Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study

Short running title: Preventing the money laundering and terrorist financing risks of emerging technologies

Eray Arda Akartuna, Shane D. Johnson and Amy Thornton

Declarations of interest: none.

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

The authors advise this manuscript to be published in **colour.**

Declarations of interest: none.

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

Abstract

Financial innovation and technological advances are growing at a pace unrivalled by any other period in history. However, as more stakeholders enter these markets, criminals are exploiting their inadvertent security deficiencies to launder illicit funds and finance terrorism. This three-round policy Delphi study involved consultations with 52 experts from different industries and countries to understand future risk-prone technological developments, possible prevention measures and relevant stakeholders. Results highlight a range of money laundering and terrorist financing risks being enabled by advances in distributed ledger technologies (predominantly through cryptocurrencies), new payment methods and financial technology (FinTech). These threats include privacy-enhanced cryptoassets, transaction laundering, e-currencies and digital-only financial services. Findings also suggest that detection-based countermeasures (currently the primary preventative approach) can be coupled with more diverse countermeasures to increase effectiveness. However, the unique circumstances and constraints specific to different stakeholders will affect the nature, utility, and extent to which they can implement certain countermeasures. As such, a 'one-size-fits-all' approach to prevention is undesirable. Drawing on expert insight from the study, we propose a framework and a 3-point standard of implementation to motivate cost-effective, user-friendly, and innovation-friendly measures to improve suspicious activity detection and futureproof technologies before their criminal exploitation becomes mainstream.

Keywords: money laundering, terrorist financing, financial technology, cryptocurrency, new payment methods, customer due diligence

1. Introduction

Although the 21st century global economy has faced its share of disruptions, technological innovation has continued to digitise and challenge financial norms. In February 2021, the value of Bitcoins in circulation exceeded USD $1 trillion for the first time (though has fluctuated since), surpassing the Russian Ruble (Field, 2021). One bank tipped it as the possible future 'currency of choice' (Browne, 2021; Kuhn, 2021). Moreover, new payment methods, such as mobile point of sale (POS) payments, were forecast to account for USD $2.5 trillion in worldwide transactions (an annual increase of 24%) in 2021 (Statista, 2021). The financial technology (FinTech) sector has also continued gathering pace, with over 52,000 new finance-related applications being released on app stores between September 2019 and September 2020 (Liftoff, 2020). Many of these trends have been bolstered by the Covid-19 pandemic and the associated substitution of physical financial flows by digital ones. Other major world events, such as the Russian invasion of Ukraine in February 2022, have further demonstrated the importance of harnessing new payments technologies; Ukrainian government cryptocurrency wallets crowdfunded $6 million in cryptocurrency donations less than a day after they were advertised on *Twitter*, in the first such donation campaign of its kind (Elliptic, 2022).

Despite the substantial socioeconomic benefits of many of these developments, their inadvertent criminogenic features cannot be ignored. For example, money launderers and financiers of terrorism have already taken advantage of many new technologies, including crowdfunding sites and services such as *Uber* and *AirBnB* (Soudijn, 2019; Teicher, 2018). Moreover, in 2015, EUROPOL (2015) reported that 40% of identified illicit transactions in Europe involved Bitcoin. With money laundering (ML) representing the crucial process of legitimising criminal proceeds, countering it is critical to disincentivising predicate offences such as transnational organised crime (Jee & Hutchinson, 2019). Combined with the devastating effects of terrorist financing (TF), the importance of preventing the exploitation of new technologies for ML/TF purposes is therefore evident.

The prevailing response advocated by existing 'anti-money laundering' and 'countering the financing of terrorism' (AML/CFT) frameworks involves bringing virtual asset service providers (VASPs), such as cryptocurrency exchanges, under traditional 'know your customer' (KYC), customer due diligence (CDD) and transaction monitoring obligations (Covolo, 2019). Obliged entities are required to know their customer and understand their normal transaction patterns so that anomalies can be detected and reported (Naheem, 2018). These obligations, dating back to 1990 and historically aimed at traditional financial institutions such as banks, were devised by the Financial Action Task Force (FATF), the international standard-setter for AML/CFT regulations (Nance, 2018). Like criminals, obliged entities and the associated compliance sector have also harnessed new technologies, such as machine learning and artificial intelligence (AI), to improve transaction monitoring systems (Arner et al., 2017) - a trend known as 'RegTech' (regulatory technology).

1.1. Issues with AML/CFT and new technologies

The application of traditional AML/CFT measures to new technologies poses three main problems. First, the ability to disguise identity more easily with many new automated payment platforms means that illicit transactions are becoming increasingly harder to distinguish from legitimate ones, given the lack of collectable financial intelligence. This results in large 'false positive' rates, namely innocent accounts being identified as suspicious. False flags account for around 95-99% of conventional AML/CFT systems, though one RegTech firm has stated that using big data and machine learning can reduce false positives in the financial services sector by up to 55% (Wass, 2017). Comprehensive data is yet to emerge on the effectiveness of RegTech on technology-enhanced transactions or new payment methods (many of which are not obliged to implement them), though the implications of false positives in the sector remain significant; in 2019, several users wrongly flagged by AML algorithms were locked out of their *Monzo* (United Kingdom) digital-only bank accounts, which left many unable to pay for rent or essential items for months (BBC, 2019; Smith, 2019). Customers have also recounted poor experiences with traditional CDD requirements, citing the time-consuming, face-to-face and paperwork-intensive nature of such systems (Lootsma, 2017).

Secondly, AML/CFT systems are becoming more expensive to implement, raising concerns for FinTech start-ups with limited financial capital. In 2020, the costs of anti-financial crime compliance overall were estimated to be USD $136.5 billion in Europe and USD $31.5 billion in North America (LexisNexis, 2020). These costs are likely to be passed onto customers. Historically, AML/CFT costs have not been matched by successes; using data published since 2011, a study by Pol (2020) estimates that just 0.1% of global criminal finances are captured by traditional AML/CFT measures and decries it as the 'world's least effective policy experiment'. Even after factoring in the most generous margins of error, such a low success rate illustrates that the issue lies deeper than reducing false positives. Particularly with new technologies, present frameworks may require enhancement and alternative strategies to increase cost-effectiveness.

The final concern relates to the impact of regulations on innovation and the diffusion of its benefits to the wider population. Decentralised applications (dApps) and smart contracts are now allowing users of Blockchains - the distributed digital ledger technology on which cryptocurrencies are based - to automate and trade goods and services peer-to-peer, more efficiently than in the conventional economy (Tapscott & Tapscott, 2016). FinTech[1] start-ups, cryptocurrency projects and new payment methods, meanwhile, are providing fast and efficient financial services to underbanked populations (populations that have a low rate of access to financial services) (Gross et al., 2012). This was one of the main driving forces for El Salvador, a country where 70% of the population is unbanked and 20% of GDP comprises of overseas remittances, accepting Bitcoin as legal tender in September 2021 (Arslanian et al., 2021). Prevailing Identity and paperwork-intensive AML/CFT requirements are therefore becoming less functionally compatible with such ventures. Many start-ups also prioritise rapid customer accumulation, leading to transaction monitoring backlogs as time-consuming CDD before onboarding measures struggle to keep pace (Megaw, 2019).

1.2. The importance of futureproofing

Cost-effective and timely regulations are vital to prevent malicious actors from exploiting innovative new technologies (Goodman, 2016). Forecasting and futureproofing new developments is therefore crucial, ensuring that criminals do not accumulate a practical advantage due to delayed preventative responses (Ekblom, 1997).

The implications of not futureproofing technologies can be severe. If a regulator does not act before criminal abuse of a technology becomes mainstream, they may resort to rash actions such as banning its use outright as alternative means of control become less feasible. Such actions negatively impact legitimate users while often doing little more than relocating crime to alternative platforms, a process known as displacement (Blasco & Fett, 2019; Ladegaard, 2019). Since many new technologies are digital and allow international transactions, crime displacement is easier compared to physical crimes (DiPiero, 2017).

Examples of where efforts to restrict digital technologies have backfired are worryingly numerous (Rapoza, 2017). For example, Chinese engagement with cryptocurrencies rose by 231% in the year after the Chinese government prohibited their use due to money laundering concerns (O'Brien, 2018). Following Russian moves to restrict cryptocurrency transactions, numerous virtual asset services began registering in

[1] The term *FinTech* is broad and employs many different definitions across studies (Schueffel, 2016), occasionally also encompassing DLT and NPMs, which are treated separately in this paper. For the purposes of this study, *FinTech* denotes new technology-enhanced financial services and products (such as banking, lending, or securities trading) complementing or being introduced within the traditional financial sector.

neighbouring Estonia instead, where crypto policies are comparatively more lenient (Ghosh, 2021; TASS, 2022). One such service, namely Chatex crypto-exchange, was sanctioned by the United States in 2021 having facilitated the laundering of Russia-based ransomware and darknet market proceeds (U.S. Treasury, 2021).

1.3. Research aims

This study employs the Delphi method to consult experts across different industries to meet two core objectives. The first is to understand what technologically enabled ML/TF risks are projected to take hold in the future and what stakeholders are relevant in facilitating or preventing them. The second is to gauge different expert perspectives on how these new risks can be prevented, additionally identifying what roles different stakeholders have to play in resolving present AML/CFT deficiencies.

The Delphi methodology is briefly discussed in the next section. This is followed by a discussion of the methodology used in the current study and the findings. Utilising the perspectives offered by participants, the discussion that follows devises a widely applicable framework, intended to enhance the pre-emptive application of cost-effective measures to prevent the ML/TF risks of the future.

2. Delphi studies

Futures-oriented topics often lack concrete data or evidence needed for conventional research methods and analysis (Mitchell, 1992). The experience and insights of field experts, which can help inform professional forecasts for future scenarios, therefore become favourable alternative resources for conducting futures-based research (Devaney & Henchion, 2018). The Delphi method, created by the RAND Corporation in the 1950s, is perhaps one of the most effective methods of gauging such insights (Dalkey, 1968). It involves a series of iterative surveys, conducted amongst a pre-determined panel of experts, with group responses aggregated and presented to the panel prior to each round to inform the next series of responses (Bradley & Stewart, 2003; Vernon, 2009). By doing so, panellists are informed of the level of dissent or agreement compared to their own responses, allowing key points of consensus or dissensus to emerge as the rounds progress (Iqbal & Pipon-Young, 2009). The method has become popular in assessing future scenarios in several industries, including healthcare (Chang et al., 2010; Keeney et al., 2006), technology (Alon et al., 2019; Merfeld et al., 2019), finance (Kozak & Iefremova, 2014; Velez et al., 2020) and, to a lesser extent, crime (Coutorie, 1995).

Delphi studies are typically anonymous (panellists are not aware of each other's identity), iterative (occur across a succession of rounds), utilise controlled feedback (aggregate responses are presented to panellists after each round) and use statistical group response (to present results) (Rowe et al., 1991). Their anonymity and aggregated nature of presented results prevents 'groupthink' bias amongst panellists (GO Science, 2018), while still allowing participants to engage with other experts responses.

Delphi studies can be conducted online, face-to-face, in distinct stages or dynamically in real time (Gordon & Pease, 2006). The size of the expert population, research question, and available resources will determine the most appropriate survey design (Belton et al., 2019). Since their mainstream adoption, several proposals to standardise how they are devised, implemented, and reported have been proposed (Beiderbeck et al., 2021a; Belton et al., 2019; Bloem da Silveira Junior et al., 2018; Day & Bobeva, 2005). To increase the insight gained, data collected through Delphi studies have more recently been analysed using used a range of analytic approaches, including sentiment analysis, cross-impact analysis and fuzzy e-means algorithms (Beiderbeck et al., 2021b). The next section provides the specific methodology, based on existing studies and advised standards, taken for the current study.

3. Methodology

Based on their overall objective, Delphi studies can take different forms. These may seek to specifically build consensus (consensus Delphi), inform decisions as they take place (modified/decision Delphi) or specifically identify dissensus (Hasson & Keeney, 2011; Rauch, 1979). This study can be characterised as a 'Policy Delphi'; namely, it seeks to collate views from a diverse range of industries to inform possible solutions to an emerging problem, focusing particularly on points of dissent (Turoff, 1970). Hence, it is not only concerned about building consensus, but also observing where and why it does not exist (de Loë et al., 2016). Thus, this study is limited to three rounds, with only the final round afforded to response adjustment.

The flowchart in figure 1 summarises the methodology employed, with the subsections thereafter explaining the process in more detail. The presentation of figure 1 is adapted from similar flowcharts used by Pätäri (2010) and Kluge et al. (2020), though tailored to best visualise the specific circumstances of the current study. Relevant sections of the data supplement (highlighted in Figure 1) provide further detail.

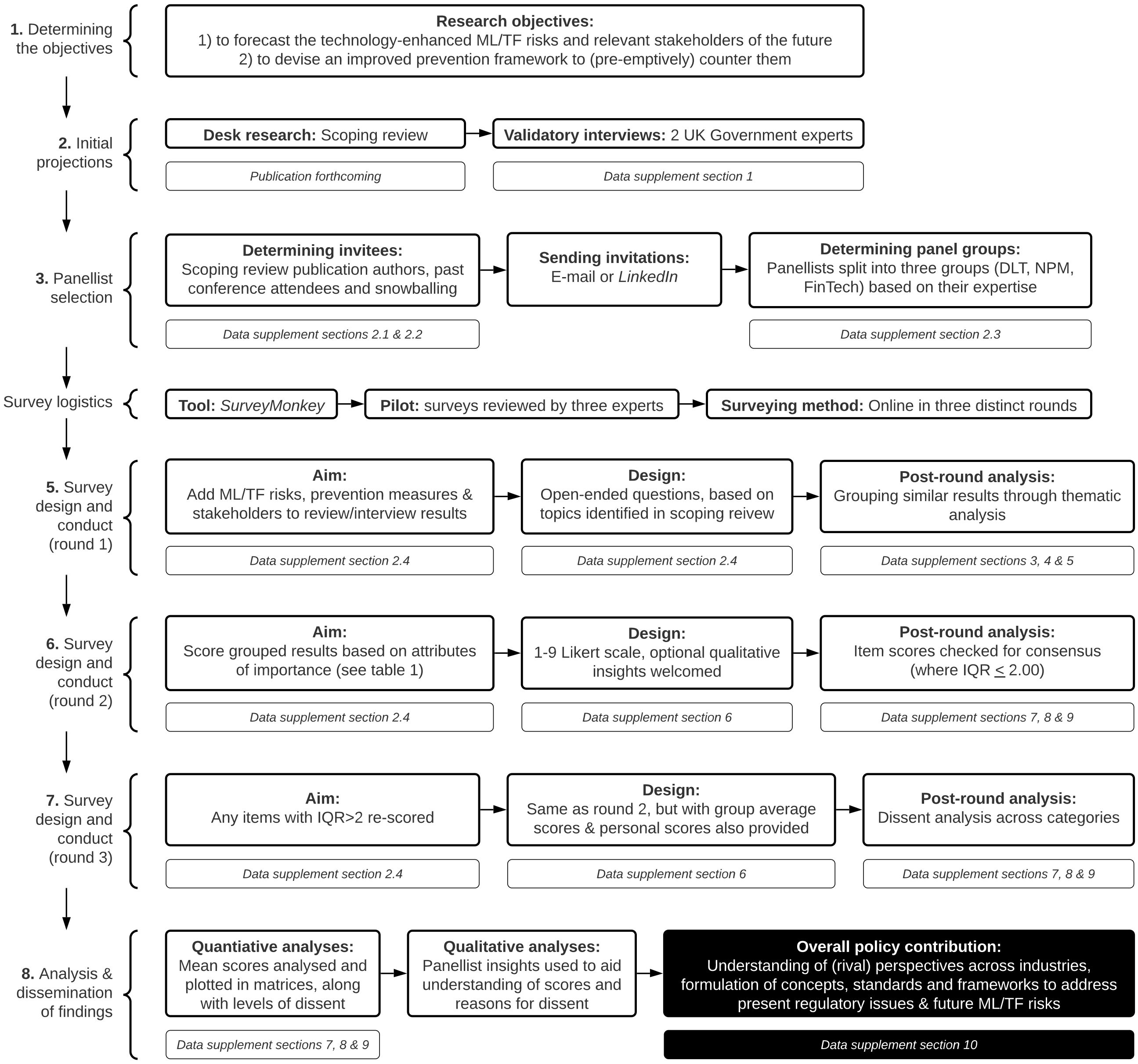
1. Determining the objectives
Research objectives:
1) to forecast the technology-enhanced ML/TF risks and relevant stakeholders of the future
2) to devise an improved prevention framework to (pre-emptively) counter them
2. Initial projections
Desk research: Scoping review
Publication forthcoming
Validatory interviews: 2 UK Government experts
Data supplement section 1
3. Panellist selection
Determining invitees: Scoping review publication authors, past conference attendees and snowballing
Data supplement sections 2.1 & 2.2
Sending invitations: E-mail or LinkedIn
Determining panel groups: Panellists split into three groups (DLT, NPM, FinTech) based on their expertise
Data supplement section 2.3
Survey logistics
Tool: SurveyMonkey
Pilot: surveys reviewed by three experts
Surveying method: Online in three distinct rounds
5. Survey design and conduct (round 1)
Aim: Add ML/TF risks, prevention measures & stakeholders to review/interview results
Data supplement section 2.4
Design: Open-ended questions, based on topics identified in scoping reivew
Data supplement section 2.4
Post-round analysis: Grouping similar results through thematic analysis
Data supplement sections 3, 4 & 5
6. Survey design and conduct (round 2)
Aim: Score grouped results based on attributes of importance (see table 1)
Data supplement section 2.4
Design: 1-9 Likert scale, optional qualitative insights welcomed
Data supplement section 6
Post-round analysis: Item scores checked for consensus (where IQR ≤ 2.00)
Data supplement sections 7, 8 & 9
7. Survey design and conduct (round 3)
Aim: Any items with IQR>2 re-scored
Data supplement section 2.4
Design: Same as round 2, but with group average scores & personal scores also provided
Data supplement section 6
Post-round analysis: Dissent analysis across categories
Data supplement sections 7, 8 & 9
8. Analysis & dissemination of findings
Quantiative analyses: Mean scores analysed and plotted in matrices, along with levels of dissent
Data supplement sections 7, 8 & 9
Qualitative analyses: Panellist insights used to aid understanding of scores and reasons for dissent
Overall policy contribution: Understanding of (rival) perspectives across industries, formulation of concepts, standards and frameworks to address present regulatory issues & future ML/TF risks
Data supplement section 10

Fig. 1 Flowchart showing the Delphi process

3.1. Developing projections

Typically, the research question and survey design are informed by prior preliminary work such as literature reviews or interviews (Day & Bobeva, 2005; Novakowski & Wellar, 2008; Schmalz et al., 2021). The current study utilises both. First, we conducted a scoping review of academic and futures-oriented literature published between 2013 and 2021 concerned with ML/TF risks and relevant stakeholders. The results and underlying trends identified in the review were then scrutinised across two interviews with UK Government experts.

The contribution of these preliminary exercises was twofold. Firstly, both studies provided a host of potential panel invitees. Secondly, the results were used to structure the open-ended first-round survey in an accessible way, including pre-identified examples of future ML/TF risks and stakeholders to assist panellists in thinking about any additional contributions they wished to provide.

3.2. Panellist selection

The effective selection of panellists is central to ensure meaningful results and continuity across rounds (Belton et al., 2021). Given the specific nature of topics and associated difficulties with finding many willing expert participants, policy Delphis have tended to use convenience rather than representative sampling to recruit participants (Belton et al., 2019). Criteria for panellist selection have usually been based on organisational and personal characteristics (de Loë et al., 2016). However, to address one of the main criticisms of policy Delphis, namely that they can lack diversity (Franklin & Hart, 2006), an emphasis was placed upon inviting panellists from a wide range of industries, professions and jurisdictions.

For this Delphi, possible panellists were identified through three sources: authors identified in the scoping review, attendees of conferences organised by the author's department (see data supplement section 2.1) or individuals identified via snowball sampling. Snowballed individuals were either suggested by one of 16 specifically contacted individuals with large networks known to the authors, or other invitees. Of the 16 specifically contacted, 11 were financial sector professionals, three government agency analysts and two academics. Personalised invitations were sent through e-mail (if an e-mail address was known) or *LinkedIn*. Invitation and response rates are shown in figure 2. The result of the recruitment phase was a medium-sized panel spanning all inhabited continents of the world (see figure 3), which carried importance given the global nature of the problem.

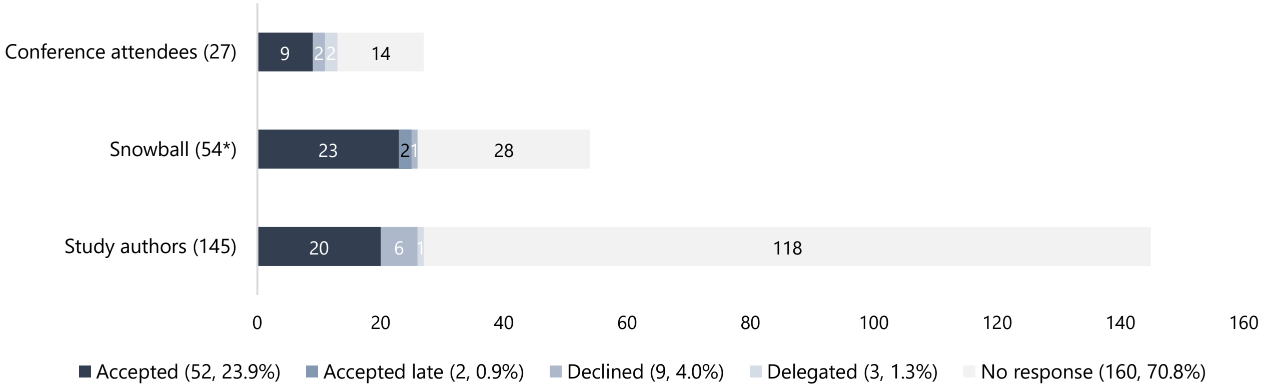

Fig. 2 Chart showing panellist invitation responses (N=226). Numbers and percentages in brackets indicate totals adhering to each category/response. 'Accepted late' denotes those submitting responses after each round had closed and subsequent analysis conducted, meaning their responses were not considered. **It was occasionally unclear how many potential panellists some gatekeepers forwarded invitations to, meaning that the number of snowballed invitees was at least 54 but likely more.*

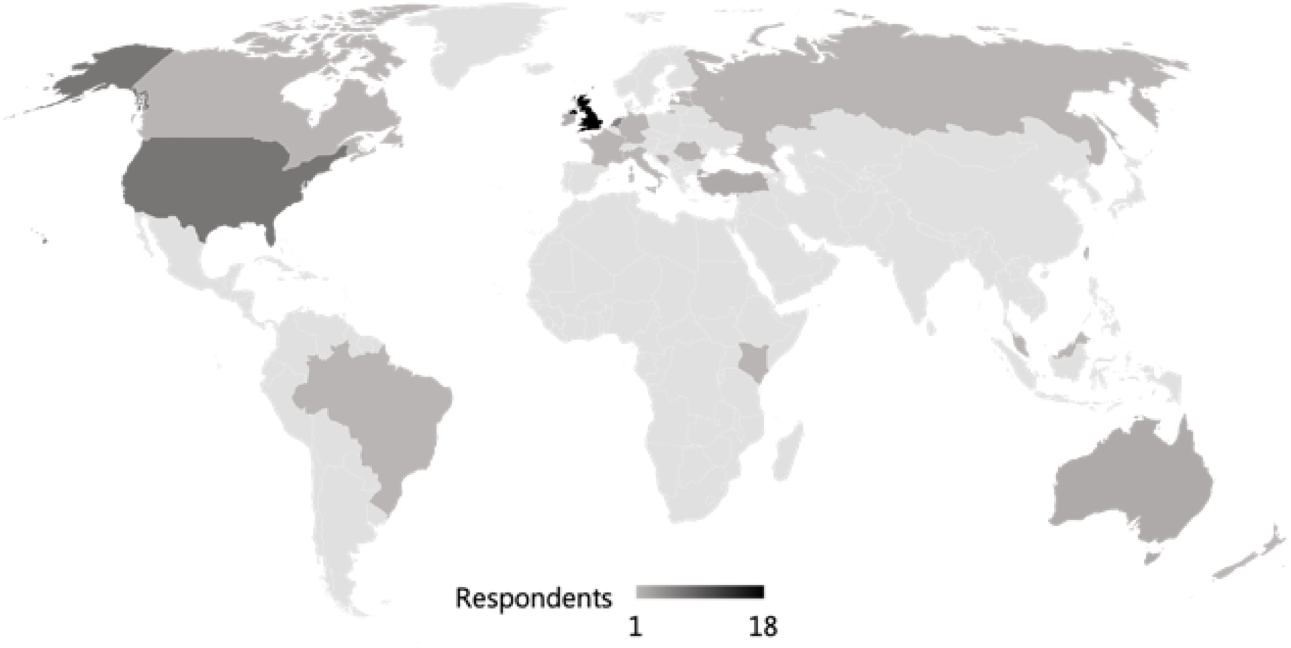

Fig. 3 Number of panellists accepting to participate by country (full breakdown in data supplement section 2.2)

Conducted during the Covid-19 pandemic across several time zones, a real-time or face-to-face Delphi was impossible. A further consideration was made on how to address the highly broad nature of topics, as an expert in one area (such as open banking) may not necessarily be an expert in another (such as privacy-enhanced cryptocurrencies). Numerous solutions exist for facilitating interactions between diverse panels to ensure more informed responses, though most involve a degree of real-time or physical contact between panellists (Dalal et al., 2011).

For feasibility reasons, this Delphi study split the 52 panellists into three groups, representing distributed ledger technologies (N=21), new payment methods (N=23) and FinTech [2] (N=18) professionals respectively. Panellists were given the opportunity to join multiple groups if they wished, and all aspects of study conduct (rounds, survey design, question styles and timeframes) were standardised across groups – the only difference being the contents of the questions themselves, which were specific to the technology category. Though these categories are by no means mutually exclusive, they were hypothesised to best reflect the fields of specialisation in modern-day finance. This meant that an open banking professional (FinTech) would not be asked questions about privacy tokens (distributed ledger technologies), for example. The industries and employment roles represented within each group are shown in figures 4 and 5 respectively.

[2] FinTech surveys were named *'new financial services and products'* to account for the definitional ambiguity surrounding the term 'FinTech'.

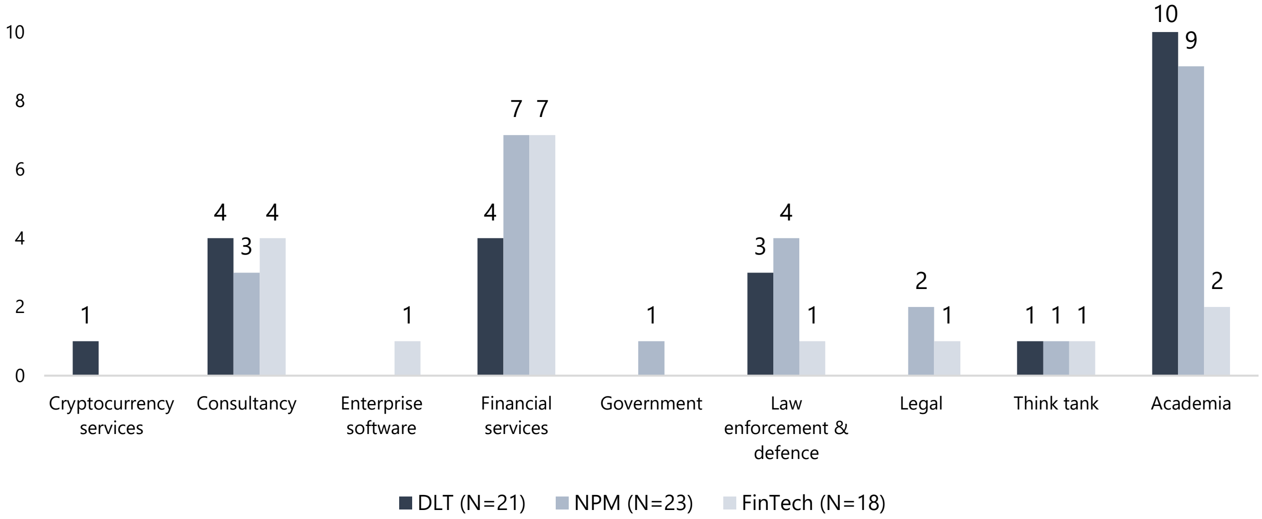

Fig. 4 Number of panellists by industry (full breakdown in data supplement section 2.2). Note: some panellists worked across multiple industries, so totals may exceed *N* values

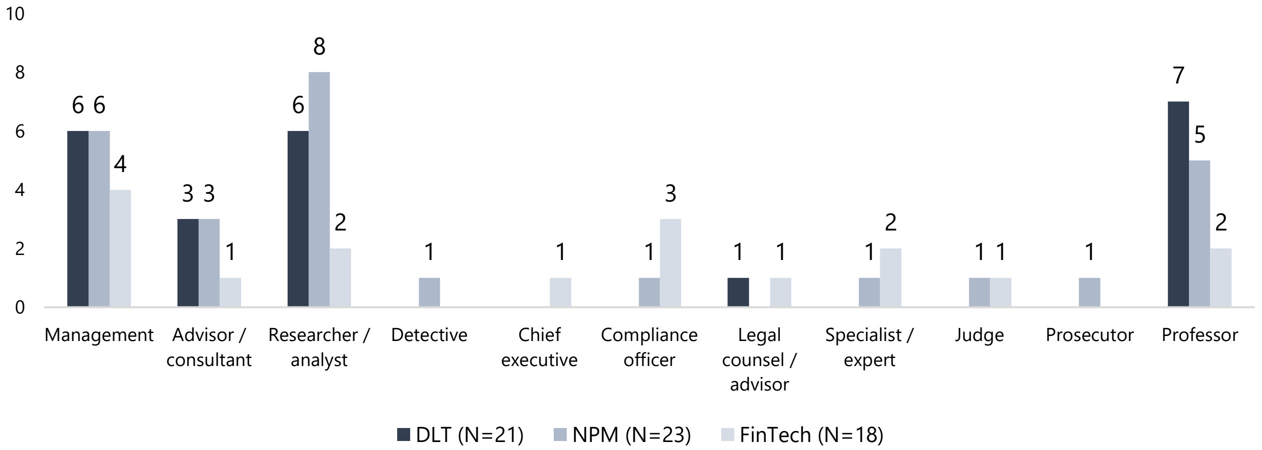

Fig. 5 Number of panellists by profession (full breakdown in data supplement section 2.2). Note: some panellists had multiple jobs, so totals may exceed *N* values

3.3. Survey design

Numerous online tools, some designed for Delphi studies specifically, exist to design surveys (Belton et al., 2019). This study uses *SurveyMonkey* to implement three rounds of surveys, adopting the same structure for DLT, NPMs and FinTech. All surveys (and preceding semi-structured interviews) were performed under conditions of anonymity with explicit consent from participants, per ethics approval and data protection registration from University College London (UCL), in compliance with General Data Protection Regulations (GDPR). All surveys were piloted across and adjusted according to recommendations from three non-participating experts who were familiar with the Delphi process.

The collective findings of the initial scoping review and interviews were used to formulate and provide examples for the first round of the study, which was formed of open-ended questions encouraging panellists to identify any other ML/TF risks, prevention measures and relevant stakeholders they could think of. Responses were subsequently combined with the scoping review and interview results through thematic analysis, leading to 93 ML/TF risks, 122 prevention measures and 122 relevant stakeholders being identified (see data supplement section 2.3, table 6).

These insights were grouped according to similarity to both combine similar insights and to make subsequent surveys more feasible in terms of length. They were then scored in the second round based on a series of attributes devised to answer the research questions, shown in table 1. A 9-point Likert scale was used for numerical scoring, based on prevalent advice in the field that recommends either 7-point (Preston & Colman, 2000) or 9-point (Fitch et al., 2001; McMillan et al., 2016) scales as best practice.

Table 1 Attributes scored in rounds 2 and 3 (see data supplement section 2.3 for full Likert score ranges)

Section	Attribute (perceived)	Score range	
		1	9
ML/TF risks	Likelihood of ML/TF risk becoming mainstream in the future	Extremely unlikely	Extremely likely
	Impact of risk, i.e. amount of ML/TF facilitated	Non-existent	Catastrophic
Prevention measures	Effectiveness	Extremely ineffective	Extremely effective
	Monetary cost	Extremely low cost	Extremely costly
	Societal cost	Extremely low cost	Extremely costly
Relevant stakeholders	Power/influence to prevent technology-enhanced ML/TF	Extremely powerless	Extremely powerful
	Responsibility to prevent technology-enhanced ML/TF	Extremely irrelevant	Extremely responsible

For all scales, '5' denoted a neutral score.

Delphi studies can employ numerous methods to identify levels of consensus, including different thresholds and measures of spread, such as standard deviations, the interquartile range (IQR) or specific metrics such as Fleiss' Kappa (Diamond et al., 2014). Based on previous work (von der Gracht, 2012), we used the IQR, and items with an IQR ≤2.00 were deemed to have reached consensus. In round 3, panellists were asked about attributes for which consensus was not reached. The survey structure was identical to round 2 but also contained reminders of the panellist's own previous response as well as the group average. Panellists were then invited to change (or not) their initial scores and to provide qualitative justifications for their choices.

Figure 6 shows participation across rounds and the dates that rounds were open. The first round was open to engage as many panellists as possible, so that the impact of subsequent attrition across rounds would be reduced. The durations of each round were in line with standard timeframes proposed for typical Delphi studies, which range from three to eight weeks (Belton et al., 2019; Keeney et al., 2006). Typical times spent on surveys were 10-15 minutes (round 1), 10-12 minutes (round 2) and 6-7 minutes (round 3). As the figure shows, panellist attrition was particularly notable, the effects of which are acknowledged and addressed in the 'further research' section of this article.

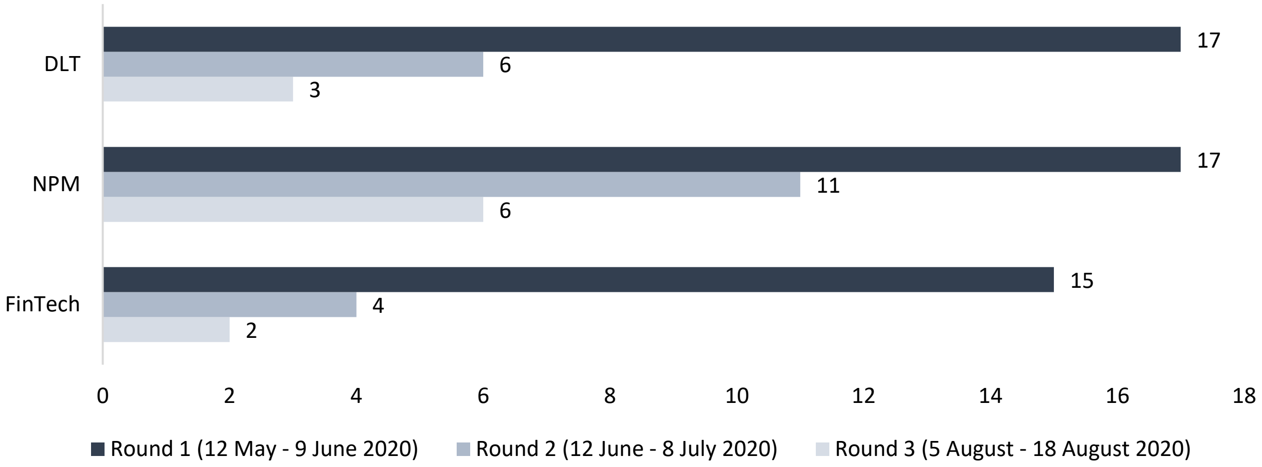

Fig. 6 Panellists fully completing each round (full breakdown: data supplement section 2.4)

4. Results

The three sections below report the identified insights post-thematic analysis (in tables) and post-round 3 attribute scores (in charts) for ML/TF risks, prevention measures and relevant stakeholders respectively. Each section is split into subsections for DLT, NPM and FinTech survey results. The tables are accompanied by brief descriptions of each insight unless they are self-explanatory or not elaborated upon by panellists. The charts denote the mean scores for each insight per respective attributes. All mean scores are based on round 3 scores unless they had already reached consensus in round 2 (in which case they were not subject to rescoring in round 3). Where consensus did not exist, they are shown in red with error bars (denoting the upper and lower quartiles).

Each section then provides an overview of the issues identified across the three technology categories, including their perceived criminogenic characteristics. This is based on both the attribute scores and qualitative insights provided (if any) by panellists. Since panellists were not obliged to explain their scores, some insights present in tables may be omitted from the overview of their criminogenic characteristics. A comparison of consensus changes across rounds (dissent analysis) is provided at the end of the results question

4.1. Issues to note when comparing results

The difference in scores across the three technology categories broadly reflect the differences between each category in terms of risk likelihood/impact, prevention measure cost-effectiveness and stakeholder powers/responsibilities. However, it should be noted that the panellists involved differed for each technology category (DLT, NPM, FinTech). As it is possible that different groups may have calibrated their scoring differently (e.g., one group may have been more conservative than another), comparisons that consider how absolute values vary across categories should be done cautiously.

It should be noted that only four panellists provided scores for FinTech, which is the lower end of the typical sample size (minimum 5) acceptable for Delphi studies (Delbeq et al., 1976; Rowe & Wright, 2001). Thus, while their results are shown, subsequent discussions are weighted towards the scores gained from DLT (6 panellists) and NPM (11 panellists) responses, which FinTech results largely complemented. The small sample sizes did not allow for more comprehensive statistical tests beyond the reporting of mean values (for scores) and changes in items achieving consensus (for dissent analysis) (Belton et al., 2019).

5. ML/TF risks

Tables 2-4 list and describe the identified ML/TF risks for DLT, NPMs and FinTech, respectively. Figures 7-9 show these identified risks scored by panellists on the 'likelihood' and 'impact' dimensions. Items located in the top (bottom) right (left) are those that were perceived to be most (least) likely to be exploited and that would have the largest (least) impact on offending.

5.1. DLT ML/TF risks and likelihood/impact scores

Table 2 DLT ML/TF risks

Risk	Description	Source
Bitcoin ATMs	Specialised cryptocurrency ATMs that allow users to convert cash into Bitcoin (and sometimes vice versa)	Review
Coloured coins / non-fungible tokens	Cryptocurrencies with asset information attached to them, such as fine art, gambling chips, etc	First round
Cryptocurrency mining	Offering computing power to verify blockchain transactions, earning cryptocurrency in the process	Interview
Crypto-mules	Willing or defrauded individuals transferring illicit cryptocurrencies through their wallets for criminals	First round
Initial coin offerings (ICOs)	Crowdfunding opportunities allowing individuals to invest in new tokens issued by businesses	Review
Mixers/tumblers	Services that increase anonymity by mixing potentially illicit cryptocurrency, thereby reducing its traceability	Review
Privacy coins	Cryptocurrencies that conceal transaction amounts and history (examples include *Monero* and *Ghost*).	First round

Security token offerings (STOs)	Digital initial product offerings where tokenised digital securities (security tokens) are traded on an online exchange.	Review
Smart contracts	Automatically executed contracts (e.g. conditional transactions) that are built into lines of code.	First round
Stablecoins	Cryptocurrencies with a fixed exchange rate to standard currencies	Review
Storing cryptocurrency in satellites	Purchasing access to a satellite vault using a space start-up and storing cryptocurrency in it to evade earthly regulations	Review
Storing cryptocurrency in USBs / body-embedded chips	*No description/self-explanatory*	First round

N_{Round 1}=17

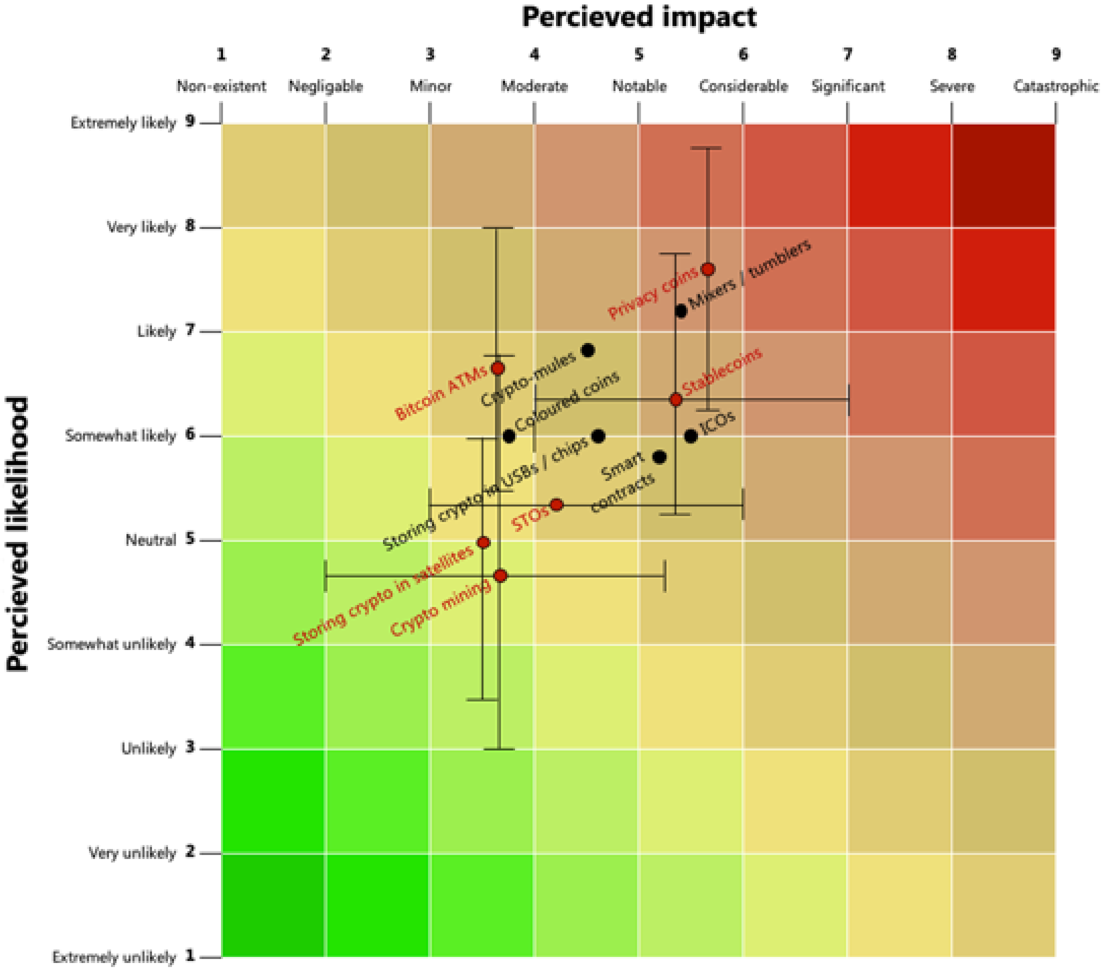

Fig. 7 DLT ML/TF risk matrix of likelihood and impact scores *($N_{Round\ 2}$=6, $N_{Round\ 3}$=3).* Error bars are shown for items in red where consensus was not reached (i.e., IQR > 2)

5.2. NPM ML/TF risks and likelihood/impact scores

Table 3 NPM ML/TF risks

Risk	**Description**	**Source**
Customer loyalty rewards	Tradable items such as airline vouchers, loyalty reward points and similar instruments that hold some value	First round
Fake goods and services traded online	Using relevant apps or digital marketplaces to list fake goods/services, allowing accomplices to 'purchase' them and transfer illicit funds in the process	First round
Faster payment methods	For example contactless, Apple Pay, G-Pay, Bluetooth payments, 5G-enabled payment technologies (etc.)	First round
Software, apps and games as tradable commodities	Using software, apps and games as instruments of value that can be purchased with illicit funds and traded	First round
Misuse of electronic money transmitters	Examples include *PayPal* and chargeback fraud, where a payment using illicit funds is made and immediately contested, so that funds are returned and recorded as a refund	Review
Payments using social media and communications technologies	Examples include the ability to send and receive money on Facebook Messenger, Skype and over e-mail	Review
Transaction laundering	Using the merchant account of a front business to process illicit transactions (for example for drugs or firearms)	Review
Transferring funds online during live broadcasts and other ephemeral content	For example collecting 'donations' during a live social media video, which then disappears after 24 hours, thus reducing traces of criminal intent	First round
Virtual currencies and commodities	Including online gaming currencies, unique game characters that are valued amongst players and other virtual assets such as e-metals	First round

$N_{Round\ 1}$=17

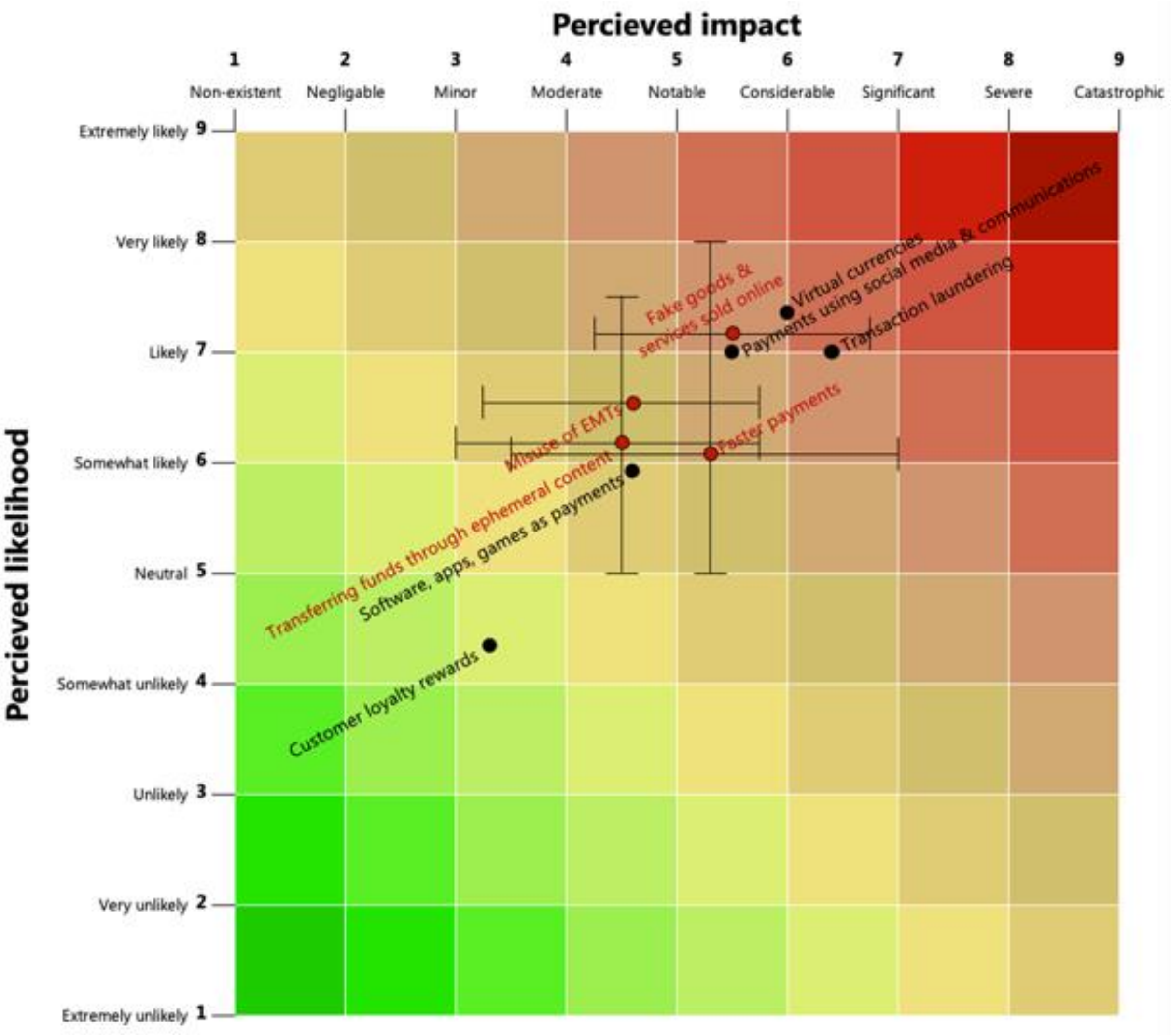

Fig. 8 NPM ML/TF risk matrix of likelihood and impact scores *($N_{Round\ 2}$=11, $N_{Round\ 3}$=6)*. Error bars are shown for items in red where consensus was not reached (i.e., IQR > 2)

5.3. *FinTech ML/TF risks and likelihood/impact scores*

Table 4 FinTech ML/TF risks

Risk	**Description**	**Source**
Central bank digital currencies (CBDCs)	Standard currency issued in digital form, which can make securities settlements easier due to automated payouts	First round
Charter cities and free-trade zones	Special economic zones with unique laws and often low regulations, designed to encourage trade and commerce	Review
Crowdfunding	Services that allow individuals to set up fundraising pages for a cause of business venture, allowing individuals to donate or invest	Review

Digital-only banks and financial service providers	Online banks, securities trading or other financial services with no physical branch presence	First round
Open banking	Third party developers that use open-source data, provided by banks via open APIs, to create services such as finance management apps	First round
Robotic processes that can be rigged and taken over	Examples include robo-advisors, automated KYC bots, smart ATMs and other semi- or fully automated processes	First round
Services using DLT	Including 'smart contracts', blockchain-powered financial services or services dealing with cryptocurrencies	First round
Trading in obscure financial products	Products that may be traded anonymously or be obscured to easily conceal malicious intent from authorities (e.g., complex derivatives)	First round

$N_{Round\ 1}$=15

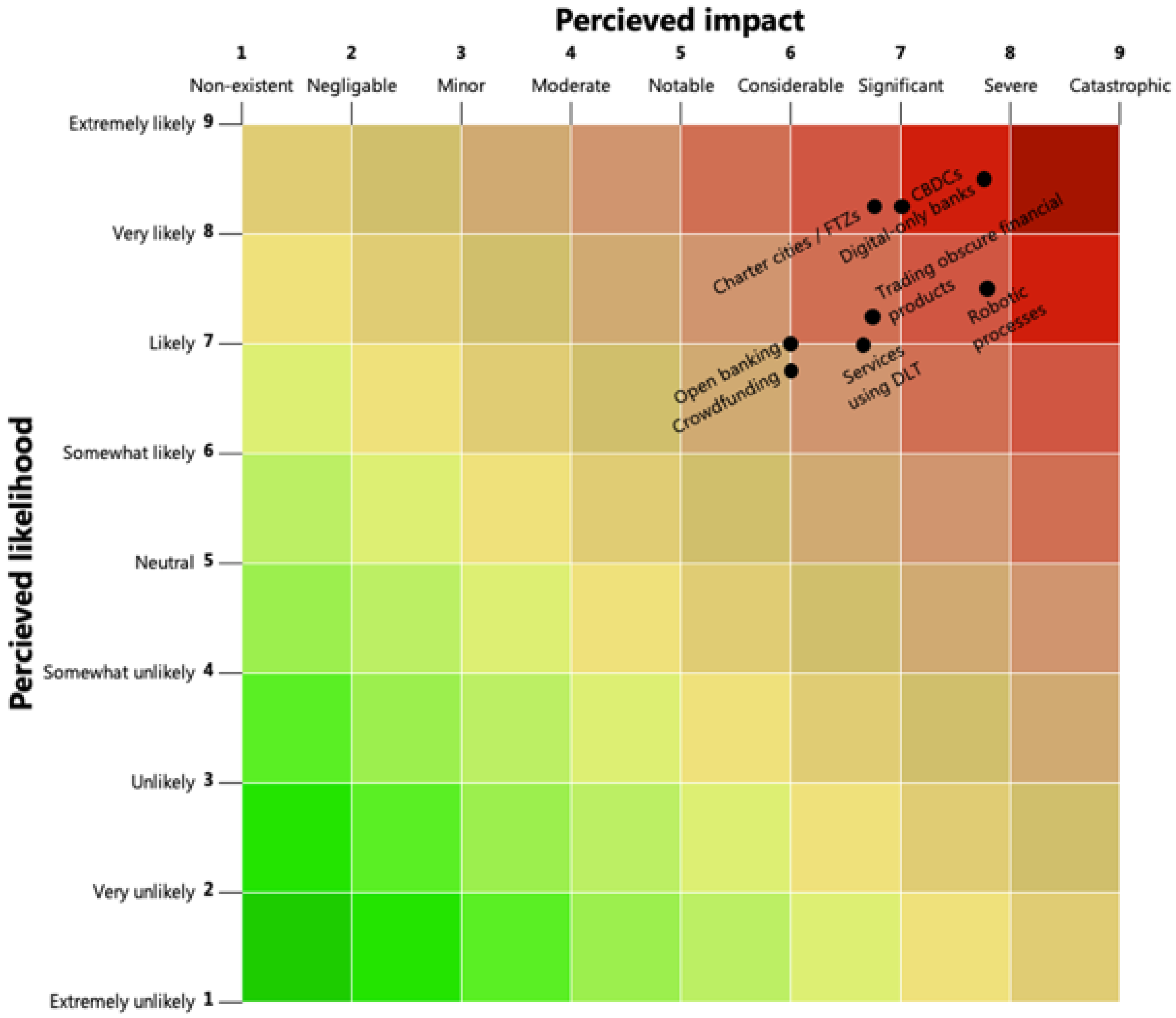

Fig. 9 FinTech ML/TF risk matrix of likelihood and impact scores *($N_{Round\ 2}$=4, $N_{Round\ 3}$=2)*

5.4. Insights from semi-structured interviews

Besides helping to devise round 1 of the study, the two interviews with the UK Civil Service also offered some qualitative insights into the UK government perspective on ML/TF risks, which are worth briefly reporting as a sidenote. In the DLT field, Initial Coin Offerings (ICOs), crypto-exchanges and crypto-gambling/auctions were discussed as the three main risks with government priority. In the FinTech field, open banking was cited as a risk warranting further law enforcement investigation, a finding confirmed by the scoping review. 5G-enabled payments were mentioned as a 'weak signal' that had arisen out of the wider hype at the time about 5G and possible national security risks, in particular the involvement of the China-based *Huawei* (Levy, 2019).

5.5. Overview of scores and qualitative insights

As might be expected, panellists tended to identify more criminogenic features for those technologies that were rated higher for impact and likelihood (or both). These features are now discussed in more detail.

Anonymity was a core criminogenic feature identified throughout panellist qualitative insights, prevalent for nearly all threats across all three technology categories. Particularly highly scored for likelihood/impact were technologies that were both intentionally and inherently anonymous, such as privacy coins (DLT) and virtual currencies (NPMs). In contrast, scores were lower for technologies holding large amounts of data on their users, such as social media platforms, where deanonymising suspicious actors would be substantially easier. Panellists nevertheless expressed caution, as even low-anonymity platforms such as social media are constantly creating new features that can inadvertently conceal ML/TF offenders. One panellist offered the example below in the case of ephemeral content (content only visible for a certain time, such as live videos, Snapchat or Instagram stories).

> "These broadcast channels [that host live videos and donations campaigns] may appear to be individualised and their connections with criminal groups can be hard to chase. Also, these live broadcasts may allow for global access and donations, making the source of funds hard to locate."

Many of the more anonymous technologies have additional criminogenic features, such as being decentralised (in the case of privacy coins) that make deanonymising them particularly difficult. Since there is a lack of a central authority governing transactions on such platforms, standard prevention measures (such as increased ID requirements) cannot logistically be applied. In contrast, centralised technologies, such as Bitcoin ATMs and customer loyalty points, were scored low for both likelihood and impact given their oversight and control by distinct entities (such as ATM operators, retail stores or airlines), that can easily implement KYC, detect, and block suspicious transactions. Customer loyalty rewards were additionally identified as low-risk due to their closed-circuit nature that prevents them from being easily exchanged between currencies or customers, highlighting the ease of transfer/exchange as another feature affecting crime exposure.

Another criminogenic feature of concern to panellists was the diversity of exploitable actors or entities available to spread risks across. Transaction laundering (the re-routing of payments for illicit goods/services via seemingly legitimate front businesses) was one of the highest scored NPM risks, with panellists drawing attention to the large numbers of e-commerce sites that could be exploited this way. This also applied to digital invoice manipulation-based risks in general, as one panellist described:

> "Digital invoice manipulation is a step up from the traditional invoice manipulation used for ML. Any technical/digital solution available on the [world wide web] is sufficient for manipulation of 'documents' including digital application forms et cetera."

Transaction laundering was additionally scored highly due to another criminogenic feature, namely the absence of value limits on transactions. Most NPMs, such as payment apps, are designed for small yet rapid payments, meaning that large-scale transactions on such a platform will likely be detected by internal fraud teams. This decreases their utility for large-scale ML/TF and is reflected in the lower scores attributed to them compared to (say) transaction laundering.

Automation was another criminogenic factor identified for FinTech developments in particular. Panellists mentioned the development of the Generative Pre-trained Transformer 3 (GPT-3) autoregressive language by AI company *OpenAI*. GPT-3 generates human-like text that can be used to programme automated robotic advisors to interact with clients (Floridi & Chiriatti, 2020, p. 3). Though specific risks were not mentioned, GPT-3 and other advances will likely reduce human oversight in financial institutions, particularly in customer relationship management (or 'robo-advisory'), increasing the avenues for cyberattacks and undetected suspicious transactions.

A final feature identified was the low-cost nature of exploiting many of these risks, including cryptocurrencies in particular. Risks where panellists identified high monetary barriers to entry, such as storing cryptocurrencies in satellites through high-end space start-ups, were therefore scored low for both likelihood and impact. Using software, apps and games as mediums of payment was also scored low due to the costs and skillsets associated with their initial creation.

These insights suggest that prevention measures will depend on numerous considerations regarding the ML/TF risk being addressed, including anonymity, decentralisation, diversity of exploitable actors/entities, ease of transfer/exchange, value limits, automation and barriers to entry. In line with this, panellists proposed a wide range of prevention measures, corresponding with different perspectives, that could be more (or less) effective in different situations depending on the technical specifications of the ML/TF risk being addressed. These measures and perspectives are presented next.

6. Prevention measures

Tables 5-7 show the identified prevention measures for DLT, NPMs and FinTech, respectively. Since none of the preceding research (scoping review or interviews) to this study identified prevention measures, all measures were identified during the Delphi study first round. Figures 10-12 show the identified measures scored for monetary costs (left chart) and societal costs (right chart), both plotted against scores for expected effectiveness. In these charts, measures are assigned a letter (see tables) and presented graphically as such for legibility purposes. For all charts, the top left quadrants represent low-cost measures with perceived high effectiveness, while the bottom right quadrants represent high-cost measures with perceived low effectiveness.

6.1. DLT prevention measures and cost/effectiveness scores

Table 5 DLT prevention measures

Letter	Prevention measure	Description / additional information
A	Ability to analyse other devices (e.g. phone and e-mail) linked to suspected accounts	Providing better intelligence to determine whether a suspected wallet holder is suspicious
B	Better suspicious activity detection algorithms	Including spending analyses and tracking software offered by cybersecurity firms
C	Control of exchange points (i.e. crypto-exchanges) where cryptocurrencies are converted into standard currency	This includes making conversions more difficult
D	Enhanced due diligence	Requiring wallets and exchanges to understand the source of clients' wealth, as well as mandatory reporting of foreign deposits and 'hot' money flows
E	Harm the reputation of and/or increase the inconvenience of using cryptocurrencies	Including reduced security of stored funds, increased price volatility, introducing or increasing taxes on crypto-transactions (etc.)
F	Improved training, policies and procedures for firms engaging with DLT	Including the licensing of firms and encouraging best practices and training to spot malpractice
G	Increase designated crypto-police and detective units	Intended to improve the capacity to investigate crypto-related malpractice and increase prosecutions
H	Increase merchant account provider control of cryptocurrency payments	Allow the merchant account providers of cryptocurrency-accepting businesses to have greater oversight over payments
I	Information sharing between relevant entities	To improve the detection of suspicious actors and activities
J	Outright prohibition or restriction of easily exploitable and anonymous technologies	Such as privacy coins or mixers/tumblers
K	Public education of crypto-users on scams and risks	Particularly those vulnerable to crypto-mule recruitment

L	Public shaming of non-compliant entities or individuals	To discourage non-compliance and malpractice
M	Regional / global regulations or regulatory bodies	*No description/self-explanatory*
N	Require coins and contracts to allow law enforcement 'hacking' (intervention) in cases where malpractice is clearly occurring	This can involve 'smart controls' or 'embedded control methods' in code that allow relevant bodies to intervene real-time and stop transactions confirmed as suspicious

$N_{Round\ 1}$=17

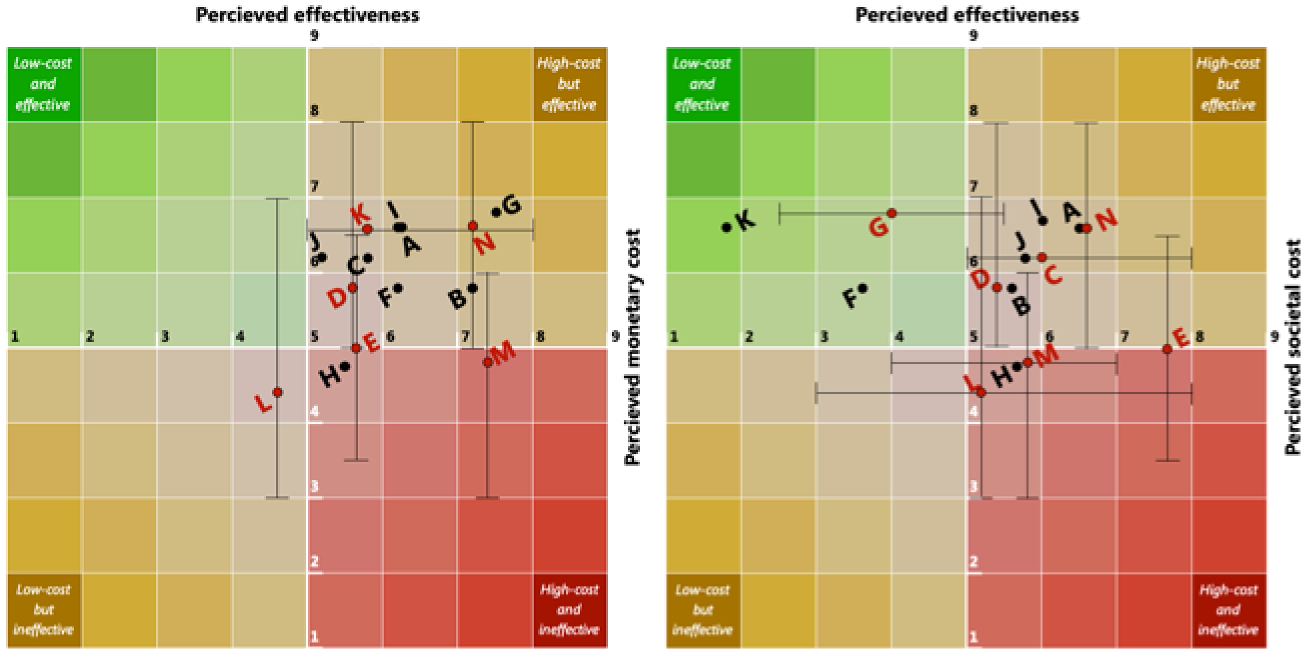

Fig. 10 DLT prevention measures monetary cost (left chart) and societal cost (right chart), plotted against effectiveness scores *($N_{Round\ 2}$=6, $N_{Round\ 3}$=3)*. Error bars are shown for items in red where consensus was not reached (i.e., IQR > 2)

6.2. NPM prevention measures and cost/effectiveness scores

Table 6 NPM prevention measures

Letter	Prevention measure	Description / additional information
A	Better detection algorithms to identify suspicious payments	including network analysis, pattern analysis, digital anomaly detection, computer tracing (etc.)
B	Checks by websites/mobile apps on genuine nature of users, good/service listings and proof of use	Can include better account verification, cross-checking payments data with tax authorities and making sure that the good/service offered are real and are actually used by purchasers (etc.)
C	Clearer due diligence, ID checks and restrictions on anonymity	To prevent anonymous access to payments mediums
D	Encouragement of customers to report suspicious listings and other users	For example if a user spots a listing for accommodation on a mobile renting app that is clearly suspicious due to location, pricing, host (etc.)
E	Greater confidential data sharing between service providers and regulators	Allowing each a better understanding of the sort of suspicious activity to look out for
F	Improvement in digital law enforcement resources and prosecutions	Allowing more effective digital policing investigations
G	Incentives analysis to determine the propensity of a client to commit ML/TF offences	Including their association with high-risk individuals, political economy of residing country (etc.)
H	Internationally orchestrated regulation	Through supranational or international organisations that allow consistency across countries
I	Outright prohibition of easily exploitable payment methods	Including those with low oversight or high anonymity
J	Phasing out the use of cash	*No description/self-explanatory*
K	Regulation and due diligence of app developers and companies themselves	To identify non-compliant app developers that may be creating platforms susceptible to (or designed exclusively for) ML/TF offences

L	Tough controls over points of conversion back to standard currency	To prevent illicit funds in alternative mediums (such as virtual currencies) from re-entering the regulated financial system
M	Use of blockchain to make transactions more transparent	Allowing all transfers to be viewable by everyone on a digital public ledger
N	Value limits or mandatory reporting of high value transfers	For example daily/weekly maximum transaction thresholds on pre-paid cards, alternative mediums, service-providing apps (etc.) to limit criminals' ability to launder large amounts of funds

$N_{Round\ 1}$=17

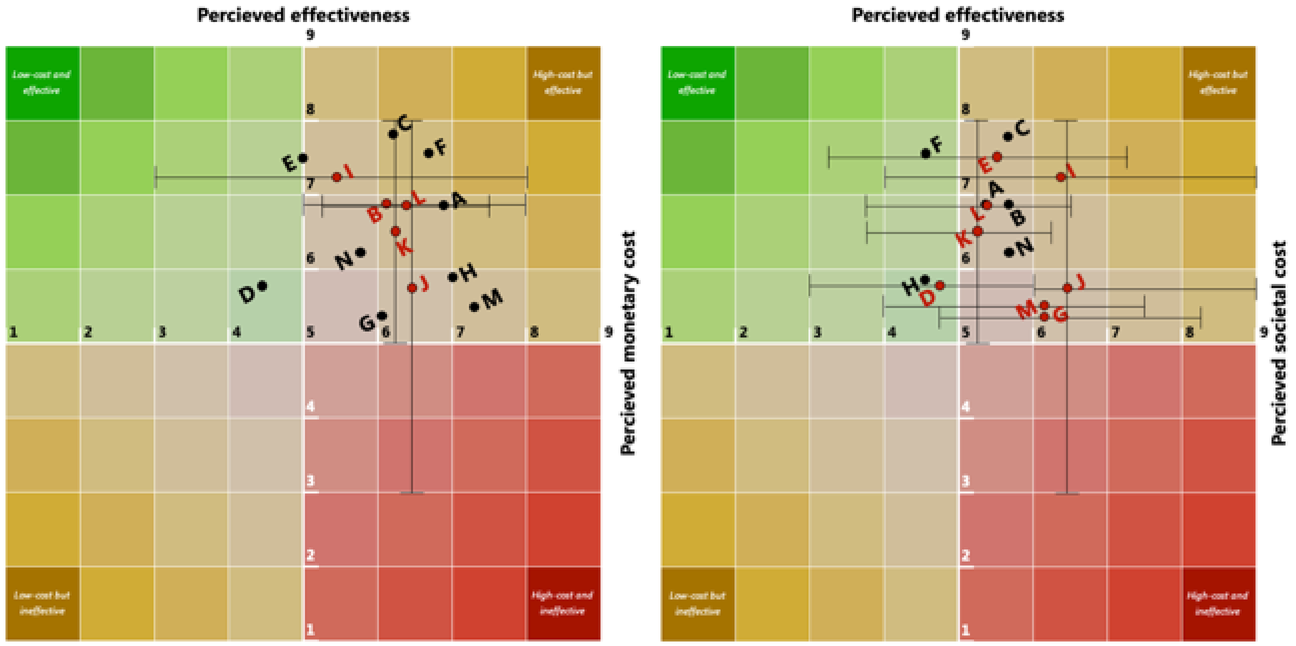

Fig. 11 NPM prevention measures monetary cost (left chart) and societal cost (right chart), plotted against effectiveness scores *($N_{Round\ 2}$=11, $N_{Round\ 3}$=6)*. Error bars are shown for items in red where consensus was not reached (i.e., IQR > 2)

6.3. *FinTech prevention measures and cost/effectiveness scores*

Table 7 FinTech prevention measures

Letter	Prevention measure	Description / additional information
A	Better detection algorithms	Including machine learning, anti-malware and strong cybersecurity solutions
B	Clear regulations on minimum acceptable KYC/anti-fraud standards for new technologies	Including minimum ID standards
C	Coordination between financial institutions and law enforcement	To facilitate quick expert feedback into detection and investigation systems, as well as democratised ID databases/data sharing to provide advance manual information to financial institutions
D	Comprehensive ID and due diligence requirements to open accounts	Such as face-to-face contact requirements, on-the-spot selfies to ensure that the ID matches the account-opener
E	Comprehensive security audits	To test cybercrime capabilities of systems vulnerable to ML/TF exploitation
F	More emphasis on the behavioural attributes that drive customer decisions	For example taking into account behavioural economics and decision-making theories to better understand which transactions are normal and which are suspicious
G	Outright prohibition of easily exploitable financial services and products	*No description/self-explanatory*
H	Require a degree of human oversight / semi-automation of processes	Attempt to avoid full automation where possible or at least delay it until the security of the system is beyond doubt
I	Require further comprehensive training for AML/CFT professionals to spot malicious activity	*No description/self-explanatory*
J	Sharing of data and suspicious activity reports between financial institutions	*No description/self-explanatory*

K	Solving conflicting regulations in favour of strict data protection laws	For example the apparent conflict between the European GDPR, which requires customer data protection, and the European Payments Directive (PSD2), which requires data sharing to allow open banking innovation
L	Two factor authentication requirements when opening accounts	*No description/self-explanatory*

$N_{Round\ 1}$=15

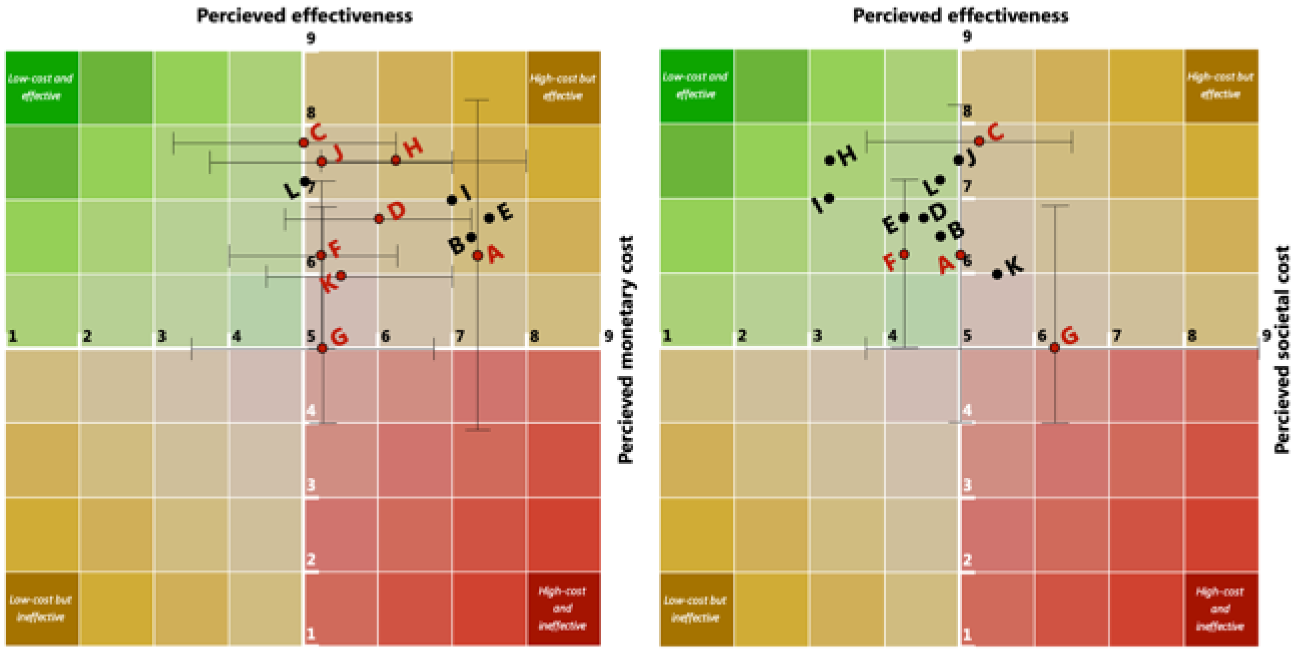

Fig. 12 FinTech prevention measures monetary cost (left chart) and societal cost (right chart), plotted against effectiveness scores *($N_{Round\ 2}$=4, $N_{Round\ 3}$=2).* Error bars are shown for items in red where consensus was not reached (i.e., IQR > 2)

6.4. Overview of scores and qualitative insights

In all cases, panellists tended to perceive that the economic cost of measures would be higher than would the associated societal costs. Moreover, with one exception ('encouraging NPM users to report suspicious activity'), for all three technology categories, no prevention measure was perceived to be both highly effective and to carry a low monetary cost. With neutral average scores (5.00) for effectiveness, 'two-factor authentication' and 'co-ordination between financial institutions and authorities' came the closest (both measures were suggested for FinTech). With respect to societal costs, there was less consensus, and a particular point of contention emerged regarding the degree of privacy afforded or infringed upon by different measures.

All prevention measures were deemed effective to some degree, though ‘outright prohibition of risky technologies’ for NPMs and FinTech was scored as only neutrally effective (5.00). A lack of consensus existed where panellists had conflicting opinions on crime displacement opportunities. Low consensus was also observed for measures previously implemented to prevent traditional ML/TF (for example in conventional financial services); while some panellists gave generous scores on the grounds that they would be effective in theory, others were more pessimistic based on poor results they had shown in practice.

As expected, due to the diversity of industries represented, panellists proposed a wide range of different prevention measures. These can be categorised into five main approaches, which are discussed next.

6.4.1. Detection-based approaches

Detection-based approaches involve improving transaction monitoring systems using (for example) machine learning, big data, Blockchain and advanced analytics, and updating them to be receptive to the latest technology-enhanced illicit transaction trends. Their popularity amongst panellists is reflective of the ‘default’ status of RegTech in contemporary AML/CFT. Numerous detection-based prevention measures, including better algorithms and clear ID/KYC requirements were mentioned for all three technology categories (DLT, NPMs, FinTech). Improved KYC training was suggested for DLT and FinTech, while ‘incentives analyses’ on customer decision making (i.e. analysing the behavioural aspect behind transaction patterns) to determine suspicious activity was suggested for NPMs and FinTech. Using Blockchain for transaction transparency and for reducing detection costs was suggested uniquely for NPMs.

Panellist views could be described as ‘traditionalist’ (extending transaction monitoring systems), ‘moderate’ (improving transaction monitoring systems) or ‘reformist’ (criticising and calling for reform of transaction monitoring systems because of their inefficiency). A key drawback of detection-based approaches, articulated by a panellist adhering to a reformist view, was the low success rate of detection-based approaches in general, as well as the high societal cost associated with false positives (which the panellist argued as below).

> “[AML/KYC] is all well and good until your account is blocked, yet most AML specialists choose to see the tiny fraction of 'successes' and discount to zero the harm caused to hundreds of thousands of ordinary people and legitimate businesses.”

The issue of false positives in detection-based approaches was a significant point of disagreement across FinTech panellists, who had conflicting opinions on whether KYC systems should be fully automated. While some advocated a move to entirely digital solutions, others (such as the panellist below) emphasised the continued importance of human oversight-based KYC.

> “In many cases, only the ‘human touch’ can spot anomalies and/or outliers in data that may be indicative of money laundering.”

Another significant societal cost identified by panellists was the issue of privacy. Given the large-scale customer data involved in maintaining RegTech systems, panellists warned of the potential for *Cambridge Analytica*-like scandals. This was a particular point of disagreement; for example, some panellists criticised using Blockchains for tracing transactions as a concerning development for privacy, while others emphasised that the semi-anonymous nature of Blockchains did not make them transparent enough. This was reflected in the average societal cost score (6.14) of this measure, which did not reach consensus (IQR=3.50).

Moderate and reformist panellists emphasised that a purely detection-oriented prevention approach was not sufficient in the modern age, particularly given the increasingly anonymous and decentralised nature of risk-prone technologies. Failure to appreciate the diversification of technologies in this regard, panellists warned, would lead to the overburdening of new enterprises with unnecessary compliance costs and a knock-on discouragement of innovation. It was also noted that different prevention approaches may be more effective on different technologies depending on the nature of stakeholder-risk interaction scenarios, argued as below.

> "Whether an alternative medium [a means of holding value, such as cryptocurrencies or pre-paid cards, as a substitute to traditional means such as bank accounts or cash] should be regulated and prohibited simply because it may be abused is a policy question that requires an understanding of the medium and its context."

In recognition that detection-based approaches can be enhanced and complemented by other perspectives (particularly if stakeholder-risk interaction scenarios make it suitable), the second perspective identified by panellists – namely educational approaches – is discussed next.

6.4.2. Educational approaches

Educational approaches involve raising awareness of ML/TF risks to encourage responsible, safe and innovation-friendly engagement with new technologies. Such approaches can be applicable to a wide range of circumstances, ranging from encouraging users to report suspicious activities on legitimate platforms to avoiding non-compliant illicit ones. They can take the form of awareness campaigns or negative messaging (such as public shaming of illicit entities) and can be directed towards a range of different stakeholders, such as users, technology providers or policymakers (to encourage effective but innovation-friendly regulations). One panellist responding to the DLT survey summarised a possible focus of such approaches as follows.

> "There is room for a larger debate on ethics as it relates to crypto and AML/CTF. If emerging tech is purposefully fabricated to undermine existing regulations, protocols, capacity, policies, strategies, alliances, etc., and are known to have facilitated criminal activity, including terrorism, then the public should be better informed and outraged at those individuals responsible for developing the tech in the first place. There are parallels to be found in public response/revulsion to animal welfare, child abuse, sexual exploitations, climate change, etc."

Specific prevention measures included harming the reputation or increasing the inconvenience of using risk-prone technologies, public education of new technology users, public shaming of non-compliance and encouraging users to be aware of and to report suspicious activity. In particular, the last measure (suggested for NPMs) was received positively due to the financial intelligence it would contribute to transaction monitoring systems, being the only measure to be considered to likely be effective (5.78) and having a low economic (4.44) and societal (4.75) cost. Additional positive consequences of educational approaches raised by panellists included the prevention of scams and frauds on online payment platforms.

Less approving panellists cautioned that reputation-harming campaigns had been ineffective against traditional financial services, despite high-profile lawsuits and fines for AML/CFT deficiencies. Legitimate technology providers and start-ups may also inadvertently suffer from negative messaging. Measures will also need to break the optimism bias ('it will never happen to me') (McKenna, 1993), which may incite user indifference towards cyber-awareness programmes.

Much like detection-based approaches, educational approaches are insufficient for effectively countering technology-enhanced ML/TF. However, by enhancing suspicious activity data collection, dissuading use of risky platforms, and encouraging effective policymaking, such approaches could have a complementary effect to other interventions. For example, raising public awareness could incentivise greater co-operation between relevant stakeholders, a frequently mentioned approach that is discussed next.

6.4.3. Co-operation-based approaches

Co-operation was seen as an important and currently underutilised form of prevention against technology-enhanced ML/TF by panellists. Fundamentally, co-operation involves enriching financial intelligence and ensuring regulatory consistency both across institutions and across states.

Suggested approaches took three forms. The first involved international co-operation (e.g. at the United Nations level) to encourage globally uniform regulations. This would ensure that no state could 'undercut' others to encourage risky innovation, while also addressing the cross-border nature of technologies such as cryptocurrencies. Joint intelligence gathering across allies could also enhance the collection and sharing of financial intelligence.

Secondly, co-operation both between and across the public and private sectors could help enrich the data collected by each. This could, for example, allow the substitution of suspicious activity data with criminal records, or vice versa, as described by one panellist as below.

> "Any service provider that offers legitimate business opportunities [...] has access to data that allows for anomaly detection. For this to succeed it is important to also involve Government teams that have access to more confidential information such as criminal records etc."

Thirdly, co-operation between regulators and obliged entities can improve the quality and implementation of regulations. Panellists emphasised the need for a constructive regulator-obliged entity relationship, rather than one based on supervision and penalties. Giving obliged entities a greater consultative role in the forming of regulations can encourage reforms to cumbersome KYC requirements. Regulators and law enforcement, meanwhile, can rapidly assist in identifying and addressing the KYC deficiencies of private sector partners, as one panellist described:

> “Sharing of data among financial institutions would be a game changer, including SARs, [along with] co-ordination of law enforcement to provide contemporaneous expert feedback into the detection-investigation system.”

In short, a ‘feedback-not-fines’ approach that rethinks the public-private relationship can improve both the speed and effectiveness of forthcoming regulations. Mediums for such co-operation, such as regulatory sandboxing (where firms can trial prototypes of their services to ensure they meet requirements before general release) already exist and can be encouraged further.

Related to improving regulatory quality, obliged entities have several different measures at their disposal to defend their systems against suspicious activity or cyberattacks. These defence-based approaches, which can also be enhanced with regulatory co-operation, will be discussed next.

6.4.4. Defence-based approaches

Cybersecurity and technical risk mitigation were deemed to be of increasing importance due to the digital and automated nature of most new and emerging ML/TF risks. As one panellist described below, digital AML/KYC systems have become increasing targets for cybercriminals, thereby emphasising the need for constructive regulatory oversight, frequent penetration tests and up-to-date cybersecurity protocols.

> “This will let them work with a growing range of interested regulatory bodies more quickly, easily and accurately, on everything from stress tests and periodic exams to individual requests. By doing so, they will improve their credibility with regulators today and be ready for the future.”

Suggestions also included digital licensing or due diligence procedures for new technology providers and start-ups themselves (as opposed to just their clients) to ensure that their systems and coding protocols are adequately protected. This would encourage technology providers to devise crime-resistant services from their inception, thus reducing the need for costly and time-consuming patches or alterations in the future.

Other technical interventions included restrictions on transfers and value limits on risk-prone technologies. However, panellists made note of their societal cost to legitimate users and abundance of crime displacement opportunities. An example of the latter was described by a panellist as below.

> “Proceeds of crime will shift into barter trade and other forms while society will suffer and pay the costs of payment intermediation.”

Similar displacement concerns were raised for other measures, such as value limits on transfer and storage amounts for alternative mediums such as pre-paid cards. One panellist described how criminals could circumvent such measures (and the extensive countermeasures entities would need to implement) as below.

> “To enforce the [reduced] limit effectively for prepaid cards or apps, you need an identification and registration system to prevent a user securing multiple cards and apps to process larger transactions.”

Additional controls on points of exchange from alternative mediums (such as cryptocurrencies) to fiat currency (those backed by a government) were also proposed, though panellists deemed them costly for start-ups. Cryptocurrency exchanges were identified as a key stakeholder for such measures, with panellists arguing that a growing number were now accepting privacy coins because of rising demand.

The more extreme option of outrightly prohibiting risk-prone technologies was scored negatively by panellists given the large-scale social cost to legitimate users and innovation. One panellist argued that banning technologies outright for crime prevention purposes was permissible in only certain circumstances, namely if the technology posed negative externalities in other aspects, argued as below.

> "Outright prohibition should tackle only those mediums that are in a grey zone and could potentially bring other [non-ML/TF related] harms to the community (say, online gambling)."

Overall, defence-based approaches acknowledge the increasingly digital and automated nature of ML/TF risks. However, one aspect of technology-enabled ML/TF not yet addressed is the speed of modern transactions, which can render measures with time delays ineffective. A final enforcement-based approach, suggested by some panellists, is therefore discussed next.

6.4.5. Enforcement-based approaches

Enforcement-based approaches involve improving technical capabilities for direct intervention, thereby matching the rapid and convenient nature of modern payments technologies with real-time interventions designed to stop suspicious activity as it is occurring.

Enforcement-based approaches were generally considered effective but costly, either monetarily or societally. Monetarily costly approaches included increasing metaverse detective units with specific expertise on cryptocurrencies or NPM platforms (such as P2P marketplaces) to improve surveillance of these platforms. Panellists noted that while their deployment may be effective, the training costs for such units would be substantial.

Approaches with high societal cost included built-in 'smart' coding protocols to allow designated authorities to intervene in digital services and prevent obvious ML/TF activity as it is occurring. Though perceived and scored by panellists as effective, such extreme and intrusive measures can have implications for innovation, privacy and inconvenience to both users and technology providers. However, there perhaps exist more socially acceptable compromises such as indirectly intervening in a platform via approval of its designated fraud department, or similar agreements.

Since enforcement-based approaches aim to match the speed of modern criminal transactions, it is inevitable that they would rely on a degree of integration with detection-based approaches and automated responses (such as real-time account locking). Panellists cautioned that this may cause significant societal costs, as the risk of false positives remains prevalent (demonstrated in the *Monzo* example discussed previously).

7. Relevant stakeholders

Tables 8-10 show the identified relevant stakeholders for DLT, NPMs and FinTech respectively. Figures 13-15 show the identified stakeholders scored for their perceived power and responsibility to prevent technology-enhanced ML/TF. As before, measures are assigned a letter (shown in the tables) to aid their presentation. The top right quadrants represent stakeholders that are both perceived to be powerful and responsible, which accounted for most stakeholders scored for all three technology categories.

7.1. DLT relevant stakeholders and power/responsibility scores

Table 8 DLT relevant stakeholders

Letter	Stakeholder	Description	Source
A	Cryptocurrency banks (decentralised finance - DeFi)	Financial institutions that mimic traditional banking services but for cryptocurrencies (such as deposits, withdrawals, savings, lending and investment)	Review
B	Cryptocurrency exchanges	Services that allow users to convert cryptocurrencies into other cryptocurrencies or into standard currency	First round
C	Custodial wallet providers	Services that allow users to hold cryptocurrency in digital wallets and trade them with other users	First round
D	(Fin)tech firms and start-ups	Firms developing (risky) technologies or issuing coins or tokens	First round
E	Government	Political decision-makers that make policies and laws regarding cryptocurrencies	First round
F	Law enforcement (domestic)	Including the intelligence community	First round
G	Law enforcement (regional)	Regional bodies set up to police, regulate and investigate cryptocurrency transactions	First round
H	Law enforcement (international)	International bodies set up to police, regulate and investigate global cryptocurrency transactions	First round
I	Payment service providers and payment gateways that accept cryptocurrency	*No description/self-explanatory*	First round
J	Regulators	Including financial conduct, revenue and customs	First round

K	Retailers engaging in blockchain / accepting crypto-payments	For example auction houses, art galleries and other high-value goods dealers	First round
L	States pioneering new technological developments	*No description/self-explanatory*	First round
M	Traditional financial services	Central banks or banks that hold virtual asset service provider accounts (etc.)	First round
N	Vulnerable persons that can be exploited as crypto-mules and defrauded	For example students and elderly individuals	First round

$N_{Round\ 1}$=17

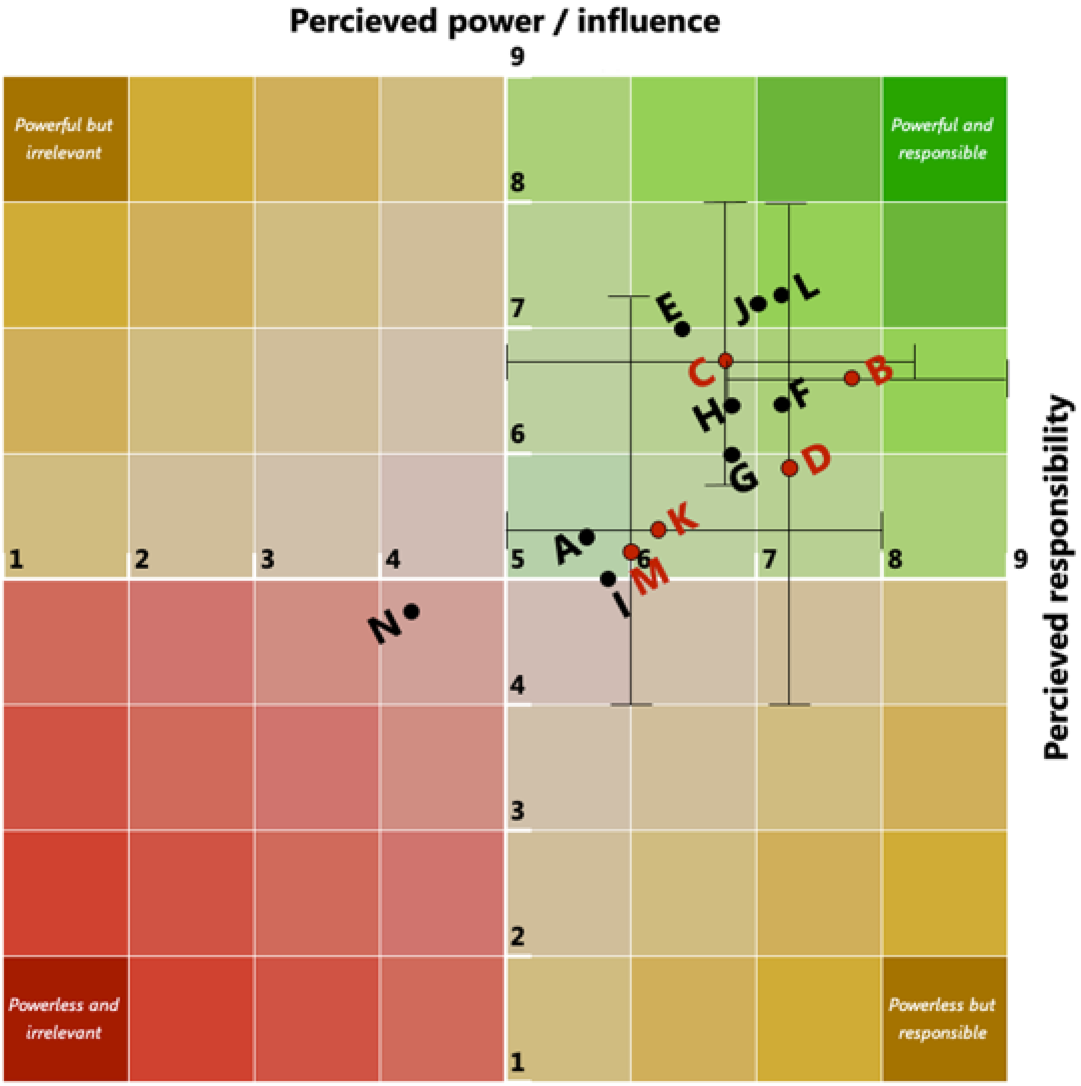

Fig. 13 DLT relevant stakeholder power/responsibility scores *($N_{Round\ 2}$=6, $N_{Round\ 3}$=3)*. Error bars are shown for items in red where consensus was not reached (i.e., IQR > 2)

7.2. NPM relevant stakeholders and power/responsibility scores

Table 9 NPM relevant stakeholders

Letter	Stakeholder	Description	Source
A	Accountants and accountancy firms	*No description/self-explanatory*	First round
B	Central banks and financial institutions	For example banks that handle accounts for alternative medium issuers and other relevant fintech firms	First round
C	Digital wallet providers	For example Apple Pay, Google wallet, Venmo (etc.) as well as online social media providers, such as Facebook Messenger	First round
D	(Fin)tech firms and start-ups	Companies engaging in new payments technologies (and specifically their top management)	First round
E	Hosting companies that host the servers of NPM-related technology firms and platforms	These companies may (un)intentionally be hosting easily exploitable payment systems	First round
F	Investors and exporters of technologies	*No description/self-explanatory*	First round
G	Law enforcement	*No description/self-explanatory*	First round
H	Mobile apps/websites providing a platform where users can list and trade goods/services	For example ride hailing, real estate agents and accommodation renting, pet sitting and digital marketplace apps	First round
I	Mobile app store ecosystems	For example Apple App Store or Google Play, where exploitable apps may be hosted and downloaded	First round
J	Issuers of alternative value instruments	For example virtual currency and pre-paid card issuers (etc.) that allow funds to be converted to these mediums and back	First round

K	Payment service providers and payment gateways	*No description/self-explanatory*	First round
L	Political decision-makers	Lawmakers in charge of devising financial laws and regulations	First round
M	Regulators	Including data protection, payment services regulators and tax authorities	First round
N	Vulnerable customers that can be exploited by criminals	For example elderly individuals or students at risk of scams or money mule recruitment	First round

$N_{Round\ 1}$=17

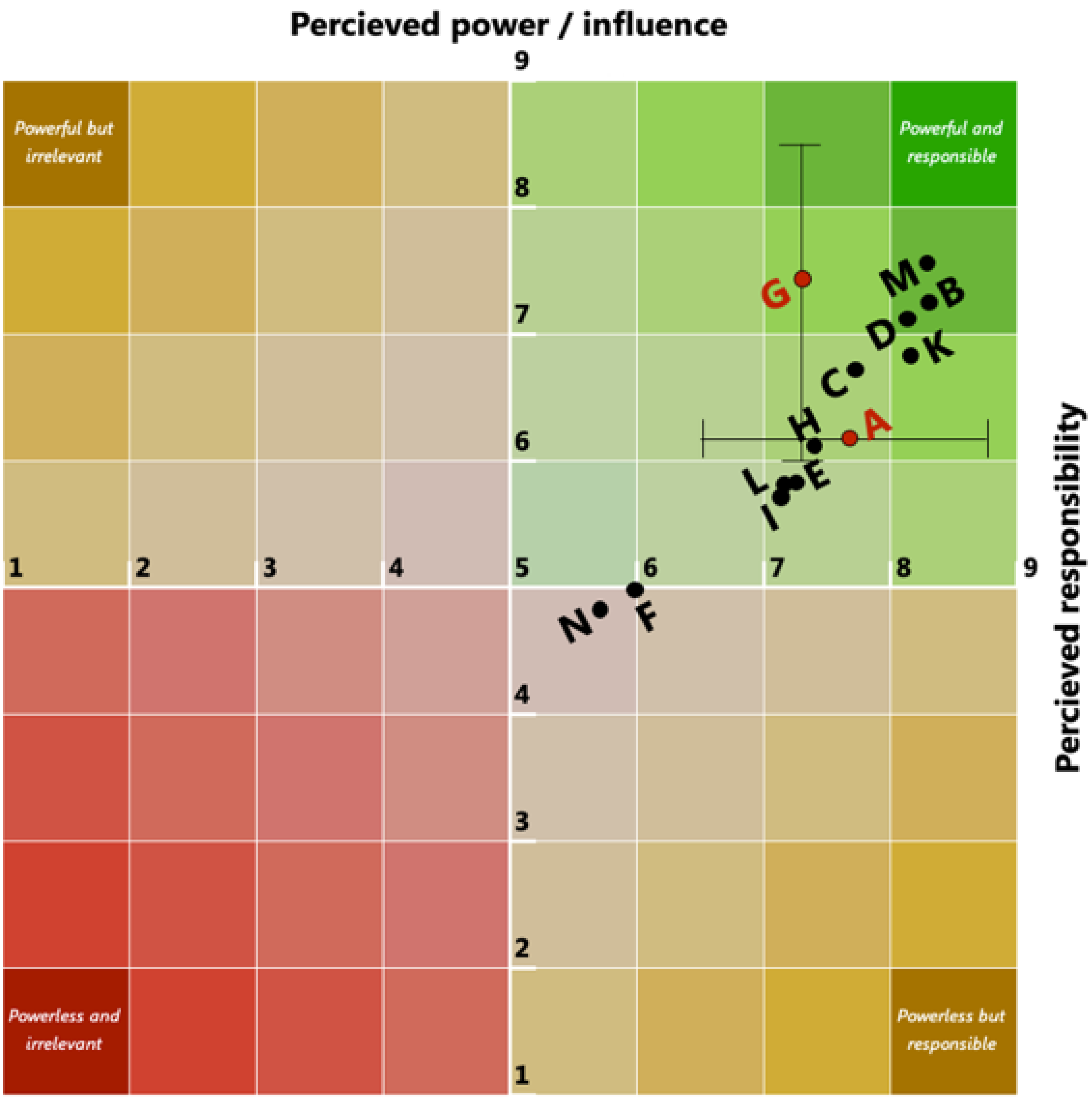

Fig. 14 NPM relevant stakeholder power/responsibility scores *($N_{Round\ 2}$=11, $N_{Round\ 3}$=6)*. Error bars are shown for items in red where consensus was not reached (i.e., IQR > 2)

7.3. FinTech relevant stakeholders and power/responsibility scores

Table 10 FinTech relevant stakeholders

Letter	Stakeholder	Description	Source
A	Audit services	Services that assess the accuracy and fairness of financial statements, often provided by accountancy or professional services firms	First round
B	Automated clearing houses (ACH)	Automated electronic transaction processing systems that facilitate payments between participating financial institutions	First round
C	Clients and customers	Including vulnerable customers that can be susceptible to fraud and account hacking	First round
D	Crowdfunding sites / business funding platforms	*No description/self-explanatory*	Review
E	Data protection officers (DPOs)	Employees of companies overseeing their data protection processes and compliance with privacy legislation	First round
F	(Fin)tech firms and start-ups	Such as digital-only banks and other providers of new financial services or products	First round
G	Issuers, developers and/or brokers of electronic currencies	*No description/self-explanatory*	First round
H	Law enforcement and government ministries	Including border agencies and Ministries of the Interior	First round
I	Online third-party payment processors	Including peer-to-peer networks such as *PayPal*	First round
J	Regulators	*No description/self-explanatory*	First round
K	Risk services	Including companies that assess the security of an entity's internal services and systems	First round
L	Securities traders	Including brokers and commodities / futures traders	First round

M	Traditional financial institutions	Including banks, credit unions and mortgage firms	First round

$N_{Round\ 1}$=15

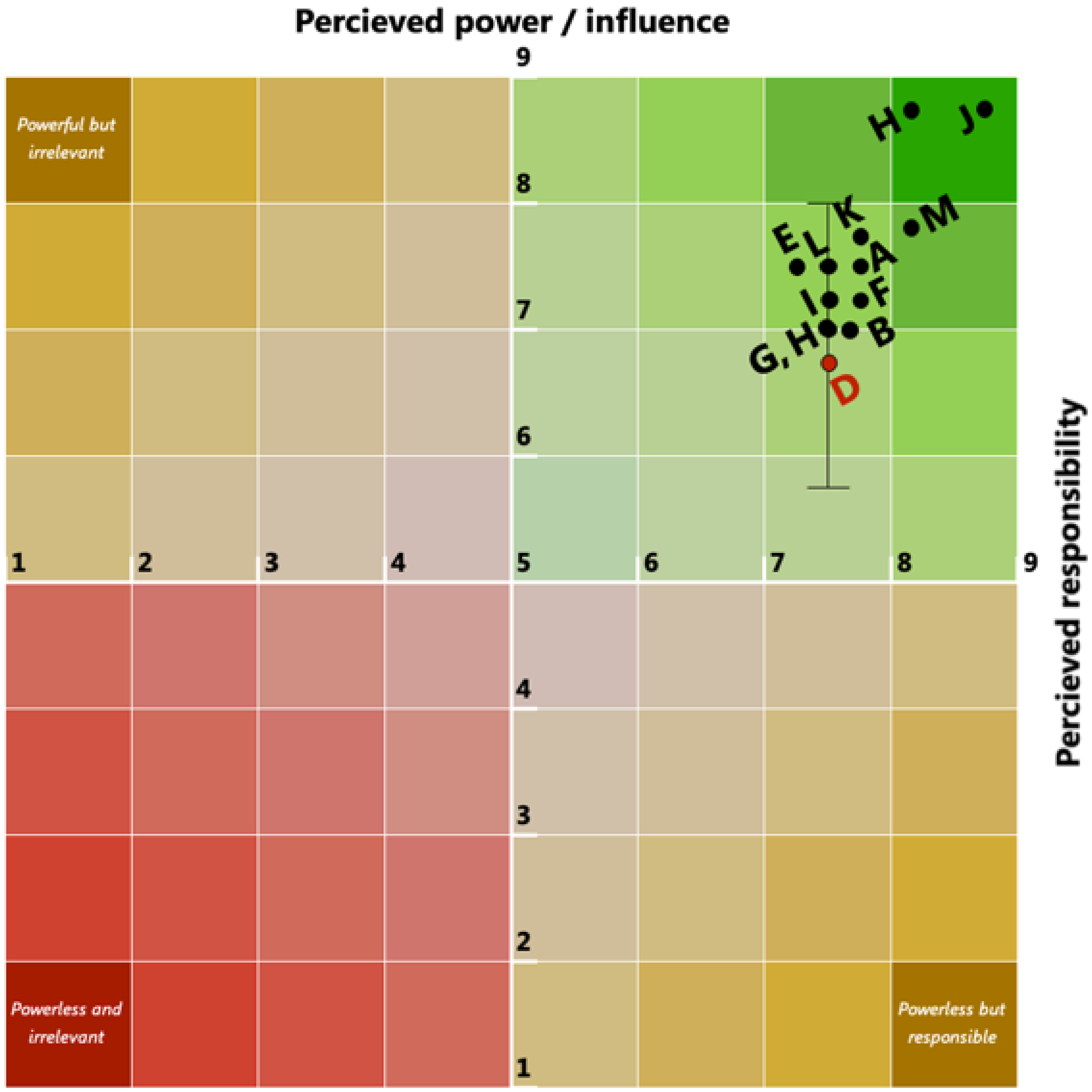

Fig. 15 FinTech relevant stakeholders power/ responsibility scores *($N_{Round\ 2}$=4, $N_{Round\ 3}$=2)*. Error bars are shown for items in red where consensus was not reached (i.e., IQR > 2)

7.4. Overview of scores and qualitative insights

All stakeholders, bar vulnerable users/customers, were deemed both powerful and responsible for all three technology categories. Traditionally relevant stakeholders such as regulators and obliged entities generally received the highest scores. Consensus for both attributes (power and responsibility) were largely achieved for NPMs and FinTech stakeholders, though was notably absent from key DLT stakeholders.

This lack of consensus appeared to be connected to a wider disagreement across panellists on what the powers and responsibilities of stakeholders involved. Some panellists gave high power/responsibility scores due to stakeholders' ability to implement detection-based measures, while more critical panellists gave high scores due to their ability to reform (rather than implement) them. This was particularly the case for regulatory and financial stakeholders. The clearest disagreements were observed across DLT panellists, one of which argued against imposing AML/CFT detection measures on private DLT-based services as below.

> "The harsh reality is that bad regulations, unreflectively imposed and extended ad nauseum - and the steadfast failure to face up to the proverbial elephant in the room [ineffectiveness of regulations] - is more to blame than just about all the private sector scapegoats put together."

Concerns over burdening new technology providers with cumbersome detection obligations were also repeated for NPMs and FinTech. One panellist argued against imposing them on FinTech start-ups (as below) due to negative effects on innovation.

> "It's crazy to predict the regulation of start-ups, for example, except those start-ups like mobile banks or other fintech, to develop AML policies. Innovations should not be killed by unnecessary prohibition."

Another panellist criticised detection obligations not due to their cost but due to their incompatibility with the diversifying range of relevant stakeholders. Some, such as hosting platforms for NPM servers, have only become relevant to AML/CFT recently, albeit in an indirect manner (they host the services that carry ML/TF risks, as opposed to carrying ML/TF risks themselves). Traditional AML/CFT measures are therefore not designed for such entities, with panellists doubting whether their implementation would be fair (given their detached nature from the problem) or effective. The unfairness of widening the scope of obliged entities was argued by one panellist as below, with a comparison made to what the traditional AML/CFT equivalent would be of doing so.

> "Consider all other hosting sites, including hotels, restaurants, etc, and the implications of requiring them to prevent crimes from being planned during meetings on their sites."

Similarly, panellists noted that the modernising nature of risks required fresh co-operation between stakeholders that were previously unrelated. Tax authorities and audit services, for example, were identified as crucial sources of data for apps accepting payments such as *AirBnB,* as they could determine whether a user actually owned an asset that they claimed to be hosting out for rent, for example. One panellist noted:

> "Tax authorities are best-placed as they profile buyers and sellers and would be able to identify if rental flows to a person who does not own property and does not have a registered real estate agency. ML/TF laws combined with tax laws will already address much of this problem, to the extent it occurs."

The changing web of relevant stakeholders, along with their diversifying powers and responsibilities, are becoming more widespread and integrated as innovation continues. Panellist insights have uncovered a range of new technology providers, users and regulators, each offering a different contribution to preventing technology-enabled ML/TF, with tax authorities and NPM hosting platforms (per the insights discussed above) being just some examples. The appropriate prevention strategy for each stakeholder is likely to be different and unique, based on a combination of the prevention approaches discussed previously, due to their specific contexts and likely stakeholder-risk interaction scenarios. Emerging disagreements across panellists, between the nature of powers and responsibilities, have also highlighted the difference of perspectives based on industry. The section below will summarise the levels of dissent across the three technology categories to highlight these key policy divisions.

8. Dissent analysis

Dissent analysis involves the investigation of both the extent and reasons behind divergences of opinion. The investigation of dissensus is central to policy Delphis, as a core objective is to understand (rather than reduce) key points of contention between panellists of diverse backgrounds (Meskell et al., 2014; Warth et al., 2013). Typically, this would involve analyses of bipolarity, outliers, desirability bias and stakeholder groups (Beiderbeck et al., 2021a). While the lower panellist count for the current study limited the statistical options available for dissent analysis, plenty of (predominantly qualitative) insights into policy disagreements emerged and these are now discussed.

This section first explores the change of dissensus across rounds 2 and 3 and then summarises the key areas of dissent, accompanied by possible explanations that have already emerged from qualitative insights. Keeping low panellist numbers in mind, statistical analysis is only conducted by measuring the change in IQRs across rounds. Round 2-3 changes are shown in figure 16, per technology category and attributes scored. Black bars show items already reaching consensus (IQR≤2.00) after the initial round (2) of scoring, dark grey bars show items reaching consensus after round 3, and the light grey bars show items for which consensus was not achieved after round 3.

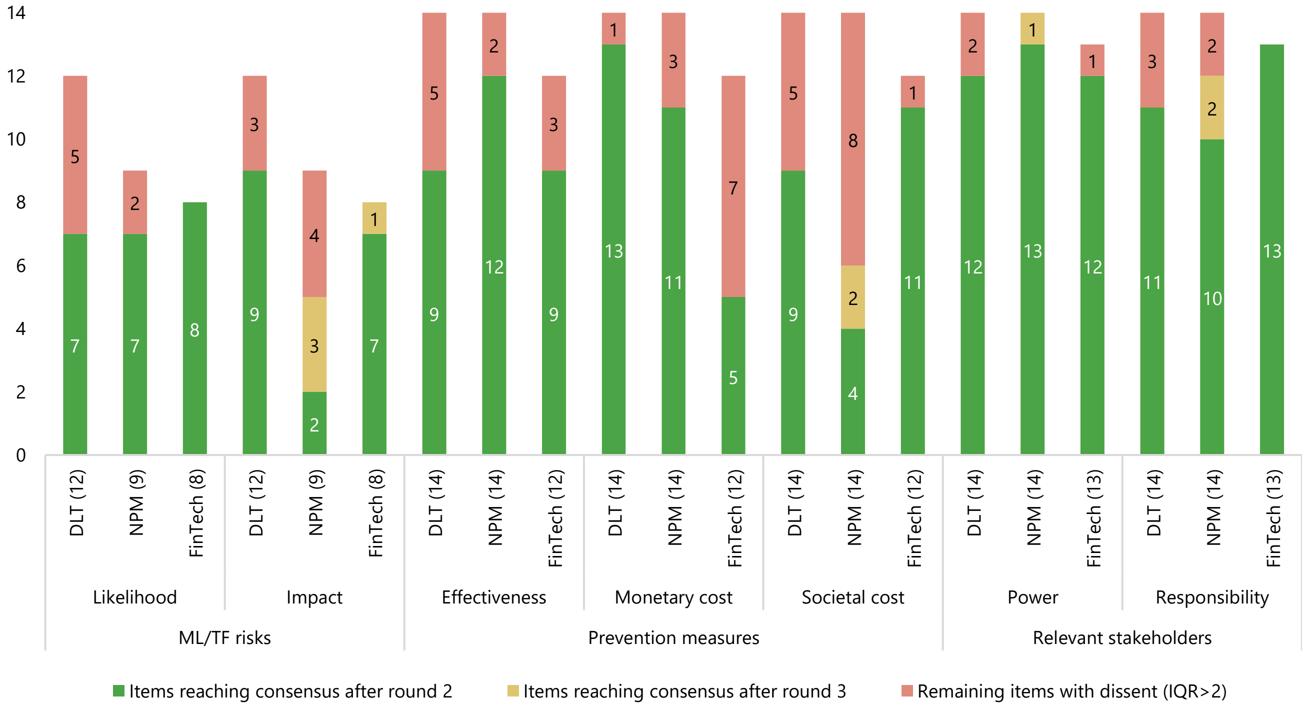

Fig. 16 Changes in consensus across rounds

Given the low number of responses for round 3 (N_{DLT} = 3, N_{NPM} = 6, $N_{FinTech}$ = 2), significant changes were not observed across rounds. The only shifts where IQRs dropped to 2 or below between rounds were observed for 'Impact' (for NPMs and FinTech), 'Societal cost', 'Power' and 'Responsibility' (all for NPMs only). Of the items gaining consensus after round 3, NPM scores were slightly reduced for 'Power' and 'Responsibility' by -0.14 mean score on average. They were slightly increased for 'Societal cost' and 'Impact' by +0.34 and +0.03 mean score on average respectively. The sole re-scored item for 'Impact' in FinTech, namely robotic process automation, had its mean score revised up by +0.75.

Qualitative insights explaining dissent have already emerged in previous discussions, particularly for items with notably low consensus such as monetary and societal cost. Key points of contention centred on the amount of anonymity that should be protected in the realm of new measures, whether (or not) human input should be preserved, and the extent to which measures would harm wider innovation. For likelihood and impact scores, dissent was notable for developments where ML/TF risks were not immediately obvious or short-term. Though not statistically verifiable, qualitative insights from panellists suggest that the perception of likelihood/impact were also affected by their perception of how well existing AML/CFT measures worked.

Though stakeholder attributes demonstrate comparatively higher consensus compared to prevention measures or ML/TF risks, qualitative data has suggested – as previously discussed – that those high scores were afforded for different reasons. The nature of responsibility ranged depending on whether panellists advocated more existing AML/CFT measures (typically regulators or traditional financial service professionals) or their outright reform (typically academics and technology professionals). While IQR changes in figure 16 do not make this clear, stakeholder-group analyses (if possible) would have likely identified this key point of dissent. Nevertheless, in-depth thematic analyses of qualitative insights were fruitful in accounting for these statistical limitations.

The reasons for dissent demonstrate that different constraints to implementation based on a stakeholder's particular risk interaction scenario will require a unique set of prevention measures to be countered effectively. A multi-level approach, implemented based on core standards to ensure their effectiveness, can allow a more selective application of prevention measures to best suit a given stakeholder's circumstances. The discussion that follows will aim to synthesise the findings of this study overall into workable concepts and frameworks that can be utilised by these stakeholders.

9. Discussion

Panellist insights have largely shown that as ML/TF risks modernise and diversify across a growing number of stakeholders, traditional AML/CFT approaches are becoming insufficient. This is because said stakeholders will be exposed to risks in different ways and at different levels to traditionally obliged entities. Their contextual circumstances will result in unique constraints to implementation, meaning that their ability to implement different prevention measures, as well as the effectiveness thereof, will vary. This issue will be discussed next.

9.1. Constraints to implementation

Constraints to implementation (or CtIs) denote specific contextual realities or limitations that stakeholders may face while attempting to prevent technology-enabled ML/TF. For example, ID checks were seen by panellists as a viable method to prevent the exploitation of Bitcoin ATMs, but not privacy coins. This was attributed to the former being a legitimate service provided by a centralised stakeholder with ID checking capabilities, while the latter was decentralised with built-in anonymity and often traded on deliberately illicit exchanges. This example demonstrates that anything from centrality to the nature of service offered could alter the feasibility of prevention measures in each stakeholder-risk interaction scenario.

Panellists identified numerous CtIs throughout their insights, derived from a wide range of considerations, particularly when asked to score stakeholders for their power and responsibilities. PESTLE analysis (Perera, 2017), namely the consideration of political, economic, social, technological, legal and environmental factors to identify constraints, is an ideal framework to categorise CtIs. A non-exhaustive list, developed from panellist insights, is provided in table 11.

Table 11 Identified CtIs listed according to PESTLE

PESTLE	CtI	Explanation
Political	Vitality	How crucial the service provided by a technology (and associated stakeholders) are to critical infrastructure or systems
Economic	Barriers to entry	Whether preconditions (such as large initial investments) are required to access and exploit a risky stakeholder or technology
	Demand	How popular the stakeholder (and provided technology) is to users
	Financial capital	Budget available to stakeholders for crime prevention measures
	Stakeholder role	Whether the stakeholder is a pioneer, supplier, host, user or regulator of new technologies
	Transaction capabilities	The volume of funds that can be moved using a technology or stakeholder with a reasonable expectation of not being flagged as suspicious
Social	Ethical uses	The nature of the general audience using a provided technology (e.g., predominantly criminal for privacy coins, compared to legitimate for crowdfunding)
	Externalities to society	Whether the threat provides a wider benefit (e.g. central bank digital currencies) or cost (e.g. online gambling) to society
Technological	Anonymity	The inherent privacy offered by the technology/stakeholder to users
	Automation	The susceptibility of the stakeholder/technology to criminal activity due to a lack of human oversight or vulnerability in their cyber systems
	Centrality	Whether the stakeholder or technology is centralised (e.g., customer loyalty points issuance) or decentralised (e.g., cryptocurrencies)
	Detection capabilities	The extent to and speed with which a stakeholder can detect and intervene to prevent a suspicious activity

	Displacement	How easily criminals can circumvent security protocols of, or switch to a similar substitute to, a given stakeholder or technology
	Manipulation risk	How easily financial intelligence related to the stakeholder or technology can be manipulated by customer activity (e.g., fake social media profiles)
	Proximity / exposure to risk	Whether the stakeholder is directly exposed to ML/TF risk, or whether their degree of exposure is secondary (e.g., NPM providers compared to the platforms hosting their servers respectively)
	Source of risk	The specific aspect of a new technology that constitutes an ML/TF risk (for example anonymity or automation)
Legal	AML/CFT obligations	Whether the providing stakeholder is obliged under AML/CFT regulations
	Financial intelligence	The amount and detail of customer data that can be collected by a stakeholder/for a given technology
	Insider threats	Whether or not the relevant stakeholder is prone to corruption or complicity with ML/TF offenders
	Legal powers	The authority to reprimand offenders or to address ML/TF risks
Environmental		*None identified*

CtIs cause prevention measures to be feasible and effective in some stakeholder-risk interaction scenarios but not others. Recognising contextual circumstances, and the constraints (or advantages) that they create is therefore important for devising a feasible prevention strategy; a 'one-size-fits-all' approach to prevention may not be feasible, especially given the diverse range of new technologies (and associated unique CtIs) being developed and exploited. If prevention measures are to diversify accordingly, certain standards are necessary to ensure cost-effectiveness. The next section motivates one such standard.

9.2. A standard for implementation: 'Protect, Provide, Promote'

Many technologies referred to in this study as 'ML/TF risks' have, mostly and by a far greater extent, highly beneficial uses. In recognition of this, panellists have criticised the inconveniences (e.g. false positives in suspicious activity detection or negative marketing) that certain regulations cause to legitimate users. The cost of such measures and their burden on innovation were also frequently criticised. These common criticisms can be combined into a 3-point standard that future prevention measures might strive to abide by, namely 'Protect', 'Provide' and 'Promote'. Table 12 introduces these principles, hereafter referred to as the '3P standard'.

Table 12 The '3P' standard

Principle	**Explanation**
Protect legitimate users	Prevention measures should ensure that users and their privacy are protected from intrusive KYC and inconveniences associated with false positive suspicious activity flags

Provide efficient compliance	Burdensome compliance costs are often passed onto paying users of a service (through commission or transaction fees). Unnecessary costs should therefore be reduced to ensure that users have access to reasonably priced financial services
Promote beneficial innovation	Start-ups and sustainable innovation should not be discouraged by high regulatory costs. Regulators and other government agencies should consider providing initial financing or support to innovators when costly regulations cannot be avoided.

9.3. Devising 3P-compliant prevention measures

Most prevention measures identified by panellists are customisable and can be considered on an 'implementation scale' ranging from the most extreme form of implementation to the least. For example, outright prohibition – a measure suggested for all three technology categories – could be implemented as a blanket ban for all technologies (such as a cryptocurrency ban) or a targeted ban on the most high-risk aspects of a technology only (such as a ban on privacy coins). Similar scales can be considered for controlling exchange points (the toughness of controls), value limits (the size of the limit and for which mediums or users it applies) or detection algorithms (cost and level of privacy afforded). In this sense, 'implementation strategies' can be considered as a subset of prevention measures, representing various ways of implementing them by changing certain parameters.

To assist in striking the correct balance, the different implementation strategies for each prevention measure can be imagined on a three-dimensional chart formed of X, Y and Z axes representing 'Protect', 'Provide' and 'Promote' respectively. Implementation strategies at co-ordinates (0,0,0) would represent strategies with zero consideration all three factors. As strategies are adjusted to better adhere to each factor, their respective co-ordinates would increase. Based on the plotted implementation strategies, stakeholders will be able to visualise, adjust and select strategies based on their CtIs. In theory, stakeholders would aim to select and adjust implementation strategies to achieve the highest possible co-ordinates in all three dimensions. An example model for 'outright prohibition', with some possible implementation strategies, is shown in Figure 17. This is purely an example; the scores and strategies shown are not based on any findings.

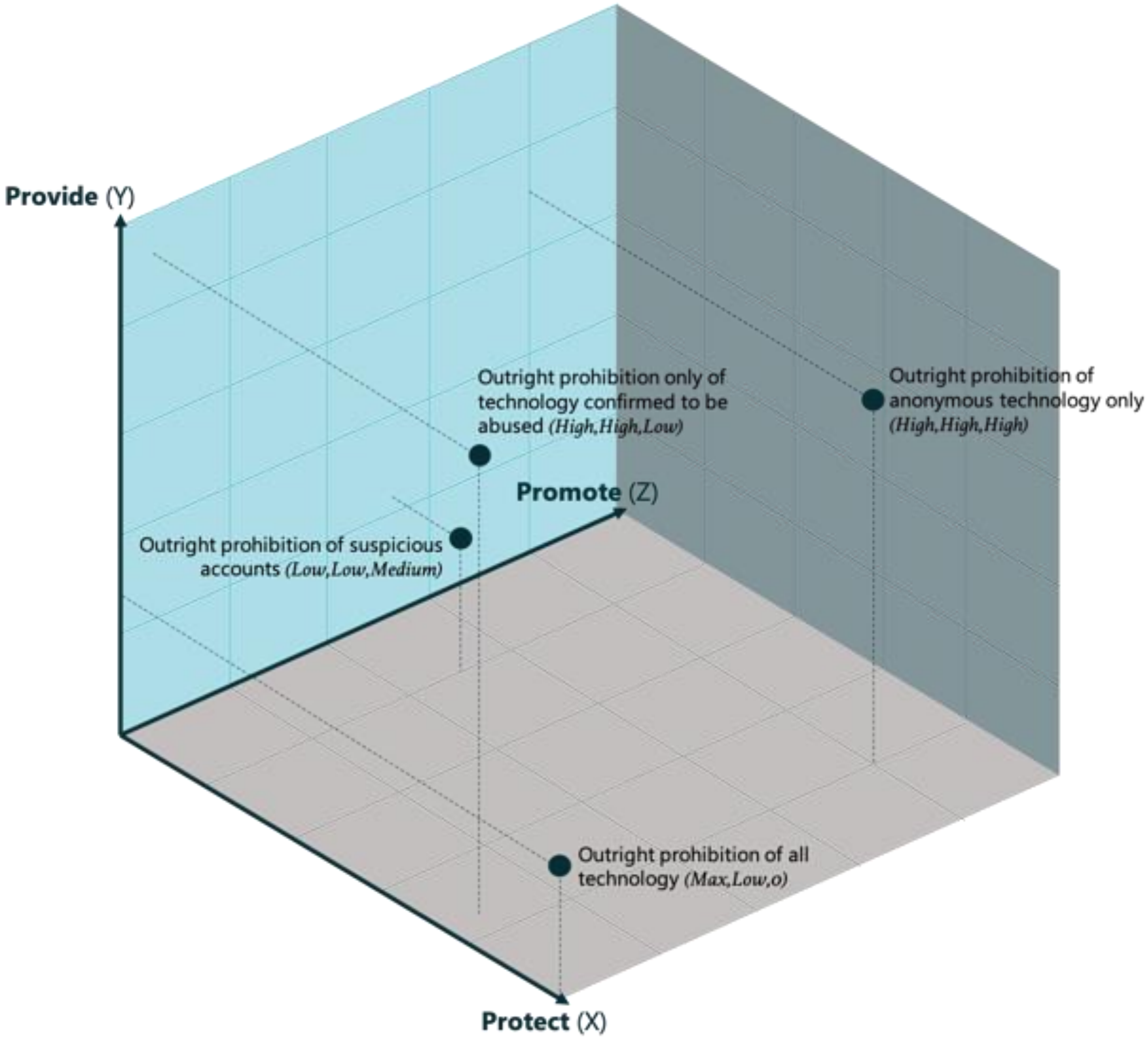
Provide (Y)
Outright prohibition only of technology confirmed to be abused (High,High,Low)
Outright prohibition of anonymous technology only (High,High,High)
Promote (Z)
Outright prohibition of suspicious accounts (Low,Low,Medium)
Outright prohibition of all technology (Max,Low,o)
Protect (X)

Fig. 17 An example 3P model for different implementation strategies of 'outright prohibition'

Such a model need not assume that all 3Ps present a trade-off between themselves and effectiveness of measures. It is entirely feasible to suggest, for example, that a targeted ban on privacy coins could prevent more ML/TF than a ban on cryptocurrencies entirely. In fact, a core advantage of this model is to demonstrate that the most effective measures could also be the most user/innovation friendly.

Naturally, CtIs will affect the feasible levels of 'Protect', 'Provide', 'Promote' that can be afforded in each stakeholder-risk interaction scenario. However, stakeholders need not stick to only one prevention strategy, as combining different approaches can be overall better suited depending on CtIs, while also improving both effectiveness and 3P compliance. Based on 3P modelling, stakeholders will be able to identify the most feasible and effective combinations of measures. One major advantage of this Delphi study was that it consulted stakeholders across different industries. This meant that the prevention measures identified, corresponding to five underlying approaches, were highly diverse. The next section summarises these approaches and formulates a framework that can aid their implementation.

9.4. The DECODE framework

Embodying their diverse backgrounds, panellists proposed numerous prevention measures that were reported in the results under five general approaches. These were ***D**etect, **E**ducate, **C**o-**o**perate, **D**efend* and ***E**nforce* or, in short, DECODE. Table 13 shows a summary of all the prevention measures identified in the results section split into these five approaches. Given its applicability to all three technology categories considered (DLT, NPM, FinTech), the framework demonstrates its utility across many different emerging technologies.

Table 13 The DECODE framework

Approach	Prevention measures
Detect	Improve digital anomaly detection and tracking using machine learning and AI Improve spending, network, pattern, behavioural and incentives analyses Clearer ID/due diligence requirements and restrictions on anonymity Use of blockchain technology to make transactions more transparent Maintain a healthy balance between digital KYC and human oversight Improved training and procedures for firms engaging with new technologies Ensure algorithms are updated to detect the latest crime trends within recent innovation Financial assistance or funds for start-ups to cover compliance costs
Educate	Public education of users on scams and risks of new technologies Encourage users to report possible scams and suspicious activity Harm the reputation of or increase the inconvenience of using risk-prone technologies Public shaming of non-compliant entities or individuals Raise awareness to promote healthy regulation that protects innovation
Co-operate	Greater data sharing between and across compliant institutions and authorities Constructive relations between regulators and compliant entities to identify KYC deficiencies Internationally orchestrated regulation with widespread global compliance Stakeholder consultations to improve regulations and solve conflicting ones
Defend	Checks on the genuine nature of users and goods/services listings on online marketplaces Prohibition of risk-prone services and mediums of value (potentially including cash) Controlling exchange points between alternative value mediums and fiat currency Value limits on funds convertible and storable in alternative value mediums Licensing of tech firms to require crime-resistant coding protocols Security audits and periodic stress tests of resilience to cyber threats
Enforce	Improve the numbers of asset seizures and success rates of prosecutions Allow merchant account providers more control of payments from alternative value mediums

	Increase designated technology-specific (e.g., metaverse) police and detective units
	Require 'smart' controls in code for quick interventions by designated authorities
	Analysis of other devises registered to suspicious users for further investigation
	Instant blocking of suspicious transfers and freezing of suspected accounts

When the mean monetary cost, societal cost and effectiveness scores of the prevention measures above were taken and aggregated for each overall approach, they were found to be similar overall (see data supplement section 10). Detection-based approaches, for example, did not have any major cost-benefit advantage over other approaches, despite their central focus in AML/CFT. This suggests that no specific approach is outrightly superior to others. CtIs and 3P standards should therefore drive selective prevention strategies, with varying combinations and extents, based on contextual circumstances. The cost-effectiveness scores above apply only for the abstract prevention measures overall and may change widely depending on the respective stakeholders and specific implementation strategies chosen.

9.5. Enhancing DECODE and further research

The study presents three paths for further research. The first involves identifying more constraints to implementation and to which stakeholders they apply. The second involves further investigating the utility of the 3P standard, such as through assessing whether prevention measures are more effective when implementation strategies are devised through 3P modelling. The third involves submitting the DECODE framework for stakeholder scrutiny, investigating the effectiveness of different prevention measure combinations on different stakeholders based on their CtIs. Combined, all three of these paths can formulate a powerful protocol for devising the optimal prevention strategy for different stakeholder-risk interaction scenarios.

One limitation of this exercise is that, despite extended invitations and deadlines for responses, panellist attrition was notable across rounds. Since the study was conducted over three time-intensive rounds across experts with presumably comprehensive schedules, this was expected and perhaps solvable with additional incentives for participation (Witkin & Altschuld, 1995) – a solution that was not covered under the study ethics approval. The FinTech aspect of this study was particularly affected by attrition. However, the study nevertheless yielded plenty of qualitative insights that were sufficient for deriving the outcomes reported. Further studies should nevertheless prioritise global participation and measures for maintaining engagement amongst panellists.

10. Conclusion

Developments since the conduct of this Delphi study, such as the surge of non-fungible tokens (NFTs, an example of 'coloured coins'), emphasise the plausibility of the assessed risks and the importance of pre-empting technology-enhanced financial crime threats. The historic embrace of cryptocurrencies by El Salvador and Ukraine, albeit for very different reasons, also emphasise that new technologies are not losing prominence and, to the contrary, are gaining mainstream acceptance. The results of this Delphi study therefore remain relevant for consideration alongside wider global economic, political and social trends, as these may accelerate the prevalence of threats identified here by surveyed panellists. Other developments, such as Russia softening its Bitcoin mining policy amid western sanctions and expulsion from the SWIFT banking system during the 2022 invasion of Ukraine, also increase sanctions evasion risks for NPMs and FinTech services.

Arguably more important in terms of the current study's findings, however, is the prevention-related insights and the two frameworks proposed as a result of expert consultation. Regardless of whether the risks discussed take hold (if anything, they are accelerating on the cryptocurrency front), the prevention frameworks and core arguments will remain constantly valid. The importance of identifying stakeholder-risk interaction scenarios before applying the most effective prevention implementation strategies is crucial regardless of what risk might or might not take hold. Through the 3P standard and DECODE framework, this paper offers relevant stakeholders methods for doing so not only in a structured manner, but also potentially at a faster pace than previous prevention initiatives. This is particularly important due to the rapidly changing global developments and fast-growing innovations we experience on a contemporary basis.

The prevention strategies that comprise these frameworks also demonstrate growing relevance in the context of recent developments. For example, as millions of dollars are now being invested into virtual real estate in blockchain-powered digital worlds (a vector for money laundering), entire countries such as Barbados are seeking to open virtual embassies in the 'metaverse' (Wyss, 2021). Coupled with *Facebook's* rebranding to *'Meta'* and growing investment into virtual reality technologies, the prospect of metaverse-specific detective units (proposed under 'Enforce') has become an increasingly plausible idea.

The findings of this study aim to complement and improve the pragmaticism, pre-emptive risk detection and cost-effectiveness of dominant (CDD/KYC) approaches, encapsulating varying approaches in a single (DECODE) framework, while ensuring – based on the 3P standard – that technologies with the potential of transforming our lives for the better continue to innovate sustainably and securely.

References

Alon, I., Guimón, J., & Urbanos-Garrido, R. (2019). What to expect from assisted reproductive technologies? Experts' forecasts for the next two decades. *Technological Forecasting and Social Change*, *148*, 119722. https://doi.org/10.1016/j.techfore.2019.119722

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). *FinTech and RegTech in a Nutshell, and the Future in a Sandbox.* CFA Institute Research Foundation.

Arslanian, H., Donovan, R., Blumenfeld, M., & Zamore, A. (2021). *El Salvador's law: A meaningful test for Bitcoin* (p. 11). Pwc. https://www.pwc.com/gx/en/financial-services/pdf/el-salvadors-law-a-meaningful-test-for-bitcoin.pdf

BBC. (2019, October). *BBC One—Watchdog—Monzo*. BBC Watchdog. https://www.bbc.co.uk/programmes/articles/2qS0HM6nBkcPMx0W8t7fqVJ/monzo

Beiderbeck, D., Frevel, N., von der Gracht, H. A., Schmidt, S. L., & Schweitzer, V. M. (2021a). Preparing, conducting, and analyzing Delphi surveys: Cross-disciplinary practices, new directions, and advancements. *MethodsX*, *8*, 101401. https://doi.org/10.1016/j.mex.2021.101401

Beiderbeck, D., Frevel, N., von der Gracht, H. A., Schmidt, S. L., & Schweitzer, V. M. (2021b). The impact of COVID-19 on the European football ecosystem – A Delphi-based scenario analysis. *Technological Forecasting and Social Change*, *165*, 120577. https://doi.org/10.1016/j.techfore.2021.120577

Belton, I., MacDonald, A., Wright, G., & Hamlin, I. (2019). Improving the practical application of the Delphi method in group-based judgment: A six-step prescription for a well-founded and defensible process. *Technological Forecasting and Social Change*, *147*, 72–82. https://doi.org/10.1016/j.techfore.2019.07.002

Belton, I., Wright, G., Sissons, A., Bolger, F., Crawford, M. M., Hamlin, I., Taylor Browne Lūka, C., & Vasilichi, A. (2021). Delphi with feedback of rationales: How large can a Delphi group be such that participants are not overloaded, de-motivated, or disengaged? *Technological Forecasting and Social Change*, *170*, 120897. https://doi.org/10.1016/j.techfore.2021.120897

Blasco, N. J., & Fett, N. A. (2019). Blockchain Security: Situational Crime Prevention Theory and Distributed Cyber Systems. *International Journal of Cybersecurity Intelligence and Cybercrime*, *2*(2), 44–59.

Bloem da Silveira Junior, L. A., Vasconcellos, E., Vasconcellos Guedes, L., Guedes, L. F. A., & Costa, R. M. (2018). Technology roadmapping: A methodological proposition to refine Delphi results. *Technological Forecasting and Social Change*, *126*, 194–206. https://doi.org/10.1016/j.techfore.2017.08.011

Bradley, L., & Stewart, K. (2003). A Delphi study of Internet banking. *Marketing Intelligence & Planning*, *21*(5), 272–281. https://doi.org/10.1108/02634500310490229

Browne, R. (2021, March 1). Bitcoin is at a tipping point and could become ‘currency of choice’ for global trade, Citi says. *CNBC*. https://www.cnbc.com/2021/03/01/bitcoin-btc-is-at-a-tipping-point-citi-says.html

Chang, A. M., Gardner, G. E., Duffield, C., & Ramis, M.-A. (2010). A Delphi study to validate an Advanced Practice Nursing tool. *Journal of Advanced Nursing*, *66*(10), 2320–2330. https://doi.org/10.1111/j.1365-2648.2010.05367.x

Coutorie, L. E. (1995). The future of high-technology crime: A parallel Delphi study. *Journal of Criminal Justice*, *23*(1), 13–27. https://doi.org/10.1016/0047-2352(94)00042-5

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

Dalal, S., Khodyakov, D., Srinivasan, R., Straus, S., & Adams, J. (2011). ExpertLens: A system for eliciting opinions from a large pool of non-collocated experts with diverse knowledge. *Technological Forecasting and Social Change*, *78*(8), 1426–1444. https://doi.org/10.1016/j.techfore.2011.03.021

Dalkey, N. C. (1968). *Predicting the Future* (P-3948). RAND Corporation. https://www.rand.org/pubs/papers/P3948.html

Day, J., & Bobeva, M. (2005). A Generic Toolkit for the Successful Management of Delphi Studies. *In: Electronic Journal of Business Research Methods*, *3*(2), 103–116.

de Loë, R. C., Melnychuk, N., Murray, D., & Plummer, R. (2016). Advancing the State of Policy Delphi Practice: A Systematic Review Evaluating Methodological Evolution, Innovation, and Opportunities. *Technological Forecasting and Social Change*, *104*, 78–88. https://doi.org/10.1016/j.techfore.2015.12.009

Delbeq, A. L., Van de Ven, A. H., & Gustafson, D. H. (1976). Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes. *Group & Organization Studies*, *1*(2), 256–256. https://doi.org/10.1177/105960117600100220

Devaney, L., & Henchion, M. (2018). Who is a Delphi ‘expert’? Reflections on a bioeconomy expert selection procedure from Ireland. *Futures*, *99*, 45–55. https://doi.org/10.1016/j.futures.2018.03.017

Diamond, I. R., Grant, R. C., Feldman, B. M., Pencharz, P. B., Ling, S. C., Moore, A. M., & Wales, P. W. (2014). Defining consensus: A systematic review recommends methodologic criteria for reporting of Delphi studies. *Journal of Clinical Epidemiology*, *67*(4), 401–409. https://doi.org/10.1016/j.jclinepi.2013.12.002

DiPiero, C. (2017). Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web Notes. *University of Illinois Law Review*, *2017*(3), 1267–1298.

Ekblom, P. (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), 249–265.

Elliptic, E. T. (2022, March 9). *Live Updates: Ukraine Government Turns to Crypto to Crowdfund Millions of Dollars*. https://www.elliptic.co/blog/live-updates-millions-in-crypto-crowdfunded-for-the-ukrainian-military

EUROPOL. (2015). *The Internet Organised Crime Threat Assessment (IOCTA) 2015*. EUROPOL. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015

Field, M. (2021, February 9). Bitcoin value overtakes Russian ruble at $860bn. *The Telegraph*. https://www.telegraph.co.uk/technology/2021/02/09/bitcoin-value-overtakes-russian-ruble-at860bn/

Fitch, K., Bernstein, S. J., Aguilar, M. D., Burnand, B., LaCalle, J. R., Lazaro, P., van het Loo, M., McDonnell, J., Vader, J., & Kahan, J. P. (2001). *The RAND/UCLA Appropriateness Method User's Manual*. RAND Corporation. https://www.rand.org/pubs/monograph_reports/MR1269.html

Floridi, L., & Chiriatti, M. (2020). GPT-3: Its Nature, Scope, Limits, and Consequences. *Minds and Machines*, *30*(4), 681–694. https://doi.org/10.1007/s11023-020-09548-1

Franklin, K. K., & Hart, J. K. (2006). Idea Generation and Exploration: Benefits and Limitations of the Policy Delphi Research Method. *Innovative Higher Education*, *31*(4), 237–246. https://doi.org/10.1007/s10755-006-9022-8

Ghosh, M. (2021, October 19). *Is Estonia, the 1st to regulate crypto, now killing it off?* Forkast. https://forkast.news/estonia-wants-to-rescind-crypto-licenses/

GO Science. (2018). *The Futures Toolkit: Tools for Futures Thinking and Foresight across UK Government* (Edition 1.0; p. 116). UK Government Office for Science (GO Science). https://www.gov.uk/government/publications/futures-toolkit-for-policy-makers-and-analysts

Goodman, M. (2016). *Future Crimes: Inside The Digital Underground and the Battle For Our Connected World*. Corgi.

Gordon, T., & Pease, A. (2006). RT Delphi: An efficient, "round-less" almost real time Delphi method. *Technological Forecasting and Social Change*, *73*(4), 321–333. https://doi.org/10.1016/j.techfore.2005.09.005

Gross, M. B., Hogarth, J. M., & Schmeiser, M. D. (2012). Use of Financial Services by the Unbanked and Underbanked and the Potential for Mobile Financial Services Adoption. *Federal Reserve Bulletin*, *98*(4), 0–0. https://doi.org/10.17016/bulletin.2012.98-4

Hasson, F., & Keeney, S. (2011). Enhancing rigour in the Delphi technique research. *Technological Forecasting and Social Change*, *78*(9), 1695–1704. https://doi.org/10.1016/j.techfore.2011.04.005

Iqbal, S., & Pipon-Young, L. (2009). The Delphi method | The Psychologist. *The Psychologist*, *22*(7), 498–601.

Jee, J., & Hutchinson, F. (2019). RegTech Opportunities in a Post-4MLD/5MLD World. In J. Barberis, D. W. Arner, & R. P. Buckley (Eds.), *The RegTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation*. John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119362197.ch33

Keeney, S., Hasson, F., & McKenna, H. (2006). Consulting the oracle: Ten lessons from using the Delphi technique in nursing research. *Journal of Advanced Nursing*, *53*(2), 205–212. https://doi.org/10.1111/j.1365-2648.2006.03716.x

Kluge, U., Ringbeck, J., & Spinler, S. (2020). Door-to-door travel in 2035 – A Delphi study. *Technological Forecasting and Social Change*, *157*, 120096. https://doi.org/10.1016/j.techfore.2020.120096

Kozak, M., & Iefremova, O. (2014). Implementation of the Delphi technique in finance. *E-Finanse: Financial Internet Quarterly*, *10*(4), 36–45. https://doi.org/10.14636/1734-039X_10_4_004

Kuhn, D. (2021, February 19). Bitcoin Is Worth $1T and OKCoin Delists BCH and BSV. *Coindesk*. https://www.coindesk.com/bitcoin-dollar-okcoin-bsv-and-bch

Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy*, *63*, 113–121. https://doi.org/10.1016/j.drugpo.2018.09.013

Levy, I. (2019, February 22). Security, complexity and Huawei; protecting the UK's telecoms networks [UK Government]. *National Cyber Security Centre*. https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks

LexisNexis. (2020). *True Cost of Financial Crime Compliance Study: Global Report*. LexisNexis Risk Solutions. https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report

Liftoff. (2020). *2020 Mobile App Trends Report*. Liftoff. https://content.liftoff.io/hubfs/Reports/2020/2020%20Mobile%20App%20Trends%20Report/2020%20Mobile%20App%20Trends%20Report%20EN.pdf?_ga=2.115811973.2048508816.1614882141-1389372869.1614882141

Lootsma, Y. (2017). Blockchain as the Newest Regtech Application—The Opportunity to Reduce the Burden of KYC for Financial Institutions. *Banking & Financial Services Policy Report*, *36*(8), 16–21.

McKenna, F. P. (1993). It won't happen to me: Unrealistic optimism or illusion of control? *British Journal of Psychology*, *84*(1), 39–50. https://doi.org/10.1111/j.2044-8295.1993.tb02461.x

McMillan, S. S., King, M., & Tully, M. P. (2016). How to use the nominal group and Delphi techniques. *International Journal of Clinical Pharmacy*, *38*(3), 655–662. Scopus. https://doi.org/10.1007/s11096-016-0257-x

Megaw, N. (2019, May 22). Regulator orders N26 to improve anti-money laundering controls. *Financial Times*. https://www.ft.com/content/cb06a354-7c97-11e9-81d2-f785092ab560

Merfeld, K., Wilhelms, M.-P., Henkel, S., & Kreutzer, K. (2019). Carsharing with shared autonomous vehicles: Uncovering drivers, barriers and future developments – A four-stage Delphi study. *Technological Forecasting and Social Change*, *144*, 61–81. https://doi.org/10.1016/j.techfore.2019.03.012

Meskell, P., Murphy, K., Shaw, D. G., & Casey, D. (2014). Insights into the use and complexities of the Policy Delphi technique. *Nurse Researcher*, *21*(3), 32–39. https://doi.org/10.7748/nr2014.01.21.3.32.e342

Mitchell, V. (1992). Using Delphi to Forecast in New Technology Industries. *Marketing Intelligence & Planning*, *10*(2), 4–9. https://doi.org/10.1108/02634509210012069

Naheem, M. A. (2018). TBML suspicious activity reports – a financial intelligence unit perspective. *Journal of Financial Crime*, *25*(3), 721–733. https://doi.org/10.1108/JFC-10-2016-0064

Nance, M. T. (2018). The regime that FATF built: An introduction to the Financial Action Task Force. *Crime, Law and Social Change*, *69*(2), 109–129. https://doi.org/10.1007/s10611-017-9747-6

Novakowski, N., & Wellar, B. (2008). Using the Delphi Technique in Normative Planning Research: Methodological Design Considerations. *Environment and Planning A: Economy and Space*, *40*(6), 1485–1500.

O'Brien, K. (2018, December 13). More Than 7.5 Million Chinese Use Crypto-Related Apps, Analysis Shows. *CryptoGlobe*. 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

Pätäri, S. (2010). Industry- and company-level factors influencing the development of the forest energy business—Insights from a Delphi Study. *Technological Forecasting and Social Change*, *77*(1), 94–109. https://doi.org/10.1016/j.techfore.2009.06.004

Perera, R. (2017). *The PESTLE Analysis*. Nerdynaut.

Pol, R. F. (2020). Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. *Policy Design and Practice*, *3*(1), 73–94. https://doi.org/10.1080/25741292.2020.1725366

Preston, C. C., & Colman, A. M. (2000). Optimal number of response categories in rating scales: Reliability, validity, discriminating power, and respondent preferences. *Acta Psychologica*, *104*(1), 1–15. https://doi.org/10.1016/S0001-6918(99)00050-5

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

Rauch, W. (1979). The decision Delphi. *Technological Forecasting and Social Change*, *15*(3), 159–169. https://doi.org/10.1016/0040-1625(79)90011-8

Rowe, G., & Wright, G. (2001). Expert Opinions in Forecasting: The Role of the Delphi Technique. In J. S. Armstrong (Ed.), *Principles of Forecasting: A Handbook for Researchers and Practitioners* (pp. 125–144). Springer US. https://doi.org/10.1007/978-0-306-47630-3_7

Rowe, G., Wright, G., & Bolger, F. (1991). Delphi: A reevaluation of research and theory. *Technological Forecasting and Social Change*, *39*(3), 235–251. https://doi.org/10.1016/0040-1625(91)90039-I

Schmalz, U., Spinler, S., & Ringbeck, J. (2021). Lessons Learned from a Two-Round Delphi-based Scenario Study. *MethodsX*, *8*, 101179. https://doi.org/10.1016/j.mex.2020.101179

Schueffel, P. (2016). Taming the Beast: A Scientific Definition of Fintech. *Journal of Innovation Management*, *4*(4), 32–54. https://doi.org/10.24840/2183-0606_004.004_0004

Smith, L. (2019, October 24). Digital Bank Monzo Denies Unfairly Freezing Customer Accounts. *MoneyExpert*. https://www.moneyexpert.com/news/digital-bank-monzo-denies-unfairly-freezing-customer-accounts/

Soudijn, M. 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. ProQuest Central; Social Science Premium Collection. https://doi.org/10.1007/s10610-018-9379-0

Statista. (2021). *Digital Payments report 2021*. Statista. https://www.statista.com/outlook/dmo/fintech/digital-payments/mobile-pos-payments/worldwide

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution*. Penguin.

TASS. (2022, February 18). *The Central Bank has prepared a bill to ban the issuance and circulation of cryptocurrencies in Russia*. TASS. https://tass.ru/ekonomika/13754269?utm_source=coindesk.com&utm_medium=referral&utm_campaign=coindesk.com&utm_referrer=coindesk.com

Teicher, R. (2018, March 18). How Uber ghost rides are linked to online money laundering. *The Next Web*. https://thenextweb.com/contributors/2018/03/18/uber-ghost-rides-linked-online-money-laundering/

Turoff, M. (1970). The design of a policy Delphi. *Technological Forecasting and Social Change*, *2*(2), 149–171. https://doi.org/10.1016/0040-1625(70)90161-7

U.S. Treasury. (2021, November 8). *Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange*. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/jy0471

Velez, S., Neubert, M., & Halkias, D. (2020). Banking Finance Experts Consensus on Compliance in US Bank Holding Companies: An e-Delphi Study. *Journal of Risk and Financial Management*, *13*(2), 28. https://doi.org/10.3390/jrfm13020028

Vernon, W. (2009). The Delphi technique: A review. *International Journal of Therapy and Rehabilitation*, *16*(2), 69–76. https://doi.org/10.12968/ijtr.2009.16.2.38892

von der Gracht, H. A. (2012). Consensus measurement in Delphi studies: Review and implications for future quality assurance. *Technological Forecasting and Social Change*, *79*(8), 1525–1536. https://doi.org/10.1016/j.techfore.2012.04.013

Warth, J., von der Gracht, H. A., & Darkow, I.-L. (2013). A dissent-based approach for multi-stakeholder scenario development—The future of electric drive vehicles. *Technological Forecasting and Social Change*, *80*(4), 566–583. https://doi.org/10.1016/j.techfore.2012.04.005

Wass, S. (2017, May 10). Regtech could save banks £2.7bn on AML compliance. *Global Trade Review (GTR)*. https://www.gtreview.com/news/global/regtech-could-save-banks-2-7bn-yearly-on-aml-compliance/

Witkin, B. R., & Altschuld, J. W. (1995). *Planning and Conducting Needs Assessments: A Practical Guide*. SAGE Publications Ltd. https://uk.sagepub.com/en-gb/eur/planning-and-conducting-needs-assessments/book5003

Wyss, J. (2021, December 14). Barbados Is Opening a Diplomatic Embassy in the Metaverse. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2021-12-14/barbados-tries-digital-diplomacy-with-planned-metaverse-embassy