] Through its online campaign 'Jahezona' meaning 'equip us' in Arabic, ITMC added an option to donate funds in Bitcoin, posting detailed instructions online in the use of the technology. At the time this activity was identified, only two transactions had been made to the related Bitcoin address, totalling approximately 0.929 Bitcoin, or approximately USD 540, at the time. However, as of March 2018, the associated Bitcoin address had received approximately 1.46 Bitcoin, which, owing to the significant rise in Bitcoin's price, totalled approximately USD 8,000.[82]

The examples above relate to religiously-motivated, and specifically jihadist, activity; but political extremist activity also warrants consideration. Evidence suggests growing political extremist activity across Europe and the US. A study by the Royal United Services Institute in 2016 on *Countering Lone Actor Terrorism*[83] indicates that 33 % of plots between 2000-2014 involved right-wing extremists. Europol's most recent *EU Terrorism Situation and Trend Report (TE-SAT) (*2017*)*[84] indicates an increasing stream of violent assaults from right-wing extremists against asylum seekers and ethnic minorities. Of course, certain political extremist activity, such as the dissemination of propaganda, may not always fall within the EU's definition of 'terrorism', which includes activity such as seriously intimidating a population and seriously destabilising or destroying political, economic and social structures.[85] Nonetheless, examining broad patterns of extremist use of VCs can assist in understanding how VCs could be used by those extremists who do engage in terrorism.

VCs may appeal to certain political extremist actors for both ideological and practical reasons. The adoption of cryptocurrencies by the far-right is underpinned by an ideology of deep-rooted mistrust of institutions. Cybersecurity expert John Bambenek has observed that far-right extremists active online have used Bitcoin, a phenomenon underpinned by an ideology of deep-rooted mistrust of financial institutions. Indeed, Richard Spencer, the American white

[80]Fanusie, Yaya, 'The New Frontier in Terrorist Financing,' *The Cipher Brief*, 24 August 2016, https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin.
[81] US Department of State, 'Terrorist Designation of the Mujahidin Shura Council in the Environs of Jerusalem (MSC),'US Department of State website, Terrorism Designations Press Releases 19 August 2014, https://www.state.gov/j/ct/rls/other/des/266549.htm.
[82] Analysis of the Bitcoin blockchain suggest the Jahezona address is associated with 14 other Bitcoin addresses that had received a total of approximately 10.4 Bitcoin (or approximately USD 80,000) as of March 2018. The purpose of these related transfers is unclear, but the relationship between these addresses suggests they are controlled by the same entity used in the Jahezona campaign. (This data was provided to the authors of the study by the blockchain intelligence firm Elliptic).
[83] Ellis, Claire, et. al, *Countering Lone Actor Terrorism Series No. 11: Lone Actor Terrorism, Final Report*, Royal United Services Institute, London, April 2016, https://rusi.org/sites/default/files/201604_clat_final_report.pdf.
[84] Europol, *EU Terrorism Situation and Trend Report (TE-SAT)*, The Hague, 2017, https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.
[85] European Parliamentary Research Service, 'Understanding Definitions of Terrorism,' November 2015, http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/571320/EPRS_ATA(2015)571320_EN.pdf.

supremacist, has claimed that Bitcoin is the 'currency of the alt-right.'[86] Bambenek suggests that for the far-right cryptocurrencies are a 'political statement', closely connected to the belief that financial institutions are part of a global Jewish conspiracy. According to Julia Ebner, a researcher at the Institute for Strategic Dialogue, Bitcoin's libertarian origins appeal to neo-Nazis with anti-establishment beliefs.[87] According to research by the Southern Poverty Law Center (SPLC) in the US, Andrew Anglin, editor of the *Daily Stormer*[88] received 14.88 Bitcoin (which at the time was worth USD 60,000). In an interview with the Washington Post, Anglin confirmed that he uses Bitcoin 'almost exclusively' and has stated that it has 'helped us out a lot.'[89]

The far-right's adoption of Bitcoin is not only an ideological matter, but a practical one. Having lost access to popular crowdfunding sites such as Patreon, alt-right extremists have developed a website, Hatreon, for fundraising, including using cryptocurrencies.[90] Such sites remain resilient to efforts to force them off web-hosting services and other platforms, often reappearing shortly after being dismantled.[91] The SPLC has reported a notable increase of VCs across the far-right movement in the US to compensate for their loss of access to services such as PayPal, which have in some cases banned right-wing extremists from their services.[92] This suggests some extremist actors may see cryptocurrencies as a useful workaround where they lack access to the formal financial system.

At present, open-source reporting does not indicate the uptake of VCs by left-wing extremists. Nonetheless, the potential for a broader range of extremist actors to adopt VCs on both an ideological and practical basis should not be overlooked.

3.2. TF Risk Features of VCs

The examples noted above indicate limited overall uptake of VCs by terrorist actors but suggest that terrorists and a broader range of extremist actors may find certain features of VCs useful for select purposes. The following sections consider those risk features of VCs that influence the current TF picture, examines several more cases of their use and assesses how this picture could evolve.

3.2.1. Anonymity and Pseudonymity

Media reports frequently describe Bitcoin as 'anonymous' and 'untraceable' but this is oversimplified and inaccurate. Bitcoin is more appropriately described as 'pseudonymous': Bitcoin users are represented on the blockchain with alphanumeric addresses associated with their Bitcoin wallet. Whilst a user's actual identity is not visible on the blockchain, information about their transactions – such as dates, values, and the Bitcoin addresses of counterparties – are all recorded publicly. Furthermore, because the blockchain is a chronological record of transactions, it is possible to derive a reliable picture of the movement of Bitcoin.

[86] Pearson, Jordan, 'Can the Bitcoin Community Stop Neo-Nazis From Using the Digital Currency?' *Vice*, 18 August 2017, https://motherboard.vice.com/en_us/article/vbbb5y/can-the-bitcoin-community-stop-neo-nazis-from-using-the-digital-currency.
[87] Ebner, Julia, 'The currency of the far-right: why neo-Nazis love Bitcoin,' *The Guardian*, 24 January 2018, https://www.theguardian.com/commentisfree/2018/jan/24/bitcoin-currency-far-right-neo-nazis-cryptocurrencies.
[88] The Daily Stormer is a neo-Nazi online publication in the United States
[89] Timberg, Craig, 'Bitcoin's boom is a boon for extremist groups,' *Washington Post*, 26 December 2017, https://www.washingtonpost.com/business/technology/bitcoins-boom-is-a-boon-for-extremist-groups/2017/12/26/_9ca9c124-e59b-11e7-833f-155031558ff4_story.html?noredirect=on&utm_term=.ce1091ce7715.
[90] Ebner, Julia, 'The currency of the far-right: why neo-Nazis love Bitcoin.'
[91] Coledeway, Devin, 'How hate speech crowdfunding outfit Hatreon crept back online,' *TechCrunch*, 12 December 2017, https://techcrunch.com/2017/12/12/how-hate-speech-crowdfunding-outfit-hatreon-crept-back-online/.
[92] Timberg, Craig, 'Bitcoin's boom is a boon for extremist groups.'

Thus, where an individual or entity is known to be the owner of a public Bitcoin address, substantial amounts of information can be gleaned about their activity conducted within the network. A number of private firms now specialise in de-anonymising Bitcoin transactions and developing tools for analysing illicit activity in Bitcoin. These blockchain forensic companies provide solutions both to LEAs and to cryptocurrency exchanges, which can conduct analysis of customers' transactions and scrutinise them for signs of suspicion. Some of these blockchain forensic companies are developing tools for analysing transactions in alt-coins, such as Litecoin and Ethereum, which contain traceability features akin to Bitcoin.[93]

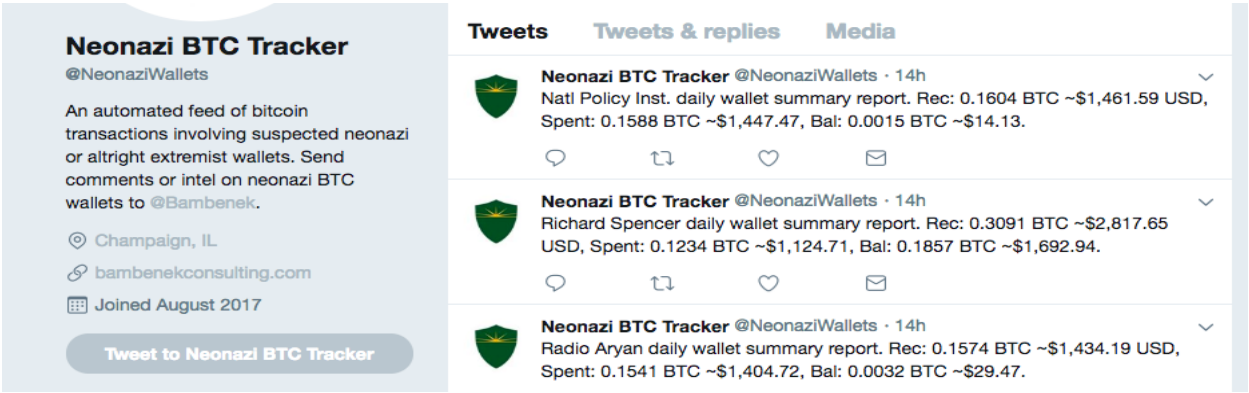
Figure 1: A Bitcoin Transaction

The above image shows a transaction on the Bitcoin blockchain. The address to the right of the green arrow is the recipient of .06 Bitcoin (or approximately USD 500 at the time it was sent). The address was used by the perpetrator of the WannaCry ransomware attack that infected hundreds of thousands of users internationally. The address to the left of the arrow is the payer's address, likely representing the payment of a ransom. **Source:** Website of Blockchain.info

Terrorist actors who have used Bitcoin may see its pseudonymity as useful. After all, posting a Bitcoin address to a social media account or public channel on a messaging platform is likely advantageous to posting bank account details online.

Ultimately, however, Bitcoin's traceability may limit its utility to terrorist actors. Indeed, as the Jahezona crowdfunding campaign indicates, security analysts have been able to monitor the movement of jihadists' Bitcoin in real-time. Similarly, John Bambenek monitors far-right Bitcoin activity through a Twitter-bot called the 'Neonazi BTC Tracker' (see figure below) that automatically tweets every transaction of thirteen Bitcoin addresses used by extremists.

Figure 2: Neonazi Bitcoin Tracker



Source: Twitter

[93] Redman, Jamie, 'Chainalysis Raises $16Mn – Plans to Monitor Multiple Blockchains,' *Bitcion*.com, 6 April 2018, https://news.bitcoin.com/chainalysis-raises-16mn-plans-to-monitor-multiple-blockchains/.

Despite Bitcoin's traceability, several methods exist for adding a layer of anonymity. One is the use of 'mixers' or 'tumblers', services that aggregate Bitcoin from many users and redistribute them, scrambling the trail of transactions to make it more difficult to decipher the flow. These include mixing services such as CoinJoin, as well as DarkWallet, a service which integrates mixing features into a user's Bitcoin wallet. Whilst certainly not all mixing activity is illegal, one recent study suggests that mixers account for a disproportionate amount of laundering of illicit Bitcoins, and that much of this illicit mixing activity takes place through a very small number of mixers.[94]

As early as July 2014, ISIS-affiliated individuals advocated the use of Bitcoin mixing technology to conceal the movement of funds. An individual identified as Taqiul-Deen al-Munthir wrote a blog post entitled 'Bitcoin and the Charity of Violent Struggle', calling for ISIS to use services such as DarkWallet. The blog states:

> 'DarkWallet's beta release will be published within the next coming months, the mujahideen Dawlatul Islam would simply need to set up a wallet and post their addresses online. Then, Muslims from across the globe could simply copy the wallet address, login to their [wallets], purchase whatever amount of bitcoin they wish to send, and send them over'. [95]

This study did not identify any confirmed cases of terrorists using Bitcoin mixers. But the above quote, whilst from a lone blog post and not necessarily indicative of ISIS's broader strategic intent, at least reveals that some jihadists aspire for access to anonymous online financial transfers.

Recent years have seen substantial innovation in the use of new privacy-focused alt-coins that feature greater anonymity than Bitcoin. Whilst they operate using open-source, public blockchains, like Bitcoin, the same set of identifying details are not visible. Examples of these privacy-focused alt-coins include:

- **Monero:** Created in 2014, Monero does not provide visible indication of the sender, recipient or value of transactions on its blockchain. It utilises 'stealth addresses', or new addresses generated for one-time use to ensure only a sender and recipient have access to transaction details; it also employs a form of cryptography known as 'ring signatures', which enable for the signing of transactions among a group of users so that outside observers cannot decipher the individual signer of a transaction.
- **Dash:** Also created in 2014, Dash utilises a variation of CoinJoin mixing known as 'PrivateSend' to reduce the traceability of coins on its blockchain. Unlike Monero, Dash does not integrate these features as a default feature of its protocol, but rather as an added feature.
- **Zcash:** Released in 2016, Zcash derives its name from an advanced and innovative form of cryptography known as 'zero-knowledge proof', which enables parties to reach consensus about the validity of information whilst keeping that information encrypted. This ensures the legitimacy of transactions in the Zcash network whilst allowing the identity of counterparties to remain shielded. Unlike Monero, where the shielding of addresses is enforced, in Zcash anonymity is optional. Zcash transactions may be fully transparent (i.e. both sender and

[94] Fanusie, Yaya J. and Robinson, Tom, *Bitcoin Laundering : An Analysis of Illicit Flows into Digital Currency Services*, Foundation for Defense of Democracies and Elliptic, 12 January 2018, p. 7, http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf.
[95] Higgins, Stan, 'ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide,' *CoinDesk*, 7 July 2014, https://www.coindesk.com/isis-bitcoin-donations-fund-jihadist-movements/.

recipient addresses and transaction details are visible on the Zcash blockchain), partially shielded (i.e. one party's address is visible on the blockchain whilst the other's is shielded) or fully shielded (i.e. information about the parties and their transaction details is not visible on the blockchain).[96]

Advocates of privacy coins point to Bitcoin's traceability as a flaw. They argue that Bitcoin users are not afforded sufficient confidentiality, an essential component of many commercial interactions, making users vulnerable to hacking, theft or other intrusions on their financial activity. Privacy coin advocates also note that Bitcoin's traceability limits its fungibility; that is, the ability to see that a Bitcoin intersected with an illicit actor (i.e. a Dark Web market place) potentially devalues it permanently, even after it has passed to a legitimate user.[97]

One discussed use case for privacy-focused alt-coins and their encryption solutions is in 'enterprise blockchain' functions, or efforts by businesses to develop DLT solutions. Large corporations, because of their need to maintain confidentiality, are generally hesitant to experiment with those DLT solutions that enable ready traceability. As such, some have looked to the technologies underpinning privacy coins for use in commercial applications. In 2017, investment bank JP Morgan announced the development of Quorum, a DLT platform that uses the zero-knowledge proof techniques employed in Zcash, to allow a degree of confidentiality in transactions, whilst also enabling transactions to be auditable.[98]

Several recent studies suggest privacy coins are gaining traction among criminals. Europol, in its October 2017 IOCTA, indicates that it has seen evidence of criminals utilising privacy-focused alt-coins, particularly Monero, more frequently,[99] One US academic study estimates that approximately 25 % of all Monero activity as illicit.[100] A highly-visible instance of criminal usage of Monero occurred in August 2017, when the perpetrators of the WannaCry ransomware attack, which has been attributed to North Korea, exchanged their illicit Bitcoin for Monero through the ShapeShift cryptocurrency exchange based in Switzerland.[101] Monero has also featured recently in a growing number of crypto-jacking campaigns.[102]

The utility of privacy-focused cryptocurrencies has become apparent to some extremist and terrorist actors, if on a far less substantial scale. Julia Ebner indicates that far-right extremists are expanding their use of Monero to overcome Bitcoin's traceability features[103]; however, John Bambanek's research suggests that far-right users of Monero are generally unable to convert it to fiat currency and may therefore use it primarily as a method of storage.[104]

---

[96] 'What are zkSNARKS? Zero Knowledge Proofs Simplified,' *Investing.com*, 6 April 2016, https://www.investing.com/news/cryptocurrency-news/what-are-zksnarks-zero-knowledge-proofs-simplified-1382453.

[97] Vorick, David, 'Ensuring Bitcoin Fungibility in 2017 (And Beyond),' *CoinDesk*, 28 December 2017, https://www.coindesk.com/ensuring-bitcoin-fungibility-in-2017-and-beyond/.

[98] Del Castillo, Michael 'JP Morgan Integrates Zcash Tech Into Quorum Blockchain,' CoinDesk, 17 October 2017, https://www.coindesk.com/jpmorgan-integrates-zcash-privacy-tech-enterprise-blockchain/.

[99] Europol, *Internet Organised Threat Assessment (IOCTA 2017),* 2017, p. 13.

[100] Möser, Malte; Soska, Kyle; Hellman, Ethan; Lee, Kevin; Heffan, Henry; Srivastava, Shastvat; Hogan, Kyle; Hennessey, Jason; Miller, Andrew; Narayanan, Arvind; and Christin, Nicolas, 'An Empirical Analysis of Traceability in the Monero Blockchain,' to appear in Privacy Enhancing Technologies Symposium (PETS), 2017, p. 1, https://arxiv.org/pdf/1704.04299.pdf.

[101] Suberg, William, 'Bitcoin Exchange ShapeShift Helps Police as WannaCry Attacker Converts to Monero,' CoinTelegraph, 4 August 2017, https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero.

[102] Osborne, Charlie, 'PyCryptoMiner enslaves your PC to mine Monero,' *ZDNe*t, 4 January 2018, https://www.zdnet.com/article/pycryptominer-enslaves-your-pc-to-mine-monero/.

[103] Ibid.

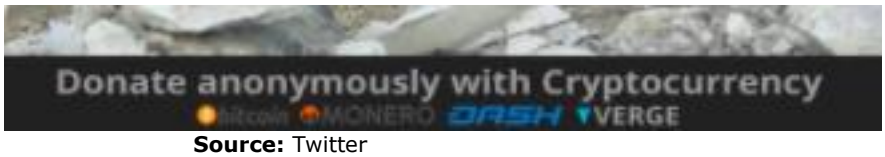
[104] Author interview with John Bambenek.

Evidence has also emerged of a jihadist campaign soliciting donations in privacy coins. The al-Sadaqah Organisation, which describes itself as a charity, conducted a crowdfunding campaign towards the end of 2017 across al-Qaeda-linked social media channels and Telegram. The campaign initially requested that supporters 'donate anonymously and securely with bitcoin'[105] to fund a project to build facilities at a location in Latakia province in Syria. On 30 November 2017, the al-Sadaqah address was sent 0.075 Bitcoin, worth USD 685; the next day, the funds were transferred to another address, with an increased value of USD 803, reflecting Bitcoin's rapid price increase.[106] Having been subject to public scrutiny, the campaign now appears to be experimenting with the use of more highly-anonymised coins: the organisation's Twitter account indicates it now accepts the privacy-focused alt-coins Monero, Dash and Verge. As recently as 1 April 2018, al-Sadaqah has solicited donations via Twitter, calling on followers to 'support the Mujihideen in Syria with your wealth 100% anonymous and completely untraceable'.[107]

Figure 3: **Al-Sadaqah Twitter Account Requesting Donations in Bitcoin and Monero**

Source: Twitter

Figure 4: **Image from Al-Sadaqah Twitter Account Requesting Alt-Coins**



Source: Twitter

It is difficult to draw firm conclusions about the overall volume of illicit activity, including TF, that may be occurring using privacy-focused coins. There is also substantial debate as to how much genuine anonymity privacy-focused alt-coins afford users at present and how impervious they or other cryptocurrencies may remain to de-anonymisation. Academics in the US recently demonstrated that Monero transactions can be deciphered with greater

[105] Fanusie, Yaya, 'Terrorist Networks Eye Bitcoin as Cryptocurrency's Price Rises, *The Cipher Brief*, 21 December 2017, https://www.thecipherbrief.com/terrorist-networks-eye-bitcoin-cryptocurrencys-price-rises.
[106] Ibid.
[107] Twitter.

accuracy than had previously been assumed.[108] Privacy coins remain difficult to access and lack liquidity, as few regulated cryptocurrency exchanges offer them to users; what's more, in those cases where regulated exchanges offer them and do provide liquidity, some of the benefits of anonymity may be lost, as Know Your Customer (KYC)/CDD measures are required on users. Purchasing or selling certain alt-coins in exchange for fiat currency frequently requires first obtaining Bitcoin and then exchanging it again. This reliance on Bitcoin can ultimately reduce some of the benefits of anonymity along the transaction trail.

Nonetheless, these highly-anonymous coins are growing in number and availability, and they present LEAs with substantial challenges in detection relative to Bitcoin. Furthermore, as discussed in Chapter 4, the EU's 5AMLD applies only to those VC exchange platforms that exchange cryptocurrency for fiat currency and does not explicitly cover the exchange of one cryptocurrency for another – a fact that may make it easier for users to undertake the conversion of Bitcoin for privacy coins without KYC or other measures being applied at the point of exchange.

In addition to incorporating anonymity features directly, VCs also present TF risks when used with other anonymising technologies, such as the Dark Web. The Dark Web is a subset of the Deep Web[109] and is a collection of thousands of websites that use services such as the Tor protocol to conceal IP addresses and encrypt communications.[110] Payments on the Dark Web rely largely on cryptocurrencies. Bitcoin still predominates, but alt-coins such as Monero feature as well. Before it was taken down by Dutch law enforcement, the Dark Web market Alphabay had adopted Monero to enable payments for illicit goods and services.[111]

In January 2015, *Haaretz* reported that independent cybersecurity analysts identified an ISIS supporter, Abu Mustafa, who ran a fundraising page on the Dark Web and raised approximately USD 1,000 worth of donations[112], although another researcher notes that the association of this individual with ISIS has not been confirmed.[113]

The Dark Web also offers prospects for procurement of items that are of use to terrorist actors. They have also become hidden spaces for the distribution of prohibited content such as extremist material.[114] A 2016 report by Belgium's FIU indicates that VCs are increasingly used for payments on illicit trade platforms hidden on the Dark Web, for example for the purchase of fake documents and airline tickets[115] – goods and services that lone actor or small cell networks may find useful to travel abroad or commit attacks.

[108] Malte Möser, et. al.
[109] The 'Deep Web' is not to be confused with the 'Dark Web'. The Deep Web is merely part of the Internet that is not accessible via search engines, meaning that you won't be able to access websites through Google or Yahoo. However, to all intents and purposes they are normal websites.
[110]Greenberg, Andy, 'Hacker Lexicon: What's the Dark Web?' *Wired,* 19 November 2014, https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.
[111] Torpey, Kyle, 'AlphaBay Comments on Bitcoin Congestion, Monero Adoption and Zcash Possibilities,' Bitcoin Magazine, 21 December 2016, https://bitcoinmagazine.com/articles/alphabay-comments-on-bitcoin-congestion-monero-adoption-and-zcash-possibilities-1482345512/.
[112] Harman, Danna, 'U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests,' *Haaretz*, 29 January 2015, https://www.haaretz.com/.premium-isis-uses-bitcoin-for-fundraising-1.5366305.
[113] Cox, Joseph, 'Is the Islamic State Using Bitcoin? That's the Last Thing We Should Worry About,' *Vice*, 25 February 2015, https://motherboard.vice.com/en_us/article/z4m8ee/is-the-islamic-state-using-bitcoin-thats-the-last-thing-we-should-worry-about.
[114] For a taxonomy of high-level categories of activity over the Dark Web, see Moore, Daniel and Rid, Thomas, Cryptopolitik and the Darknet, *Survival*, 58:1, pp. 7 – 38, February-March 2016, https:// www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085?needAccess=true.
[115] CTIF-CFI, *23rd Annual Report*, Belgian Financial Intelligence Processing Unit (CTIF-CFI), 2016, p.41, http://www.ctif-cfi.be/website/images/EN/annual_report/ar2016en.pdf.

A determined lone actor or small cell might also find the Dark Web a useful venue to purchase firearms. The UK's *National Risk Assessment of Money Laundering and Terrorist Financing 2017*, notes the potential of VCs to buy and sell goods such as firearms, although it admits that there is no evidence of this occurring at present in the UK. [116] However, a 2018 report by the Flemish Peace Institute notes that the use of the Internet to obtain firearms from the Dark Web is a real possibility, and according to Belgium's Federal Prosecutor's Office, is typical of lone actors owing to their not having connections in established, physical arms markets.[117]

A recent report by *The Cipher Brief* observes that for self-radicalised individuals in the West, access to a larger assortment of arms, explosive materials and related expertise is becoming more prevalent over the Dark Web.[118] Analysts for RAND conclude whilst that the scale of the Dark Web-enabled firearms trade is relatively small compared to the Dark Web marketplace for drugs, the potential impact on security is still significant. [119] The Dark Web removes historical geographical barriers that previously shaped the arms trade, enabling swift sale and purchase on opposite ends up the world in merely a few clicks.

Cases have emerged indicating the availability of firearms on the Dark Web in Europe. In 2016, a Belgian man was convicted of ordering guns from the United States, claiming he wanted to protect his family from ISIS.[120] The case of David Ali Sonboly, the 18-year-old who killed nine and injured 35 in Munich in July 2017, is also demonstrative of this vulnerability. Sonboly is believed to have bought the Glock 17 pistol used during the attack over a Dark Web marketplace, and the man accused of selling it to Sonboly has since been arrested.[121]

It is worth noting that whilst the Dark Web removes the geographical barriers in purchasing weapons and affords it does not overcome procurement barriers. Weapons must still be physically shipped, adding a layer of risk for the purchaser and a disruption opportunity for law enforcement. According to Danish Police (as noted by the Flemish Peace Institute), the trade in illegal firearms over the Dark Web is primarily conducted by gun enthusiasts who have no criminal intent, and that criminals remain risk averse to this mode of purchase.[122] Thus, whilst it is important to remain aware of the risk that the Dark Web could be used to procure firearms for terrorism purposes, its scale requires important contextualisation. As RAND's study notes, while Dark Web market places are global in nature, they are ultimately small in scale.[123]

The often-cited crime/terror nexus,[124] which entails the commission of crime by terrorists, or the interaction between terrorist and criminal groups, is a factor that could shape terrorist

[116] HM Treasury and the Home Office, *National risk assessment of money laundering and terrorist financing*, London, October 2017, pp. 40 -41, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.
[117] Duquet, Nils (ed.), *Triggering Terror: Illicit Guns Markets and Firearms Acquisition of Terrorist Networks in Europe,* Flemish Peace Institute, Brussels, 2017, p.59, http://www.flemishpeaceinstitute.eu/sites/vlaamsvredesinstituut.eu/files/wysiwyg/boek_safte_bw_lowres.pdf.
[118] Maxey, Levi, 'Terrorists Stalk the Dark Web for Deadlier Weaponry,' *The Cipher Brief*, 17 January 2018, https://www.thecipherbrief.com/terrorists-stalk-dark-web-deadlier-weaponry.
[119] Aldridge, Judith; Paoli, Giacomo Persi; Ryan, Nathan; Warnes, Richard, *Behind the curtain: the illicit trade of firearms, explosives and ammunition on the dark web*, RAND Corporation, 2017, *xiv*, https://www.rand.org/pubs/research_reports/RR2091.html.
[120] Duquet, p. 53.
[121] 'Darknet administrator arrested over Munich massacre gun,' *Sky News*,12 June 2017, https://news.sky.com/story/darknet-administrator-arrested-over-munich-massacre-gun-10913376.
[122] Duquet, p. 140.
[123]Aldridge, et. al, p. 65.
[124] See, for example, Reitano, Tuesday; Clarke, Colin; Adal, Laura, *Examining the Nexus Between Organised Crime and Terrorism*, CT Morse, 2017, https://icct.nl/wp-content/uploads/2017/04/OC-Terror-Nexus-Final.pdf.

use of the Dark Web. The nexus has historically manifested at various levels, with OCGs and terrorist actors converging for the sake of convenience, or small cells engage in petty criminality to fund attacks. Researchers at King's College London's International Centre for the Study of Radicalisation have observed how criminal and extremist 'milieus' are converging in Europe, whereby individuals with criminal backgrounds are utilising their criminal skills for terrorist purposes, not only for practical reasons, but to wage 'Jihad'.[125]

The Dark Web may remove the traditional geographical barriers that have characterised this nexus in the past; however, significant further research is required to determine the extent to which any crime/terror nexus may be shifting online. Nonetheless, the technology alone presents features and indicators of how it could do so. Terrorists may seek to use Dark Web marketplaces to obtain stolen credit card details or to engage in the sale of drugs to raise funds for their activities. The potential return of foreign fighters from Islamic State back into Europe, who will be seeking to conceal their identities, presents a real risk. Passports and false documentation are widely available on the Dark Web, which could provide a useful venue for terrorist actors to acquire them.

Figure 5: German Passports for Sale on the Dark Web

Source: International Business Times (see: https://www.ibtimes.co.uk/dark-web-vendors-sell-blank-british-passports-entry-passport-database-just-2000-1509564)

Whilst confirmed instances of terrorist actors in Europe using the Dark Web for procurement purposes have not been documented publicly, it remains an area warranting law enforcement vigilance. Due to the minimal amounts of funding required to obtain illicit items for facilitation or execute an attack using Dark Web-acquired weapons, detection and disruption of VCs if used by lone actors poses a particularly difficult challenge to LEAs. It is also probable that technological barriers that may have limited terrorist actors' use of the Dark Web in the past are eroding. Whilst a certain level of internet-literacy and technical skill is required to use the Dark Web, the complexities are likely to have decreased since the early days of the Silk Road, with 'how-to' guides easily available online for the willing Dark Web-adoptee.

However, it is important to remember that identifying lone-actor and small cell activity is a significant challenge for LEAs irrespective of the presence of VCs. The isolated use of VCs for such purposes would likely represent the extension of an already substantial law enforcement challenge, rather than an entirely new problem.

[125] Neumann, Richard and Basra, Rajan, *Crime as Jihad: Developments in the Crime-Terror Nexus in Europe*, *CTC Sentinel*, October 2017, Volume 10, Issue 9, Combatting Terrorism Center, https://ctc.usma.edu/crime-as-jihad-developments-in-the-crime-terror-nexus-in-europe/.

Messaging apps and social media are other channels through which terrorist and extremist actors can seek anonymity. In the terrorist crowdfunding campaigns identified to date, potential donors are often directed via Twitter and Facebook to encrypted messaging applications such as Telegram. The potential benefits of this approach are clear: crowdfunding campaigns allow sympathisers to 'support the cause' without having to leave the confines of their own home, and with an additional layer of anonymity around their communications.

In early 2018, reports surfaced that Telegram was considering releasing its own cryptocurrency, the Gram, for use in P2P payments on its platforms.[126] As of the date of this study's publication, reports suggest Telegram was abandoning the project; but the fact it is being discussed suggests that a future of online communications platforms with readily integrated cryptocurrency settlement options may not be far off. The proliferation of crowdfunding platforms using VCs along with encrypted messaging apps thus presents an emerging risk that should be closely monitored, even if current detected use is relatively limited.

3.2.2. P2P Cross-Border Transfer and Portability

Another feature of VCs that may hold some appeal for terrorist actors is their ability to enable value transfers internationally whilst avoiding regulated intermediaries.

As noted previously, cryptocurrencies have thus far failed to enable very rapid payments for everyday use at scale. Nonetheless, cryptocurrencies provide a relatively effective means for transferring value P2P across borders. This feature is attractive to criminals, such as ransomware attackers, who receive payments from victims located anywhere in the world without having to pass through a bank or other financial institution. A small number of anecdotal cases suggest terrorist actors may be attempting to exploit this feature to move funds.

In early 2017, Indonesia's financial intelligence unit (FIU) reported that Bahrun Naim, a jihadist who planned 2016 attacks in Jakarta, used PayPal and Bitcoin to transfer funds from the Middle East to support Indonesia-based terror cells across Java.[127] Another example is that of US citizen Zoobia Shanaz, who was indicted in December 2017 for laundering over USD 85,000 in Bitcoin and other cryptocurrencies derived from the proceeds of stolen card fraud to support ISIS militants in Iraq and Syria[128]; however, the US indictment does not describe how exactly this was done.

The widespread use of VCs to transfer funds internationally to support terrorism has not yet emerged, although it is certainly likely there have been undetected instances. The lack of a broader trend is likely attributable to the fact that in conflict zones where cash is paramount, opportunities to exchange VCs into cash are limited. As researchers for the Center for New American Security note, 'If VCs become sufficiently liquid and easily convertible … and if terrorist groups in places such as sub-Saharan Africa, Yemen, and the Horn of Africa

[126] Cutherbertson, Anthony, 'Telegram Cancels $1.7 Billion ICO Cryptocurrency Crowdfund,' *Independent*, May 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/telegram-ico-cryptocurrency-bitcoin-ton-a8334551.html.

[127] Soeriaatmadja, Wahyudi, 'Militant Bahrun Naim used PayPal, bitcoin to transfer funds for terror attacks in Indonesia,' *Straights Times*, 9 January 2017, http://www.straitstimes.com/asia/se-asia/militant-bahrun-naim-used-paypal-bitcoin-to-transfer-funds-for-terror-attacks-in.

[128] US Department of Justice, 'Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists, 14 December 2017, https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists.

obtain the kinds of technical infrastructure needed to support VC activity, then the threat may become more significant.'[129]

The potential of Bitcoin ATMs as a method of international funds movement has not been lost on the al-Sadaqah campaign, which includes on its Twitter feeds maps of Bitcoin ATMs and implores supporters to send funds using them[130] – a method that, as noted earlier, Colombian drug traffickers have employed across Europe. The Republic of Ireland's National Risk Assessment for Money Laundering and Terrorist Financing 2017 outlines growing concerns amongst Irish LEAs that Bitcoin ATMs in Dublin could be used for illicit purposes. [131]

VCs also can prove readily and easily portable, surmounting the limitations of carrying physical cash. One can carry cryptocurrencies across borders simply by carrying a paper or hardware wallet, or keeping a software wallet application on a phone, tablet or other portable device. Pre-paid cryptocurrency cards can serve a similar function, as they can be loaded with the underlying online cryptocurrency wallet and carried from place to place.

In April 2018, Spanish authorities acted against members of a cybercrime network that used Bitcoin prepaid cards to launder funds.[132] It is not outside the realm of possibility that terrorist networks could begin to adopt such methods to transfer value among members of support networks, even if no such instances have been publicly reported thus far.

The previously mentioned crime/terror nexus could also shape the nature of how such risks might emerge. Experts interviewed for this report indicated that terrorist actors often exploit established methods of moving illicit funds used by money launderers and other criminals. Insofar as there is a growing general criminal use of new platforms such as Bitcoin ATMs and cryptocurrency debit cards, the likelihood increases that terrorist actors will eventually use them too.

Thus, the use of VCs to facilitate international transfers between terrorist actors is likely an area of lower risk presently in terms of actual values and frequency, but one that could accelerate under the right conditions.

3.2.3. Decentralisation

Research conducted for this study did not identify any instances of terrorists using centralised VCs. Rather, the cases noted to date suggest terrorists are experimenting with cryptocurrencies owing to the perceived advantages of decentralisation.

Because they are open-source, decentralised applications, cryptocurrencies are often described as 'permissionless'; that is, access to them cannot be restricted. There is no single, central authority that can prevent an individual from accessing the Bitcoin network. The Bitcoin network cannot be subpoenaed, penalised or shut down in the manner of a centralised

[129] Goldman, Zachary; Maruyama, Ellie; Rosenberg, Elizabeth; Saravalle, Eduardo; Solomon-Strauss, Julia, *Terrorist Use of Virtual Currencies: Containing the Potential Threat*, Center for New American Security, Washington, 3 May 2017, https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies.
[130] Malik, Nikita, *Terror in the Dark: How Terrorists Use Encryption, the Dark Net, and Cryptocurrencies,* The Henry Jackson Society, London, April 2018, p. 42, *http*://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf.
[131] Department of Finance and Department of Justice and Equality, *National Risk Assessment for Ireland: Money Laundering and Terrorist Financing*, Dublin, October 2016, p. 86. http://www.justice.ie/en/JELR/National_Risk_Assessment_Money_Laundering_and_Terrorist_Financing_Oct16.pdf/Files/National_Risk_Assessment_Money_Laundering_and_Terrorist_Financing_Oct16.pdf.
[132] Europol, 'Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain,' Europol press release, 26 March 2018, https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain.

entity such as Liberty Reserve. As one observer notes, cryptocurrencies can enable 'digital marketplaces where users can exchange all types of goods and services, without the fear of being censored, having their accounts frozen or interfered with in any way.'[133] This open, resilient, 'censorship resistant' feature is what some see as Bitcoin's unique innovation.

Censorship resistance has obvious appeals to actors who seek uninhibited access to methods for raising or moving funds. From the perspective of a terrorist actor, merely obtaining a Bitcoin address they can post online is, in theory, a simple way to raise funds with little effort.

In practice, however, cryptocurrency networks are populated by centralised intermediaries. Among these are cryptocurrency exchanges and custodial wallet providers. Whilst two users can trade Bitcoin P2P relatively simply within the Bitcoin network, moving between the Bitcoin network to other cryptocurrencies, or to fiat currencies, often proves difficult without third-party assistance. Novices who wish to access cryptocurrencies for the first time especially require a simple manner to exchange their fiat currency for cryptocurrency. Cryptocurrency exchanges fill this void. Large exchanges such as Binance, Bitstamp, Bitfinex, Coinbase and Kraken facilitate large volumes of Bitcoin trading and provide users with custodial wallets. Given the current state and level of cryptocurrency adoption, exchanges play an important role in providing the average user with access to cryptocurrencies.

Cryptocurrency exchanges can restrict user access to services just as banks do. In the wake of violent demonstrations in Charlottesville, Virginia, Coinbase blocked transfers to the *Daily Stormer*. Whilst refusing to comment on individual cases, Coinbase stated that it 'prohibits the use of an account which would abuse, harass, threaten or promote violence against others [and it] continues to act to enforce this policy across our platform, including to restrict access to Coinbase services and to close accounts.'[134]

This centralised aspect of an otherwise decentralised ecosystem creates natural 'chokepoints' for regulation and oversight. Indeed, the problem of converting VC into fiat currency has created problems for criminals more broadly. Exchanges like Coinbase often place limits around user activity, for example, only allowing users to cash out up to USD 15,000 per week. As John Bambenek notes, this is a practical problem if an individual is sitting on an eight or nine figure sum of illicit cryptocurrency they want to convert into fiat.[135] Thus, whilst the decentralised, open nature of cryptocurrencies may have an appeal to illicit actors, in practical terms the ability of terrorists to exploit this feature faces constraints.

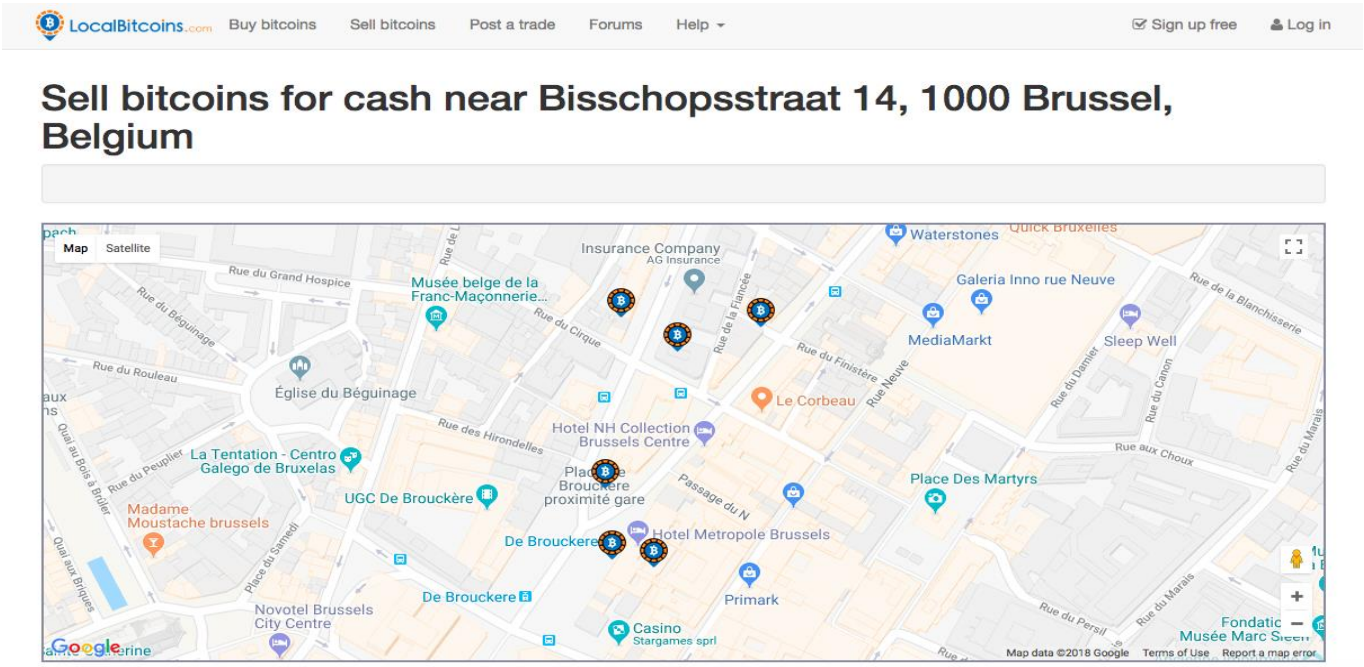
However, in keeping with the libertarian ethos of Bitcoin's founding, some developers have focused on creating decentralised applications that may hold the prospect of reducing reliance on large, centralised cryptocurrency exchanges, which, in addition to offering a regulatory chokepoint, can be vulnerable to hacking, loss of user funds or action by regulators.

A relatively low-tech method for by-passing centralised cryptocurrency exchanges is to use websites, such as LocalBitcoins.com, that enable users of cryptocurrencies to find users of fiat currency, and to swap these directly. Several recent cases have emerged of individuals acting as cryptocurrency brokers on LocalBitcoins, charging a commission to arrange the exchange of cash for cryptocurrencies. In the US, authorities have brought charges against

[133] Rauchs, Michael, 'Cryptocurrencies won't be going away any time soon,' *Oxbridge Business Review*, April 2018, https://www.oxbridgebr.org/cryptocurrencies-are-here-to-stay.
[134] Burns, Janet, 'Cut Off From Big Fintech, White Nationalists Are Using Bitcoin to Raise Funds,' *Forbes*, 3 January 2018, https://www.forbes.com/sites/janetwburns/2018/01/03/cut-off-from-big-fintech-white-. supremacists-are-using-bitcoin-to-raise-funds/#49f5334633b3.
[135] Gilbert, David, 'Criminals are racing to cash out their Bitcoin. Here's how they're doing it,' *Vice*, 19 March 2018, https://news.vice.com/en_ca/article/7xdzqa/criminals-are-racing-to-cash-out-their-bitcoin-heres-how-theyre-doing-it .

LocalBitcoins brokers for acting as unlicensed money transmitters.[136] However, because it is merely a webpage platform over which users of cryptocurrencies may connect with one another and is not itself involved in the process of exchanging funds, LocalBitcoins and similar sites are not subject to comprehensive AML/CFT regulation. This offers a means for bypassing KYC requirements at the point of cryptocurrency swaps.

Map 2: **LocalBitcoins Map of Locations to Sell Bitcoins in Brussels**



Source: LocalBitcoins website

Other, more sophisticated decentralised exchange platforms (DEXs) have been developed to enable direct P2P exchanges cryptocurrency users.[137] DEXs are software platforms that utilise innovations such as multi-signature escrow accounts to enable users to exchange cryptocurrencies P2P without requiring third party custody of funds. DEXs are still in a developmental phase and generally do not enable the range of more complex trading features available on large, centralised cryptocurrency exchanges. Popular DEXs include IDEX, Bitsquare, OpenLedger, CryptoBridge and Bitshares. Because these platforms do not provide a custodial service, they do not function in the manner of an easily regulated gatekeeper.

Another related innovation underway is the use of 'atomic swaps', or methods for enabling two parties to swap two cryptocurrencies directly across separate blockchains, instantaneously and without interruption.[138] The first successful atomic swap was completed in September 2017 when developers of the Decred and Litecoin cryptocurrencies conducted an atomic swap.[139] Proponents argue that if successful at scale, atomic swaps would enable a user-friendly method of decentralised exchange suited for use across a wide range of cryptocurrency ecosystems. One commentator suggests atomic swaps 'will make it trivial to move between different cryptos' without the need for third-party involvement.[140]

[136] Kelso, C. Edward, 'Michigan Localbitcoins User Charged with Unlicensed Money Transmitting,' *Bitcoin.com*, 29 October 2017; see: https://news.bitcoin.com/localbitcoins-user-charged-with-unlicensed-money-transmitting/.
[137] Madiera, Antonio, 'What is a Decentralised Exchange?' *CryptoCompare*, 28 September 2017, https://www.cryptocompare.com/exchanges/guides/what-is-a-decentralized-exchange/.
[138] Madiera, Antonio, 'What Are Atomic Swaps?' *CryptoCompare*, 5 April 2018, https://www.cryptocompare.com/coins/guides/what-are-atomic-swaps/.
[139] Peaster, William M., 'What Are Atomic Swaps? Our Guide to a Revolution in Decentralization,' Blockonomi, 10 January 2018, https://blockonomi.com/atomic-swaps/.
[140] Ibid.

As Chapter 4 of this study describes, because the emphasis of regulatory regimes to date has been on placing oversight where users interact with centralised third-party gatekeepers, it remains unclear whether the regulatory regime as set out in the 5AMLD will remain relevant in the face of a growing range of DEXs, atomic swaps and other P2P applications that may sit outside the historical paradigm of the AML/CFT regime.

Indeed, it is doubtful whether the existing AML/CFT regime has ready responses to these technological developments at all.

3.3. Other Potential Risks

The cases noted above reveal the relatively small scale and sporadic use of VCs by religiously-inspired terrorists and political extremists; however, they suggest certain types of risks that are emerging and could develop. To-date, VCs appear to present a risk only in the context of limited usage for very specific aims. Terrorist actors seeking to operate in online environments requiring some combination of anonymity, borderless P2P transfer and permissionless, decentralised access may find some limited utility in cryptocurrencies.

Nonetheless, the minimal costs required to commit a terrorist attack and the relatively small amounts of money raised should not minimise the potential harm that can be done.

Perhaps further on the horizon, but certainly warranting consideration, is the prospect that terrorist networks could engage in a range of more complex, disruptive and lucrative activities involving VCs. The following two sections will describe contexts and scenarios that are perhaps less likely to manifest in the near-term and thus remain speculative in nature, but nonetheless are areas of potential risk for the future.

3.3.1. The Convergence of Cybercrime and Terrorism

Cryptocurrency-enabled cybercrime has appealed to certain actors intent on inflicting widespread disruption and in need of financing.

For example, North Korea has increasingly looked to cybercrime to raise funds in its sanctions-evasion efforts. It was behind the WannaCry ransomware attack[141], which disrupted the UK's National Health Service and demonstrated the havoc that cybercrime can inflict on key infrastructure. WannaCry raised Bitcoin worth approximately USD 140,000 before it was withdrawn[142]. Whilst hardly insubstantial, WannaCry was not particularly successful in terms of the level of funding raised through other ransomware attacks. However, North Korea has also been associated with large-scale cyberthefts from cryptocurrency exchanges, including theft of Bitcoin from the South Korea-based exchange YouBit in late 2017.[143]

[141] 'Cyber-attack: US and UK blame North Korea for WannaCry,' *BBCNews*, 19 December 2017, http://www.bbc.co.uk/news/world-us-canada-42407488.
[142] Collins, Keith, 'The hackers behind WannaCry ransomware attack have finally cashed out,' *Quartz*, 3 August 2017, https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/.
[143] Chapman, Ben, 'Bitcoin latest: North Korea suspected of South Korean cryptocurrency exchange hack,' *Independent*, 21 December 2017,, https://www.independent.co.uk/news/business/news/bitcoin-latest-updates-north-korea-south-youbit-exchange-hack-cryptocurrency-a8121781.html.

VC-enabled cybercriminality may therefore offer an attractive method for other actors seeking both to raise funds and to cause disruption. In theory, it seems logical that this would be attractive to terrorist groups such as ISIS and al-Qaeda.

However, the extent of terrorist adoption of sophisticated cybercrime tactics is still a matter of debate. Europol's 2017 IOCTA suggests that whilst terrorists make use of the internet and online communication apps for coordination, propaganda, and knowledge dissemination, their ability to launch cyber-attacks remains limited.[144]

Figure 6: Image of the WannaCry Ransomware Message Sent to Victims

Source: Wired (see: http://www.wired.co.uk/article/wannacry-ransomware-virus-patch)

However, the notion of 'cyber-jihad', coined by James Scott and Drew Spaniel from the Institute for Critical Infrastructure, is becoming more common, and describes a situation where the cyber-world is fundamental to terrorist operations today. They suggest that ISIS poses an 'active cyber threat by working with lone hackers, hacker groups and by appropriating open-source online materials.'[145]

The case of Kosovo national Ardit Ferizi (known in the media as the 'Albanian Hacker') is one such example of the convergence of cybercrime, terrorism and VCs, and provides a suggestion of what the future may hold. In August 2015, Ferizi installed malware to obtain personal information of US government and military workers that was then published by ISIS as a 'hit-list'.[146] He then later demanded ransom in Bitcoin from the company to remove the malware.[147]

Although Ferizi failed to obtain any Bitcoin and was apprehended, the crime was successful insofar as it demonstrated a terrorist actor's capability to engage in hacking and obtain confidential information. It may be that from the perspective of many terrorist actors, disruption trumps financial gain as a motive for cybercriminality. However, this intersection of cybercriminality and terrorism could prove to be a new frontier in terrorist capabilities and

[144] Europol, *2017 IOCTA*, see: https://www.europol.europa.eu/ iocta/2017/THE_CONVERGENCE_OF_CYBER_AND_TERRORISM.html.
[145] Ashok, India, 'The anatomy of a "Cyber Jihad" – analysing the future and evolution of terrorism in cyberspace,' *International Business Times*, 20 June 2016, https://www.ibtimes.co.uk/anatomy-cyber-jihad-analysing-evolution-future-terrorism-cyberspace-1566184.
[146] 'Hacker who gave ISIS "hitlist" of US targets jailed for 20 years,' *Associated Press*, 24 September 2016, https://www.theguardian.com/world/2016/sep/24/hacker-who-gave-isis-hitlist-of-us-targets-jailed-for-20-years.
[147] Johnson, Tim, 'Computer hack helped feed an Islamic State Death List,' 20 July 2016, *McClatchy*, 20 July 2016, http://www.mcclatchydc.com/news/nation-world/national/article90782637.html.

could provide considerable TF opportunity should it ever accelerate at scale. It therefore requires greater understanding and law enforcement engagement to ensure it is effectively monitored, and countered over time should it emerge.

One development of concern is that the barriers to engaging in cybercrime are eroding. One can now simply buy criminal expertise and services online. In April 2018, Europol announced the dismantling of webstresser.org, a DDOS marketplace that accepted the purchase of cryptocurrencies for malware to launch DDOS attacks on financial and public sector infrastructure. As Europol notes in its press announcement of the takedown:

> *It used to be that in order to launch a DDoS attack, one had to be pretty well versed in internet technology. That is no longer the case. With webstresser.org … Fees on offer were as low as EUR 15.00 a month, thus allowing individuals with little to no technical knowledge to launch crippling DDoS attacks.*[148]

The prospect therefore cannot be discounted that terrorist actors may with time engage in a more complex array of disruptive online activity involving VCs.

3.3.2. The Creation of Virtual Currencies and Other Advanced Uses

Another prospective set of risks is that terrorist actors might aim to exploit more advanced and innovative applications of VCs, and even go so far as to create their own VCs.

In December 2017, Venezuela's regime demonstrated the potential appeal of self-deployed VCs for rogue actors when it announced the launch of the 'petro', an oil-backed VC it claimed to have developed in the face of the country's rampant hyperinflation and US sanctions. Whilst sometimes described as a cryptocurrency, the petro bears features more indicative of a centralised VC project, insofar as the Venezuelan government has indicated it will issue the petro directly to buyers and will back it with barrels of oil.[149] Regardless, and whether it will prove anything more than a publicity stunt, the launch of the petro indicates that actors seeking workarounds to the mainstream financial system are interested in digital fundraising.

A 2015 report by RAND assessed the immediate prospect for non-state actors such as terrorist groups to develop VCs as low, but indicated that, 'the trends indicate a future in which VCs could be deployed … particularly given the rate at which the needed technologies are becoming available for purchase and the gradual but widening public understanding of VCs.'[150] RAND's assessment concluded that 'a VC may be an attractive alternative for non-state actors who look to disrupt sovereignty and increase their own political and/or economic power by displacing state-based currencies. VC deployments are particularly attractive in developing countries and in countries undergoing internal turmoil, where the existing financial infrastructure is either insufficient or weakened.'[151]

A VC might appeal to a terrorist organisation aspiring to achieve financial self-sufficiency. ISIS demonstrated its general desire for financial self-sufficiency in 2015 when it announced the creation of the gold dinar, a physical currency it claimed to have created, in its own

[148] Europol, 'World's Biggest Marketplace Selling Internet Paralysing DDOS Attacks Taken Down, Europol press release, 25 April 2018, https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down.

[149] Dedi, Dylan, 'Is Venezuela's "Petro" Really a Cryptocurrency?' *CryptoSlate*, 7 December 2017, https://cryptoslate.com/venezuelas-petro-really-cryptocurrency/.

[150] Baron, Joshua; O'Mahony, Angela; Manheim, David; Dion-Schwarz, Cynthia, *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment*, RAND Corporation, Santa Monica, 2015, p. xi, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf.

[151] Ibid, p. x.

words, to avoid 'America's capitalist financial system of enslaver'.[152] Whilst it failed to supplant the US dollar in ISIS's own operations, the launch of the gold dinar represents terrorist groups' aspirations for financial independence.

Initial Coin Offerings (ICOs) are another innovation that warrant mention in this context. ICOs are predominately associated with start-up ventures, but they have proven controversial and putatively high-risk. Fraudsters have used the uneven regulatory environment around ICOs to exploit often uneducated and unprotected victims. In early 2018, the US Securities and Exchange Commission brought charges against Centra Tech Inc. for fraudulently promoting an ICO that raised USD 32 million.[153] In November 2017, a purported cryptocurrency company operating by the name Confido raised USD 375,000 through an ICO, only to disappear with the funds of duped investors.[154]

Given their fundraising potential, it is perhaps unlikely, but certainly not impossible, that terrorist actors could seek to raise funds under the guise of an ICO they have launched, either overtly or fraudulently.

However, given that the use of VCs typically requires interaction with an exchange that can be regulated, it seems unlikely that a terrorist organisation could successfully establish its own meaningful and sustainable VC. The prospect of a terrorist organisation developing a sustainable VC or VC-related project is likely still very remote. Any VC developed by a terrorist group would also need to be met with a swift and rapid response by governments, mirroring the US government's announcement that US persons are barred from dealing in the petro or any related applications developed by the Venezuelan government.[155]

Far more likely, and ultimately far more convenient for terrorists, is to exploit open-source applications created by others.

It would be unwise to dismiss entirely the prospect of terrorist organisations eventually developing and exploiting VCs and related applications – such as ICOs, and a range of new Dapps powered by a new set of coins – in the future. It is therefore a situation that should be closely monitored, combined with a general raising of awareness of how these fundraising mechanisms work and where they may be exploited.

[152] Staufenberg, Jess, 'Isis shows off currency with gold dinar coin worth £91 each – in quest for "world domination",' *Independent*, 31 August 2015, https://www.independent.co.uk/news/world/middle-east/isis-shows-off-new-currency-with-gold-dinar-coins-worth-91-each-in-quest-for-world-domination-10480121.html.
[153] Peterson, Becky, 'The SEC charges a third Centra cryptocurrency "mastermind" with fraud over its $32 million ICO,' *Business Insider*, 20 April 2018, http://uk.businessinsider.com/sec-charges-third-centra-crypto-founder-with-fraud-2018-4.
[154] Kharpal, Arjun, 'Cryptocurrency start-up Confido disappears with $375,000 from an ICO, and nobody can find the founders,' *CNBC*, 21 November 2017, https://www.cnbc.com/2017/11/21/confido-ico-exit-scam-founders-run-away-with-375k.html.
[155] Alexander, David and Wroughton, Lesley, 'U.S. bans transactions with Venezuela's digital currency,' *Reuters*, 19 March 2018, https://www.reuters.com/article/uk-crypto-currencies-venezuela-usa/u-s-bans-transactions-with-venezuelas-digital-currency-idUSKBN1GV2AX.

4. LEGAL AND REGULATORY MECHANISMS

KEY FINDINGS

- The regulation of VCs globally has varied: some countries are adopting approaches consistent with the FATF's Guidance, but many have not. The global regulatory approach around VCs remains uncoordinated and fragmented.
- 5AMLD marks an important step in aligning the EU with the FATF's efforts. One limitation of 5AMLD is that it only covers VC-to-fiat exchange platforms and does not cover VC-to-VC exchanges. This presents a risk insofar as parties trading Bitcoin for alt-coins may not be subject to AML/CFT measures.
- With the pace of technology outstripping the ability of global regulators to coordinate action, the FATF has indicated it will revisit its guidance on VCs. The EU should form an expert working group to consider what further EU-level measures and regulatory frameworks may be required going forward.
- Self-regulatory efforts underway on the part of the VC industry can advance AML/CFT efforts and provide an important compliment to 5AMLD.

4.1. The International Response

4.1.1. FATF and Virtual Currencies: Guidance for a Risk Based Approach

As has been described previously, in June 2015, the FATF published detailed guidance for countries to assist them in managing the money laundering and TF risks of VCs.

The FATF Guidance describes specific FATF Recommendations that are directly relevant to VCs. Among those the FATF highlights are:

- **Recommendation 1:** advises countries to conduct a coordinated risk assessment of VC products and services, ensure cooperation between public and private sectors to assist competent authorities, and undertake the regulation of exchange platforms between convertible VCs and fiat currency.
- **Recommendation 2:** suggests that countries consider inter-agency working groups with the inclusion of policy-makers, the national FIU, supervisors and LEAs to develop and implement effective policy and regulation.
- **Recommendation 14:** directs countries to register or license natural or legal persons providing money value transfer services, which would apply to entities providing convertible VC exchange services between VC and fiat.
- **Recommendation 15:** advises countries to identify and assess ML/TF risks surrounding new products, including VCs, and that local financial institutions take appropriate measures to manage and mitigate these risks before launching new products or developing new technologies.
- **Recommendation 26:** suggests countries should ensure convertible VC exchanges are subject to adequate regulation and supervision. Countries should also amend legal frameworks as needed to ensure effective AML/CFT regulation of decentralised VC payment mechanisms.
- **Recommendation 35:** suggests countries mandate the licensing of VC exchanges, and application of customer identification and recordkeeping requirements at exchanges, to overcome these challenges.

- **Recommendation 40:** requires countries to provide efficient and effective international cooperation to help other jurisdictions combat ML, associated predicate offences and TF, involving VCs.

The FATF Guidance sets an important a blueprint for regulating VCs. In response, jurisdictions around the world have begun taking steps to regulate VCs. Some, such as the EU, the United States, Canada, Japan and Australia, have instituted measures broadly aligned within FATF's Guidance, though with some variation.

However, the approach of these countries contrasts with jurisdictions such as China and Russia, which have taken a less tolerant approach; other countries have yet to undertake any concrete AML/CFT measures toward VCs at all.

The next section provides examples of the range of responses that have emerged outside the EU.

4.1.2. Non-EU Measures on VCs

i. The US

In 2013, FinCEN, the US FIU, issued guidance indicating that it regards VC administrators and exchangers as money transmitters subject to AML/CFT requirements. 'Money transmission services' are defined as 'the acceptance of currency, funds, or other value that substitutes for currency to another location or person by any means.' [156]

This requires licensing any natural or legal person engaged in accepting convertible VC from one person and transmitting it to another person or location; it thereby covers cryptocurrency exchanges, centralised VC administrators and individual brokers of VCs. Importantly, the US provision covering the conversion of 'value that substitutes for currency' applies to exchanges of VCs for VCs, and not merely VC-to-fiat exchanges. This is important, as it ensure US regulation captures parties who facilitate the exchange of Bitcoin to alt-coins such as Monero.

US regulators state that regulation has enabled them to exercise meaningful oversight of the VC sector. As US Treasury Under Secretary Sigal Mandelker notes, VC companies in the US 'are subject to comprehensive, routine AML/CFT examinations, just like financial institutions in the securities and futures markets.'[157] The US has also used its enforcement powers to aggressively move against violators of AML/CFT requirements. In July 2017, FinCEN levied a USD 110 million penalty against the BTC-e cryptocurrency exchange for acting as an unlicensed money transmitter and failing to implement AML/CFT measures.[158]

The early move by the US to regulate VC businesses has arguably acted as a deterrent to illicit actors: a report from blockchain analytics firm Elliptic and the Foundation for the Defense of Democracies indicates that between 2013 and 2016, Europe received five times

[156] Financial Crimes Enforcement Network, 'Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies,' FinCEN Guidance, 18 March 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
[157] United States Department of the Treasury, 'U.S. Department of the Treasury Under Secretary Sigal Mandelker, Speech before the Securities Industry and Financial Markets Association Anti-Money Laundering & Financial Crimes Conference,' Statements & Remarks, 13 February 2018, https://home.treasury.gov/news/press-release/sm0286.
[158] Financial Crimes Enforcement Network, 'Assessment of Civil and Monetary Penalty in the Matter of BTC-e a/k/a Canton Business Corporation and Alexander Vinik,' July 2017, https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment_for_BTCeVinnikFINAL_SignDate_07.26.17.pdf

more illicit Bitcoin than North American services.[159] Whilst not necessarily conclusive evidence that criminals have deliberately sought out regulatory loopholes in the EU, it is a compelling data point and worth further study.

ii. Canada

In June 2014, Canada announced its plan to bring VC-to-fiat exchangers into the scope of its AML/CFT framework by defining them as MSBs. As of early 2018, those measures were still being finalised. They require that any entity conducting VC business must register with the Canadian FIU, the Financial Transactions and Reports Analysis Centre, report STRs, conduct KYC/CDD measures and establish if any of their customers are high risk. The law also applies exchanges that operate outside Canadian territory, but which 'direct services or persons within Canada.'[160]

iii. Japan

In April 2017, an amendment to the Payment Services Act of Japan came into effect, which introduced a bespoke regulation for Japanese VC businesses. VC exchange services must register with Japan's Financial Services Agency (FSA) to obtain a license. Covered services include: the purchase and sale of VCs, or exchange for other VCs; intermediary, brokerage or agency services; and management of cash or VCs in relation to the aforementioned activities.[161]

Japanese regulators have demonstrated their willingness to act against exchanges with lax compliance standards.[162] Following cyberthefts against Japanese Bitcoin exchange Coincheck, the FSA conducted onsite inspections of 15 exchanges.[163] As a result, in March 2018 the FSA suspended for one month the licences of two exchanges, FSHO and BitStation, that were found to have insufficient security practices.

In April 2018, *Forbes* reported that the FSA is considering restricted the types of cryptocurrencies licensed exchanges may carry, including prohibiting them from using privacy-focused alt-coins such as Monero.[164]

iv. Australia

In December 2017, the Australian Parliament passed amendments to the AML/CFT Act 2006, requiring VC exchanges (referred to locally as 'digital currency exchange services) to comply with comprehensive AML/CFT requirements.[165] All exchanges have been required to register

[159] Fanusie and Robinson, p.2.
[160] Financial Transactions and Reports Analysis Centre of Canada, 'FINTRAC Advisory regarding Money Service Businesses dealing in Virtual Currency,' 30 July 2014, http://www.fintrac.gc.ca/new-neuf/avs/2014-07-30-eng.asp.
[161] Ishida, Masahiko; Mears, Edward; Takeda, Ryutaro, 'Japan Regulatory Update on Virtual Currency Business,' DLA Piper, 29 December 2017, https://www.dlapiper.com/en/japan/insights/publications/2017/12/japan-regulatory-update-on-virtual-currency-business/.
[162] Namblampurath, Rahul, 'Japan's FSA Terminates License of Two Bitcoin Exchanges Citing Irregularities,' *BTCManager.com*, 11 March 2018, https://btcmanager.com/japans-fsa-terminates-license-two-bitcoin-exchanges-citing-irregularities/.
[163] 'Government to inspect 15 virtual currency exchanges awaiting certification in Japan,' *Japan Time*s, 16 February 2018, https://www.japantimes.co.jp/news/2018/02/16/business/government-inspect-15-virtual-currency-exchanges-awaiting-certification-japan/#.WusT_NMvzBK.
[164] Adelstein, Jake, 'Japan's Financial Regulator Is Pushing Crypto Exchanges To Drop "Altcoins" Favoured by Criminals,' *Forbes*, 30 April 2018, *https*://www.forbes.com/sites/adelsteinjake/2018/04/30/japans-financial-regulator-is-pushing-crypto-exchanges-to-drop-altcoins-favored-by-criminals/#1c27b6a1b8a3.
[165] Australian Transaction Reports and Analysis Centre, 'Digital Currency Exchange Registration Requirements,' 3 April 2018, http://www.austrac.gov.au/chapter-5-dce-registration-requirements.

with the Australian FIU, AUSTRAC, since April 2018,[166] and are required to collect CDD information, file STRs and meet other AML/CFT obligations. Under the Australian AML/CFT Act, digital currency exchange services are defined as those engaged in the exchange between fiat currency and VCs.[167]

v. Switzerland

Switzerland has taken one of the more innovative approaches to VC regulation. Switzerland has earned a reputation as friendly to VC business. A January 2018 report suggests that of the ten biggest proposed ICOs, four are based in Switzerland.[168] Rather than rely exclusively on older regulatory frameworks, the Swiss approach seeks to create a new regime tailored to a technology that does not always sit comfortably within existing regulation.

In addition to bringing VC exchanges within the scope of Swiss regulation, the Swiss Financial Market Supervisory Authority (FINMA), has created a bespoke regime for categorising and regulating ICOs. FINMA published guidance on ICOs in February 2018,[169] distinguishing between (1) *Payment tokens* (synonymous with cryptocurrencies) which are intended to be used now or in the future, as payment for acquiring goods or services as a means of money or value transfer; (2) *Utility tokens*, which are intended to provide access digitally to an application or service by means of money or value transfer; and (3) *Asset tokens*, which represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In that sense, they are analogous to equities, bonds or derivatives.

Switzerland uses these classifications to determine the proper application of AML/CFT and securities regulations to projects and platforms that use tokens. For example, FINMA's guidance indicates that payment tokens will be subject to AML/CFT requirements, whereas utility tokens may not be where their main use is in non-financial DLT applications.[170]

The purpose of this bespoke regime is to enable space for innovation by providing clarity about how the regulator will treat certain technologies whilst ensuring that new technologies cannot be adopted entirely outside the regulatory framework.

vi. China

Driven by concerns that VCs present risks to consumers and threaten financial integrity and stability, China has taken an increasingly hostile stance to cryptocurrencies across 2017 and 2018. In China, financial institutions and third-party payment providers are prohibited from accepting, using or selling VCs, after the People's Bank of China curtailed involvement with Bitcoin and other cryptocurrencies to 'protect the status of the renminbi as the statutory currency, prevent risks of money laundering and protect financial stability'.[171] General use of VCs in China remains legal. However, China has banned cryptocurrency exchanges from

[166] Letts, Stephen, 'Cryptocurrencies get AUSTRAC anti-money laundering and terrorism funding scrutiny,' *ABC,* 11 April 2016, http://www.abc.net.au/news/2018-04-11/cryptocurrencies-subject-to-anti-money-laundering-and-terrorism/9640642.
[167] Australian Transaction Reports and Analysis Centre, 'Digital Currency Exchange Registration Requirements.'
[168] Atkins, Ralph, 'Switzerland embraces cryptocurrency culture,' *Financial Times*, 25 January 2018, https://www.ft.com/content/c2098ef6-ff84-11e7-9650-9c0ad2d7c5b5.
[169] Swiss Financial Market Supervisory Authority, 'Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs),' 16 February 2018, https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.
[170] Ibid, pp. 6-7.
[171] Mullany, Gerry, 'China Restricts Banks' Use of Bitcoin,' *New York Times,* 5 December 2013, https://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html?hpw&rref=business&_r=0.

operating, blocks the use of foreign cryptocurrency exchanges and has also banned all entities and individuals from raising funds through ICOs.[172]

vii. Russia

Russia has taken an approach that has veered between outright hostility to acceptance and somewhere in between. Initially defined as a 'money surrogate', VCs were prohibited in Russia in January 2014. The Central Bank of the Russian Federation warned individuals, legal entities and credit institutions against the use of VCs due to their anonymous nature, and thus the potential to become involved unwittingly in illegal activities including money laundering and TF. This all-out prohibition appears to have shifted somewhat, as VCs have continued to grow, and in January 2018 Russia's Finance Ministry announced plans to regulate cryptocurrency transactions that involve Russian citizens and companies.[173]

Russia's approach, like China's, reflects that of several other developing countries that attempt to largely restrict the use of VCs or remain ambiguous at best about their use.

viii. India

India is one of a number of countries (others include Colombia, Nigeria and South Africa) yet to bring VC businesses within the scope of AML/CFT regulation. In April 2018, India announced a prohibition on banks or other regulated businesses dealing with cryptocurrency exchanges[174], and as of that time, had not extended AML/CFT requirements to exchanges, taking a hostile position toward the VC industry generally. In February 2018, India's finance minister stated that despite interest in exploring the use of DLT, the country's policy is to 'take all measures to eliminate the use of these crypto-assets in financing illegitimate activities or as part of the payment system.'[175]

4.2. EU Mechanisms

4.2.1. EU Fifth Anti-Money Laundering Directive

5AMLD will bring much-needed transparency to the VC sector across the EU. It will ensure that custodial wallet providers and those VC exchanges engaged in exchanges between VC and fiat currency:

- collect KYC/CDD information on customers;
- apply enhanced due diligence to high risk customers;
- monitor transactions; and
- file STRs where they suspect illicit activity.

[172] Suberg, William, 'Bank Complete: China Blocks Foreign Crypto Exchanges To Counter Financial Risks,' 5 February 2018, https://cointelegraph.com/news/ban-complete-china-blocks-foreign-crypto-exchanges-to-counter-financial-risks.
[173] 'Russia ready to regulate, not ban, cryptocurrencies,' *Reuters*, 25 January 2018, https://www.reuters.com/article/us-russia-cryptocurrencies-bill/russia-ready-to-regulate-not-ban-cryptocurrencies-idUSKBN1FE0Y0.
[174] Rooney, Kate, 'India's central bank bans financial firms from dealing with cryptocurrency,' *CNBC*, 5 April 2018, https://www.cnbc.com/2018/04/05/indias-central-bank-bans-financial-firms-from-dealing-with-cryptocurrency.html.
[175] Arun Jaitley, 'Speech of Arun Jaitley', Speech on the Budget delivered to the Parliament, 1 February 2018, p.20, http://www.thehindu.com/news/resources/article22619699.ece/BINARY/Jaitley%20full%20speech.

This is a welcome development. As noted earlier, one study suggests that Europe has outstripped other jurisdictions in terms of its Bitcoin-related money laundering exposure, possibly because of the lack of regulation to date. [176]

As of the date of publication of this study, it is anticipated that 5AMLD will be published in late spring or early summer 2018, after which time Member States will have 18 months to transpose it locally. By the end of 2019, therefore, all EU Member States should have in place comprehensive regulation around VC exchanges and custodial wallet providers.

Because most regulation on VCs is very new, measuring the efficacy of other jurisdictions' measures on VCs remains a challenging task. However, the experience of some of the countries listed in the previous section suggests some principles that EU policymakers and Member State regulators should consider as they implement 5AMLD.

Ensuring clarity: Because VCs are a new, rapidly evolving technology, it is critical that during the 5AMLD transposition period Member States clarify the scope and intent of regulation and ensure that it is clear to the private sector exactly who will be covered. For example, some expert practitioners interviewed for this study expressed confusion as to whether Bitcoin ATMs will be captured under 5AMLD's definition of VC exchange platforms and suggested that Member States should make explicit that they will be. Such clarity is important to avoid questions about the status of Bitcoin ATMs or to prevent any inconsistency in practice across Member States.

If the EU wishes to create a playing field that both fosters innovation and manages risks, it is also important that Member State regulators provide clarity to the wider financial sector on their stance and approach to regulating VCs. This can prevent bank de-risking, as has occurred in the non-profit organisation and MSB sectors. Bank de-risking describes a practice whereby a bank avoids business areas that falls outside its risk appetite, a phenomenon largely driven by a tougher international regulatory landscape. De-risking can have the unfortunate effect of pushing otherwise legitimate activity to the margins and exacerbating unwanted risks.

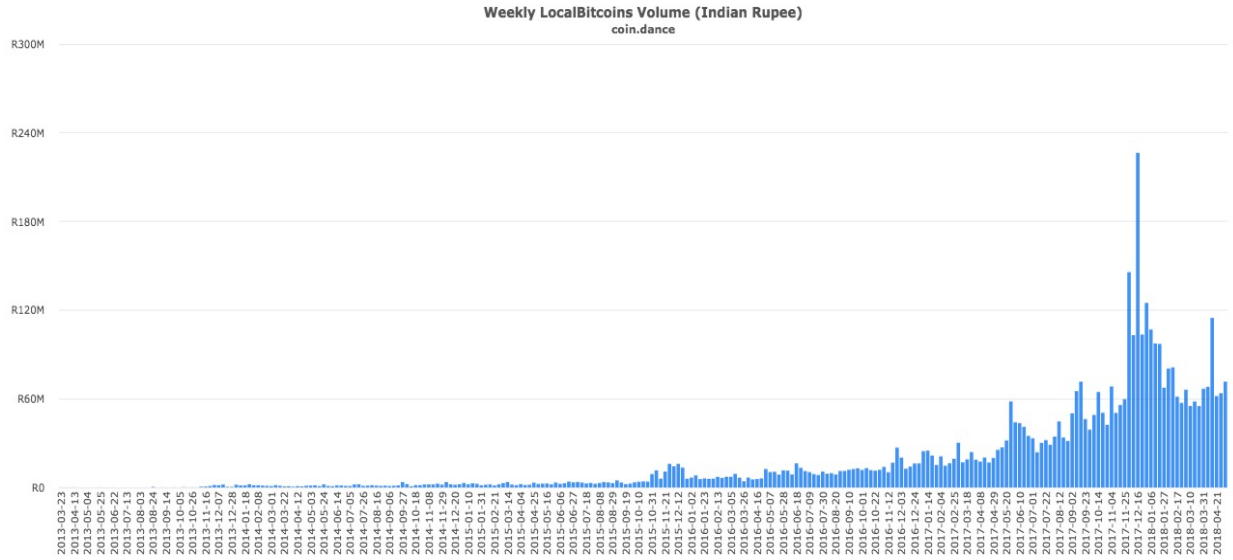
For example, one result of China's ban on VC exchanges has been a reported spike in trading on LocalBitcoins by Chinese users.[177] Similarly, India's hostile position towards Bitcoin exchanges has not prevented LocalBitcoins trading from expanding significantly over the past year, as indicated by Figure 7 below. Rather than stemming use of the cryptocurrencies, such measures may simply push users onto platforms that lack regulatory oversight and feature less transparency than regulated exchanges.

The UK's Financial Conduct Authority's (FCA) 2015 report on *Drivers and Impacts of Derisking*, cites the FinTech sector as one that may be susceptible to derisking.[178] A 2016 report by Coin Center, a US-based research centre that advocates for sound public policy toward cryptocurrencies, on *Overcoming Obstacles to Banking Virtual Currency Businesses*, notes that a lack of access to the banking system is a significant issue for many, if not most VC businesses, including wallets, exchanges, payment processors, specialised service providers, mining and blockchain services; the report claims that banks are unable and

[176] Fanusie and Robinson.
[177] Wong, Joon Ian, 'China's bitcoin investors are flocking to one of the last places to trade,' *Quartz*, 19 September 2017, https://qz.com/1081161/bitcoin-btc-investors-in-china-are-flocking-to-peer-to-peer-platform-localbitcoins-after-the-main-exchanges-shut-down/.
[178] Artingstall, David; Dove, Nick; Howell, John; Levi, Michael; *Drivers & Impacts of Derisking: A study of representative views and data in the UK,* John Howell & Co. Ltd., Shamley Green, 2016, https://www.fca.org.uk/publication/research/drivers-impacts-of-derisking.pdf.

unwilling to properly distinguish between the myriad of VC businesses within the ecosystem.[179] Interviews conducted for this study suggest that EU financial institutions are generally reluctant to provide services to VC businesses owing to the lack of a clear regulatory position to date.

Figure 7: **LocalBitcoins Trading Volumes in India (March 2013 – April 2018)**



Source: Coin.Dance (see: https://coin.dance/volume/localbitcoins/INR)

EU regulators should take this into consideration as they seek to promote innovation in financial services; ultimately, the ability for VCs and DLT-related projects to thrive remains dependent on the underlying banking infrastructure.

Ensuring meaningful enforcement and a harmonised approach. Additionally, it is important that once regulations come into effect, Member States ensure scrutiny and enforcement, as Japan and the US have done, by imposing measures, such as fines and revocations of licences, against those who fail to comply with AML/CFT requirements.

What's more, for 5AMLD to remain effective, it is important it is not undermined by gaps in other countries' regulation. Despite nearly three years having passed since the FATF issued its guidance, some countries have yet to undertake or clarify any AML/CFT measures on VCs at all. Considering these gaps, and the divergences noted above, international coordination is necessary to ensure that an appropriate global framework is in place with a consistent set of aims. The EU has taken on an important role at the G20 in advocating for a cohesive approach, and will need to build on these efforts to ensure successful global coordination.

Ensuring a comprehensive and adaptive approach. Lastly, it is important that 5AMLD is treated as only the first step in establishing a comprehensive EU-wide regulatory framework for VCs. It is the first block on which other measures can be built to ensure the EU has a comprehensive framework in place. For example, like Canada and Australia's measures, whilst 5AMLD follows the FATF's guidance in regulating VC-to-fiat exchange platforms, 5AMLD does not address VC-to-VC exchanges, which countries such as the US and Japan have addressed through their regulation. This is a gap in 5AMLD that may be exploitable by illicit

[179] Fauvre, David; Shipe, Andrew; Vallabhaneni, Pratin; *Overcoming Obstacles to Banking Virtual Currency Business*, Coin Center Report, Washington, D.C., 2016, https://coincenter.org/wp-content/uploads/2016/05/banking-obstacles.pdf.

actors trading Bitcoins for more anonymous cryptocurrencies and warrants addressing. Extending regulation to VC-to-VC exchanges would ensure that parties trading Bitcoin for Monero, for example, would be subject to KYC/CDD measures, and would require that VC-to-VC exchange platforms file STRs where they observe suspicious activity.

Furthermore, as VCs and related technologies develop, and at a rapid pace, it is worth considering whether the regulations will be able to keep pace with the technology. The FATF Guidance itself is now three years old, and whilst it remains useful in understanding VCs in a general sense, the understanding of the risks has changed since 2015. The EU will need to begin the process now of considering how future regulation around VCs may need to evolve. For example, it will be important to consider how regulatory regimes can treat more complex VC-related developments such as DEXs and other P2P exchange platforms such as LocalBitcoins.

Additionally, it may be that other innovative regulatory approaches and frameworks are required to ensure that the EU can keep pace with these developments. As Switzerland has demonstrated, one option is to create new, bespoke frameworks for VC-related regulation that considers specific features of the technology and addresses a range of risks and issues that may not be addressed by pre-existing regulatory frameworks. It may be that, with time, similarly bespoke arrangements could prove necessary at the EU level.

The next section explores some examples of innovative regulatory approaches being undertaken by select European jurisdictions and which may have relevance for the EU more broadly.

4.2.2. Innovative Approaches to VC Regulation Across Europe

i. Gibraltar

The UK overseas territory of Gibraltar has introduced the world's first bespoke licensing framework for firms wishing to use DLT, including VC exchanges.

In May 2017, HM Government of Gibraltar published *Proposals for a DLT Regulatory Framework*, which outlines a more 'flexible, adaptive approach' in which 'regulatory outcomes remain central but are better achieved through the application of hard principles rather than rigid rules.' [180], It states, 'for businesses based on rapidly-evolving technology … hard-and-fast rules can quickly become out-dated and unfit for purpose.'[181] Gibraltar's framework is thus intended to provide regulatory certainty for nascent DLT technology, encouraging growth of innovative businesses, whilst ensuring a safe environment for their development.

Since 2018, any firm carrying out business that uses DLT for storing or transmitting value must be authorized by the Gibraltar Financial Services Commission (GFSC). The GFSC has issued Nine Regulatory Principles to ensure that desired outcomes are achieved,[182] including ensuring that DLT service providers undertake consumer protection measures, have in place appropriate AML/CFT measures and maintain effective governance arrangements. Nicky

[180] HM Government of Gibraltar, *Proposals for a DLT Regulatory Framework*, Gibraltar, May 2017, http://www.gibraltarfinance.gi/downloads/20170508-dlt-consultation-published-version.pdf?dc_%3D1494312876.
[181] Ibid.
[182] Gibraltar Financial Services Commission, 'Distributed Ledger Technology Regulatory Framework,' GFSC website, http://www.gfsc.gi/dlt.

Gomez, the GFSC's head of risk and innovation, describes the measures as the 'first instance of a purpose-built legislative framework for businesses that use blockchain or DLT.'[183]

This marks a contrast with most other jurisdictions, which focus on regulating VCs exchanges within the context of traditional regulatory approaches. In February 2018 Gibraltar announced that it was drafting ICO-specific regulation,[184] similar to Switzerland's approach.

ii. Malta

Like Gibraltar, Malta has signalled its intention to provide a welcome environment to DLT businesses and cryptocurrency companies.

Malta has proposed the creation of a Malta Digital Innovation Authority (MDIA), a dedicated authority for regulating and overseeing the development of DLT innovations and other tech projects. The MDIA will act as a regulatory body with the technical expertise to evaluate DLT projects and register them as Technology Service Providers. According to Malta's public consultation document, the aim of creating the MDIA is to ensure 'that Malta can take the greatest advantage of new technology arrangements while at the same time protect the public interest.'[185]

In February 2018, Malta's government also proposed a 'VC Bill', which would create a regulatory framework for 'brokers, exchanges, wallet providers, asset managers, investment advisors and market makers dealing in VCs.'[186] The VC Bill also provides for a bespoke regulatory framework for ICOs.[187]

iii. The UK

Another potentially valuable way of testing new technologies such as VCs is through regulatory sandbox mechanisms, such that provided through 'Project Innovate', which was set up by the UK's FCA in 2016 to provide a space for businesses to test their products in a controlled environment.[188]

Within the first cohort of this initiative, DLT technology was tested across multiple firms, revealing the potential for efficient business operations, facilitating cross-border payments and benefiting consumers with reduced transaction times at better exchange rates.[189] Project Innovate made note of the potential risks around DLT and VCs, but stated that testing the products within the sandbox environment gave new firms the space to better understand and manage the risks sufficiently.

The FCA notes that, 'the ability to test on a small scale has allowed firms to prove the potential benefits, better understand the risks involved and improve their risk management processes in preparation for a full-scale launch.'[190] In March 2018, the FCA announced that it is

[183] Jones, Huw, 'Gibraltar launches financial services licence for blockchain,' *Reuters,* 14 December 2017, https://uk.reuters.com/article/uk-gibraltar-regulator-blockchain/gibraltar-launches-financial-services-licence-for-blockchain-idUKKBN1E81JP.
[184] Milano, Annaliese, 'Gibraltar Will Take Market-Driven Approach to ICOs,' *CoinDesk*, 21 February 2018, https://www.coindesk.com/gibraltar-take-market-driven-approach-ico-rules-officials-say/.
[185] Parliamentary Office for Financial Services, Digital Economy and Innovation, Office of the Prime Minister, *Malta: A Leader in DLT Regulation*, February 2018, p.11, https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF.
[186] Ibid., p. ii.
[187] Ibid.
[188] https://www.fca.org.uk/firms/regulatory-sandbox
[189] Financial Conduct Authority, 'Regulatory Sandbox,' 11 May 2015, https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf.
[190] Financial Conduct Authority, *Regulatory sandbox lessons learned report*, Financial Conduct Authority, London, October 2017, London, pp. 10 – 11, https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf.

considering the launch of a 'global sandbox' and would begin working with interested regulators across Europe, the US and the Far East.[191]

The approach undertaken by Project Innovate is one that other regulators may wish to consider when seeking to engage with the VC sector and with DLT platforms more broadly. It allows the businesses and regulators to work collaboratively to determine the true nature of the risks posed. In this way, new technologies are developed with sufficient controls, whilst not stifling innovation early on.

4.3. The Role of Self-Regulation

Self-regulatory frameworks can act as important complement to formal regulation.

Self-regulation refers to the establishment of organisations and mechanisms for enabling similar businesses – whether similar by sector, location or function – to develop and enforce common standards and requirements that ensure their member's integrity and reputation. Effective self-regulatory bodies set clear and robust standards that are binding as a condition of membership. Self-regulation, importantly, is not meant to be a complete supplement for formal regulation. Rather, self-regulatory bodies enable industry participants to establish common practices and standards, and to achieve certain goals.

Some observers argue that the dynamic, fast-changing nature of technologies such as cryptocurrencies can benefit from self-regulatory arrangements, which can promote and enforce standards of responsible practice among their membership. This view has been increasingly endorsed by regulators globally. In February 2018, a commissioner from the US Commodity Futures Trading Commission suggested that the cryptocurrency industry would benefit from self-regulatory bodies.[192] South Africa's central bank has also indicated publicly its interest in establishing a self-regulatory organisation for the cryptocurrency industry there.[193]

The cryptocurrency industry has begun to respond. In March 2018, 16 Japanese cryptocurrency exchanges announced their intention to establish a self-regulatory body.[194] In the same month, a proposal was put forward in the US for a Virtual Commodity Association.[195] In Australia, industry participants formed a self-regulatory body in 2016.[196]

Within the EU, February 2018 saw the formation of CryptoUK, a self-regulatory body comprised of eight companies involved in the cryptocurrency and blockchain industries. Members must adhere to the organisation's Code of Conduct, which includes a requirement

[191] Dickinson, Clare, 'FCA plans global testing ground for fintech startups,' *Financial News*, 19 March 2018, https://www.fnlondon.com/articles/fca-to-set-up-global-fintech-sandbox-20180319.
[192] Aitken, Roger, 'U.S CFTC Commissioner Says Cryptocurrency Exchanges Adopting Self Regulation Could Spur Standards,' *Forbes*, 15 February 2018, https://www.forbes.com/sites/rogeraitken/2018/02/15/u-s-cftc-commissioner-says-cryptocurrency-exchanges-adopting-self-regulation-could-spur-standards/ - 12f7508145e1.
[193] 'South Africa's central bank mulls cryptocurrency self-regulation,' *Finextra*, 4 April 2014, https://www.finextra.com/newsarticle/31907/south-africas-central-bank-mulls-cryptocurrency-regulations.
[194] Wada Takahiko and Wilson, Thomas, 'Japan's cryptocurrency exchanges to set up self-regulatory body,' *Reuters,* 2 March 2018, https://www.reuters.com/article/us-crypto-currencies-japan/japans-cryptocurrency-exchanges-to-set-up-self-regulatory-body-idUSKCN1GE037.
[195] Gemini 'A Proposal for a Self-Regulatory Organisation for the Virtual Currency Industry,' Gemini website, 13 March 2018, https://gemini.com/blog/a-proposal-for-a-self-regulatory-organization-for-the-u-s-virtual-currency-industry/.
[196] Higgins, Stan, 'Australian Digital Currency Advocates Launch Self-Regulatory Efforts,' *CoinDesk*, 1 December 2016, https://www.coindesk.com/australia-digital-currency-self-regulation/.

that members 'commit to undertaking due diligence checks on platform users to protect against illegal activity, including the financing of terrorism.'[197]

In the EU, the VC industry could pursue pan-European self-regulatory bodies, as well as other country-specific bodies. The presence of self-regulatory groups would be a boon as well for Member State regulators, which could engage these self-regulatory groups to ensure the establishment of effective AML/CFT practices across the industry.

[197] CryptoUK, 'Principles & Code of Conduct,' CryptoUK website, https://www.cryptocurrenciesuk.info/code-of-conducts/.

5. COOPERATION AND PARTNERSHIP ACROSS THE EU

KEY FINDINGS

- European LEAs have made substantial strides in their ability to investigate, detect and disrupt the illicit use of VCs. This has resulted in significant arrests across Europe, particularly related to the use of Bitcoin on the Dark Web and in cybercrime.
- Europol has played an important role in supporting and coordinating these actions, and in providing training and educational awareness to LEAs across the EU.
- Despite progress, Member States efforts on preventing the illicit use of VCs are still in a developmental stage and are often ad hoc and uncoordinated at the Member State level. Greater strategic focus is required, in addition to resources to support further training for LEAs.
- Both Europol and individual Member States have engaged with the VC industry on an informal basis to ensure cooperation in acting against illicit finance. This interaction can be deepened through the establishment of formalised, VC-focused PPPs.

5.1. EU Law Enforcement Responses to VCs

VCs present LEAs with several substantial practical challenges. Merely keeping educated and informed about emerging technologies is a significant hurdle. LEAs must also acquire new analytical skills, tools and resources. The confiscation of VCs during criminal investigations can prove technically challenging, demanding law enforcement make creative use of available resources and legal authorities, which may not have been designed with VCs in mind.

At both the EU and Member State level, LEAs have demonstrated an improving capacity for investigating, analysing and disrupting the illicit use of VCs. Table 2 in Annex III provides examples of significant EU-wide law enforcement actions involving VCs over the past four years. The sections that follow consider the role of Europol and Member State LEAs in detail.

5.1.1. Europol's Role

As the EU's law enforcement agency, Europol has been the focal point for information gathering and intelligence analysis on criminal activity involving VCs across Europe, and has supported related law enforcement action across the EU. Central to this mission is Europol's European Cybercrime Centre (EC3), established in 2013. EC3 provides strategic direction to Europe's counter-cybercrime efforts, supports counter-cybercrime operations across the EU, generates intelligence and develops digital forensic capabilities. EC3 also conducts research into what it describes as 'cross-cutting enablers of cybercrime', such as cryptocurrencies.

In this capacity, EC3 has published its annual IOCTA reports since 2014. The IOCTAs have been Europol's primary platform for public distribution of intelligence assessments related to criminal use of VCs and have documented the steady rise in cryptocurrencies in cybercrime.

Concurrent with the development of these intelligence products, Europol has developed a practical set of capabilities to enhance support for Member States in investigations involving VCs. In February 2016, EC3 entered a Memorandum of Understanding with Chainalysis to

support Europol in its cybercrime investigations.[198] In September of that year, Europol announced the formation of a Digital Currencies Working Group in coordination with Interpol and the Basel Institute of Governance. The Working Group aims to facilitate the exchange of non-operational information among these organisations, establish an expert network and organise regular workshops, and considers issues related to TF as part of its mandate.[199]

This emphasis on fostering and supporting an enhanced capacity for investigations involving cryptocurrencies has borne fruit in the form of several recent high-profile arrests. Most substantial among these was the takedown in July 2017 of the two largest Dark Web marketplaces at the time, AlphaBay and Hansa. In that case, Dutch police, supported by Europol and in coordination with US law enforcement, undertook a highly-sophisticated action to dismantle these two marketplaces and sow distrust among Dark Web users. After arresting AlphaBay's administrators and seizing its servers, Dutch police took control of Hansa and gathered information on its users before shutting it down. The case provided European law enforcement with a wealth of information on Dark Web users.[200]

Figure 8: AlphaBay and Hansa Pages After Seizure by Law Enforcement

Source: Europol website

Through the Digital Currency Working Group, Europol has also worked to develop principles and strategies for combatting the illicit use of cryptocurrencies. In January 2018, the Working Group held a meeting in Basel featuring investigators from more than 30 countries.[201] Several themes have emerged from Europol's workshops, including findings that:

[198] Europol, 'Europol and Chainalysis Reinforce Their Cooperation in The Fight Against Cybercrime,' Europol news article, 19 February 2016, https://www.europol.europa.eu/newsroom/news/europol-and-chainalysis-reinforce-their-cooperation-in-fight-against-cybercrime.
[199] Europol, 'Money Laundering with Digital Currencies: Working Group Established,' Europol press release, 9 September 2016, https://www.europol.europa.eu/newsroom/news/money-laundering-digital-currencies-working-group-established.
[200] Europol, 'Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation,' Europol press release, 20 July 2017, https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.
[201] Europol, 'Global Workshop for Financial Investigators on Detection, Investigation , Seizure and Confiscation of Cryptocurrencies,' Europol press release, 26 January 2018, https://www.europol.europa.eu/newsroom/news/global-workshop-for-financial-investigators-detection-investigation -seizure-and-confiscation-of-cryptocurrencies.

- commercial and law enforcement tools enabling forensic analysis of Bitcoin transactions are valuable in supporting investigations;
- there is currently a lack of tracing tools for alt-coins, which presents challenges for law enforcement investigations; and
- Bitcoin mixers provide a substantial challenge to law enforcement investigations, and action should be taken against those facilitating criminal activity.

The introduction of 5AMLD will prove useful for Europol, as VC exchanges and custodial wallet providers become subject to regulation and face requirements to file STRs. Europol can play a role in ensuring that Member States share information from these STRs and coordinate investigations that utilise information from STRs. Europol currently hosts FIU.net[202], a decentralised intelligence platform that enables Member State FIUs to share and exchange information on STRs generated within their borders.

5.1.2. Other EU-Wide Initiatives

In addition to Europol's ongoing work, the EU has sponsored other efforts to mitigate the risks of criminal and terrorist use of VCs.

In May 2017, a consortium of research institutes and LEAs from seven EU countries[203] formed the TITANIUM project with funding from the EU. TITANIUM aims 'to curtail criminals and attackers from using blockchain technology to avoid law detection, while at the same time respecting the privacy rights of legitimate users.'[204] The project seeks to develop open-source tools to enable the detection of money laundering typologies and other criminal use of VCs, and to train law enforcement in the use of these tools. This includes facilitating 'cross-ledger analysis', or the development of tools for analysing information from alt-coin blockchains.[205]

Another EU-funded project with relevance to CFT efforts is the DANTE project ('Detecting and analysing terrorist-related online contents and financing activities').[206] While not specifically focused on VCs, the project has as its aims the detection and analysis of terrorist online fundraising activities, and terrorist activity on the Dark Web. It is also closely coordinated with the EU-funded Project PROTON, which seeks to better understand organised criminal and terrorist recruitment behaviour and their intersection with cybercrime.[207]

5.1.3. Member State Responses

As indicated by Table 2 in Annex III, individual EU Member States are achieving notable successes in investigating the illicit use of VCs.

Member States' LEAs are increasingly utilising commercial Bitcoin forensic track and trace tools to assist in cybercrime and money laundering cases. In the dismantling of the Alphabay and Hansa Dark Web markets, Dutch authorities demonstrated impressive use of these techniques. In 2017, Denmark announced that it had developed its own Bitcoin blockchain tracing solution and has secured prosecutions using it.[208]

---

[202] See: https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net.
[203] Austria, Denmark, Finland, Germany, the Netherlands, Spain and the UK.
[204] TITANIUM Project, 'Project to prevent criminal use of the dark web and cryptocurrencies launched by international consortium,' 19 May 2017, https://www.titanium-project.eu/news/articles/titanium-project/.
[205] King, Ross Dr., 'TITANIUM: Early Research and Outlook,' 21st European Police Congress, Berlin, 2018, http://www.europaeischer-polizeikongress.de/wp-content/uploads/2018/03/King_2018.pdf.pdf.
[206] DANTE project website, http://www.h2020-dante.eu/.
[207] Project PROTON, 'About,' Project PROTON website, https://www.projectproton.eu/about/.
[208] Keirns, Garrett, 'Danish Police Claim Breakthrough in Bitcoin Breakthrough in Bitcoin Tracking,' *CoinDesk*, 22 February 2017, https://www.coindesk.com/danish-police-claim-breakthrough-bitcoin-tracking/.

As has been noted throughout this report, Member State governments in countries such as Belgium, France, Ireland and the UK have conduct assessments of the illicit financing risks VCs presented locally. Member States that have yet to conduct risk assessment on VCs could benefit from doing so, as it is aligned with the FATF recommendations and can assist in determining appropriate regulatory and law enforcement priorities.

Member States have also begun to secure successful prosecutions in cybercrime and money laundering cases involving cryptocurrencies. This demands that public prosecutors understand the underlying technology and are comfortable that local money laundering and asset confiscation legislation is applicable to VCs. Many of these cases increasingly feature the forfeiture of Bitcoin by authorities. Member States can apply existing asset confiscation legislation to VCs; however, the actual process for confiscating Bitcoin or other cryptocurrencies can prove practically and technically challenging. Issues that may arise whilst confiscating VCs include:

- law enforcement officers and prosecutors may not always be aware that existing legal provisions can be applied to the confiscation of VCs, so may miss opportunities to do so;
- law enforcement officers may lack the technical skill to recognise technology-specific items, such as hardware wallets, that could be subject to confiscation so risk over-looking them during an investigation;
- law enforcement officers may not have experience interacting with VC exchanges and custodial wallet providers so may struggle to understand what information they should request;
- LEAs may not have cryptocurrency wallets readily available to which they can transfer confiscated cryptocurrencies during an investigation;
- the volatility of cryptocurrencies can threaten the obligation of public authorities to avoid the depreciation of seized assets; and
- LEAs may not always have coverage by insurance policies which adequately cover them in the event of loss of confiscated VCs.

In general, research conducted for this study suggests that that the competency of Member State LEAs, FIUs and prosecutors is improving, and that staff involved in investigating the illicit use of VCs are learning rapidly and making creative use of resources, tools and authorities at their disposal.

However, our research suggests that expertise on VCs in Member States is often concentrated amongst a small number of individuals who may have obtained their knowledge and understanding through self-education and ad-hoc up-skilling, rather than in-depth and ongoing training. These individuals are often dispersed across under-resourced agencies with competing priorities. In December 2017, a report to the European Parliament noted that customs authorities across the EU do not have sufficient resources to monitor the movement of cryptocurrencies across borders,[209] a gap that could further heighten the risks presented by easily portable cryptocurrency wallets and products such as debit cards.

[209] European Parliament, Committee on Economic and Monetary Affairs and Committee on Civil Liberties, Justice and Home Affairs *Report on the proposal for a regulation of the European Parliament and of the Council on controls on cash entering or leaving the European Union and repealing Regulation (EC) No 1889/2005,* European Parliament*, 8* December 2017, Amendment 8, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0394&llanguage=EN

This picture, however, is changing, as some Member States are looking to develop formalised operational training programmes for a broad range of staff. One such effort is the N8 Policing Researching Partnership in the UK, which led a collaborative project between academics and law enforcement to address the knowledge gaps around Bitcoin among UK law enforcement. The research project focused on understanding how cryptocurrencies facilitate crime and resulted in the development of practical guidance for UK law enforcement. Furthermore, the study called for the development of a strategic training programme for UK law enforcement, including training staff as 'Bitcoin experts' capable of providing expert witness testimony.[210]

Similarly, the Austrian Ministry of the Interior and Ministry of Finance have co-sponsored an academic study, VIRTCRIME, to explore the possibilities of developing tools for the analysis of alt-coin blockchains, including privacy-focused coins such as Zcash and Monero.[211]

5.2. The Role of Public-Private Partnership

International policymakers have stressed the importance of PPPs in advancing CFT efforts. Policymakers recognise that LEAs have detailed information on security threats, and that private sector financial institutions possess valuable customer and transactional information that may assist in the disruption of criminality. However, both sides often operate in 'silos', failing to exchange information that might be of mutual benefit.

In December 2015, the UN Security Council highlighted the importance of public-private partnership when it passed Resolution 2253, which called on UN Member States 'to engage with financial institutions and share information on [TF] risks to provide greater context for their work in identifying potential TF activity . . . and to promote stronger relationships between governments and the private sector in countering terrorist financing.'[212] The FATF has also made the improvement of information sharing a focus of its work, noting that, 'Multinational money laundering schemes do not respect national boundaries . . . This underscores the importance of having rapid, meaningful and comprehensive sharing of information from a wide variety of sources, across the national and global scale.'[213]

Member States have worked to enable greater PPPs in practice. One highly publicised example in the EU is the UK's Joint Money Laundering Task Force (JMLIT)[214], an initiative that brings together UK law enforcement with representatives from the banking sector to share operational information on money laundering cases.

In this vein, the EU and individual member states should undertake efforts to expand public private partnership involving the VC sector. The public sector across Europe should aim to engage with cryptocurrency exchanges to establish formal arrangements for operational information sharing and related to threats including cybercrime, money laundering and TF.

To date, some initiatives have helped to foster initial contact between EU LEAs and the VC industry. One such effort is the Blockchain Alliance, a public-private initiative in which Europol

[210] Larratt, Phillip; Taylor, Paul; Wall, David S.; Naqvi, Syed; Shillito, Matthew; Stokes, Rob, *Policing Bitcoin : Investigating, Evidencing and Prosecuting Crimes Involving Bitcoin*, N8 Policing Research Partnership, 13 July 2017, p. 2, http://n8prp.org.uk/wp-content/uploads/2017/08/N8-Cryptocurrency-Report.pdf.
[211] VIRTCRIME Project, 'Forensic Methods and Solutions for The Analysis of Criminal Transactions in Post-Bitcoin Cryptocurrencies,' Austrian Institute of Technology, https://www.ait.ac.at/en/research-fields/data-science/projects/virtcrime/.
[212] United Nations Security Council, Resolution 2253 (2015), 17 December 2015, paragraph 24.
[213] Financial Action Task Force, *Private Sector Information Sharing*, FATF Guidance, Paris, November 2017, p.2, http://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf.
[214] See: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit.

participates and which brings together cryptocurrency exchanges, providers of blockchain forensic services and LEAs from across North America and Europe to discuss observed criminal activity.[215] Europol's Digital Currency Working Group has also featured workshops involving the private sector, in which cryptocurrency industry participants can share information about AML/CFT best practice, as well as trends in criminal activity.[216]

Interviews conducted for this paper suggest that EU-wide LEAs have had positive interactions with many cryptocurrency exchanges and have received important support from them in the course of investigations. In a recent report on STR reporting practices across the EU, Europol noted that despite the lack of formal regulation, many VC exchange platforms in Europe 'aim to comply with AML requirements' and 'have shown themselves to be willing and capable of supporting LEA investigations.'[217]

[215] Blockchain Alliance website, http://blockchainalliance.org/.
[216] Europol, 'Europol Hosted 4th Conference on Virtual Currencies,' Europol news article, 5 July 2017, https://www.europol.europa.eu/newsroom/news/europol-hosted-4th-conference-virtual-currencies.
[217] Europol, *From Suspicion to Action: Converting financial intelligence into greater operational impact*, Europol, The Hague, 2017, p. 18, https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact.

6. POLICY RECOMMENDATIONS

KEY FINDINGS

- 5AMLD is just the first step in building the EU's VC regulatory framework. The EU must now look ahead to further measures, such as regulation of VC-to-VC exchanges. It should form an expert working group to explore next steps in EU-wide VC regulation.
- To ensure its efforts are not undermined by gaps elsewhere, the EU should continue to act as a global advocate for a coherent and coordinated international regulatory framework around VCs
- Further strategic training and capacity building are needed to ensure LEAs across the EU operate with a standard level of competency in investigating, tracing and disrupting the illicit use of VCs.
- Establishing dedicated VC intelligence taskforces can provide Member States with a holistic view of risks, which can in turn foster more effective responses.
- At both the EU and Member State level establishing formal, dedicated PPPs on VCs should be a priority.

Based on the findings outlined in this study, this section provides recommendations for public and private sector stakeholders across the EU.

6.1. Ensuring Effective, Robust and Comprehensive Regulation

Because VCs are rapidly-evolving, borderless technologies that pose a range of complex risks, it is essential that the EU maintain a regulatory framework that is implemented effectively now and remains relevant into the future.

The passage and transposition of 5AMLD are only first steps in developing a comprehensive and meaningful EU-wide regulatory framework for VCs.

Once 5AMLD is transposed locally, Member States should clarify the scope and purpose of regulation to ensure that it is implemented comprehensively. This should include, for example, clarifying the status of Bitcoin ATMs and other innovative products and services. Member States must also ensure meaningful enforcement of those requirements through close supervision of VC exchanges and custodial wallet providers, and should be willing to impose sanctions, such as fines and revocation of licences. The experience of the US suggests that comprehensive AML/CFT regulation around the VC industry, supported by meaningful enforcement action, can mitigate exposure to illicit finance risks.

Regulators should also draft guidance that takes a nuanced approach to characterising the risks VCs pose in different contexts and for different purposes. For example, the illicit finance risks the traceable cryptocurrencies such as Bitcoin present is generally not as significant as that presented by privacy-focused alt-coins. Regulators could provide detailed guidance that indicates the nature of CDD and KYC measures VC exchanges should apply where they encounter users of cryptocurrencies with high levels of anonymity. By providing the private

sector with a clear view of the nature of risk, regulators can ensure that private sector effort is directed at mitigating those risks that are most pressing.

It is also important that Member States support their local regulatory frameworks with comprehensive legal arrangements designed to prevent and disrupt illicit activity in VCs. This should include ensuring that local law enables the confiscation of VCs during criminal investigations.

Given the speed at which VC innovations are accelerating, it is important that the EU prepare now for undertaking further regulatory measures. As a priority, the EU should expand on 5AMLD's regulation of VC-to-fiat exchange platforms and take steps to regulate VC-to-VC exchange platforms. This can assist in mitigating the risks posed by illicit actors who seek to swap cryptocurrencies such as Bitcoin for more highly-anonymised cryptocurrencies.

More broadly, the EU should convene an expert working group to assess further measures that may be required to supplement 5AMLD over time. This should include exploring how the innovative regulatory approaches being undertaken across the EU described in Chapter 4 could be scaled across the EU. The working groups should also explore how future regulatory regimes can respond to the emergence of P2P, DEXs and other decentralised financial products and ecosystems that this study described in Chapter 3.

To ensure that gaps in the global regulatory framework do not undermine its efforts, the EU should also play a leadership role in advocating for a consistent global regulatory approach to AML/CFT regulation around VCs. The EU should build on efforts undertaken at the G20 to press for coordinated approaches, and to ensure that countries that have not yet undertaken AML/CFT regulation of the VC industry do so.

In line with efforts to promote responsible innovation, at both the EU level and at the Member State level, policymakers should take steps to prevent de-risking of the VC industry, which can both hinder innovation and exacerbate risks. Regulators across the EU should provide banks and other financial institutions with clarity about the regulatory status of VC industry participants, and should clarify that the purpose of regulation is to enable the responsible development of the sector.

To further this aim last aim, the VC industry across the EU and within Member States should demonstrate its commitment to robust implementation of AML/CFT standards by forming self-regulatory bodies. Member State regulators should encourage and foster these efforts.

6.2. Developing Law Enforcement Knowledge and Capacity

VCs are complex technologies that require the development of new law enforcement techniques, knowledge and resources. Illicit actors can adapt to these technologies faster than law enforcement can adjust.

It is therefore essential that Member States expand and accelerate efforts to ensure LEAs have sufficient levels of competency to investigate and disrupt the illicit use of VCs. Member State LEAs should develop strategic training programmes for all staff, and should develop a practical baseline technical understanding across front-line officers to support ongoing operations. This can include, for example, training in how to identify cryptocurrency hardware wallets and other related technology that might otherwise go overlooked during an investigation.

Member States should also develop formalised advanced VC training programmes for staff in cybercrime units and FIUs who require a more thorough understanding and technical capability. These efforts should strive to cultivate and appoint dedicated staff within public sector agencies who possess deep domain expertise on VCs.

This expertise-building should include training a greater number of staff in the advanced use of track and trace tools, such as those that are commercially available. However, Member States may also seek to develop their own tools, or to make use of open-source forensic tools that are currently being developed through projects such as those described above in Chapter 5.

Furthermore, Member States should ensure that efforts at education and capacity include training on how to utilise local authorities in the confiscation of VCs, as well as technical training to assist in challenges that arise in undertaking confiscations, such as how to appropriately store seized VCs.

As noted in Chapter 5, whilst EU-wide law enforcement agencies are already making important progress, much of this progress is uneven and lacks strategic focus. The EU, led by Europol, should prioritise formal, strategic and sustained operational law enforcement training to enhance the capacity for investigating illicit activity involving VCs. These efforts should be directed at ensuring a standard level of law enforcement competency across the EU, so that certain Member States do not fall behind.

6.3. Developing an Enhanced Intelligence Picture

As described throughout this study, VCs are feature in a growing range of criminal activity, and the risk landscape is evolving at tremendous speed. Whist terrorist use of VCs is small compared to that of other illicit actors, the nature of TF risks VCs pose could evolve significantly.

As VCs expand in their general adoption and feature in a greater range of products and services, the likelihood of terrorist exploitation will naturally grow. Moreover, developments such as the growing availability of cryptocurrencies with high levels of anonymity and terrorist adoption of technology more broadly will shape how this risk manifests over time.

To ensure these risks are adequately monitored, Member States should conduct risk assessments of VC activity locally, using findings from those assessments to develop strategies for regulatory and law enforcement approaches over the short, medium and long-term.

Member States should also develop dedicated VC intelligence taskforces that enable them to obtain multi-disciplinary and holistic intelligence view of the use of VCs across a range of applications and threats. These intelligence taskforces should develop of CFT-specific strategies as they relate specifically to VCs.

However, efforts to assess and disrupt terrorist use of VCs must not occur in a vacuum. Europol and Member States should ensure that both at an EU-wide level, and locally, efforts to detect and disrupt terrorist use of VCs are closely coordinated with similar efforts related to the detection of cybercrime and OCG use of VCs. This coordination is essential to understanding the broader intelligence picture within which the TF risks of VCs may be understood, and for illuminating the both the distinctions and convergences in usage of VCs by a range of illicit actors.

6.4. Enabling Public-Private Partnership

The public sector cannot develop effective regulation, enhance knowledge and improve intelligence acting alone. Cooperation and interaction with businesses in the VC-industry is essential.

As described in Chapter 5, Europol and Member State LEAs are demonstrating positive but largely informal interaction. This interaction should be deepened, formalised and elevated in priority. Member States should develop dedicated fora for sharing information with local VC industry participants, including sharing of intelligence for operational purposes. At the EU level, Europol should build on its existing efforts and establish dedicated fora for exchanges of operational information between public and private sector stakeholders EU-wide.

This study has shown that VCs are a rapidly changing set of innovative technologies that offer prospects for innovation but pose emerging risks, including those related to TF, and present policymakers with numerous substantial challenges. But by undertaking the recommendations set out above, the EU can both mitigate the risks and navigate the challenges effectively.

REFERENCES

Adelstein, Jake, 'Japan's Financial Regulator Is Pushing Crypto Exchanges To Drop "Altcoins" Favoured by Criminals,' *Forbes*, 30 April 2018, *https*:// www. forbes.com/ sites/ adelsteinjake/2018/04/30/japans-financial-regulator-is-pushing-crypto-exchanges-to-drop-altcoins-favored-by-criminals/#1c27b6a1b8a3.

Aitken, Roger, 'U.S CFTC Commissioner Says Cryptocurrency Exchanges Adopting Self Regulation Could Spur Standards,' *Forbes*, 15 February 2018, https://www.forbes.com/sites/rogeraitken/2018/02/15/u-s-cftc-commissioner-says-cryptocurrency-exchanges-adopting-self-regulation-could-spur-standards/ - 12f7508145e1.

Aldridge, Judith; Paoli, Giacomo Persi; Ryan, Nathan; Warnes, Richard, *Behind the curtain: the illicit trade of firearms, explosives and ammunition on the dark web*, RAND Corporation, 2017, https://www.rand.org/pubs/research_reports/RR2091.html.

Alexander, David and Wroughton, Lesley, 'U.S. bans transactions with Venezuela's digital currency,' *Reuters*, 19 March 2018, https://www.reuters.com/article/uk-crypto-currencies-venezuela-usa/u-s-bans-transactions-with-venezuelas-digital-currency-idUSKBN1GV2AX.

Artingstall, David; Dove, Nick; Howell, John; Levi, Michael; *Drivers & Impacts of Derisking: A study of representative views and data in the UK,* John Howell & Co. Ltd., Shamley Green, 2016, https://www.fca.org.uk/publication/research/drivers-impacts-of-derisking.pdf.

Arun Jaitley, 'Speech of Arun Jaitley', Speech on the Budget delivered to the Parliament, 1 February 2018, p.20, http://www.thehindu.com/news/ resources/article22619699.ece/ BINARY /Jaitley%20full%20speech.

Ashok, India, 'The anatomy of a "Cyber Jihad" – analysing the future and evolution of terrorism in cyberspace,' *International Business Times*, 20 June 2016, https://www.ibtimes.co. uk/ anatomy-cyber-jihad-analysing-evolution-future-terrorism-cyberspace-1566184.

Atkins, Ralph, 'Switzerland embraces cryptocurrency culture,' *Financial Times*, 25 January 2018, https://www.ft.com/content/c2098ef6-ff84-11e7-9650-9c0ad2d7c5b5.

Australian Transaction Reports and Analysis Centre, 'Digital Currency Exchange Registration Requirements,' 3 April 2018, http://www.austrac.gov.au/chapter-5-dce-registration-requirements.

Bank for International Settlements, *Central Bank Digital Currencies*, study by the Committee on Payments and Market Infrastructures and the Markets Committee, March 2018, https://www.bis.org/cpmi/publ/d174.pdf.

Bank Frick, 'Bank Frick allows direct investments in leading cryptocurrencies,' Bank Frick website, 28 February 2018 https://www.bankfrick.li/en/about-bank-frick/news/bank-frick-allows-direct-investments-in-leading-cryptocurrencies.

Baron, Joshua; O'Mahony, Angela; Manheim, David; Dion-Schwarz, Cynthia, *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment*, RAND Corporation, Santa Monica, 2015.

Barret, David and Whitehead, Tom, 'Middle Class Daughter of Magistrate Who Turned to Suicide Bomb Plotter', *The Telegraph*, 20 December 2015; Bowcott, Owen, 'Couple Found Guilty of 7/7 Anniversary London Bomb Plot', *The Guardian*, 29 December 2015.

'Berlin Police Arrest 33-Year Old for Buying A Shotgun and Ammunition on the Darknet,' DeepDotWeb, 11 November 2016, https://www.deepdotweb.com/2016/11/11/berlin-police-arrest-33-year-old-buying-shotgun-ammunition-darknet/.

Blockchain Alliance website, http://blockchainalliance.org/.

Buchko, Stephen, 'How Long do Bitcoin Transactions Take?' *CoinCentral,* 12 December 2017, https://coincentral.com/how-long-do-bitcoin-transfers-take/.

Burns, Janet, 'Cut Off From Big Fintech, White Nationalists Are Using Bitcoin to Raise Funds,' *Forbes*, 3 January 2018, https://www.forbes.com/sites/janetwburns/2018/01/03/cut-off-from-big-fintech-white-. supremacists-are-using-bitcoin-to-raise-funds/#49f5334633b3.

Chainalysis, 'Report: The Changing Nature of Cryptocrime,' Chainalysis blog, 18 January 2018, https://blog.chainalysis.com/crypto-crime/.

Chapman, Ben, 'Bitcoin latest: North Korea suspected of South Korean cryptocurrency exchange hack,' *Independent*, 21 December 2017, https://www.independent.co.uk/news/business/news/bitcoin-latest-updates-north-korea-south-youbit-exchange-hack-cryptocurrency-a8121781.html.

CheckPoint Software Technologies, 'December's Most Wanted Malware: Crypto-Miners Affect 55% of Businesses Worldwide,' 15 January 2018, https://globenewswire.com/news-release/2018/01/15/1289323/0/en/December-s-Most-Wanted-Malware-Crypto-Miners-Affect-55-of-Businesses-Worldwide.html.

CoinATM Radar, 'Bitcoin ATMs in Austria,' https://coinatmradar.com/countries/.

CoinMarketCap, https://coinmarketcap.com/.

Coledeway, Devin, 'How hate speech crowdfunding outfit Hatreon crept back online,' *TechCrunch*, 12 December 2017, https://techcrunch.com/2017/12/12/how-hate-speech-crowdfunding-outfit-hatreon-crept-back-online/.

Collins, Keith, 'The hackers behind WannaCry ransomware attack have finally cashed out,' *Quartz*, 3 August 2017, https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/.

Council of the EU, 'Money laundering and terrorist financing: new rules adopted,' press release, 14 May 2018, http://www.consilium.europa.eu/en/press/press-releases/ 2018/05/14/money-laundering-and-terrorist-financing-new-rules-adopted/.

Couvée, Koos, 'European Traffickers Pay Colombian Cartels Through Bitcoin ATMs : Europol Official,' *ACAMS moneylaundering.com*, 28 February 2018, https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/.

Cox, Joseph, 'Dutch Police Bust Multi-Million Dollar Bitcoin Laundering Ring,' *Vice*, 20 January 2016, https://motherboard.vice.com/en_us/article/ezpnze/dutch-police-bust-multi-million-dollar-bitcoin-laundering-ring.

Cox, Joseph, 'Is the Islamic State Using Bitcoin? That's the Last Thing We Should Worry About,' *Vice*, 25 February 2015, https://motherboard.vice.com/en_us/article/z4m8ee/is-the-islamic-state-using-bitcoin-thats-the-last-thing-we-should-worry-about.

CryptoUK, 'Principles & Code of Conduct,' CryptoUK website, https://www.cryptocurrenciesuk.info/code-of-conducts/.

CTIF-CFI, *23rd Annual Report*, Belgian Financial Intelligence Processing Unit (CTIF-CFI), 2016, http://www.ctif-cfi.be/website/images/EN/annual_report/ar2016en.pdf.

'Cyber-attack: US and UK blame North Korea for WannaCry,' *BBCNews*, 19 December 2017, http://www.bbc.co.uk/news/world-us-canada-42407488.

'Cryptocurrency exchange EXMO adds WebMoney for Payments,' *CryptoNinjas*, 22 March 2017, https://www.cryptoninjas.net/2017/03/22/cryptocurrency-exchange-emxo-adds-webmoney-for-payments/.

Cutherbertson, Anthony, 'Telegram Cancels $1.7 Billion ICO Cryptocurrency Crowdfund,' *Independent*, May 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/telegram-ico-cryptocurrency-bitcoin-ton-a8334551.html.

DANTE project website, http://www.h2020-dante.eu/

'Darknet administrator arrested over Munich massacre gun,' *Sky News*,12 June 2017, https://news.sky.com/story/darknet-administrator-arrested-over-munich-massacre-gun-10913376.

Davies, Natasha, 'Bristol man charged with theft of Bitcoin worth £1 million,' *Bristol Post*, 29 June 2017, https://www.bristolpost.co.uk/news/bristol-news/bristol-man-charged-theft-bitcoin-148215.

Dedi, Dylan, 'Is Venezuela's "Petro" Really a Cryptocurrency?' *CryptoSlate*, 7 December 2017, https://cryptoslate.com/venezuelas-petro-really-cryptocurrency/.

Del Castillo, Michael 'JP Morgan Integrates Zcash Tech Into Quorum Blockchain,' CoinDesk, 17 October 2017, see https://www.coindesk.com/jpmorgan-integrates-zcash-privacy-tech-enterprise-blockchain/.

Department of Finance and Department of Justice and Equality, *National Risk Assessment for Ireland: Money Laundering and Terrorist Financing*, Dublin, October 2016, p. 86. http://www.justice.ie/en/JELR/National_Risk_Assessment_Money_Laundering_and_Terrorist_Financing_Oct16.pdf/Files/National_Risk_Assessment_Money_Laundering_and_Terrorist_Financing_Oct16.pdf.

Dickinson, Clare, 'FCA plans global testing ground for fintech startups,' *Financial News*, 19 March 2018, https://www.fnlondon.com/articles/fca-to-set-up-global-fintech-sandbox-20180319.

Duquet, Nils (ed.), *Triggering Terror: Illicit Guns Markets and Firearms Acquisition of Terrorist Networks in Europe,* Flemish Peace Institute, Brussels, 2017, http://www.flemishpeaceinstitute.eu/sites/vlaamsvredesinstituut.eu/files/wysiwyg/boek_safte_bw_lowres.pdf.

'Dutch police instruct Slovaks to arrest Bitcoin extortionist,' *RTV*, 21 February 2018 https://enrsi.rtvs.sk/articles/news/156973/dutch-police-instruct-slovaks-to-arrest-bitcoin-extortionist.

Ebner, Julia, 'The currency of the far-right: why neo-Nazis love Bitcoin,' *The Guardian*, 24 January 2018, https://www.theguardian.com/commentisfree/2018/jan/24/bitcoin-currency-far-right-neo-nazis-cryptocurrencies.

Ellis, Claire, et. al, *Countering Lone Actor Terrorism Series No. 11: Lone Actor Terrorism, Final Report*, Royal United Services Institute, London, April 2016, https://rusi.org/sites/default/files/201604_clat_final_report.pdf.

European Banking Authority 'Warning to Consumers on Cryptocurrencies,' 12 December 2013,https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf.

European Banking Authority, *EBA Opinion on Virtual Currencies*, *4 July 2014, https*://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual +Currencies.pdf.

European Central Bank *Virtual Currency Schemes*, Frankfurt, October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

European Commission, 'Blockchain to enable medical data to be stored and transmitted safely and effectively,' Projects Story, 10 April 2018, https://ec.europa.eu/digital-single-market/en/news/blockchain-enable-medical-data-be-stored-and-transmitted-safely-and-effectively.

European Commission, *Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight against Terrorist Financing*, Strasbourg, 2 February 2016, http://eur-lex.europa.eu/legal-content/ EN/TXT/?qid =1455113825366&uri=CELEX:52016DC0050.

European Commission, 'European Commission launches the EU Blockchain Observatory and Forum,' press release, 1 February 2018, https://ec.europa.eu/digital-single-market/en/news/european-commission-launches-eu-blockchain-observatory-and-forum.

European Commission, 'FinTech: Commission takes action for a more competitive and innovative financial market,' press release, 8 March 2018, http://europa.eu/rapid/press-release_IP-18-1403_en.htm.

European Commission, Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Brussels, 26 June 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0241.

European Parliament, 'Anti-money laundering : MEPs vote to shed light on the true owners of companies,' press release,' 19 April 2018, http://www.europarl.europa.eu/news/en/press-room/20180411IPR01527/anti-money-laundering-meps-vote-to-shed-light-on-the-true-owners-of-companies.

European Parliament Resolution on Virtual Currencies, 26 May 2016, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0228 &language=EN&ring=A8-2016-0168

European Parliament, Committee on Economic and Monetary Affairs and Committee on Civil Liberties, Justice and Home Affairs Report on the proposal for a regulation of the European Parliament and of the Council on controls on cash entering or leaving the European Union and repealing Regulation (EC) No 1889/2005, European Parliament, 8 December 2017, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0394&language=EN.

European Parliament, Position of the European Parliament adopted at first reading on 19 April 2018 with a view to the adoption of Directive (EU) …/… of the European Parliament and of the Council 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*, 19 April 2018,

http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2018-0178.

European Parliamentary Research Service, 'Understanding Definitions of Terrorism,' Novem ber 2015, http://www.europarl. europa.eu/RegData/etudes/ ATAG/2015/571320/ EPRS _ATA(2015)571320_EN.pdf.

Europol, *Changes in the modus operandi of Islamic State terrorist attacks,* Europol, The Hague*, January 2016.*

Europol, *EU Terrorism Situation and Trend Report (TE-SAT)*, Europol, The Hague, 2017, https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.

Europol, 'Europol and Chainalysis Reinforce Their Cooperation in The Fight Against Cybercrime,' Europol news article, 19 February 2016, https://www.europol.europa.eu/newsroom/news/europol-and-chainalysis-reinforce-their-cooperation-in-fight-against-cybercrime.

Europol, 'Europol Hosted 4th Conference on Virtual Currencies,' Europol news article, 5 July 2017,https://www.europol.europa.eu/newsroom/news/europol-hosted-4th-conference-virtual-currencies.

Europol, *From Suspicion to Action: Converting financial intelligence into greater operational impact*, Europol, The Hague, 2017, p. 18, https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact.

Europol, 'Global Workshop for Financial Investigators on Detection, Investigation , Seizure and Confiscation of Cryptocurrencies,' Europol press release, 26 January 2018, https://www.europol.europa.eu/newsroom/news/global-workshop-for-financial-investigator detection-investigation-seizure-and-confiscation-of-cryptocurrencies.

Europol, *Internet Organised Crime Threat Assessment (IOCTA 2017),* The Hague, 2017, p.11 ,https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017;

Europol, *Internet Organised Crime Threat Assessment (IOCTA 2016)*, The Hague, 2016, p. 24, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

Europol, 'Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation, ' Europol press release, 20 July 2017, https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

Europol, 'Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain,' Europol press release, 26 March 2018. https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain.

Europol, 'Money Laundering with Digital Currencies: Working Group Established,' Europol press release, 9 September 2016, https://www.europol.europa.eu/newsroom/news/money-laundering-digital-currencies-working-group-established.

Europol, 'World's Biggest Marketplace Selling Internet Paralysing DDOS Attacks Taken Down, Europol press release, 25 April 2018, https://www.europol.europa .eu/ newsroom/

news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down.

Fanusie, Yaya J. and Robinson, Tom, *Bitcoin Laundering : An Analysis of Illicit Flows into Digital Currency Services*, Foundation for Defense of Democracies and Elliptic, 12 January 2018, p. 7 ; http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf.

Fanusie, Yaya, 'The New Frontier in Terrorist Financing,' *The Cipher Brief*, 24 August 2016, https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin.

Fanusie, Yaya, 'Terrorist Networks Eye Bitcoin as Cryptocurrency's Price Rises, *The Cipher Brief*, 21 December 2017, https://www.thecipherbrief.com/terrorist-networks-eye-bitcoin-cryptocurrencys-price-rises.

Fauvre, David; Shipe, Andrew; Vallabhaneni, Pratin; *Overcoming Obstacles to Banking Virtual Currency Business*, Coin Center Report, Washington, D.C., 2016, https://coincenter.org/wp-content/uploads/2016/05/banking-obstacles.pdf.

Financial Action Task Force, *Emerging Terrorist Finance Risks*, FATF Report, October 2015, p.36, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.

Financial Action Task Force, *Financing of Terrorism for Recruitment Purposes*, FATF Report, January 2018, p.20, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.

Financial Action Task Force, 'FATF FinTech and RegTech Initiative,' website of the FATF, http://www.fatf-gafi.org/fintech-regtech/?hf=10&b=0&s=desc(fatf_releasedate).

Financial Action Task Force, *FATF Report to G20 Finance Ministers and Central Bank Governors*, Paris, March 2018; see http://www.fatf-gafi.org/media/fatf/documents/FATF-G20-FM-CBG-March-2018.pdf

Financial Action Task Force, *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF Guidance, Paris, June 2015, http://www.fatf-gafi.org/media/ fatf/documents/reports/ Guidance -RBA-Virtual-Currencies.pdf.

Financial Action Task Force, *The Forty Recommendations of the Financial Action Task Force*, 1990, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations 1990.pdf.

Financial Action Task Force, *The FATF IX Special Recommendations,* FATF Standards, Paris, 20 October 2001 http://www.fatf-gafi.org/publications/ fatfrecommendations/ documents/ixspecialrecommendations.html.

Financial Action Task Force, *Money Laundering Using New Payment Method*s, FATF Report, Paris, October 2010, http://www.fatf-gafi.org/media/fatf/documents/reports/ML using New Payment Methods.pdf.

Financial Action Task Force, *Report on New Payment Method*s, FATF Report, Paris, 13 October 2006,http://www.fatf-gafi.org/media/fatf/documents/reports/Report on New Payment Methods.pdf.

Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FATF Report, June 2014, http://www.fatf-gafi.org/media/fatf/ documents/reports/ Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

Financial Action Task Force, 'Who we are,' website of the FATF, http://www.fatf-gafi.org/about/.

Financial Conduct Authority, 'Regulatory Sandbox,' 11 May 2015, https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf.

Financial Conduct Authority, *Regulatory sandbox lessons learned report*, Financial Conduct Authority, London, October 2017, London, pp. 10 – 11, https://www.fca.org.uk/ publication/research -and-data/regulatory-sandbox-lessons-learned-report.pdf.

Financial Crimes Enforcement Network, 'Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies,' FinCEN Guidance, 18 March 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

Financial Crimes Enforcement Network, 'Assessment of Civil and Monetary Penalty in the Matter of BTC-e a/k/a Canton Business Corporation and Alexander Vinik,' July 2017, https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment_for BTCeVinnik FINAL SignDate 07.26.17.pdf

Financial Transactions and Reports Analysis Centre of Canada, 'FINTRAC Advisory regarding Money Service Businesses dealing in Virtual Currency,' 30 July 2014, http://www.fintrac.gc.ca/new-neuf/avs/2014-07-30-eng.asp.

FundYourselfNow, '2018 The Year of Dapps,' *Medium*, 15 January 2018, https://medium.com/the-mission/2018-the-year-of-dapps-dbe108860bcb.

Gibraltar Financial Services Commission, 'Distributed Ledger Technology Regulatory Framework,' GFSC website, http://www.gfsc.gi/dlt.

'French police dismantle illegal Bitcoin exchange,' *Reuters*, 7 July 2014, https://www.reuters.com/ article/us-france-bitcoin/french-police-dismantle-illegal-bitcoin-exchange-idUSKBN0FC19220140707.

Gemini 'A Proposal for a Self-Regulatory Organisation for the Virtual Currency Industry,' Gemini website, 13 March 2018, https://gemini.com/blog/a-proposal-for-a-self-regulatory-organization-for-the-u-s-virtual-currency-industry/.

Geneva Centre for Security Policy, 'GCSP Discusses ISIS Funding with CNN Money,' 11 December 2015, https://www.gcsp.ch/News-Knowledge/Global-insight/GCSP-discusses-ISIS-funding-with-CNN-Money.

Gilbert, David, 'Criminals are racing to cash out their Bitcoin. Here's how they're doing it,' *Vice*, 19 March 2018, https://news.vice.com/en_ca/article/7xdzqa/criminals-are-racing-to-cash-out-their-bitcoin-heres-how-theyre-doing-it .

Glenny, Misha, 'Partners in crime: Why mafia groups and cybercriminals are joining forces,' World Economic Forum, 10 April 2018, https://www.weforum .org/agenda/ 2018/04/ partners-in-crime-why-mafia-groups-and-cybercriminals-are-joining-forces.

Goldman, Zachary; Maruyama, Ellie; Rosenberg, Elizabeth; Saravalle, Eduardo; Solomon-Strauss, Julia, *Terrorist Use of Virtual Currencies: Containing the Potential Threat*, Center for New American Security, Washington, 3 May 2017, https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies.

'Government to inspect 15 virtual currency exchanges awaiting certification in Japan,' *Japan Time*s, 16 February 2018, https://www.japantimes.co.jp/ news/ 2018/ 02/16/ business/ government-inspect-15-virtual-currency-exchanges-awaiting-certification-japan/#.WusT NMvzBK.

Greenberg, Andy, 'End of the Silk Road : FBI Says It's Busted the Web's Biggest Anonymous Druge Market,' *Forbes*, 2 October 2013, https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/ - 1190f0dc5b4f.

Grimes Law, 'Money Transmitter Licensing, http://www.grimeslawaz.com/money-transmitter-licensing/.

'Hacker who gave ISIS "hitlist" of US targets jailed for 20 years,' *Associated Press*, 24 September 2016, https://www.theguardian.com/world/2016/sep/24/hacker-who-gave-isis-hitlist-of-us-targets-jailed-for-20-years.

Harman, Danna, 'U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests,' *Haaretz*, 29 January 2015, https://www.haaretz.com/.premium-isis-uses-bitcoin-for-fundraising-1.5366305.

Higgins, Stan, 'Australian Digital Currency Advocates Launch Self-Regulatory Efforts,' *CoinDesk*, 1 December 2016, https://www.coindesk.com/australia-digital-currency-self-regulation/.

Higgins, Stan, 'ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide,' *CoinDesk*, 7 July 2014, https://www.coindesk.com/isis-bitcoin-donations-fund-jihadist-movements/.

Hileman, Garrick and Rauchs, Michael, *Global Cryptocurrency Benchmarking Study,* Cambridge Centre for Alternative Finance and University of Cambridge Judge Business School*,* 2017, p.10, https://www.jbs.cam.ac.uk/ fileadmin/user upload/ research/centres/ alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf.

HM Government of Gibraltar, *Proposals for a DLT Regulatory Framework*, Gibraltar, May 2017, http://www.gibraltarfinance.gi/downloads/20170508-dlt-consultation-published-version.pdf?dc %3D1494312876.

HM Treasury, *Digital currencies: response to the call for information*, London, March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment data/file/414040/digital currencies response to call for information final changes.pdf.

HM Treasury and the Home Office, *National risk assessment of money laundering and terrorist financing*, London, October 2017, https://www.gov.uk/government/uploads/system/uploads/attachment data/file/655198/National risk assessment of money laundering and terrorist financing 2017 pdf web.pdf.

Howmuch.net, 'Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?', https://howmuch.net/articles/crypto-transaction-speeds-compared

Ishida, Masahiko; Mears, Edward; Takeda, Ryutaro, 'Japan Regulatory Update on Virtual Currency Business,' DLA Piper, 29 December 2017, https://www.dlapiper.com/en/japan/insights/publications/2017/12/japan-regulatory-update- on-virtual-currency-business/.

Johnson, Tim, 'Computer hack helped feed an Islamic State Death List,' 20 July 2016, *McClatchy*, 20 July 2016,http://www.mcclatchydc.com/news/nation-world/ national/article90782637.html.

Jones, Huw, 'Gibraltar launches financial services licence for blockchain,' *Reuters,* 14 December 2017, https://uk.reuters.com/article/uk-gibraltar-regulator-blockchain/gibraltar-launches-financial-services-licence-for-blockchain-idUKKBN1E81JP.

Kaminska, Izabella, 'Growing scepticism challenges the blockchain hype,' *Financial Times*, 20 June 2017, https://www.ft.com/content/b5b1a5f2-5030-11e7-bfb8-997009366969.

Katz, Lily, 'Most Cryptocurrency Trading is Moving to Malta, at Least Legally,' *Bloomberg*, 25 April 2018, https://www.bloomberg.com/news/articles/2018-04-25/most-cryptocurrency-trading-is-moving-to-malta-at-least-legally?&utm_source=Newsletter&utmmedium=email &utm_content=Nasdaq%3A+the+next+killer+crypto+exchange%3F&utm_campaign=Weekly+Brief+5%2F2.

Keirns, Garrett, 'Danish Police Claim Breakthrough in Bitcoin Breakthrough in Bitcoin Tracking,' *CoinDesk*, 22 February 2017, https://www.coindesk.com/danish-police-claim-breakthrough-bitcoin-tracking/.

Kelso, C. Edward, 'Michigan Localbitcoins User Charged with Unlicensed Money Transmitting,' *Bitcoin.com*, 29 October 2017; see: https://news.bitcoin.com/localbitcoins-user-charged-with-unlicensed-money-transmitting/.

Kharpal, Arjun, 'Cryptocurrency start-up Confido disappears with $375,000 from an ICO, and nobody can find the founders,' *CNBC*, 21 November 2017, https://www.cnbc.com/2017/11/21/confido-ico-exit-scam-founders-run-away-with-375k.html.

Larratt, Phillip; Taylor, Paul; Wall, David S.; Naqvi, Syed; Shillito, Matthew; Stokes, Rob, *Policing Bitcoin : Investigating, Evidencing and Prosecuting Crimes Involving Bitcoin*, N8 Policing Research Partnership, 13 July 2017, http://n8prp.org.uk/wp-content/uploads/2017/08/N8-Cryptocurrency-Report.pdf.

Letter from France and Germany to the G20 Ministers, 7 February 2018, https://www.politico.eu/wp-content/uploads/2018/02/G20-Letter-on-crypto-assets-tokens.pdf.

Letts, Stephen, 'Cryptocurrencies get AUSTRAC anti-money laundering and terrorism funding scrutiny,' *ABC,* 11 April 2016, http://www.abc.net.au/news/2018-04-11/cryptocurrencies-subject-to-anti-money-laundering-and-terrorism/9640642.

Lopp, Jameson, 'Bitcoin and the Rise of the Cypherpunks,' *CoinDesk*, 9 April 2016, https://www.coindesk.com/the-rise-of-the-cypherpunks/.

Madiera, Antonio, 'What is a Decentralised Exchange?' *CryptoCompar*e, 28 September 2017, https://www.cryptocompare.com/exchanges/guides/what-is-a-decentralized-exchange/.

Madiera, Antonio, 'What Are Atomic Swaps?' *CryptoCompare*, 5 April 2018, https://www.cryptocompare.com/coins/guides/what-are-atomic-swaps/.

Malik, Nikita, *Terror in the Dark: How Terrorists Use Encryption, the Dark Net, and Cryptocurrencies,* The Henry Jackson Society, London, April 2018, p. 42, *http*://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf.

Möser, Malte; Soska, Kyle; Hellman, Ethan; Lee, Kevin; Heffan, Henry; Srivastava, Shastvat; Hogan, Kyle; Hennessey, Jason; Miller, Andrew; Narayanan, Arvind; and Christin, Nicolas, 'An Empirical Analysis of Traceability in the Monero Blockchain,' to appear in Privacy Enhancing Technologies Symposium (PETS), 2017, p. 1, https://arxiv.org/pdf/1704.04299.pdf.

Maxey, Levi, 'Terrorists Stalk the Dark Web for Deadlier Weaponry,' *The Cipher Brief*, 17 January 2018, https://www.thecipherbrief.com/terrorists-stalk-dark-web-deadlier-weaponry.

Milano, Annaliese, 'Gibraltar Will Take Market-Driven Approach to ICOs,' *CoinDesk*, 21 February 2018, https://www.coindesk.com/gibraltar-take-market-driven-approach-ico-rules-officials-say/.

Ministere des Finances et des Comptes Publics, *Regulating Virtual Currencies: Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering*, Virtual Currencies Working Group Report, June 2014, https://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf.

Moore, Daniel and Rid, Thomas, Cryptopolitik and the Darknet, *Survival*, 58:1, pp. 7 – 38, February-March2016,https://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085? needAccess=true.

Mullany, Gerry, 'China Restricts Banks' Use of Bitcoin,' *New York Times,* 5 December 2013, https://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html?hpw&rref=business&_r=0.

Nakamoto, Satoshi, 'Bitcoin: A Peer-to-Peer Electronic Cash System', https:// bitcoin.org/bitcoin .pdf.

Namblampurath, Rahul, 'Japan's FSA Terminates License of Two Bitcoin Exchanges Citing Irregularities,' *BTCManager.com*, 11 March 2018, https://btcmanager.com/japans-fsa-terminates-license-two-bitcoin-exchanges-citing-irregularities/.

National Crime Agency, 'Man tried to buy hand grenades on the dark web with Bitcoin,' 14 December 2017,' National Crime Agency press release, 14 December 2017, http://www.nationalcrimeagency.gov.uk/news/1259-man-tried-to-buy-hand-grenades-on-the-dark-web-with-bitcoins.

National Cyber Security Centre and the National Crime Agency, *The cyber threat to UK business*, London, 2017-2018 Report, p.25, https:// www.ncsc.gov.uk/ file/3077/ download?token=Z5h53HP-.

Neumann, Richard and Basra, Rajan, *Crime as Jihad: Developments in the Crime-Terror Nexus in Europe*, *CTC Sentinel*, October 2017, Volume 10, Issue 9, Combatting Terrorism Center, https://ctc.usma.edu/crime-as-jihad-developments-in-the-crime-terror-nexus-in-europe/.

Osborne, Charlie, 'PyCryptoMiner enslaves your PC to mine Monero,' *ZDNe*t, 4 January 2018, https://www.zdnet.com/article/pycryptominer-enslaves-your-pc-to-mine-monero/.

Parliamentary Office for Financial Services, Digital Economy and Innovation, Office of the Prime Minister, *Malta: A Leader in DLT Regulation*, February 2018, p.11, https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF.

Pearson, Jordan, 'Can the Bitcoin Community Stop Neo-Nazis From Using the Digital Currency?' *Vice*, 18 August 2017, https://motherboard.vice.com/en_us/article/vbbb5y/can-the-bitcoin-community-stop-neo-nazis-from-using-the-digital-currency.

Peaster, William M., 'What Are Atomic Swaps? Our Guide to a Revolution in Decentralization,' Blockonomi, 10 January 2018, https://blockonomi.com/atomic-swaps/.

Peterson, Becky, 'The SEC charges a third Centra cryptocurrency "mastermind" with fraud over its $32 million ICO,' *Business Insider*, 20 April 2018, http://uk.businessinsider.com/sec-charges-third-centra-crypto-founder-with-fraud-2018-4.

Project PROTON, 'About,' Project PROTON website, https://www.projectproton.eu/about/.

Rauchs, Michael, 'Cryptocurrencies won't be going away any time soon,' *Oxbridge Business Review*, April 2018, https://www.oxbridgebr.org/cryptocurrencies-are-here-to-stay.

Redman, Jamie, 'Chainalysis Raises $16Mn – Plans to Monitor Multiple Blockchains,' *Bitcion.*com, 6 April 2018; see: https://news.bitcoin.com/chainalysis-raises-16mn-plans-to-monitor-multiple-blockchains/.

Reitano, Tuesday; Clarke, Colin; Adal, Laura, *Examining the Nexus Between Organised Crime and Terrorism*, CT Morse, 2017, https://icct.nl/wp-content/uploads/2017/04/OC-Terror-Nexus-Final.pdf.

Rooney, Kate, 'India's central bank bans financial firms from dealing with cryptocurrency, '*CNBC*, 5 April 2018, https://www.cnbc.com/2018/04/05/indias-central-bank-bans-financial-firms-from-dealing-with-cryptocurrency.html

King, Ross Dr., 'TITANIUM: Early Research and Outlook,' 21st European Police Congress, Berlin, 2018, http://www.europaeischer-polizeikongress.de/wp-content/uploads/2018/03/King_2018.pdf.pdf.

Silva, Shiroma, 'Criminals hide "billions" in crypto-cash – Europol,' *BBC News*, 12 February 2018, http://www.bbc.co.uk/news/technology-43025787.

Soeriaatmadja, Wahyudi, 'Militant Bahrun Naim used PayPal, bitcoin to transfer funds for terror attacks in Indonesia,' *Straights Times*, 9 January 2017, http://www.straitstimes.com/asia/se-asia/militant-bahrun-naim-used-paypal-bitcoin-to-transfer-funds-for-terror-attacks-in.

'South Africa's central bank mulls cryptocurrency self-regulation,' *Finextra*, 4 April 2014, https://www.finextra.com/newsarticle/31907/south-africas-central-bank-mulls-cryptocurrency-regulations.

Staufenberg, Jess, 'Isis shows off currency with gold dinar coin worth £91 each – in quest for "world domination",' *Independen*t, 31 August 2015, https://www.independent. co.uk /news/ world/middle-east/isis-shows-off-new-currency-with-gold-dinar-coins-worth-91-each-in-quest-for-world-domination-10480121.html.

Suberg, William, 'Bank Complete: China Blocks Foreign Crypto Exchanges To Counter Financial Risks,' 5 February 2018, https://cointelegraph.com/news/ban-complete-china-blocks-foreign-crypto-exchanges-to-counter-financial-risks.

Suberg, William, 'Bitcoin Exchange ShapeShift Helps Police as WannaCry Attacker Converts to Monero,' CoinTelegraph, 4 August 2017, https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero.

Swiss Financial Market Supervisory Authority, 'Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs),' 16 February 2018, https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.

Timberg, Craig, 'Bitcoin's boom is a boon for extremist groups,' *Washington Post*, 26 December 2017, https://www.washingtonpost.com/business/technology/bitcoins-boom-is-a-boon-for-extremist-groups/2017/12/26/9ca9c124-e59b-11e7-833f-155031558ff4_story.html?noredirect=on&utm_term=.ce1091ce7715

TITANIUM Project, 'Project to prevent criminal use of the dark web and cryptocurrencies launched by international consortium,' 19 May 2017, https://www.titanium-project. eu/news/articles/titanium-project/.

Torpey, Kyle, 'AlphaBay Comments on Bitcoin Congestion, Monero Adoption and Zcash Possibilities,' Bitcoin Magazine, 21 December 2016, https://bitcoinmagazine.com/articles/alphabay-comments-on-bitcoin-congestion-monero-adoption-and-zcash-possibilities-1482345512/.

Town, Sam, 'Bitcoin vs. WoW Gold: Why Aren't Cryptos Treated Like In-Game Currencies?' *Cryptoslat*e, 19 March 2018, https://cryptoslate.com/crypto-in-game-currencies/.

'True scale of Bitcoin extortion revealed,' MIT Technology Review, 19 April 2018, https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/.

'The Secrets of Online Money Laundering,' MIT Technology Review, 18 October 2013, https://www.technologyreview.com/s/520501/the-secrets-of-online-money-laundering/.

'UK: Police Seize Bitcoin Worth £300,000 in Money Laundering Investigation,' KYC360.com, 9 January 2018, https://kyc360.com/news/uk-police-seize-bitcoin-worth-300000-money-laundering-investigation/.

United Nations Security Council, Resolution 2253 (2015), 17 December 2015.

United States Department of Justice, 'Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of Dollars,' Justice News, 6 May 2016,https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars.

United States Department of Justice, 'Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists, 14 December 2017, https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists.

United States Department of Justice, 'Virginia Teen Pleads Guilty to Providing Material Support to ISIS,' Justice News, 11 June, 2015, https://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil.

US Department of State, 'Terrorist Designation of the Mujahidin Shura Council in the Environs of Jerusalem (MSC),'US Department of State website, Terrorism Designations Press Releases 19 August 2014, https://www.state.gov/j/ct/rls/other/des/266549.htm.

United States Department of the Treasury, 'U.S. Department of the Treasury Under Secretary Sigal Mandelker, Speech before the Securities Industry and Financial Markets Association Anti-Money Laundering & Financial Crimes Conference,' Statements & Remarks, 13 February 2018, https://home.treasury.gov/news/press-release/sm0286.

Varruciu, Massimiliano, 'Bitcoin and remittance, where are we?' *Fintastico*, 6 July 2017, https://www.fintastico.com/blog/bitcoin-and-remittance-where-are-we/.

VIRTCRIME Project, 'Forensic Methods and Solutions for The Analysis of Criminal Transactions in Post-Bitcoin Cryptocurrencies,' Austrian Institute of Technology, https://www.ait.ac.at/en/research-fields/data-science/projects/virtcrime/.

Voge, Cady, 'Where Could Bitcoin Succeed as a Currency? In a Failed State,' *Wired*, 22 March 2018, https://www.wired.com/story/where-could-bitcoin-succeed-as-a-currency-in-a-failed-state/.

Vorick, David, 'Ensuring Bitcoin Fungibility in 2017 (And Beyond),' *CoinDesk*, 28 December 2017, https://www.coindesk.com/ensuring-bitcoin-fungibility-in-2017-and-beyond/.

Wada Takahiko and Wilson, Thomas, 'Japan's cryptocurrency exchanges to set up self-regulatory body,' *Reuters,* 2 March 2018, https://www.reuters.com/article/us-crypto-currencies-japan/japans-cryptocurrency-exchanges-to-set-up-self-regulatory-body-idUSKCN1GE037.

WebMoney, 'About the System,' WebMoney website, https://www.wmtransfer.com/eng/information/short/index.shtml.

'What are zkSNARKS? Zero Knowledge Proofs Simplified,' *Investing.com*, 6 April 2016, https://www.investing.com/news/cryptocurrency-news/what-are-zksnarks-zero-knowledge-proofs-simplified-1382453.

Wong, Joon Ian, 'China's bitcoin investors are flocking to one of the last places to trade,' *Quartz*, 19 September 2017, https://qz.com/1081161/bitcoin-btc-investors-in-china-are-flocking-to-peer-to-peer-platform-localbitcoins-after-the-main-exchanges-shut-down/.

Zhao, Wolfie, 'Japan Could Have More than 3 Million Crypto Trades,' CoinDesk, 10 April 2018, https://www.coindesk.com/3-5-million-traders-japan-releases-domestic-cryptocurrency -statistics/.

ANNEX I - RELEVANT LEGAL AND REGULATORY MECHANISMS

FATF Guidance

1.Financial Action Task Force, *Guidance for a Risk-Based Approach: Virtual Currencies*, June 2015

http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies pdf .

2. Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 2014

http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and- potential-aml-cft-risks.pdf.

EU 5AMLD

1. European Parliament, Position of the European Parliament adopted at first reading on 19 April 2018 with a view to the adoption of Directive (EU) …/… of the European Parliament and of the Council 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*, 19 April 2018.

http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA- 2018-0178.

EU Reports, Research Projects and Risk Assessments

1. European Banking Authority, *EBA Opinion on Virtual Currencies*, 4 July 2014

https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+ Virtual+Currencies.pdf.

European Banking Authority 'Warning to Consumers on Cryptocurrencies', 12 December 2013

https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf.

2. European Central Bank, *Virtual Currency Schemes*, October 2012

https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

3. European Commission, Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Brussels, 26 June 2017

http://europeanmemoranda.cabinetoffice.gov.uk/files/2017/07/10977-17-ADD-2.pdf.

4. European Parliament, Committee on Economic and Monetary Affairs and Committee on Civil Liberties, Justice and Home Affairs *Report on the proposal for a regulation of the European Parliament and of the Council on controls on cash entering or leaving the European Union and repealing Regulation (EC) No 1889/2005,* European Parliament*, 8* December 2017

http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0394&language=EN.

5. European Parliament Resolution on Virtual Currencies, 26 May 2016

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0228 +0+DOC+XML+V0//EN

6. DANTE Project

http://www.h2020-dante.eu/

7 Project PROTON

https://www.projectproton.eu/about/.

8 TITANIUM Project

https://www.titanium-project.eu/news/articles/titanium-project/.

Member State Reports, Research Projects and Risks Assessments

1. Belgian Financial Intelligence Processing Unit (CTIF-CFI), *23rd Annual Report*, 2016

http://www.ctif-cfi.be/website/images/EN/annual_report/ar2016en.pdf.

2. Department of Finance and Department of Justice and Equality, *National Risk Assessment for Ireland: Money Laundering and Terrorist Financing*, October 2016

http://www.justice.ie/en/JELR/National_Risk_Assessment_Money_Laundering_and_Terrorist_Financing_Oct16.pdf/Files/National_Risk_Assessment_Money_Laundering_and_Terrorist_Financing_Oct16.pdf.

3. Financial Conduct Authority (UK), *Regulatory sandbox lessons learned report*, October 2017

https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-_report.pdf.

4.Gibraltar Financial Services Commission, 'Distributed Ledger Technology Regulatory Framework', January 2018

http://www.gfsc.gi/dlt.

5. HM Government of Gibraltar, *Proposals for a DLT Regulatory Framework*, May 2017

http://www.gibraltarfinance.gi/downloads/20170508-dlt-consultation-published-version.pdf?dc_%3D1494312876.

6. HM Treasury (UK), *Digital currencies: response to the call for information*, May 2015

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf

7. HM Treasury and the Home Office (UK), *National risk assessment of money laundering and terrorist financing*, October 2017

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.

8.Ministere des Finances et des Comptes Publics, *Regulating Virtual Currencies: Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering*, Virtual Currencies Working Group Report, June 2014

https://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf

9. N8 Policing Research Partnership, I*nvestigating, Evidencing and Prosecuting Crimes Involving Bitcoin*, 13 July 2017

http://n8prp.org.uk/wp-content/uploads/2017/08/N8-Cryptocurrency-Report.pdf

10. Parliamentary Office for Financial Services, Digital Economy and Innovation, Office of the Prime Minister, *Malta: A Leader in DLT Regulation*, February 2018

https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF

11. VIRTCRIME Project, Austrian Institute of Technology

https://www.ait.ac.at/en/research-fields/data-science/projects/virtcrime/

Non-EU Measures

1. Australian Transaction Reports and Analysis Centre, 'Digital Currency Exchange Registration Requirements', April 2018

http://www.austrac.gov.au/chapter-5-dce-registration-requirements.

2. Swiss Financial Market Supervisory Authority, 'Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)', February 2018

https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

3.Financial Transactions and Reports Analysis Centre of Canada, 'FINTRAC Advisory regarding Money Service Businesses dealing in Virtual Currency', 30 July 2014

http://www.fintrac.gc.ca/new-neuf/avs/2014-07-30-eng.asp

4. Japan Financial Services Agency, 'Details of Screening for New Registration Application as Virtual Currency Exchange Provider', September 2018

https://www.fsa.go.jp/en/news/2017/20170930-1/02.pdf

5. US Financial Crimes Enforcement Network, 'Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies', 18 March 2018

https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

ANNEX II - VALUES OF MAJOR CRYPTOCURRENCIES

Table 1: Values of Major Cryptocurrencies

Cryptocurrency	USD Value as of 8 May 2018
Bitcoin	USD 160 billion
Ethereum	USD 75 billion
Ripple	USD 32 billion
Bitcoin Cash	USD 28 billion
EOS	USD 15 billion
Litecoin	USD 9 billion
Cardano	USD 8 billion
Stellar	USD 7.4 billion
IOTA	USD 6.6 billion
TRON	USD 5.5 billion
NEO	USD 5.1 billion
Dash	USD 3.7 billion
Monero	USD 3.6 billion
Ethereum Classic	USD 2.3 billion
Verge	USD 1.1 billion
Zcash	USD 1.1 billion
Decred	USD 619 million

Source: CoinMarketCap website (https://coinmarketcap.com/)

ANNEX III - SIGNIFICANT LAW ENFORCEMENT ACTIONS

Table 2: Significant Law Enforcement Actions

Date	EU Agencies and Countries Involved	Summary of Action
May 2018	UK	Police arrested and confiscated Bitcoin worth GBP 500,000 from a hacker who had obtained the proceeds by selling stolen identity and account information on the Dark Web.[218]
April 2018	Europol, the Netherlands, UK	Administrators and users of the DDOS marketplace webstresser.org, which used cryptocurrencies, were arrested across the UK, Croatia, Serbia, Canada, the Netherlands, Italy, Spain, Hong Kong and Australia. The investigation, which was supported by Europol, led to the seizure of related infrastructure.[219]
April 2018	Europol, Spain, Finland	Spanish authorities, with support from Europol and Finnish law enforcement, arrested 11 individuals accused of laundering funds using cryptocurrencies on behalf of OCGs. The launderers assisted narcotics traffickers in converting the cash proceeds of drug sales in Europe into Bitcoin, before converting it into Columbian pesos. The conversion occurred at a Finnish cryptocurrency exchange. The group laundered more than EUR 8 million.[220]
April 2018	UK	UK authorities confiscated approximately GBP 50,000 worth of Bitcoin from a fraudster who used VCs to launder the proceeds of fraud. The individual in question stole PayPal account details from his employer, used the funds to purchase Linden Dollars, which he then converted into Bitcoin.[221]
March 2018	Europol, Spain, Romania	The Spanish National Police arrested the head of a cybercriminal organisation that developed the Cobalt and Carbanak malware strains used to steal more than EUR 1 billion from over 100 financial institutions. The proceeds of these thefts were laundered using cryptocurrencies, including through cryptocurrency pre-paid cards. Europol's EC3 unit

[218] Davenport, Justin and Tristan Kirk, 'Moment undercover cops pounce on £500k master Bitcoin hacker Grant West as he accessed dark web on board train,' Evening Standard, 3 May 2018.
[219] See, Europol, 'World's Biggest Marketplace Selling Internet Paralysing DDOS Attacks Taken Down.'
[220] 'Illicit Network Used Cryptocurrencies and Credit Cards to Launder More than EUR 8 Million From Drug Trafficking,' Europol Press Release, 9 April 2018 ; see : https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking.
[221] Cheyenne Roundtree, 'Cyber criminal, 23, becomes one of first in Britain to have his Bitcoin stash worth £50,000 by police after elaborate fraud using work's IT system,' Daily Mail, 4 April 2018 ; see
.

		supported the investigation, which was also coordinated with LEAs in Romania and the US.[222]
February 2018	The Netherlands, Slovakia	Acting on a European Arrest Warrant, Slovak authorities arrested an individual accused of seeking Bitcoin extortion payments. The individual is to be extradited and tried in the Netherlands.[223]
January 2018	United Kingdom	Authorities in Lancashire, UK, seized £300,000 in Bitcoin from an individual involved in money laundering.[224]
December 2017	United Kingdom	UK authorities secured a conviction against an individual who attempted to purchase hand grenades on Alphabay using Bitcoin.[225]
July 2017	Europol, the Netherlands	In an action supported by Europol, Dutch police and law enforcement in the US shut down Alphabay and Hansa, two of the largest Dark Web marketplaces. The action lead to the detection and seizure of millions of pounds' worth of cryptocurrencies. Servers used by the marketplaces' administrators were seized, and law enforcement obtained information on tens of thousands of users.[226]
June 2017	United Kingdom	An individual was arrested in Bristol, UK, for the alleged theft of £1 in Bitcoin.[227]
November 2016	Germany	An individual was arrested for using Bitcoin worth EUR 2,000 to purchase a shotgun on the Dark Web.[228]
January 2016	The Netherlands	In January 2019, Dutch police arrested 10 individuals who used Bitcoin to launder EUR 10 to 20 million.[229]
July 2014	France	French authorities seized Bitcoin worth approximately EUR 200,000 after arresting

[222] Europol, 'Masterminded Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain.'
[223] 'Dutch police instruct Slovaks to arrest Bitcoin extortionist,' *RTV*, 21 February 2018 https://enrsi.rtvs.sk/articles/news/156973/dutch-police-instruct-slovaks-to-arrest-bitcoin-extortionist.
[224] 'UK: Police Seize Bitcoin Worth £300,000 in Money Laundering Investigation,' KYC360.com, 9 January 2018, https://kyc360.com/news/uk-police-seize-bitcoin-worth-300000-money-laundering-investigation/.
[225] National Crime Agency, 'Man tried to buy hand grenades on the dark web with Bitcoin,' 14 December 2017,' National Crime Agency press release, 14 December 2017, http://www.nationalcrimeagency.gov.uk/news/1259-man-tried-to-buy-hand-grenades-on-the-dark-web-with-bitcoins.
[226] Europol, 'Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation,' Europol press release, 20 July 2017, https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.
[227] Davies, Natasha, 'Bristol man charged with theft of Bitcoin worth £1 million,' *Bristol Post*, 29 June 2017, https://www.bristolpost.co.uk/news/bristol-news/bristol-man-charged-theft-bitcoin-148215.
[228] 'Berlin Police Arrest 33-Year Old for Buying A Shotgun and Ammunition on the Darknet,' DeepDotWeb, 11 November 2016, https://www.deepdotweb.com/2016/11/11/berlin-police-arrest-33-year-old-buying-shotgun-ammunition-darknet/.
[229] Cox, Joseph, 'Dutch Police Bust Multi-Million Dollar Bitcoin Laundering Ring,' *Vice*, 20 January 2016, https://motherboard.vice.com/en_us/article/ezpnze/dutch-police-bust-multi-million-dollar-bitcoin-laundering-ring.

		individuals running an illegal online gambling website.[230]

[230] 'French police dismantle illegal Bitcoin exchange,' *Reuters*, 7 July 2014, https://www.reuters.com/article/us-france-bitcoin/french-police-dismantle-illegal-bitcoin-exchange-idUSKBN0FC19220140707.

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the TERR Committee, explores the terrorist financing (TF) risks of virtual currencies (VCs), including cryptocurrencies such as Bitcoin. It describes the features of VCs that present TF risks, and reviews the open source literature on terrorist use of virtual currencies to understand the current state and likely future manifestation of the risk. It then reviews the regulatory and law enforcement response in the EU and beyond, assessing the effectiveness of measures taken to date. Finally, it provides recommendations for EU policymakers and other relevant stakeholders for ensuring the TF risks of VCs are adequately mitigated.

Print ISBN 978-92-846-3090-5| doi: 10.2861/110107| QA-03-18-004-EN-C
PDF ISBN 978-92-846-3091-2|doi: 10.2861/955161| QA-03-18-004-EN-N