The Money Laundering and Terrorist Financing Risks of New & Disruptive Technologies: A Futures-oriented Scoping Review

Abstract

New and disruptive technologies, including cryptocurrencies and new payment methods, are revolutionising the way people engage with finance. Although they provide significant benefits to consumers, they are also inadvertently creating new money laundering and terrorist financing risks. This paper examines the risks that are, or are predicted to be, prevalent in three technology sectors – distributed ledger technologies, new payment methods and financial technologies (FinTech), through a systematic scoping review process. Specifically, the paper identifies enablers of both crimes, the precise criminal methods they might facilitate, at-risk stakeholders (of exploitation and/or complicity) and risk characteristics. The study involves systematic scoping reviews of the academic and futures literatures as well as a consultation exercise with experts to assess the likely veracity of the findings. In addition to identifying an array of specific risks, we identify six underlying trends that facilitate them. We discuss these, their policy implications, future directions for research and their benefit for conducting risk assessments to assess forthcoming technological developments.

Keywords: money laundering, terrorist financing, blockchain, cryptocurrencies, new payment methods, FinTech

Introduction

On 18 March 2018, details emerged about how *Uber's* ride-hailing application was being abused by criminals to produce 'ghost rides' to launder money (Teicher 2018a). The same year, it transpired that a 2017 Chinese ban on cryptocurrencies, initiated due to money laundering concerns, had backfired, with Chinese engagement in cryptocurrency services increasing by 231% throughout the next year (O'Brien 2018; Rapoza 2017). More recently in 2019, German anti-money laundering authorities criticised a prominent digital-only bank for their transaction monitoring backlog, arising from their rapid rise in customers (Megaw 2019).

These revelations may initially seem unrelated. However, they all signify ways in which new and disruptive technologies are creating criminal opportunities for disguising illicit funds. This process, namely money laundering (ML), also shares similarities with methods used for terrorist financing (TF). For both crimes, offenders have long utilised several different techniques, exploiting vulnerabilities across a large array of financial services, to conduct illicit transactions without being detected. Traditional methods to bypass detection include mingling illicit cash through cash-intensive businesses to declare it as legitimate income, converting proceeds into foreign currency or funnelling cash through illicit accounts, casinos, securities or shell companies, amongst others (He 2010). All these methods are now being enhanced by the widespread adoption of new and disruptive technologies.

New and disruptive technologies

Disruptive technologies refer to innovations that substantially alter existing markets and operations due to vastly superior attributes (Smith 2020). The examples with which this article began highlight the risks posed by three particular strands of technologies, namely distributed ledger technologies (cryptocurrencies), new payment methods and financial technology (FinTech).

Distributed ledger technologies (DLT) provide a digital, decentralised ledger platform open for a specific or limitless number of users (Christie 2018). Unlike normal ledgers, however, they are not governed by a central authority such as a government or bank (Barone and Masciandaro 2019; Choo 2015). Instead, the ledger (and copies of it) is maintained by its users, acting semi-anonymously through consensus mechanisms to authenticate and add new transactions using cryptographic methods (Choo 2015). Blockchain is perhaps the most prominent example of a distributed ledger, where users can trade cryptocurrencies (digital tokens representing value) with each other (Campbell-Verduyn 2018). DLT is also evolving further to allow the trade of other forms of assets, represented digitally through associated crypto-tokens, without mediators or central authority oversight (Tapscott and Tapscott 2016).

New payment methods (NPMs), which represent modern ways of completing financial transactions, have long been regarded ML/TF risks (FATF 2006a), particularly in developing countries lacking extensive financial services or regulation compliance (Buku and Meredith 2012; Vlcek 2011). NPMs include mobile money transfers and pre-paid cards, which allow users to store, transfer and withdraw funds without needing a bank account. Other NPMs, such as mobile payment apps with in-app payment processing capabilities mentioned above (e.g. *Uber*), are newer developments that diversify possibilities available to criminals.

Financial services, meanwhile, are currently the main focus of 'anti-money laundering' (AML) and 'countering the financing of terrorism' (CFT) regulations. These require financial institutions to conduct customer due diligence (CDD) on clients to understand 'normal' transaction patterns, allowing suspicious transactions to be detected and reported to designated national financial intelligence units (Mugarura 2014). However, FinTech innovation is rapidly digitising traditional services, allowing increasingly remote and anonymous access to online banking, fundraising and securities trading. Exemplifying their risks, the United Kingdom has identified a 'significant growth' of suspicious activity reports filed between 2017 and 2020 by such services (HM Treasury and Home Office 2020, 55), though this could be due to better employee training or a pre-emptive drive for compliance with forthcoming regulations. This paper defines FinTech as technology-enabled financial services and products, specifically distinct from non-bank payment technologies (covered in NPMs) and blockchain technology (covered in DLT). Other research may adopt different definitions.

Research objectives

Since the 1990s, authorities have worryingly fallen behind the advances of the modern-day criminal (Ekblom 1997), who have devised innovative ways to bypass AML/CFT regulations. There exists an evident need to further understand the ML/TF risks of new and disruptive technologies to develop better pre-emptive countermeasures. In addition to technological changes, the Covid-19 pandemic serves as a reminder that the convergence of multiple trends can accelerate change. For example, the pandemic has caused a decline in physical cash use and a convergence to risk-prone digital payments mediums (Sheluchin 2020). Online crime, in particular Covid-19-related fraud, has subsequently increased (FATF 2020; Nolte et al. 2021; EUROPOL 2021), emphasising the urgency associated with understanding the new digital laundering trends that consequently arise.

In response, this paper presents a scoping review to gain an understanding of the three technology categories described above (DLT, NPMs, and FinTech) and their future ML/TF risks. It then assesses findings for common deficiencies and underlying trends of innovation and criminal abuse. These are intended to form the basis of risk assessments that assess future developments for their ML/TF risk, which can assist in futureproofing them during development by identifying the specific 'vectors' through which developing technologies can exhibit ML/TF deficiencies. To ensure that the review focus is sufficiently futures-oriented, this paper adopts a modified methodology, discussed next. Hence, besides the ML/TF focus, this review exercise also explores possible ways of improving the horizon scanning utility of scoping reviews as a second research outcome.

METHODS

Scoping reviews are used to review existing literature or evidence on a given subject (Grant and Booth 2009). Their aims, which are often less specific than systematic reviews, can include exploring evidence in an emerging field, mapping existing concepts to categories, uncovering new trends, identifying gaps in existing literature and/or summarising evidence for policymakers (Arksey and O'Malley 2005; Peters et al. 2015).

This review complies with the PRISMA-ScR checklist (see supplementary material), a standardised framework designed to ensure quality and reproducible results (Tricco et al. 2018), with three additional modifications, namely:

1. The use of two distinct databases to source academic and futures-oriented publications
2. A quality assessment of publications to account for the diversity of material consulted
3. An expert verification of the review outcomes

The aim of these modifications was to maximise the futures-oriented focus of the paper, to contrast the sorts of insights provided by material identified using the two databases, and to assess (given the often speculatory nature of the material consulted) the extent to which field experts concurred with the findings of our review. The application of these considerations, bar the expert verification (which is explained after the results of the scoping review), are discussed throughout the methodology below.

Identifying relevant studies

The choice of two distinct databases (academic and futures-oriented) was based on the findings of a study by Hiltunen (2008, 30), who surveyed 65 futurists (researchers or consultants in futures-oriented subjects) and found that more than half considered 'popular science and economic magazines' and reports of research institutes as good sources for 'weak signals'. Weak signals are initial indicators of potentially significant forthcoming change not necessarily present in peer-reviewed empirical journal articles (Dufva 2019).

The academic database chosen for this review was ProQuest Central (PQC). This is the largest multidisciplinary academic full-text database available, incorporating 47 specific databases and 175 topic areas. These include region-specific databases and subject-specific ones, ranging from medicine to social sciences. Journal articles, books, working papers, pre-prints and conference papers/proceedings are indexed by PQC and were included in our search criteria.

The futures-oriented database chosen was *Shaping Tomorrow* (ST), a strategic foresight platform which uses 'semantic and big data analysis, taxonomies [and] natural language processing' to search news and other media. ST scans 15,000 futures-oriented news and expert sources daily (Shaping Tomorrow, n.d.).

Each search was run separately for ML/TF on both databases (for a total of four searches). An initial search was completed for the period 1 January 2013 to 15 January 2020 (ST produced no meaningful results before 2013). A follow-up search was subsequently conducted to cover the period 15 January to 31 December 2020. In total, PQC produced 272 and 76 results for ML and TF respectively, while ST produced 220 and 48 respectively. The search strings used and the results per search are shown in appendix 1.

Study selection

Collected studies were subject to a three-phase hierarchical exclusion process which involved (A) excluding miscategorised publications, (B) excluding irrelevant PQC publications based on their abstract and (C) excluding irrelevant publications based on a full text review. Phase B could not be applied to ST publications as the vast majority of them did not have abstracts. The process is shown in more detail in appendix 2.

Since ML/TF had separate search queries, some publications were identified by and relevant to both searches. However, some publications – 10 identified using PQC and 16 identified using ST – retrieved for one crime only were deemed relevant to (and included in the analyses for) both after full-text analyses. Therefore, the eventual number of PQC publications analysed for ML and TF were 44 and 24, respectively, while the number of ST publications increased to 49 and 24 respectively.

Quality assessment

A quality assessment is not required for scoping reviews (Arksey and O'Malley 2005). However, the diversity of publication types arising from consulting two distinct databases, ranging in this case from governmental reports to unedited blog posts, creates disparity in the quality of the consulted evidence. A general assessment of the state of the art is therefore useful for acknowledging this and determining the level and reliability of intelligence obtained from them.

To do this, publications were scored (out of 4) for *neutrality, evidence, relevance* and *clarity*. *Neutrality* concerned the level of external review to which publications were subjected. *Evidence* concerned the validity and originality of evidence on which publications based their findings. *Relevance* concerned the quantity of relevant information that was coded from publications, while *clarity* focused more on the quality – namely, the extent to which the ML/TF implications of findings were explicitly discussed. The specific criteria is shown in table A2, appendix 3.

The formation of this protocol was an iterative process, developed to assess the types of publication reviewed here specifically. Before scoring, a sample (10% across databases) of publications were scored by three raters to ensure that the assessment criteria were clear and illustrative, with a second round of scoring after initial adjustments. High levels of inter-rater reliability were achieved after the second round (ranging from κ=0.6807–0.8438, see appendix 2 table A3).

Extracting data

Data extraction was conducted by the lead author. Publication author, date, type and topic were extracted for both databases (PQC and ST). Study methodology was retrieved for PQC publications only, while publication source (such as 'news site' or 'international organisation') was coded for ST only. This data is available in the supplementary dataset; publication type data is also presented in figure 1 as a summary, to showcase the sources from which the results (and the subsequent discussion) derive.

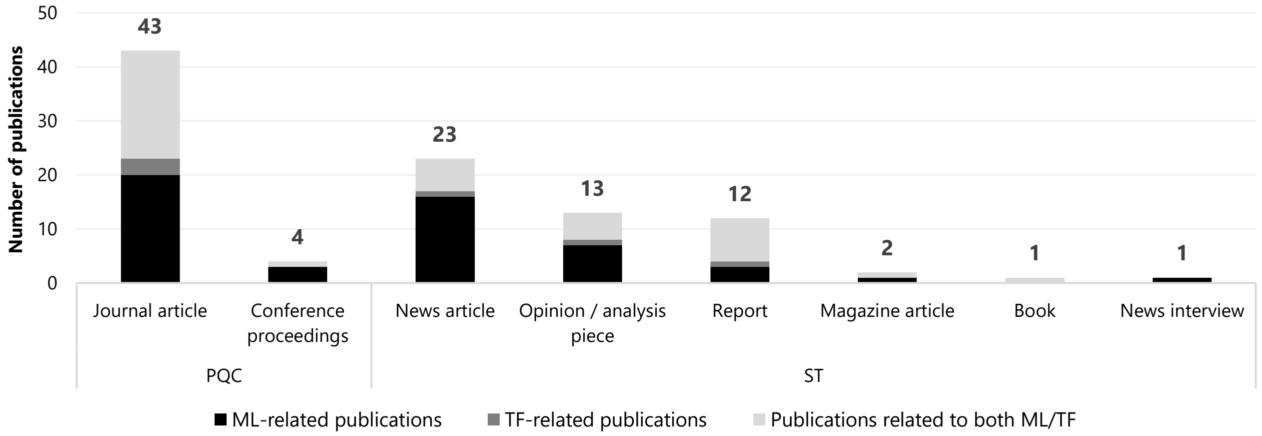

Fig. 1 Consulted publication types

Research-specific insights (see table 1) were also collected and are reported in the results section below. In line with realistic evaluation and review (Pawson and Tilley 1997), the aim was to collect information not just about what could be exploited but the mechanism(s) through which (i.e. *how*) it could be exploited.

Table 1 Research-specific data collected from publications

Insight	Description
Enablers	Specific developments that present (or could present) ML/TF risks
ML/TF methods	Potential ways of committing ML/TF offences using the identified enablers
At-risk stakeholders	Entities that could be exploited by and/or be complicit with ML/TF offenders
Risk characteristics	Criminogenic features of enablers that make them ideal for ML/TF purposes

RESULTS

The number of publications relevant to each technology category is shown in table 2. Some publications related to more than one category or crime type, so the column totals add up to more than the identified publications.

Table 2 Number of publications with relevant content per technology category

Category	PQC		ST		Totals
	ML (44)	**TF** (24)	**ML** (49)	**TF** (24)	
Distributed ledger technologies (DLT)	36	18	43	24	121
New payment methods (NPMs)	15	11	10	6	42
Financial technology (FinTech)	10	7	9	3	29

Figures in parentheses show total publications included for each search

Given the futures-oriented nature of this review, the timespan of the reviewed content is worth noting. The median quarter-year of publications was Q1 2018 for PQC and Q3 2017 for ST – representing a similar temporal trend in publications for both databases. It should be noted that, given the time delay associated with peer-review and publication of academic articles, their date of publication may not necessarily reflect the time period discussed in the research. The inclusion of ST articles, which include content (such as news articles) with a comparatively faster review-to-publish timeframe, was therefore additionally beneficial in this regard.

Quality assessment scores

ST average total scores (9.20 for ST_ML and 8.96 for ST_TF) were more than 2 points below those of PQC (11.61 for PQC_ML and 12.08 for PQC_TF), a statistically significant difference (Mann Whitney U=609, z=-4.29, p<0.01). Detailed results can be seen in Appendix 3 Table A2.

On average, neutrality, relevance and clarity scores were particularly lower for ST. This was because many were news articles or corporate blogs with less robust editing standards than PQC journal articles. Also, ST publications were comparatively briefer and often tackled issues from a compliance perspective rather than the nature of new threats, leading to lower clarity and relevance scores. However, ST publications were comparable to PQC publications for 'evidence', since low scores for blog posts and other such publications were coupled with high scores for governmental or institutional reports.

The results below provide a narrative synthesis of the insights acquired from publications, drawing on the relevant literature. The vast majority of cited material in the results are reviewed publications. However, in some instances, publications from outside the review are drawn on to provide definitional clarifications or to link discussions arising from the review to wider (and perhaps more recent) developments of relevance.

We first present findings that are specific to each technology category and then – in a subsequent discussion section – draw out themes that emerged across them. As previously stated, these themes were then assessed by an expert panel. All the findings discussed are listed in the supplementary material with definitions. Figure 2 shows the overall number of research-specific data insights coded per each technology category.

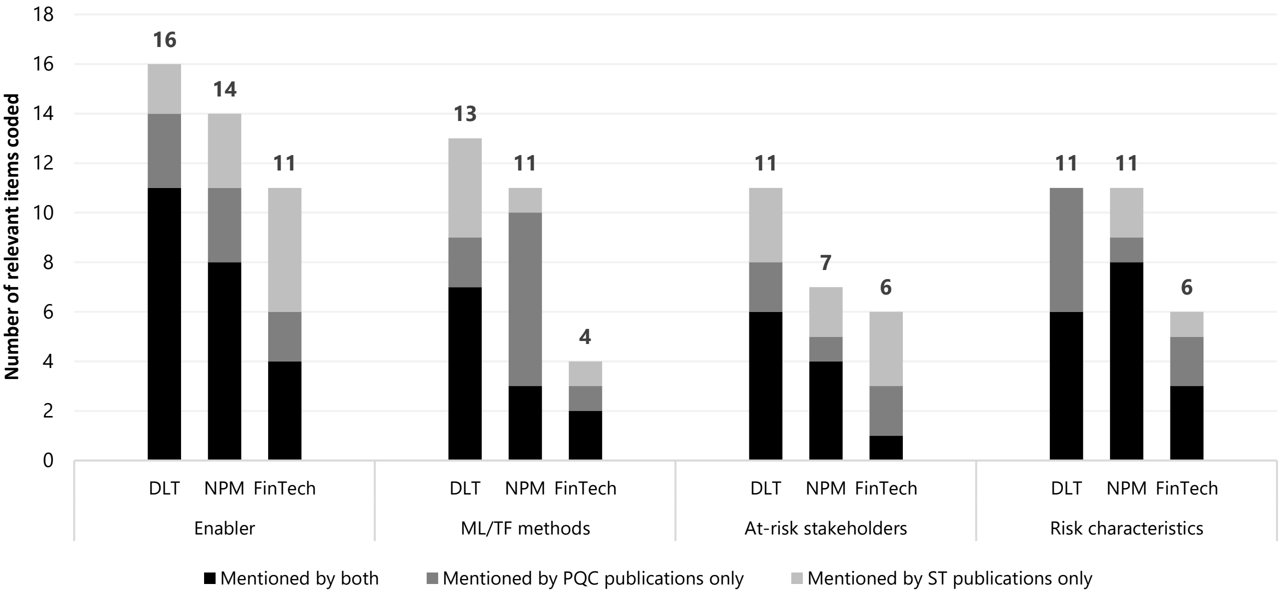

Fig. 2 Number of enablers, ML/TF methods, at-risk stakeholders and risk characteristics coded per technology category from each database

Distributed ledger technologies (DLT) results

DLT publications from PQC were often qualitative articles, though seven were quantitative studies, which employed exploratory modelling, algorithmic tests, reverse-engineering tests, 'cash-out' experiments or mathematical modelling to understand illicit crypto-transaction patterns. Academic articles scored higher on all quality assessment categories than ST publications, which were mainly news articles about regulatory loopholes. These often lacked comprehensive discussions of the ML/TF threats, and so scored low on relevance and clarity in particular.

Enablers

Identified DLT enablers broadly reflected two trends. The first was the noticeably diverse range of cryptoassets that publications mentioned were becoming mainstream. Besides traditional cryptocurrencies (or 'exchange tokens') such as Bitcoin (the most frequently identified enabler), a number of publications identified stablecoins (tokens with fixed exchange rates to standard currency), 'coloured coins' (coins with additional asset ownership information attached to them), utility/security tokens (powering decentralised finance protocols) and privacy coins (tokens with obfuscated blockchains) as alternative forms of cryptoassets gaining popularity. In particular, coloured coins, in the form of non-fungible tokens (NFTs), soared in popularity following this review throughout 2021. Utility and security tokens, meanwhile, reflect the similarly soaring popularity of decentralised finance (DeFi) protocols, which are now offering financial services in a decentralised manner using blockchain technology.

The second trend was the diversification of transaction methods, which included increasingly anonymous ways of trading this diverse selection of assets. For some enablers, this is not necessarily their core intention; identified in this regard were smart contracts, which could allow illicit funds to be traded in a complex and automated manner (Letourneau and Whelan 2017). The *Mimblewimble* protocol and Layer 2 scaling solutions such as the Lightning Network, intended to make transactions faster and reduce transaction fees, also have the effect of anonymising crypto transfers (Covolo 2019). Other enablers however, such as mixers and enhanced-privacy 'dark wallet' providers, were identified as being deliberately anonymous and of growing concern, given their active non-compliance with existing AML regulations.

ML/TF methods

In contrast to enablers, ML/TF methods were discussed relatively equally across articles identified using the two databases. They did, nevertheless, conform to the two main trends identified, namely (1) the conversion of illicit funds into alternative assets and (2) the use of more elusive methods for doing so. The former trend consisted of methods such as securities trading, gambling, auctions and owning real-world commodities through representative crypto-assets (coloured coins and security tokens), all as means for disassociating funds from their criminal origin (NIKKEI Asian Review 2013; Swanson 2014). The latter consisted of setting up illicit coin/security offerings (ICOs/STOs) to facilitate such exchanges (Allison 2019; Barone and Masciandaro 2019), storing cryptocurrency in satellite vaults to evade worldly regulations (Tucker 2015), mingling cryptoassets with legitimate funds using mixers (Covolo 2019; van Wegberg, Oerlemans, and van Deventer 2018), using low-KYC cryptoasset ATMs for cash-crypto exchanges (O'Donnell and Wilson 2019; Reutzel 2016) and obfuscating transactions with privacy coins or smart contracts (Virga 2015).

For terrorist financing, the possible use of a decentralised autonomous organisation (DAO), which utilises smart contract technology to democratically sustain a crypto investment pool, was mentioned as a highly advanced variant of typical charity-based fundraising (Zamfir 2017). Theoretically, terrorist financing pools could use this technology to transfer, by consensus, collective funds to terrorist entities.

Many identified ML/TF methods were modernised variants of traditional ML/TF. For example, 'mixing' illicit cryptocurrency fulfils a similar function to cash-intensive businesses, a traditional method of mingling illicit cash proceeds with legitimate ones. Numerous similar parallels can be drawn; satellite crypto-vaults can be considered the 'off-world' variant of 'off-shore' tax havens, while smart contracts (in an ML context) can be considered the DLT variant of complex legal documents disguising shell corporation activities. Other traditional methods, such as converting illicit cash into casino chips or high-value goods, can now be replicated on the

Blockchain using coloured coins representing such assets in digital casinos or auctions respectively. The abundance of such examples demonstrates the widespread ML/TF 'modernisation' capabilities of DLT.

At-risk stakeholders

Publications offered varied perspectives on what constituted at-risk stakeholders. Due to existing AML/CFT regulations associated with virtual asset service providers (VASPs), cryptocurrency wallet providers and exchanges were mentioned the most. New regulations were the focal point in many publications, in particular the EU's 5th Anti-Money Laundering Directive (5AMLD) in 2017 classifying them as AML/CFT-compliant entities (Guarascio 2016; Hughes and Middlebrook 2015).

More broadly, any entity issuing tokens or providing an anonymising service was mentioned. Social media sites, for example, were mentioned due to their growing interest in launching stablecoins (BBC 2019), and because some still allow terrorist groups to promote and provide links for cryptocurrency donations on their profiles (Goldman et al. 2017). In the decentralised finance (or 'DeFi') space, any token-issuing protocols and decentralised exchanges (DEXs) were also regarded as at-risk. Related to these entities were cryptocurrency banks and payment gateways (Tu and Meredith 2015), which facilitate loans and online purchases with cryptoassets respectively. Stakeholders were also discussed relatively evenly (but more briefly) across PQC and ST publications.

Risk characteristics

Identified risk characteristics consisted of technical capabilities (such as irrevocability of payments) and regulatory difficulties (such as the abundance of non-compliant cryptoasset services). PQC publications covered more issues and were more detailed, particularly in the case of technical features that make DLT criminogenic.

Many of the identified characteristics have a causal relationship with each other. For example, the 'lack of adequate regulation' (a commonly identified characteristic) exasperates the risks of 'anonymity' and 'lack of traceability', two other commonly identified characteristics (Virga 2015). However, the 'abundance of non-compliant virtual asset services' reciprocally makes solving the lack of adequate regulation difficult (O'Donnell and Wilson 2019). Perhaps in part due to the abundance of such services, blockchain technology has enjoyed a widening yet potentially risky global acceptance, making effective regulation more difficult. Indeed, wider global acceptance was mentioned as a risk characteristic in numerous publications from 2015 through to 2019, indicating the continuity of this issue over time (Albrecht et al. 2019; Gomber, Koch, and Siering 2017; Tu and Meredith 2015).[1] The cyclical relationship of all these risk characteristics poses a difficult dilemma for law enforcement and regulators.

New payment methods (NPMs)

All PQC publications for NPMs employed a qualitative methodology. ST publications mostly included news articles and reports. Although NPMs have been a long-established ML/TF risk, publications were often ambiguous about more recent developments and their crime implications, meaning that evidence, relevance

[1] Since this review, El Salvador has become the first country to accept Bitcoin as legal tender in September 2021 (Arslanian et al. 2021).

and clarity scores were often low. Most publications considered financial or regulatory topics, with several discussing NPMs alongside blockchain-related issues.

Enablers

Similar to DLT, many identified NPM enablers were value instruments that allow users to exchange, transfer or hold funds in a secure form alternative to cash or traditional bank accounts. These included virtual (non-crypto) currencies, such as online gaming currencies and other digital value assets such as 'e-gold' (Choo 2015; Peterson 2013). Pre-paid cards, which hold funds digitally without the need for a bank account, were also frequently mentioned (FFIEC 2016), as were more obscure variants such as carbon emissions permits (Williams 2013). Such examples suggest that NPMs may not necessarily arise from technological advances, but (in the case of carbon emissions permits) from developments in legal or environmental policy. Also discussed in a similar respect were the diversifying methods for storing funds, in either traditional currency or alternative format, in a less regulated setting. These could be mobile payment services, payment processors or e-commerce sites, where users can hold funds in digital accounts (Martin 2019; Peterson 2013).

Publications also mentioned improvements to payment technologies that would make payments faster, more efficient and potentially harder to detect or prevent suspicious activity. The rise of Bluetooth or infrared payments (FFIEC 2016), mobile wallets such as *Apple Pay* or *Google Pay* (Rossi 2014), alongside social media or mobile-enabled payments, were mentioned in particular.

Other noted enablers pertained to the rising phenomenon of trading goods or services via new mobile applications or through e-commerce on online marketplaces such as *Facebook Marketplace* (Rossi 2014; Furst 2018). These developments were mentioned due to the growing simplicity of facilitating online transactions via apps, to which AML regulations do not apply in many jurisdictions and with which payment functionalities are integrated. This was perceived to enable additional criminal opportunities, along with an extra layer of complexity when it comes to identifying possible offenders.

ML/TF methods

Most identified NPM ML/TF methods came from academic sources, with little contribution from ST. Some methods, such as structuring, were traditional ML methods adapted to NPMs. For terrorist financing in particular, traditional cash couriering across borders was mentioned as a process that could be significantly enhanced (in terms of volumes transferred) and better concealed by couriering pre-paid cards instead (Goldman et al. 2017; HM Treasury and Home Office 2020).

However, several identified methods were uniquely enabled by NPMs. An example identified for online gaming virtual currencies was real-world trading, namely purchasing online gaming currency or high-value items with illicit funds and selling them to other players for clean funds (Ramos, Funderbuck, and Gebelein 2018; Peterson 2013). More long-term and resource-intensive possibilities were also identified, including establishing environmentally-friendly front companies with illicit funds, claiming carbon emissions permits from the government, and trading them for clean funds (Williams 2013). Acquiring or establishing deliberately illicit payment processing companies to reduce the risk of suspicious activity reporting were also mentioned in this regard (Virga 2015; Alsaibai et al. 2020).

Some methods, such as chargeback fraud (transferring illicit funds on a payment processor and then requesting a refund of clean funds) or false payments for non-existent goods/services, highlighted how illicit activity and ML can occur simultaneously. Notably, transaction laundering is a highly elusive technique for doing this and will be discussed later in detail.

At-risk stakeholders

NPM publications identified stakeholders briefly at best. Most commonly identified were issuers of virtual currencies, such as online gaming assets, carbon permits or indeed any asset of value that can be freely exchanged or traded for a government backed currency. The remaining stakeholders were facilitators of payments, such as mobile apps and e-commerce sites. Similar to ML/TF methods, stakeholders were more commonly identified in academic articles.

On occasion, stakeholders were mentioned due to their risks being increased by external factors. Mobile network operators, which allow payments via mobile phones, were mentioned due to their appeal in unbanked or underbanked populations, where the scope for KYC is poor and AML regulations are not necessarily well implemented (Whisker and Lokanan 2019; Martin 2019). Online notaries were mentioned due to their increased use during the Covid-19 pandemic (Trulioo and PYMNTS.com 2020b), reducing the possibility of face-to-face identity verification.

Risk characteristics

That virtual currencies or other mediums were globally transferrable, easy to use, easily convertible, easy to handle remotely, inexpensive due to low commissions and quick to transfer were all mentioned as risk factors that would make them attractive to launderers (Dostov and Shust 2014; Whisker and Lokanan 2019). For financiers of terrorism, the secure and low-cost nature NPMs – along with their susceptibility to predicate offences (such as chargeback fraud) – were mentioned as particular risks, exemplifying their potential as scaled alternatives to more traditional terrorist money transfer methods.

Many risks are increased as NPM providers seek to improve their competitive advantage, for example when pre-paid card providers increase their transaction value limits (Choo 2013). This is a more concerning observation for NPM providers that deliberately seek to cater to an illicit audience, for which anonymity, lax ID checks and wilful oversight of criminal activity were mentioned as particular risks (Brito 2015; Martin 2019).

FinTech and new financial products

PQC publications were exclusively qualitative journal articles. ST publications were more diverse, consisting of news and magazine articles, reports by international institutions and corporate blogs. Both PQC and ST publications focused on finance, regulation and technological developments. Many focused on the benefits of technology rather than the risks, thus attaining lower relevance and clarity scores. Due to the overarching focus on *future* prospects of automation, consulted evidence was limited, leading to low scores in that category also.

Enablers

The massive growth in data generated in recent times, increases in (cloud) computing power, and advances in machine learning have allowed swathes of information to be efficiently analysed. The consequence of this, as identified in the review, is that more and more banking services are becoming automated (Vovchenko et al. 2018). Smart ATMs (allowing a range of banking procedures, such as cashing in cheques, in an automated manner) and robotic process automation (automating customer interactions with financial services) are just two examples. These are likely to further reduce human oversight of financial transactions as such enablers continue to become mainstream.

A range of other enablers, designed to enhance customer convenience potentially at the risk of inadvertent ML/TF exploitation, were also identified. These included remote deposits of cheques (FFIEC 2016), digital-only banks that do not have physical branches and operate only through websites or mobile apps (Furst 2018; Woodford and Darrah 2019), and low-regulation 'charter cities' designed as business-friendly locations for financial services themselves (Reisen 2016).

Reviewed publications also noted an increased interest in 'alternative finance' (AltFi), designed to bypass traditional financial services entirely, an ethos similar to that of blockchain technology. Peer-to-peer lending (where lenders and borrowers can interact and agree terms directly) and crowdfunding (where donors or investors can place funds in user-submitted causes or projects) were mentioned in this regard (Furst 2018; Lagarde 2018; Soudijn 2019).

In general, a growing trend of supplementary services (such as wealth advisory apps) were identified (Lagarde 2018), given their potential evolvement into future automated services engaging in transactions. Online versions of traditional services, such as *hawala* remittance or currency exchange, were also mentioned (Soudijn 2019). Publications additionally noted an increasing interest in blockchain technology by FinTech, with crypto-securities (financial products that derive their value from an underlying cryptoasset) being mentioned as potential developments (Hughes and Middlebrook 2015).[2]

ML/TF methods

Despite mentioning several enablers, publications seldom described methods for exploiting them in detail. This corresponds with both the overall lower number of publications consulted for FinTech, as well as their low *relevance* and *clarity* scores. These imply that while an ML/TF nexus was mentioned (hence their inclusion in the review), it often was not central to the publications consulted. The enablers can therefore be regarded as 'weak signals' of potential ML/TF risk rather than those with already-established ML/TF methods.

Methods that were mentioned were often discussed vaguely, often to equal extents by both PQC and ST publications. A general method, applying to a wide range of identified enablers, involved exploiting automated systems, either through malicious cyberactivity or simply identifying and utilising system faults (Trulioo and PYMNTS.com 2020b). Smart or 'white-label' ATMs (ATMs that operate with agreements of, but are not themselves, banks) were mentioned as particularly vulnerable to such attacks (Choo 2013; RNZ Insight 2018).

The remaining methods generally concerned the exploitation of anonymous or peer-to-peer services, such as online currency exchanges or crowdfunding platforms (Virga 2015; Soudijn 2019). Establishing illicit

[2] Subsequent to this review, the first bitcoin futures exchange-traded fund (ETF) started trading on the New York Stock Exchange on 19 October 2021 (Najumi 2021).

fundraisers on crowdfunding platforms and then loading it with criminal funds was identified, in particular, as both an ML and TF risk (Lagarde 2018; HM Treasury and Home Office 2020).

At-risk stakeholders

As with ML/TF methods, discussions of at-risk stakeholders were very broad. Overall, few stakeholders were identified and were infrequently discussed across both databases. Banks were naturally the most mentioned at-risk entity due to their continued centrality to the financial system. Digital-only banks were also mentioned as an at-risk entity given their reduced scope for face-to-face KYC (Breslow et al. 2017). Many require nothing more than a photo upload of a driving license, which could be forged or stolen, to open an account.

Online remittance systems and currency exchangers were an entity regarded as at-risk due to the modernisation and expansion of hawala services provided through these channels (Furst 2018; Soudijn 2019). P2P lenders were also identified as relevant stakeholders, since they carry out similar functions to crowdfunding platforms with comparatively lower regulations than traditional financial services. Payment merchants were mentioned due to the growing number of business transactions that they oversee (FFIEC 2016).

Risk characteristics

Few publications discussed FinTech risk characteristics in depth. Those that did often referred to general characteristics such as ‘automation’, rather than specific risks. As with DLT and NPMs, anonymity and fast transactions were identified as recurring risks, particularly in relation to convenience-enhancing online financial access drives that inadvertently reduce the capacity to effectively conduct identification checks on new customers.

The cost of cybersecurity solutions, in particular, was a mentioned risk characteristic that reflects the replacement of traditional human oversight with automated processes (Wewege, Lee, and Thomsett 2020). Previously, complicit employees that would circumvent AML procedures for criminal accomplices were seen as a major risk. As such positions are automated, malicious code has increasingly become the modernised equivalent of complicit employees – thereby shifting the focus from anti-corruption to resilient cyber systems. For AltFi developments, the lack of regulation was mentioned in particular (Trulioo and PYMNTS.com 2020b). Overall, no particularly surprising or terrorist financing-specific risk characteristics were identified.

Discussion

The above findings identify commonalities both within and across DLT, NPMs and FinTech. While these apply to existing or developing technologies, they also potentially apply to technologies that may emerge in the future, informing whether these are likely to pose ML/TF risks and, if so, the reason(s) why. These underlying trends – of which there were six – and their most (and least) noteworthy threats are now discussed for the purpose of informing future risk assessments.

The purpose of identifying underlying trends is to pinpoint the different ‘vectors’ by which development technologies can facilitate ML/TF, hence allowing focus on and targeted risk assessment of specific vulnerabilities. Overall, they can give a clearer understanding to stakeholders of innovative technology on where to focus pre-emptive prevention efforts, while making risk assessments more efficient. Additionally, these vectors can serve to identify or expand horizon scanning for additional risks that were not necessarily identified in this review, or are yet to be invented.

Alternative mediums

The most common trend, identified across DLTs, NPMs and once (namely crypto-securities) in FinTech, was the provision of new mediums for criminals to exchange, store and transfer illicit funds. These include but are not limited to all crypto-tokens (for DLT) and pre-paid cards and (online gaming) virtual currencies (for NPMs). Alternative mediums need not be a unique value instrument in themselves. They can also include mobile money and online payment systems that offer accounts storing fiat currency in a less detectable way than standard bank accounts.

The basic ML scheme identified for alternative mediums (see figure 3) involves exchanging illicit funds into the medium, followed by a series of transfers to obfuscate the funds trail or to send them to a criminal accomplice. Offenders can then store their funds in the medium or exchange it back, or alternatively use it (if possible) to directly purchase high value goods.

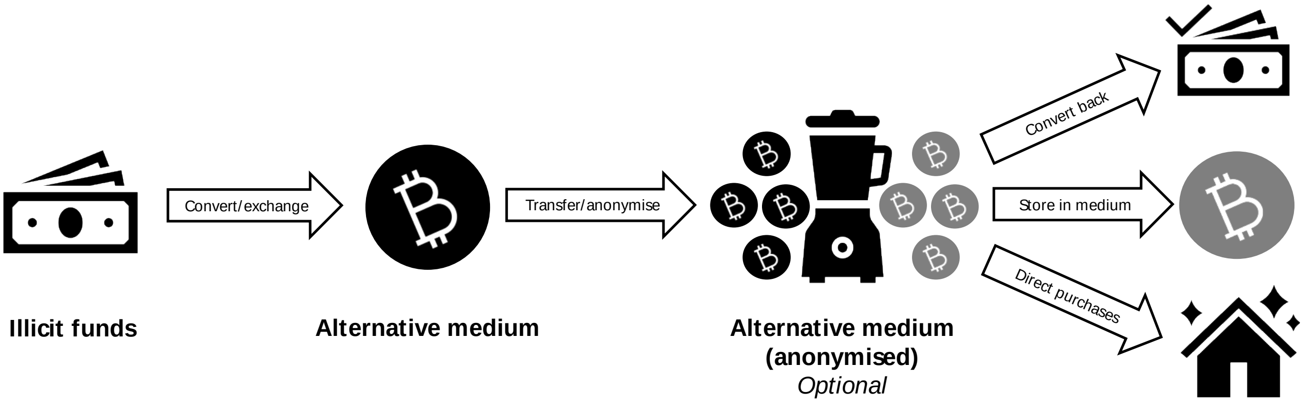

Fig. 3 Alternative mediums and ML/TF

Any enabler or stakeholder hosting, exchanging or facilitating the transfer of alternative mediums (generalisable as ‘alternative medium service providers’ or AMSPs) are at risk of exploitation of complicity. These may include crypto-exchanges, pre-paid card providers, ICOs/STOs, mobile network providers or even unwitting governments exchanging illicit funds into carbon permits. They can also include entities that accept alternative mediums (such as cryptocurrencies) for payment in return for high value goods.

Alternative mediums can constitute an ML/TF risk if they present, through whatever risk characteristic(s), features attractive to criminals. At the very least, alternative mediums need to be *easily exchangeable* (both to and from the medium)*, easily stored* and *easily transferrable*. Additional risk characteristics can include anonymity, their decentralised nature, ineffective regulations (i.e. their lack of global compliance or resilience to loopholes), widening global acceptance, high value limits, high trade volumes, low commission, stable value, ease of access and/or high transaction speed.

The widening global acceptance of alternative mediums, such as cryptocurrency, and their ‘attractiveness to predicate offences’ (another identified risk characteristic) both exemplify another issue for the traditional AML/CFT framework. For ML/TF offenders, the initial ‘placement’ phase of ML typically incurs the highest risk of detection due to the suspicious nature of large transactions (Buchanan 2004). However, the increasingly lucrative nature of cybercrime, including scams, online extortion, hacks and ransomware, typically generate cryptoassets to begin with. This negates the cybercriminal's need to initially 'place' funds and risk triggering a suspicious activity alert, as their proceeds are in a semi-anonymous medium (i.e. cryptocurrency) to begin with. With some payment gateways now providing the ability to purchase high-value assets (including real estate) directly in cryptocurrency, criminal funds can potentially be laundered entirely within the ecosystem of alternative mediums (such as blockchains) without ever leaving until the very end (Gilbert 2022).

The risk characteristics of alternative mediums can form the basis of a cost-benefit assessment to determine whether their legitimate utility outweighs their propensity for criminal exploitation. Identified in this review as particularly high-risk mediums, per the characteristics above, include stablecoins, which are a safer storage medium compared to other crypto-currencies due to their private issuance and stable values. Utility tokens, due to the relatively unregulated nature of the DeFi protocols that they power, are also high-risk. Lower risk mediums include customer loyalty points, which are often centralised and difficult to convert to any other medium.

The wider debate surrounding DeFi and stablecoins, the latter essentially being the 'privatisation' of central banking by allowing corporations to issue currency (O'Neal 2019), signals that the future directions of alternative mediums are likely to be wide-ranging amid diminishing central oversight. Pre-emptive futureproofing is therefore necessary to prevent their exploitation from spiralling out of control.

Concealment enhancers

Concealment enhancers enable additional steps that offenders can take to further anonymise the exchange, transfer or storage of alternative mediums (per the 'anonymisation' stage in Figure 4) to reduce detection risk. This trend was mostly observed for DLT, but identified methods are also compatible with NPMs and FinTech.

Concealment enhancers range from small activities such as structuring funds across accounts to large-scale operations such as establishing illicit platforms to exchange and trade alternative mediums anonymously. Such was the case for *Liberty Reserve*, a now-defunct platform allowing anonymous trading of virtual currency, the owner of which was imprisoned for facilitating the laundering of around USD$6 billion (Stempel 2015). There have been cases where illicit funds transfers have been disguised as extortionate transaction fees on tiny cryptocurrency transfers by illicit/complicit crypto-exchanges (Farrugia, Ellul, and Azzopardi 2020). For terrorist financing, DAOs were specifically discussed as an anonymity-enhanced way of pooling and donating funds.

The most commonly mentioned concealment enhancers were cryptoasset mixers, which mingle and run a series of cryptocurrency transactions with 'tainted' cryptocurrency to fool taint tracking systems which could otherwise detect them (van Wegberg, Oerlemans, and van Deventer 2018). The methods used by mixers in particular have become increasingly ingenious. A recent report gave light to 'crypto-dusting', a new method used by the now-defunct *BestMixer.io* in October 2018. This sent miniscule amounts of tainted cryptocurrency to several legitimate wallets disguised as an advertising campaign, thereby tainting them and, by making it difficult to trace the flow of the original tainted coins, fooling taint tracking analytical tools (CipherTrace, 2019; Jake, 2018). The use of privacy coins that hide transaction amounts and wallet information, such as *Monero*, can also increase the difficulty of tracking tainted crypto-assets.

Most stakeholders associated with concealment enhancers, such as mixers or illicit alternative medium providers, are aware of (and in some cases promote) their appeal to criminals. However, some good-natured developments inadvertently create concealment enhancers. For example, layer 2 solutions for blockchain systems may have legitimate purposes such as speeding up blockchain transactions, but at the cost of blockchain transparency (Covolo 2019).

Assessing the risk characteristics of concealment enhancers is crucial to determine the level of future threat and prevalence of usage. The illicit utility of a concealment enhancer is essentially a function of its cost to deploy, available substitutes and the level of additional concealment it provides. Considerations should also account for the 'base' detection risk that would be observed if the enhancer was not present, as in many cases it may be low enough to negate the economic utility of deploying more resource-intensive enhancers. For example, storing cryptocurrency in virtual reality headsets and transporting them across borders (Ramos, Funderbuck, and Gebelein 2018) is arguably not a realistic concealment enhancer; easier, cheaper and less conspicuous alternatives, such as storing cryptocurrency on USBs, exist. Storing crypto in satellite vaults is another example of a concealment enhancer that is unlikely, given that the facilitating space start-ups themselves are likely to be regulated, to generate a cost-benefit advantage to the average launderer.

Identifying concealment enhancers of the future is therefore likely to entail proofing developments that are legitimate but inadvertent (such as layer 2 scaling), locating and shutting down illicit AMSPs and unearthing new suspicious transaction patterns (such as crypto-dusting) that may correspond to anonymisation attempts. Also notable is their tendency to mimic more traditional money concealment methods already well known in the field of ML/TF, though by substituting them with technological advancements. Satellite bitcoin storage, crypto-gambling and crypto-auctions have all been previously discussed in this regard.

Digital invoice manipulation

This trend, identified exclusively for NPMs such as mobile applications with built-in payment capabilities, is essentially a modernisation of the traditional 'trade-based money laundering' (TBML) over-invoicing method. TBML would conventionally require two or more corporate structures (FATF 2006b). One would trade with the other, invoicing the goods or services at a higher or lower rate than their market price, depending on the direction of illicit flows. The recipient would then sell the goods at market price in order to complete the process (FATF 2006b). This is summarised in figure 4.

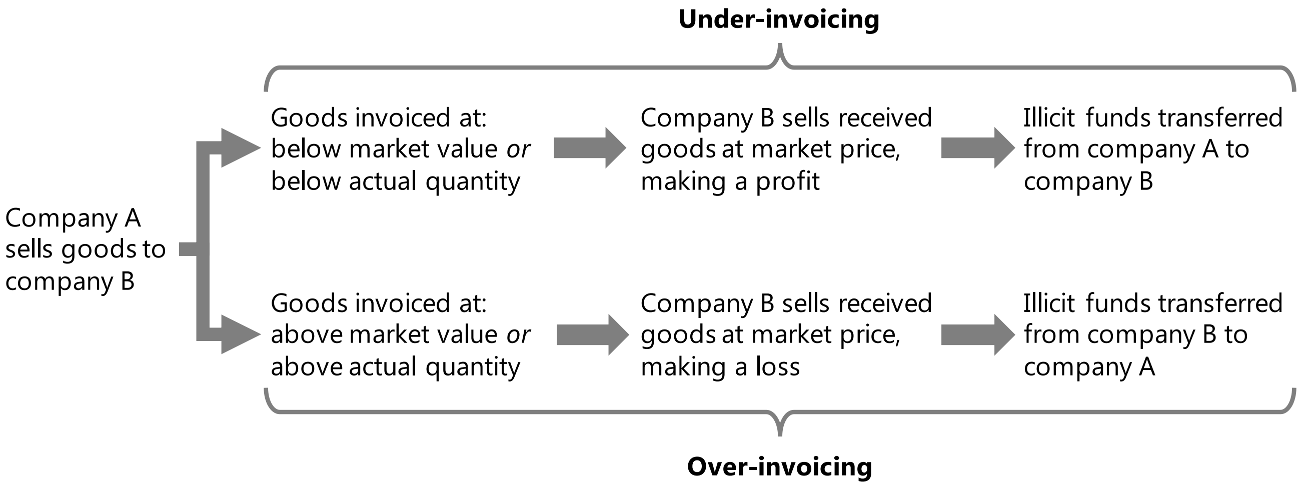
Under-invoicing
Company A sells goods to company B
Goods invoiced at: below market value *or* below actual quantity
Company B sells received goods at market price, making a profit
Illicit funds transferred from company A to company B
Goods invoiced at: above market value *or* above actual quantity
Company B sells received goods at market price, making a loss
Illicit funds transferred from company B to company A
Over-invoicing

Fig. 4: Traditional TBML

With NPMs, criminals no longer need to establish companies or trade with each other. They can simply use third party intermediaries, such as *AirBnB,* to list a fake good or service, possibly using identity concealment techniques and visual manipulations such as 'deepfakes' (convincing fake images or videos) to make them seem real (Kietzmann et al. 2020). Since these intermediaries often cannot physically verify the trade of every good or service advertised on their platform, a criminal could simply accept the 'purchase' or 'booking' of his or her accomplice without actually providing anything in return. An invoice would be generated by the intermediary application, legitimising the transaction. It should also be noted that, even if verifying app user activity in all cases is possible, there may be a lack of motivation by app developers or their account-providing traditional financial services to proactively do so (Feedzai 2021). The lengthy process of 'over-invoicing' in traditional TBML is therefore shortened substantially. Figure 5 shows the adapted 'over-invoicing' method in Figure 4 to demonstrate digital invoice manipulation.

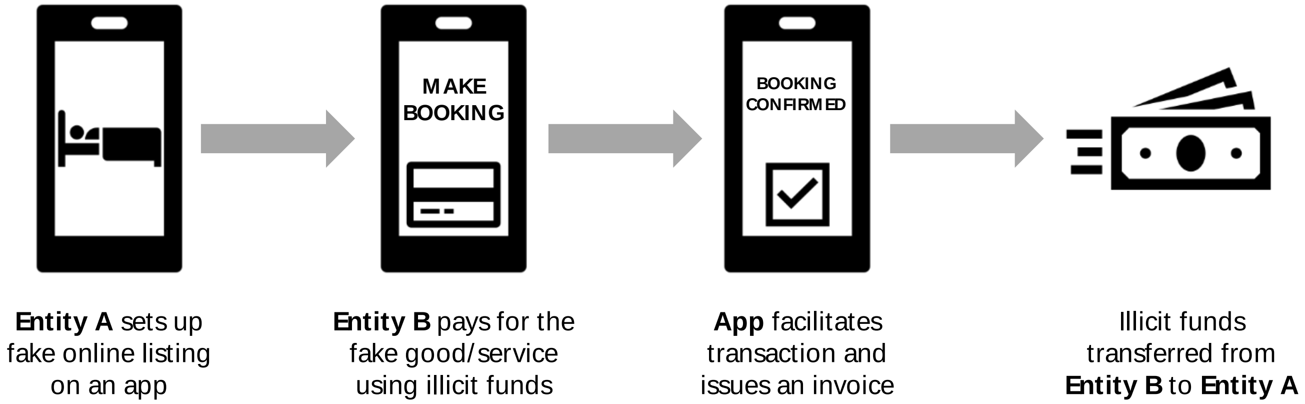
MAKE BOOKING
BOOKING CONFIRMED
Entity A sets up fake online listing on an app
Entity B pays for the fake good/service using illicit funds
App facilitates transaction and issues an invoice
Illicit funds transferred from **Entity B** to **Entity A**

Fig. 5 Technology-enhanced TBML (digital invoice manipulation)

Any mobile application facilitating good/service listings and built-in payment capabilities is at risk. This is regardless of whether it facilitates ride hailing, property renting, takeaway delivery or even pet sitters for owners on holiday – absent comprehensive verification checks, any good or service listing can be manipulated for ML/TF purposes. Apps themselves can be an ML/TF tool on their own. One publication identified how resourceful launderers were creating several functionless 'shell apps' and uploading them to *Apple App Store,* which were then being purchased and downloaded many times despite having no actual in-app utility (Ramos, Funderbuck, and Gebelein 2018).

Many app stores and app providers have internal fraud departments to detect malicious listings and activity. An example can be found in a blog post by Chen (2018) outlining *Uber's* fraud detection systems. This trend is therefore unlikely to facilitate large-scale ML/TF, as these fraud departments are certain to detect unrealistic transactions (such as a house being rented for millions of dollars on an accommodation renting app). Many publications used the term 'micro-laundering' to describe methods associated with this trend for this reason (Alsaibai et al. 2020). Nevertheless, the method may still be attractive for donations-based terrorist financing and smaller-scale operations.

Risk characteristics associated with digital invoice manipulation include their simplicity, global nature of transactions, susceptibility of at-risk stakeholders (e.g. e-commerce sites) to predicate offences such as chargeback fraud and the lax ID checks needed to establish accounts on them (Goldman et al. 2017). While not directly an ML/TF risk, the enhancement of payment technologies (both in terms of speed and options) is also a key enabler of digital invoice manipulation. Contactless, integration with mobile wallets and possible future advances such as Bluetooth and Infrared payments all enhance the convenience and speed of transactions (including illicit ones), adding further pressure on stakeholders to detect and stop suspicious transfers in a timely manner.

Transaction laundering

Transaction laundering (TL) is similar to digital invoice manipulation. However, it can be considered an 'offshoot trend' for numerous reasons. TL involves diverting illicit (often Dark Web) transactions (such as for drugs or firearms) through a front company with a merchant account, thus allowing them to be invoiced as transactions for legitimate goods/services (Chattopadhyay 2018). Upon agreeing a price for illicit drugs on the Dark Web, for example, a buyer would be rerouted to a legitimate looking e-commerce site where they would make an 'order' for innocent-looking items that do not actually exist (such as books or clothes), which would in fact be payment for the illicit goods/services agreed. Oblivious payment service providers then process and thus inadvertently launder these funds.

TL can involve setting up a front business or using a 'pass-through' business willing to offer its merchant account for illicit use (Trulioo and PYMNTS.com 2020b). An example of a TL scheme, disguised through an e-bookstore, is shown in figure 6.

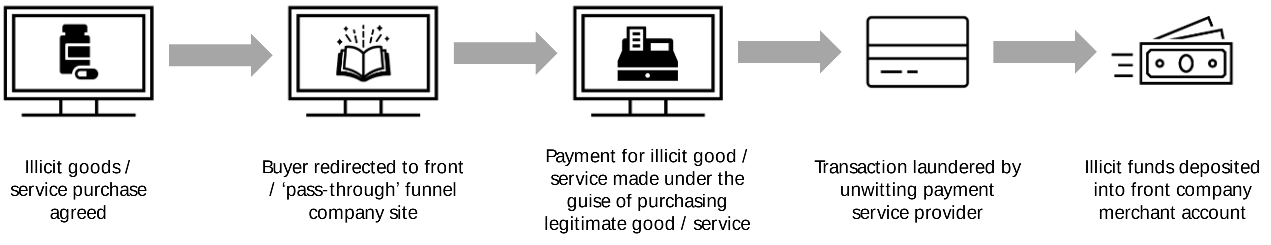
Illicit goods / service purchase agreed
Buyer redirected to front / 'pass-through' funnel company site
Payment for illicit good / service made under the guise of purchasing legitimate good / service
Transaction laundered by unwitting payment service provider
Illicit funds deposited into front company merchant account

Fig. 6 Transaction laundering

TL poses serious dangers that are less evident than other trends. Firstly, TL typically enlists a willing criminal entity to process transactions, rather than a legitimate service or mobile app. Therefore, a crucial node of possible detection, i.e. internal fraud departments, is lost. Secondly, TL effectively merges the predicate offence (such as illegal drug distribution) and the laundering of its proceeds into one transaction. Illicit funds are essentially laundered as they are generated. Finally, the relevant stakeholders or risk characteristics for TL are substantially vague, as virtually any online site with e-commerce capabilities is at risk.

Due to its elusiveness, TL has been referred to as the 'least enforced' form of contemporary ML (Teicher 2018b), and as a 'huge financial blindspot' (Kaminska 2017). TL-related technological developments are worrying. For example, with some payment service providers now accepting cryptocurrency payments, TL can now occur in the decentralised DLT ecosystem with even less detection possibilities.

Manipulating automation

This trend involves exploiting the faults and limitations of automated financial services to prevent suspicious transaction alerts from being raised (RNZ Insight 2018). Examples of manipulable FinTech developments include smart ATMs, robo-advisory (automated financial advice and customer service) and online banking. The main driver of this trend is the lack of (or delayed) human oversight, potentially allowing software manipulation to become easier and unnoticeable (Vovchenko et al. 2018). Automation also increases the chance of system faults, which can then be exploited without prior manipulation. For example, in 2017, smart ATMs operated by the Commonwealth Bank of Australia failed to generate suspicious activity reports for over 53,000 deposits exceeding the mandatory AUD$10,000 reporting threshold (RNZ Insight 2018).

Reviewed publications were not overtly technical on how automated services could be manipulated. Many emphasised the benefits of automation in improving (rather than complicating) transaction monitoring through 'RegTech', namely technology-enabled compliance software. However, the few risks described allude strongly to adversarial perturbation (AP), a growing field of machine learning. AP is where a malicious algorithm aims to understand and defeat a detector algorithm (Kurakin, Goodfellow, and Bengio 2017), such as AML/CFT detection software (Faith, Hasan, and Enshaie 2020). Such technology is already able to fool fraudulent-image ('deepfakes') detection software and inject datasets with malicious data (Qiu et al. 2019). The cyber-threat to automation therefore extends beyond ML/TF and remains a significant issue that, despite substantial investment in IT security, continues to pose serious risks.

Convenience enhancers

This trend concerns reduced CDD capabilities of financial services undergoing convenience drives. These endeavours include the increase in remote access to services such as digital-only banks (Furst 2018; Woodford and Darrah 2019), peer-to-peer lending and the integration of financial services with non-related stakeholders. The latter includes new start-ups providing the ability to make payments over social media messaging apps and chatbots (Trulioo and PYMNTS.com 2020a). Such convenience drives, often accompanied by rapid customer accumulation business models, can reduce CDD capabilities, hasten onboarding procedures and spread risk over a larger number of (often unregulated and inexperienced) stakeholders by involving them in the transaction process.

Convenience enhancers are essentially a gateway to other risks. By using fraudulent ID and passing remote CDD checks, malicious users can gain access to platforms that host alternative mediums, concealment enhancers, digital payments functionalities or manipulable systems. The same risks apply to peer-to-peer services, including online crowdfunding sites where criminals can set up and lend their own illicit funds to seemingly legitimate ventures or causes.

Convenience enhancers can also operate on the macro-level, spearheaded by governments and international organisations. Examples include charter cities, namely economic zones with reduced regulations and unique laws to bolster trade and investment by making such economic activities more convenient (Reisen 2016). However, this macro-convenience enhancing drive could inadvertently enable large-scale ML/TF, corruption, sanctions evasion and tax evasion. Such concerns led a proposed charter city project in Honduras to fail in the early 2010s (Hutchinson 2012).

While its 'gateway' status makes this trend a concern, to attempt to solve it with stricter CDD regulations will arguably be ineffective. Such measures are often expensive for start-ups, have a high false positive rate and low rates of actual detection, making them detrimental to innovation in a cost-benefit sense. It is arguable that pre-emptive detection and prevention capabilities are better allocated to countering the other underlying trends identified.

Expert reception of underlying trends

Given the often speculative and unclear nature of the publications consulted, the emerging underlying trends were subjected to expert verification. Participants were invited from three sources. These were: 1) authors of reviewed publications (contacted: 145); 2) industry experts recruited through events and conferences (contacted: 27); and, 3) snowballing (contacted: 54). Surveys (having obtained research ethics approval) were conducted anonymously online with explicit consent.

Those who participated (*N*=51, see appendix 4 for participant profiles) were invited to select the technology category (DLT, NPM, FinTech) with which they were most familiar. FinTech was referred to as 'new financial services and products' in surveys to differentiate them from the other two categories, which are sometimes encompassed in the definition of *'FinTech'*. Some chose multiple categories, with 17 selecting DLT, 17 selecting NPM and 14 selecting FinTech. The underlying trends were only presented to the respondents to which they were most relevant; DLT participants scored alternative mediums and concealment enhancers, NPM participants scored alternative mediums and digital invoice manipulation, while FinTech participants scored automation manipulation and convenience enhancers. Due to its specific nature and similarity to digital invoice manipulation, transaction laundering was not included as a stand-alone trend for scoring.

The survey (which was part of a larger study) was conducted online (12 May to 9 June 2020) and participants were provided with a brief description of the relevant underlying trends along with illustrative diagrams. Participants rated each trend for accuracy on a 1 (very inaccurate)-5 (very accurate) Likert scale, separately for both ML and TF (table 3). They were also asked to explain their scores.

Table 3 Accuracy of underlying trends

Trend (category)	Money laundering				Terrorist financing			
	N	*M*	*SD*	Range	*N*	*M*	*SD*	Range
Alternative mediums (DLT)	17 (1)	4.25	0.93	2-5	14 (5)	3.44	0.88	3-5
Concealment enhancers (DLT)	17 (1)	4.13	0.96	2-5	14 (4)	3.30	0.67	2-4
Alternative mediums (NPM)	17 (0)	4.41	0.62	3-5	13 (2)	4.08	0.90	3-5
Digital invoice manipulation (NPM)	16 (2)	4.50	0.65	3-5	14 (2)	3.91	1.22	3-5
Manipulating automation (FinTech)	14 (2)	4.12	0.67	3-5	14 (3)	4.18	0.87	3-5
Convenience enhancers (FinTech)	14 (3)	4.45	0.69	3-5	14 (4)	4.20	0.79	3-5

Numbers in brackets indicate "Don't know"

Average scores for all trends were above 4 for ML. Scores were lower for TF, with concealment enhancers only achieving an average score of 3.30. Some respondents reasoned that TF prioritises concealing recipients over transactions and that it still uses 'old school methods' (such as cash transactions) compared to ML, an assertion backed by the UK's HM Treasury and Home Office (2020). No expert identified specific *inaccuracies*, however, illustrating general overall agreement with the findings of this review.

In terms of omissions, emphasis on high-demand but low-supply goods such as personal protective equipment (PPE) was made in the context of the Covid-19 pandemic, with participants noting that high liquidity, firm demand and reduced customs checks on the trading of such essential items allowed for their use as physical alternative mediums to exchange, store and transfer illicit funds. The possibility of corrupt employees (i.e. 'insider threats') facilitating these trends within risk-prone stakeholders, was also mentioned. In the review, 'manipulating automation' was discussed as the technologically-enhanced form of employee complicity. However, experts correctly pointed out that both risks can easily occur concurrently, with complicit employees assisting the manipulation of automated systems by 'leaking' internally-identified vulnerabilities. In terms of non-conforming risks, respondents mentioned lax regulations and poorly regulated countries. These are indeed an issue complementary to the review findings. It was envisaged by one reviewed study that ICOs, for example, would mainly relocate to lax jurisdictions, such as Switzerland and Luxembourg, in the near future (Mariñas 2018).

One specific DLT risk mentioned was the use of coloured coins to represent already illicit assets and services (such as illicit arms or trafficked gemstones), perhaps at manipulated prices, on a criminal blockchain. Beyond specific interesting insights, however, respondents did not mention any omission or non-conforming risk that directly invalidated or warranted reconsideration of the identified trends.

Review strengths and limitations

Despite consulting a futures database, most of the results identified concerned contemporary developments, with notable exceptions being satellite cryptocurrency vaults, some payments technologies and possible future charter cities. Some developments that have since been identified as ML/TF risks but that were not picked up in the review were include non-fungible tokens (NFTs) (Chipolina 2021). Many publications were also ambiguous in acknowledging the difference between ML/TF; several results were often mentioned for one crime (usually ML only) despite being relevant to both, or mentioned for both despite seemingly only being compatible with one.

Nevertheless, the large array of enablers, ML/TF methods, stakeholders and risk characteristics identified, courtesy of the diversity of material consulted, allowed underlying trends to be uncovered that could alleviate these limitations and inform futures thinking. This is arguably more useful than identifying specific, stand-alone future risks. By identifying such trends based on contemporary drivers of technological change and criminal abuse, *any* future development can be assessed for crime risks accordingly; whether it was specifically identified in the review or not therefore becomes insignificant.

The diversity of consulted material and quality assessments conducted also enhanced the quality of the devised underlying trends. This was mainly due to the two databases largely accounting for the shortfalls of the other. ST publications were often shorter in length (mainly news articles), therefore offering brief insights on multiple enablers of concern but little further discussion on their specific ML/TF possibilities, relevant stakeholders or risk characteristics. In contrast, PQC publications often focused on a smaller number of enablers but in great depth, often listing risk characteristics in tables and providing examples of misuse. The complementary and cross-corroborative nature of each database allowed for the better understanding of specific examples, relevant stakeholders and risk characteristics associated with each trend. This is thus motivated as an effective strategy for futures-oriented scoping reviews to come.

The positive feedback from the expert verification exercise suggests that the underlying trends identified are accurate. This was additionally useful in confirming the utility of these findings for a practitioner audience, including law enforcement, government, finance and compliance. It is possible that agreement was affected by conformity to prevailing discourses within specific industries. However, the potential for such biases across experts is reduced given the range of different industries consulted and the fact that they were interviewed independently.

Conclusion

The review has identified a range of different ways in which distributed ledger technologies, new payment methods and financial technologies are modernising ML/TF methods. Technological innovators, however, have no apparent intention of slowing down to re-assess their ML/TF risks. By using a modified methodology motivated as effective for similar exercises in the future, this review identifies six underlying trends from which ML/TF risks of emerging developments are forecasted to derive. The discussion has also assessed the particular risks within each trend that are likely to have a higher future impact (such as stablecoins). Having been verified as accurate by experts, these trends can form the basis of risk assessments for future technologies to pre-emptively determine their risks, so that they can be futureproofed in their development phase. Further research to more precisely determine the *levels* of risk that each enabler, stakeholder or characteristic generates, which has been touched upon in abstract terms in this study, can therefore assist in devising these futures-oriented risk assessments.

Even if risks are effectively assessed, however, the question remains how subsequent futureproofing or risk mitigation might actually occur without stifling otherwise hugely beneficial innovation. This question has eluded sound responses from governments and practitioners worldwide for too long. However, by clarifying the underlying sources and nature of these risks, this review hopes to have contributed to finding solutions to this inevitable dilemma.

Declarations

Word count

Text body: 9,365

Acknowledgements

Not applicable.

Conflicts of interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Funding

This study was funded by the Dawes Centre for Future Crime at UCL.

Data availability statement

The included publications for review, along with coded insights and an associated PRISMA-ScR checklist, can be found at: [link to be provided if/when article is approved].

References

Albrecht, Chad, Kristopher McKay Duffin, Steven Hawkins, and Victor Manuel Morales Rocha. 2019. 'The Use of Cryptocurrencies in the Money Laundering Process'. *Journal of Money Laundering Control* 22 (2): 210–16. https://doi.org/10.1108/JMLC-12-2017-0074.

Allison, Ian. 2019. 'UK Finance Watchdog Issues Guidance on Regulation for Bitcoin and Crypto Assets'. *CoinDesk*, 31 July 2019, sec. Markets. https://www.coindesk.com/uk-financial-watchdog-issues-full-guidance-on-crypto-assets.

Alsaibai, Hasan, Shooq Waheed, Fatima Alaali, and Rami Abu Wadi. 2020. 'Online Fraud & Money Laundry in E-Commerce'. In . Academic Conferences International Limited.

Arksey, Hilary, and Lisa O'Malley. 2005. 'Scoping Studies: Towards a Methodological Framework'. *International Journal of Social Research Methodology* 8 (1): 19–32. https://doi.org/10.1080/1364557032000119616.

Arslanian, Henri, Robert Donovan, Matthew Blumenfeld, and Anthony Zamore. 2021. 'El Salvador's Law: A Meaningful Test for Bitcoin'. Pwc. https://www.pwc.com/gx/en/financial-services/pdf/el-salvadors-law-a-meaningful-test-for-bitcoin.pdf.

Barone, Raffaella, and Donato Masciandaro. 2019. 'Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques'. *European Journal of Law and Economics* 47 (2): 233–54. https://doi.org/10.1007/s10657-019-09609-6.

BBC. 2019. 'Facebook Urged to Pause Currency Project'. *BBC News*, 19 June 2019, sec. Technology. https://www.bbc.com/news/technology-48688359.

Breslow, Stuart, Mikael Hagstroem, Daniel Mikkelsen, and Kate Robu. 2017. 'The New Frontier in Anti–Money Laundering'. *McKinsey & Company* (blog). November 2017. https://www.mckinsey.com/business-functions/risk/our-insights/the-new-frontier-in-anti-money-laundering.

Brito, Jerry. 2015. 'Some Facts about Digital Currency and Terrorist Financing'. Medium. 19 November 2015. https://medium.com/@jerrybrito/some-facts-about-digital-currency-and-terrorist-financing-ffe5e6962c66.

Buchanan, Bonnie. 2004. 'Money Laundering—a Global Obstacle'. *Research in International Business and Finance* 18 (1): 115–27. https://doi.org/10.1016/j.ribaf.2004.02.001.

Buku, Mercy W., and Michael W. Meredith. 2012. 'Safaricom and M-PESA in Kenya: Financial Inclusion and Financial Integrity Mobile Money Symposium 2013'. *Washington Journal of Law, Technology & Arts* 8 (3): 375–400.

Campbell-Verduyn, Malcolm. 2018. 'Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance'. *Crime, Law and Social Change* 69 (2): 283–305. https://doi.org/10.1007/s10611-017-9756-5.

Chattopadhyay, Kasturi. 2018. 'Transaction Laundering – A Growing Threat in the Payments Industry'. White paper. Infosys. https://www.infosys.com/industries/financial-services/documents/transaction-laundering.pdf.

Chen, Ting. 2018. 'Advanced Technologies for Detecting and Preventing Fraud at Uber'. *Uber Engineering Blog* (blog). 14 June 2018. https://eng.uber.com/advanced-technologies-detecting-preventing-fraud-uber/.

Chipolina, Scott. 2021. 'Art Has a Money Laundering Problem. NFTs Could Make It Worse - Decrypt'. *Decrypt*, 8 May 2021. https://decrypt.co/70190/art-has-a-money-laundering-problem-nfts-could-make-it-worse.

Choo, Kim-Kwang Raymond. 2013. 'New Payment Methods: A Review of 2010–2012 FATF Mutual Evaluation Reports'. *Computers & Security* 36 (July): 12–26. https://doi.org/10.1016/j.cose.2013.01.009.

———. 2015. 'Chapter 15 - Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?' In *Handbook of Digital Currency*, edited by David Lee Kuo Chuen, 283–307. San Diego: Academic Press. https://doi.org/10.1016/B978-0-12-802117-0.00015-1.

Christie, Lorna. 2018. 'Distributed Ledger Technology'. POSTbrief 28. London: Parliamentary Office of Science and Technology (POST), Houses of Parliament.

CipherTrace. 2019. 'Cryptocurrency Anti-Money Laundering Report, 2018 Q4'. CipherTrade Cryptocurrency Intelligence. https://ciphertrace.com/wp-content/uploads/2019/01/crypto_aml_report_2018q4.pdf.

Covolo, Valentina. 2019. 'The EU Response to Criminal Misuse of Cryptocurrencies: The Young, Already Outdated 5th Anti-Money Laundering Directive'. SSRN Scholarly Paper ID 3503535. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3503535.

Dostov, Victor, and Pavel Shust. 2014. 'Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?' *Journal of Financial Crime* 21 (3): 249–63. https://doi.org/10.1108/JFC-06-2013-0043.

Dufva, Mikko. 2019. 'What Is a Weak Signal?' *Sitra* (blog). 9 January 2019. https://www.sitra.fi/en/articles/what-is-a-weak-signal/.

Ekblom, Paul. 1997. 'Gearing Up Against Crime: A Dynamic Framework to Help Designers Keep up with the Adaptive Criminal in a Changing World'. *International Journal of Risk, Security and Crime Prevention* 2 (4): 249–65.

EUROPOL. 2021. 'COVID-19: Fraud'. Europol. 2021. https://www.europol.europa.eu/covid-19/covid-19-fraud.

Faith, Joe, Bashar Awwad Sheikh Hasan, and Amir Enshaie. 2020. 'Trusting ML in Anti Money Laundering -- A Risk-Based Approach'. v1.2. Caspian.

Farrugia, Steven, Joshua Ellul, and George Azzopardi. 2020. 'Detection of Illicit Accounts over the Ethereum Blockchain'. *Expert Systems with Applications* 150 (July): 113318. https://doi.org/10.1016/j.eswa.2020.113318.

FATF. 2006a. 'Report on New Payment Methods'. Financial Action Task Force. https://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf.

———. 2006b. 'Trade Based Money Laundering'. Financial Action Task Force. https://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf.

———. 2020. 'COVID-19-Related Money Laundering and Terrorist Financing: Risks and Policy Responses'. Financial Action Task Force.

Feedzai. 2021. 'What's the Secret to Strong AML Compliance? Strong People'. Feedzai. 12 November 2021. https://feedzai.com/blog/aml-201-why-banks-should-care-about-dark-money/.

FFIEC. 2016. 'Retail Payment Systems'. IT Examination Handbook. United States: Federal Financial Institutions Examination Council (FFIEC). https://ithandbook.ffiec.gov/media/211685/retailpaymentsystems2016.pdf.

Furst, Keith. 2018. 'The Future of Entity Due Dilligence'. Data Derivatives. https://static1.squarespace.com/static/5535b1bbe4b003f18c1cec26/t/5a713dfbe4966be6e6e3b2be/1517370880584/The+Future+of+Entity+Due+Diligence+-+Data+Derivatives+-+January+2018.pdf.

Gilbert, Paul. 2022. 'Buying And Selling Real Estate With Bitcoin In 2022'. Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides. 27 February 2022. https://bitcoinmagazine.com/business/buying-and-selling-real-estate-with-bitcoin.

Goldman, Zachary K, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss. 2017. 'Terrorist Use of Virtual Currencies: Containing the Potential Threat'. Energy, Economics and Security. CNAS.

Gomber, Peter, Jascha-Alexander Koch, and Michael Siering. 2017. 'Digital Finance and FinTech: Current Research and Future Research Directions'. *Zeitschrift Für Betriebswirtschaft* 87 (5): 537–80. https://doi.org/10.1007/s11573-017-0852-x.

Grant, Maria J., and Andrew Booth. 2009. 'A Typology of Reviews: An Analysis of 14 Review Types and Associated Methodologies'. *Health Information & Libraries Journal* 26 (2): 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x.

Guarascio, Francesco. 2016. 'EU to Step up Checks on Bitcoin, Prepaid Cards to Fight Terrorism'. *Reuters*, 2 February 2016. https://www.reuters.com/article/us-eu-terrorism-financing-idUSKCN0VB1N7.

He, Ping. 2010. 'A Typological Study on Money Laundering'. *Journal of Money Laundering Control* 13 (1): 15–32. https://doi.org/10.1108/13685201011010182.

Hiltunen, Elina. 2008. 'Good Sources of Weak Signals: A Global Study of Where Futurists Look For Weak Signals'. *Journal of Futures Studies* 12 (4): 21–44.

HM Treasury and Home Office. 2020. 'National Risk Assessment of Money Laundering and Terrorist Financing 2020'. London, United Kingdom: HM Treasury and Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf.

Hughes, Sarah Jane, and Stephen T Middlebrook. 2015. 'Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries'. *Yale Journal on Regulation* 32 (2): 495–559.

Hutchinson, Brian. 2012. 'Year in Ideas: Professor Touts Special Economic Zones Known as &quot;Charter Cities&quot;'; Nationalpost. 27 December 2012. https://nationalpost.com/news/year-in-ideas-professor-touts-special-economic-zones-known-as-charter-cities.

Jake. 2018. 'ALERT: Crypto Dusting Is a New Type of Blockchain Spam That…' *CipherTrace* (blog). 19 December 2018. https://ciphertrace.com/crypto-dusting/.

Kaminska, Izabella. 2017. 'Why Transaction Laundering Is Turning into a Huge Financial Blindspot'. Financial Times. 17 March 2017. http://ftalphaville.ft.com/2017/03/17/2186157/why-transaction-laundering-is-turning-into-a-huge-financial-blindspot/.

Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. 2020. 'Deepfakes: Trick or Treat?' *Business Horizons*, ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING, 63 (2): 135–46. https://doi.org/10.1016/j.bushor.2019.11.006.

Kurakin, Alexey, Ian Goodfellow, and Samy Bengio. 2017. 'Adversarial Machine Learning at Scale'. In *ArXiv:1611.01236 [Cs, Stat]*. http://arxiv.org/abs/1611.01236.

Lagarde, Christine. 2018. ‘How Policymakers Should Regulate Cryptoassets and Fintech’. *International Monetary Fund Finance & Development Magazine*, March 2018.

Letourneau, Keith B, and Stephen T Whelan. 2017. ‘Blockchain: Staying Ahead of Tomorrow’. *The Journal of Equipment Lease Financing (Online)* 35 (2): 1–6.

Mariñas, Josephine. 2018. ‘Cryptocurrency Predictions for 2018’. *CloudEmployee* (blog). 5 March 2018. https://cloudemployee.co.uk/blog/tech-news/cryptocurrency-predictions-for-2018/.

Martin, Aaron. 2019. ‘Mobile Money Platform Surveillance’. *Surveillance & Society* 17 (1/2): 213–22.

McHugh, Mary L. 2012. ‘Interrater Reliability: The Kappa Statistic’. *Biochemia Medica* 22 (3): 276–82.

Megaw, Nicholas. 2019. ‘Regulator Orders N26 to Improve Anti-Money Laundering Controls’. *Financial Times*, 22 May 2019. https://www.ft.com/content/cb06a354-7c97-11e9-81d2-f785092ab560.

Mugarura, Norman. 2014. ‘Customer Due Diligence (CDD) Mandate and the Propensity of Its Application as a Global AML Paradigm’. *Journal of Money Laundering Control* 17 (1): 76–95. https://doi.org/10.1108/JMLC-07-2013-0024.

Najumi, Mohadesa. 2021. ‘The First Bitcoin ETF Explained: What You Need to Know’. *Capital.Com*, 22 October 2021. https://capital.com/the-first-bitcoin-etf-explained-what-you-need-to-know?utm_medium=cpc&utm_source=googleads_search&utm_campaign=eu_en_search_max_generic_2022&utm_term=&campaignid=16454991302&adgroupid=&network=x&keyword=&matchtype=&creative=&adposition=&placement=&device=c&devicemodel=&extension=&loc_physical=9072483&gclid=EAIaIQobChMIz67GmLbk9gIVSQOLCh3zlA9iEAAYASAAEgKbQPD_BwE.

NIKKEI Asian Review. 2013. ‘Bitcoin’s Luster Dims as China Clamps down on Virtual Currency- Nikkei Asian Review’. *NIKKEI Asian Review*, 19 December 2013. https://web.archive.org/web/20170117061906/http:/asia.nikkei.com/magazine/20131219-Power-play/Markets/Bitcoins-luster-dims-as-China-clamps-down-on-virtual-currency.

Nolte, Julia, Yaniv Hanoch, Stacey Wood, and David Hengerer. 2021. ‘Susceptibility to COVID-19 Scams: The Roles of Age, Individual Difference Measures, and Scam-Related Perceptions’. *Frontiers in Psychology* 12. https://www.frontiersin.org/article/10.3389/fpsyg.2021.789883.

O’Brien, Kevin. 2018. ‘More Than 7.5 Million Chinese Use Crypto-Related Apps, Analysis Shows’. *CryptoGlobe*, 13 December 2018. https://www.cryptoglobe.com/latest/2018/12/more-than-7-5-million-chinese-use-crypto-related-apps-analysis-shows/?amp=yes&original_slug=more-than-7-5-million-chinese-use-crypto-related-apps-analysis-shows&page=3.

O’Donnell, John, and Tom Wilson. 2019. ‘Global Money-Laundering Watchdog Launches Crackdown on Cryptocurrencies’. *Reuters*, 21 June 2019. https://www.reuters.com/article/us-moneylaundering-crypto-fatf-idUSKCN1TM1I8.

O’Neal, Stephen. 2019. ‘Libra Seen as Threat to National Currency Sovereignty, Pleads With G-7’. *Cointelegraph*, 19 September 2019. https://cointelegraph.com/news/libra-seen-as-threat-to-national-currency-sovereignty-pleads-with-g-7.

Pawson, Ray, and Nicholas Tilley. 1997. *Realistic Evaluation*. London: SAGE.

Peters, Micah D. J., Christina M. Godfrey, Hanan Khalil, Patricia McInerney, Deborah Parker, and Cassia Baldini Soares. 2015. ‘Guidance for Conducting Systematic Scoping Reviews’. *International Journal of Evidence-Based Healthcare* 13 (3): 141–46. https://doi.org/10.1097/XEB.0000000000000050.

Peterson, Barry. 2013. ‘Red Flags and Black Markets: Trends in Financial Crime and the Global Banking Response’. *Journal of Strategic Security* 6 (5): 298–308. https://doi.org/10.5038/1944-0472.6.3S.28.

Qiu, Shilin, Qihe Liu, Shijie Zhou, and Chunjiang Wu. 2019. ‘Review of Artificial Intelligence Adversarial Attack and Defense Technologies’. *Applied Sciences* 9 (5): 909. https://doi.org/10.3390/app9050909.

Ramos, Pedro, Pierre Funderbuck, and Jennifer Gebelein. 2018. ‘Social Media and Online Gaming: A Masquerading Funding Source’. *International Journal of Cyber Warfare and Terrorism* 8 (1): 25–42.

Rapoza, Kenneth. 2017. ‘What China Ban? Cryptocurrency Market Cap Rebounding’. *Forbes*, 28 September 2017, sec. Investing. https://www.forbes.com/sites/kenrapoza/2017/09/28/china-ico-ban-bitcoin-crypto-currency-market-cap-returns/.

Reisen, Helmut. 2016. ‘Paul Romer: Back to a U.S.-Dominated World Bank?’ *The Globalist* (blog). 23 July 2016. https://www.theglobalist.com/paul-romer-united-states-dominated-world-bank/.

Reutzel, Bailey. 2016. ‘From Seeds to Weed, Bitcoin Finds Home Where Commerce Goes Gray’. *CoinDesk*, 5 June 2016, sec. Markets. https://www.coindesk.com/bitcoin-atms-gray-areas.

RNZ Insight. 2018. ‘Insight: Money Laundering in NZ’. Radio New Zealand. 19 July 2018. https://www.rnz.co.nz/national/programmes/insight/audio/2018654295/insight-money-laundering-in-nz.

Rossi, Ben. 2014. ‘The Future of Social Technology in Banking’. *Information Age* (blog). 24 November 2014. https://www.information-age.com/future-social-technology-banking-123458668/.

Shaping Tomorrow. n.d. ‘Turn Today’s Opportunities and Risks into Tomorrow’s Great Results!’ Shaping Tomorrow. https://www.shapingtomorrow.com/media-centre/st-brochure.pdf.

Sheluchin, Anwar. 2020. 'Cash and the Coronavirus: COVID-19 Is Changing Our Relationship with Money'. The Conversation. 7 July 2020. http://theconversation.com/cash-and-the-coronavirus-covid-19-is-changing-our-relationship-with-money-138774.

Smith, Tim. 2020. 'What Is Disruptive Technology?' Investopedia. 21 March 2020. https://www.investopedia.com/terms/d/disruptive-technology.asp.

Soudijn, Melvin R J. 2019. 'Using Police Reports to Monitor Money Laundering Developments. Continuity and Change in 12 Years of Dutch Money Laundering Crime Pattern Analyses'. *European Journal on Criminal Policy and Research* 25 (1): 83–97. https://doi.org/10.1007/s10610-018-9379-0.

Stempel, Jonathan. 2015. 'Liberty Reserve Founder Must Face $6 Billion Laundering Case in U.S - Reuters'. *Reuters*, 23 September 2015. https://www.reuters.com/article/us-usa-cybersecurity-liberty-reserve/liberty-reserve-founder-must-face-6-billion-laundering-case-in-u-s-idUSKCN0RN2L820150923?mod=djemRiskCompliance.

Swanson, Tim. 2014. *Great Chain of Numbers*. https://s3-us-west-2.amazonaws.com/chainbook/Great%20Chain%20of%20Numbers%20A%20Guide%20to%20Smart%20Contracts,%20Smart%20Property%20and%20Trustless%20Asset%20Management%20-%20Tim%20Swanson.pdf.

Tapscott, Don, and Alex Tapscott. 2016. *Blockchain Revolution*. New York: Penguin.

Teicher, Ron. 2018a. 'How Uber Ghost Rides Are Linked to Online Money Laundering'. *The Next Web*, 18 March 2018. https://thenextweb.com/contributors/2018/03/18/uber-ghost-rides-linked-online-money-laundering/.

———. 2018b. 'Transaction Laundering - Money Laundering Goes Electronic in the 21st Century'. *Finextra Research* (blog). 4 June 2018. https://www.finextra.com/blogposting/15423/transaction-laundering---money-laundering-goes-electronic-in-the-21st-century.

Tricco, Andrea C., Erin Lillie, Wasifa Zarin, Kelly K. O'Brien, Heather Colquhoun, Danielle Levac, David Moher, et al. 2018. 'PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation'. *Annals of Internal Medicine* 169 (7): 467. https://doi.org/10.7326/M18-0850.

Trulioo, and PYMNTS.com. 2020a. 'AML/KYC Tracker'. Trulioo, PYMNTS.com. https://www.pymnts.com/wp-content/uploads/2020/10/PYMNTS-2020-09-Trulioo-Tracker.pdf.

———. 2020b. 'AML/KYC Tracker'. Trulioo, PYMNTS.com. https://www.pymnts.com/wp-content/uploads/2020/10/PYMNTS-2020-09-Trulioo-Tracker.pdf.

Tu, Kevin V, and Michael W Meredith. 2015. 'Rethinking Virtual Currency in the Bitcoin Age'. *Washington Law Review* 90 (1): 271–347.

Tucker, Patrick. 2015. 'The Air Force Might Have To Protect Money Laundering in Space'. *Defense One* (blog). 22 March 2015. https://www.defenseone.com/technology/2015/03/air-force-might-have-protect-money-laundering-space/108132/.

Virga, Joy Marie. 2015. 'International Criminals and Their Virtual Currencies: The Need for an International Effort in Regulating Virtual Currencies and Combating Cyber Crime'. *Revista de Direito Internacional* 12 (2). https://search.proquest.com/docview/1770948083?accountid=14511.

Vlcek, William. 2011. 'Global Anti-Money Laundering Standards and Developing Economies: The Regulation of Mobile Money'. *Development Policy Review* 29 (4): 415–31. https://doi.org/10.1111/j.1467-7679.2011.00540.x.

Vovchenko, N G, O B Ivanova, O V Andreeva, and E D Kostoglodova. 2018. 'Conceptual Approach to the Development of Financial Technologies in the Context of Digitalization of Economic Processes'. *European Research Studies* 21: 11.

Wegberg, Rolf van, Jan-Jaap Oerlemans, and Oskar van Deventer. 2018. 'Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin'. *Journal of Financial Crime* 25 (2): 419–35. https://doi.org/10.1108/JFC-11-2016-0067.

Wewege, Luigi, Jeo Lee, and Michael C. Thomsett. 2020. 'Disruptions and Digital Banking Trends'. *Journal of Applied Finance & Banking* 10 (6). https://econpapers.repec.org/article/sptapfiba/v_3a10_3ay_3a2020_3ai_3a6_3af_3a10_5f6_5f2.htm.

Whisker, James, and Mark Eshwar Lokanan. 2019. 'Anti-Money Laundering and Counter-Terrorist Financing Threats Posed by Mobile Money'. *Journal of Money Laundering Control* 22 (1): 158–72. https://doi.org/10.1108/JMLC-10-2017-0061.

Williams, Clifford Curtis. 2013. 'A Burning Desire: The Need for Anti-Money Laundering Regulations in Carbon Emissions Trading Schemes to Combat Emerging Criminal Typologies'. *Journal of Money Laundering Control* 16 (4): 298–320. https://doi.org/10.1108/JMLC-01-2013-0003.

Woodford, Isabel, and Kim Darrah. 2019. 'Digital Banks Monzo, Revolut, Starling and N26 Compared'. *Sifted* (blog). 18 December 2019. https://sifted.eu/articles/challenger-banks-monzo-starling-revolut-n26-compared/.

Zamfir, Vlad. 2017. ‘Blockchains Considered (Potentially) Harmful’. *Medium* (blog). 21 August 2017. https://medium.com/@Vlad_Zamfir/blockchains-considered-potentially-harmful-d039888c3208.

Appendix 1: Search strings for identifying relevant publications

Table A1 shows the search strings used on both ProQuest Central and Shaping Tomorrow to identify money laundering and terrorist financing related publications.

Table A4 Search strings used to retrieve relevant publications

Query	Search string	Initial (2013-20)	Follow-up (2020)	Total
PQC_ML	(("LAUNDER* MONEY" OR "MONEY LAUNDERING") NEAR/30 ((FUTURE OR LATEST OR NEW OR TECHNOLOGICAL OR EMERGING OR PROJECTED OR DEVELOPING) NEAR/4 (TREND? OR DEVELOPMENT? OR METHOD* OR TYPOLOG???? OR TECHNIQUE? OR ADVANCE? OR TECHNOLOG????)))	231	41	272
PQC_TF	("FINANC* TERROR*" OR "TERROR* FINANC*" OR "FUND* TERROR*" OR "TERROR* FUND*" OR "FINANC* OF TERROR*" OR "FUND* OF TERROR*") NEAR/30 ((FUTURE OR LATEST OR NEW OR TECHNOLOGICAL OR EMERGING OR PROJECTED OR DEVELOPING) NEAR/4 (TREND? OR DEVELOPMENT? OR METHOD* OR TYPOLOG???? OR TECHNIQUE? OR ADVANCE? OR TECHNOLOG????))	67	9	76
ST_ML	"MONEY LAUNDERING" OR "LAUNDER! MONEY"	197	23	220
ST_TF	"TERROR! FINANC!" OR "FINANC! TERROR!" OR "FUND! TERROR!" OR "TERROR! FUND!" OR "FINANC! OF TERROR!" OR "FUND! OF TERROR!"	45	3	48
Total		**540**	**76**	**616**

Boolean search operators (searching both publication title and text):
AND/OR denotes the required/optional combination of terms respectively; brackets denote order of priority; double quotation marks denote exact phrases; *'NEAR/x'* denotes word proximity limits of one term to the other; asterisks (PQC) or exclamation points (ST) denotes wildcards (any type or number of letters to complete the preceding term); question marks (PQC) denote specific number of letters allowed for completing the preceding term.

Appendix 2: Publication exclusion criteria

The exclusion criteria applied to the initially identified publications, along with the numbers excluded at each stage, is shown in figure A1.

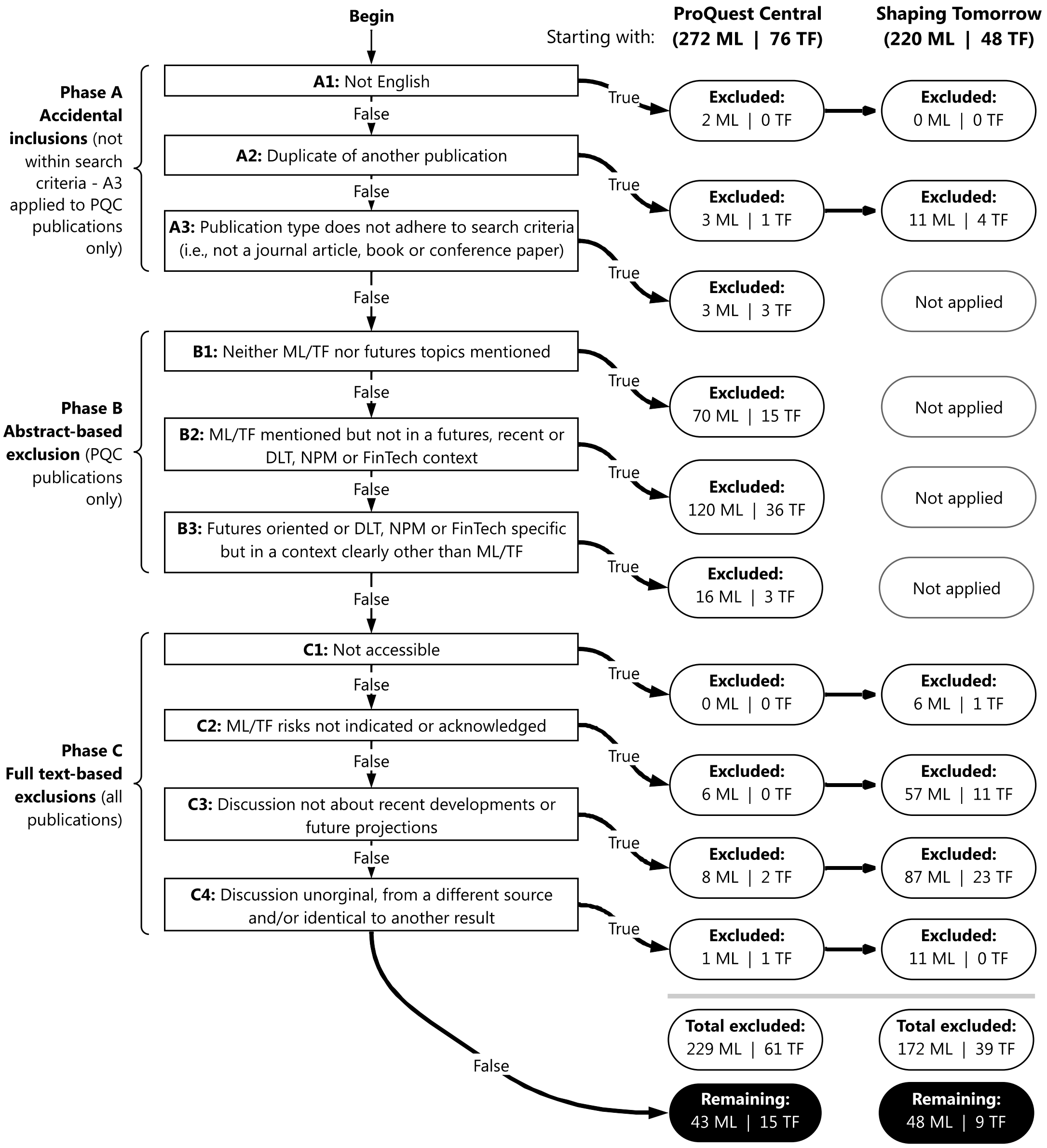
Begin
Starting with:
ProQuest Central (272 ML | 76 TF)
Shaping Tomorrow (220 ML | 48 TF)
Phase A Accidental inclusions (not within search criteria - A3 applied to PQC publications only)
A1: Not English
True
Excluded: 2 ML | 0 TF
Excluded: 0 ML | 0 TF
False
A2: Duplicate of another publication
True
Excluded: 3 ML | 1 TF
Excluded: 11 ML | 4 TF
False
A3: Publication type does not adhere to search criteria (i.e., not a journal article, book or conference paper)
True
Excluded: 3 ML | 3 TF
Not applied
False
Phase B Abstract-based exclusion (PQC publications only)
B1: Neither ML/TF nor futures topics mentioned
True
Excluded: 70 ML | 15 TF
Not applied
False
B2: ML/TF mentioned but not in a futures, recent or DLT, NPM or FinTech context
True
Excluded: 120 ML | 36 TF
Not applied
False
B3: Futures oriented or DLT, NPM or FinTech specific but in a context clearly other than ML/TF
True
Excluded: 16 ML | 3 TF
Not applied
False
Phase C Full text-based exclusions (all publications)
C1: Not accessible
True
Excluded: 0 ML | 0 TF
Excluded: 6 ML | 1 TF
False
C2: ML/TF risks not indicated or acknowledged
True
Excluded: 6 ML | 0 TF
Excluded: 57 ML | 11 TF
False
C3: Discussion not about recent developments or future projections
True
Excluded: 8 ML | 2 TF
Excluded: 87 ML | 23 TF
False
C4: Discussion unorginal, from a different source and/or identical to another result
True
Excluded: 1 ML | 1 TF
Excluded: 11 ML | 0 TF
Total excluded: 229 ML | 61 TF
Total excluded: 172 ML | 39 TF
False
Remaining: 43 ML | 15 TF
Remaining: 48 ML | 9 TF

Fig. A1 The hierarchical exclusion process

Where possible, inaccessible publications (e.g. with corrupted URLs) were retrieved using the online web archive *Wayback Machine*. Two ST_ML publications were retrieved in this way, while six ST_ML and one ST_TF result remained inaccessible (excluded at C1). Results that entirely concerned another publication (such as news articles announcing the release of a relevant report) were discarded and replaced by that publication, leading to three PQC_ML and three ST_ML results being substituted.

Appendix 3: Inter-rater reliability scores for quality assessments

Table A2 shows the quality assessment criteria applied to all included articles, for *neutrality, evidence, relevance* and *clarity*. The highest possible score for each category was a four.

Table A2 Publication quality assessment criteria

Score	Neutrality	Evidence	Relevance	Clarity
	The publishing entity…	*Publication reports…*	*Publication discusses…*	*Publication involves a…*
4	Requires publication to be peer-reviewed prior to release	Original and robust evidence, directly related to ML/TF, and formal data analysis (statistical or qualitative)	Several enabling technologies and several related elements (e.g. risky attributes, stakeholders) discussed	Clearly discusses ML/TF exploitation possibilities for all mentioned enabling technologies
3	Requires publication to be checked or edited to an extent prior to release, in a manner less rigorous than peer-review	A triangulation of different types of evidence (e.g. statistics, quotes of experts) from external sources with ML/TF inferences drawn by the author	Several enablers but little related elements OR few enablers with many related elements discussed	Clearly discusses ML/TF exploitation possibilities for some (but not all) mentioned enabling technologies
2	Does not require or explicitly state peer-review or editing at the stage at which the publication has been released (e.g. working or conference papers)	Only one type of evidence from external source offered with ML/TF inferences drawn by the author	One/few enablers but little relevant elements discussed	Discusses ML/TF exploitation possibilities in general terms and only in a broad context
1	Does not require peer-review / editing (blog or personal site)	Personal opinions without any accompanying evidence	One/few enablers discussed without any further details	Mentions ML/TF issues in an unclear context that is open to interpretation

The Fleiss' Kappa statistics for both rounds of coding are shown in table A3 with levels of agreement, according to standard interpretations of the κ statistic (McHugh 2012). Following the significant improvement in levels of agreement post-round 2, the remaining publications were coded by a single rater according to the clarified assessment criteria. Figure A2 shows the average quality scores for each technology category.

Table A3 Fleiss' Kappa statistic results for inter-rater reliability

Category	Round 1				Round 2			
	κ	*Z*	*p-value*	Agreement	*κ*	*Z*	*p-value*	Agreement
Neutrality	0.3850	3.11	0.0001	Fair	0.8438	8.46	0.0000	Almost perfect
Evidence	-0.0882	-0.71	0.7622	None	0.8043	6.14	0.0000	Almost perfect
Relevance	0.3292	3.40	0.0003	Fair	0.6956	7.00	0.0000	Substantial
Clarity	0.0867	0.88	0.1896	Slight	0.6807	6.72	0.0000	Substantial

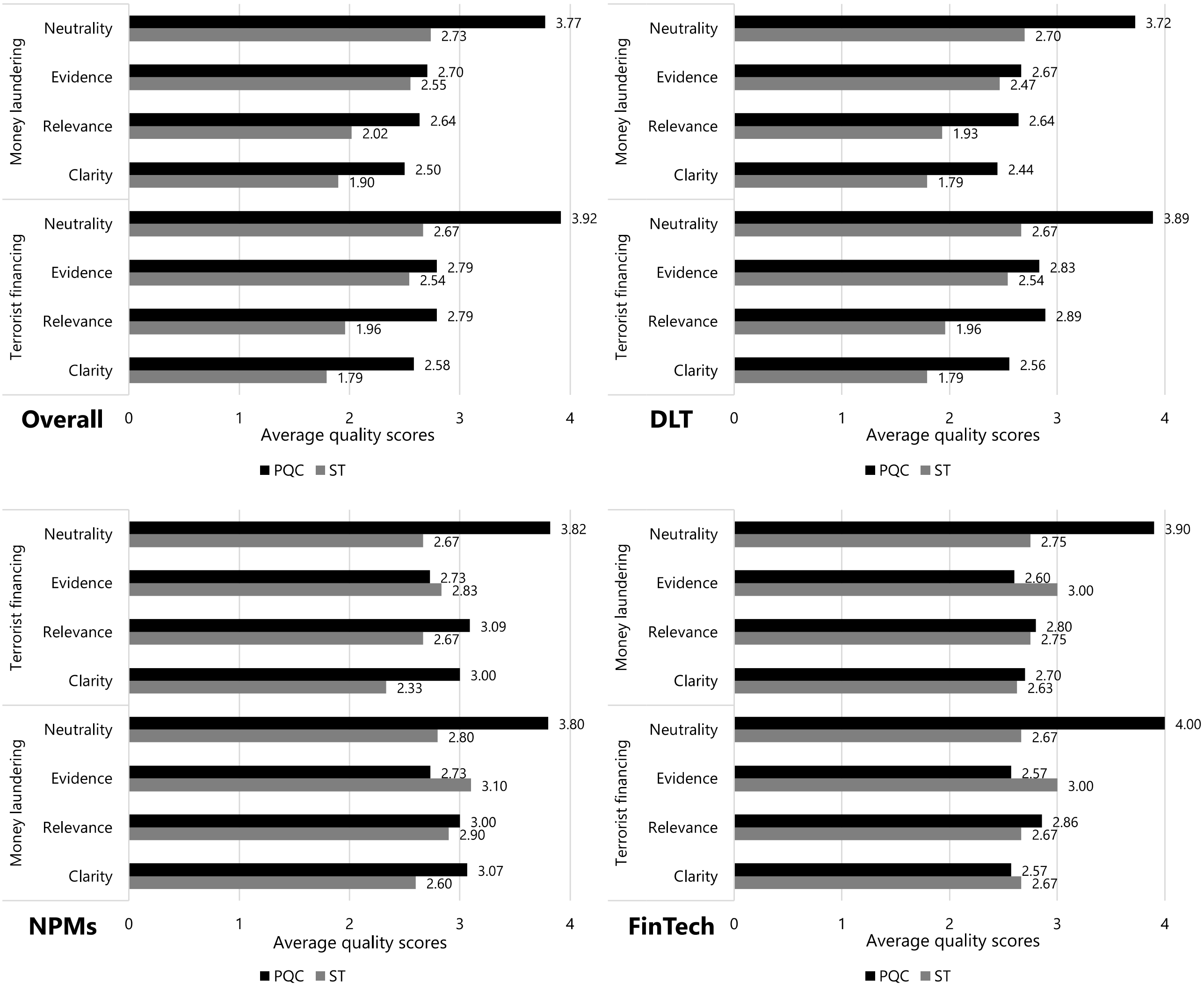

Fig. A2 Average quality assessment scores for publications by category

Appendix 4: Participant profiles for expert verification

Tables A4 and A5 show the anonymised professional and country profiles of the consulted experts for the verification phase of this review.

Table A4 Participant professional profiles for expert verification (*N*=51)

Industry	**DLT** (17)	**NPM** (17)	**FinTech** (14)
Academia	8	8	2
Consulting	2	2	3
Financial services	3	3	3
Government/international organisations	1	2	2
Information technology			1
Law enforcement	3	1	1
Legal		2	1
Think tanks/associations	1	1	1
Virtual asset services	1		

Figures in brackets denote number of participants for each technology category. Some participants had multiple occupations, meaning that column totals may exceed this number.

Table A5 Participant countries of occupation (*N*=51)

Country	**DLT** (17)	**NPM** (17)	**FinTech** (14)
Australia		2	
Brazil		1	1
Canada	1		
Estonia	1		
France			1
Germany			1
Global/worldwide	1		
Ireland	1	1	
Italy		1	
Latvia	1		
Malaysia		1	
Netherlands	1	1	1
New Zealand	1		
Russia	1	1	
Singapore		1	
Taiwan (Republic of China)			1

Turkey	1		
United Kingdom	7	4	8
United States	1	2	1

Figures in brackets denote number of participants for each technology category. Some participants had multiple countries of work, meaning that column totals may exceed this number.