Cryptocurrencies and UK FinTechs

Perspectives and Experiences of Financial Crime

White Paper

by the

FinTech FinCrime Exchange

May 2018

FINTECH
FINCRIME
EXCHANGE

Abstract

Cryptocurrencies have become the subject of increasing public sector, private sector and consumer focus, with the value of popular coins, such as Bitcoin, spiking rapidly in 2017. In response, growing concerns have been voiced on the potential of cryptocurrencies to facilitate financial crime. The UK government has stated its intention to strike a balance between both enabling innovation in the cryptocurrency space while also managing the associated risks, though regulatory developments have been slow-going.

This white paper aims to answer the following questions: how does the UK FinTech sector perceive the risks associated with cryptocurrencies, and how are they managing the challenges related to this new disruptive technology?

The research presented by the FinTech FinCrime Exchange (FFE) suggests that while some UK FinTechs have considered expanding their involvement in the cryptocurrency space, the lack of clarity around the regulatory position on cryptocurrencies and perceived financial crime risks have resulted in a cautious stance.

Those FFE members actively engaging with cryptocurrencies, through offering cryptocurrency-linked products or through interacting with cryptocurrency users, reported a more manageable financial crime landscape than broadly perceived, with red flags for suspicious behaviour and financial crime typologies aligning with what is standard in the broader financial services ecosystem.

More generally, issues of perception and reputation around cryptocurrencies drive a number of the challenges faced by those engaged with cryptocurrencies more so than the realities of engaging with cryptocurrencies in practice.

Improving financial crime controls and assurance on controls remained a concern among those engaged with cryptocurrencies, though more so with those who monitored cryptocurrency transactions rather than who offered cryptocurrency products.

Based on these observations, this white paper recommends that FinTechs apply a thorough and robust risk-based approach to AML/CTF using cryptocurrency-specific tools. Clear guidance on implementing upcoming cryptocurrency regulations should be communicated effectively to FinTechs and the financial services sector more broadly. Similarly, law enforcement should work to clarify the realities of financial crime risk within the cryptocurrency space, to help drive a realistic understanding of the risks involved with cryptocurrency innovation.

About the FFE

The FFE was established in January 2017 as an intra-industry partnership. It was founded by the Centre for Financial Crime and Security Studies (CFCS) at the Royal United Services Institute (RUSI), a London-based defence and security think tank, and FINTRAIL, a UK financial crime risk management consultancy. The FFE promotes an increased understanding of financial crime by the FinTech industry. It provides a collaborative forum for FinTechs to discuss financial crime typologies, risk management approaches and regulatory challenges. Its objective is to inform, debate and develop knowledge and best practices. Its members meet monthly to discuss these topics. As of April 2018, the FFE includes over 40 participating members from the UK FinTech industry.

Enquiries about the FFE can be directed to the FFE Secretariat. For further information please contact FFE_admin@fintrail.co.uk.

FINTRAIL

RUSI
www.rusi.org

About the Author

Meredith Beeston is an Analyst at FINTRAIL, where she helps the team advise the FinTech sector on financial crime risk management. She also coordinates the FFE. Her previous research experience at King's College London and American University cultivated her interest in cybercrime, terrorist financing and public-private partnerships.

Companies that are among the members of the FFE include:

Table of Contents

1. Introduction

In 2017, cryptocurrencies underwent a meteoric rise both in value and attention received. During the 13-fold increase in the value of Bitcoin to its December 2017 peak of US$19,000[1], hundreds of thousands of Britons began investing in the cryptocurrency[2].

Definitions:

Virtual Currencies: *'a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically'* (EU Fifth Money Laundering Directive or 5MLD).

Cryptocurrencies: *'distributed, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight.'* That is, they are a decentralised subset of virtual currencies (Financial Action Task Force or FATF).

Initial Coin Offerings (ICOs): sales of new cryptocurrencies to early investors.

The rise of cryptocurrencies left many within law enforcement, government and financial services voicing concerns about the potential for virtual currencies to facilitate financial crime. Action Fraud reported a tripling in the number of fraud cases linked to Bitcoin[3], and Europol has claimed that £4 billion is currently being laundered through cryptocurrencies within Europe[4]. While financial crime related to cryptocurrencies has inevitably risen with the surge in the value of certain coins, the overall money laundering and terrorist financing risks for cryptocurrencies remains low, according the *National Risk Assessment of Money Laundering and Terrorist Financing 2017*[5]. Compared to cash in particular, cryptocurrencies are less likely to be used in high-risk transactions[6].

Nevertheless, financial crime risks, both perceived and actual, have proven difficult to balance against the opportunities associated with virtual currencies and their underlying blockchain technology, which securely links and records data and transactions. The UK Treasury, in a 2015 report, stated that *'the government wishes to foster a supportive environment for the development of legitimate businesses in the digital currency sector, so*

[1] Coindesk, "Bitcoin (USD) Price," accessed 08 March 2018.
[2] James Titcomb and Katie Morley, "Lloyds Bank in Bitcoin crackdown: credit card owners banned from buying cryptocurrency," The Telegraph, 05 February 2018.
[3] Matthew Field, "Bitcoin fraud triples as criminals target cryptocurrency boom," The Telegraph, 26 January 2018.
[4] Adam James, "Europol Takes Down Major Bitcoin Money Laundering Network," Bitcoinist, 11 April 2018.
[5] HM Treasury, Home Office, National risk assessment of money laundering and terrorist financing 2017, 26 October 2017.
[6] David Carlisle, "Virtual Currencies and Financial Crime Challenges and Opportunities," RUSI, March 2017.

that the UK can see some of the benefits of digital currencies."[7] While Bank of England Governor Mark Carney expressed concerns about the anonymity of cryptocurrencies facilitating financial crime, he also emphasised that *"authorities should be careful not to stifle innovations which could in the future improve financial stability"*[8]

For financial institutions, the lack of regulatory clarity about how to best manage the financial crime risks of cryptocurrencies - while still pursuing innovation - has contributed to a hesitation to engage meaningfully with cryptocurrencies and cryptocurrency-related companies. However, much of the wider discourse surrounding this hesitation on cryptocurrencies has focused on traditional banks, with less attention devoted to the opinions of the broader FinTech sector and their experiences with cryptocurrencies.

Thus, this white paper aims to answer the following questions: how does the UK FinTech sector perceive the risks associated with cryptocurrencies, and how are they managing the challenges related to this new disruptive technology?

What is FinTech?

This paper uses the term FinTech to refer to new financial services companies that specialise in the provision of products and services featuring online and mobile technology as a central component of their operations, and not as an incidental or merely adaptive feature. FinTechs include challenger banks, prepaid card providers, FX companies, peer to peer lending platforms, mobile payments and several others. Cryptocurrencies are also considered to be under the FinTech umbrella, though more FFE members are not purpose-built cryptocurrency platforms.

According to research conducted by the FinTech FinCrime Exchange (FFE), while some UK FinTechs are interested in the prospects of increasing their interaction with cryptocurrencies and cryptocurrency users, many are hesitant to do so. Their main concerns relate to the lack of a clear regulatory framework and the potential for cryptocurrencies to facilitate financial crime and need to establish meaningful AML/CTF controls. Differences between perceptions and experiences with financial crime and cryptocurrencies underscored the ability of broad assumptions to influence the obstacles FinTechs face.

Methodology

Insights were gathered through a survey and a series of interviews with FFE members. The FFE is made up of compliance officers representing FinTechs operating in the UK. 32

[7] HM Treasury, "Digital currencies: response to the call for information," March 2015.
[8] Mark Carney, "The Future of Money," Speech given to the inaugural Scottish Economics Conference, Edinburgh University, 02 March 2018.

members responded to the survey and an additional 10 interviews were conducted with members. Members include a cryptocurrency exchange, cryptocurrency wallet provider, prepaid card providers, current account providers, foreign exchange services, mobile payments providers, e-wallets, payment processors and peer to peer lenders.

The survey consisted of 13 questions on subjects including:

- opinions on the business potential and challenges related to cryptocurrencies;
- functions related to cryptocurrencies currently offered and being considered;
- experiences with financial crime related to cryptocurrencies;
- regulatory understanding and perception; and
- self-declared cryptocurrency knowledge.

We used follow-up discussions to gather more detail on cryptocurrency engagement, as well as on financial crime typologies seen among members who did engage with cryptocurrencies in some fashion.

There are two limitations to this report worth highlighting. Firstly, the sample size is relatively small and derived from a voluntary membership body of FinTech companies with operations in the UK. Furthermore, all respondents surveyed and interviewed self-assessed their own experiences with cryptocurrencies, meaning there may be some degree of observation bias in the types of financial crime or general challenges related to cryptocurrencies that are reported. To help counter this, we present findings anonymously.

Taking into account these limitations, the findings of this paper nevertheless illustrate how financial crime and compliance individuals in the UK FinTech sector view cryptocurrencies and the challenges FinTechs can face in choosing whether or how to support and interact with them within their business models. This understanding is important not just for other FinTechs and financial service providers, but also for regulators and policymakers whose efforts to promote innovation and mitigate the risks related to cryptocurrencies can be enhanced through better understanding how the broad FinTech sector engages with cryptocurrencies and the concerns they hold.

2. Cryptocurrency Engagement

While FinTechs can interact with cryptocurrencies in a variety of ways, for the purposes of this paper they are best categorised into two main types of engagement: direct and indirect.

- Direct engagement: involves offering products and services such as cryptocurrency wallets or cryptocurrency exchange platforms where the FinTech actually comes into contact with the cryptocurrency.
- Indirect engagement: when a FinTech customer uses the product to purchase cryptocurrencies or deposit profits from the sale of cryptocurrencies. In these business models, FinTechs do not directly touch cryptocurrencies or crypto-assets.

Results from the FFE's survey illustrate that almost half of FFE members have some degree of exposure to cryptocurrencies or cryptocurrency users, whether direct or indirect.

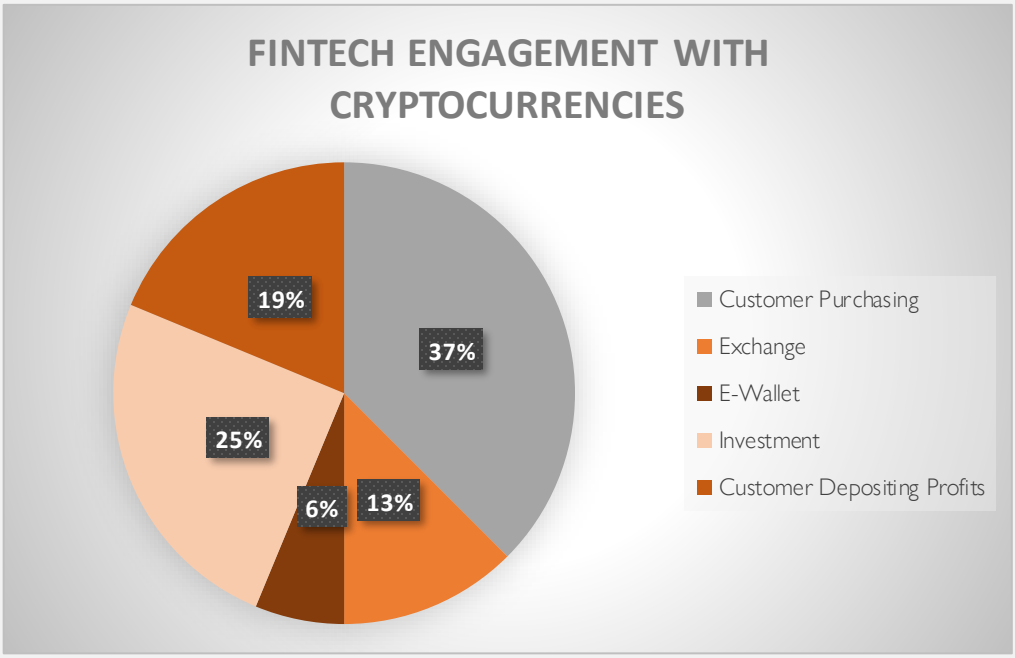


Figure I above provides detail on the different forms of FFE member engagement with cryptocurrencies. Just over half of members who claimed to interact with cryptocurrency were indirectly engaged, through customers using their products to purchase cryptocurrencies or store the profits from sales of cryptocurrencies.

3. Caution Toward Cryptocurrencies

Despite the number of respondents active in the cryptocurrency space, the FFE's overall perspective on the business potential of cryptocurrencies was mixed. Half of those surveyed held a 'neutral' outlook, while 25% held a pessimistic/somewhat pessimistic view.

Nearly one-third of respondents claimed they were considering expanding their business related to cryptocurrencies. Two-thirds of these were already engage in the cryptocurrency space, indicating that direct experience of cryptocurrencies has not deterred further business interest. If anything, interaction with cryptocurrencies has encouraged a more optimistic perspective on the business potential of cryptocurrencies.

Most respondents explained that business development plans related to cryptocurrencies were still in early stages.

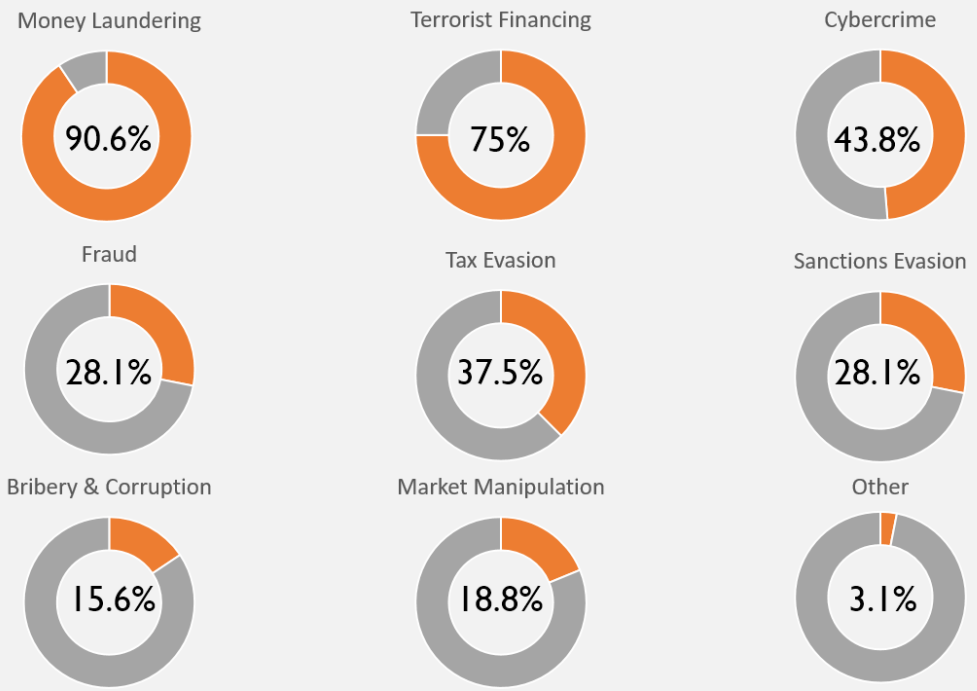
While FFE members are still in the process of formulating their opinions on cryptocurrencies, we identified two major factors behind the cautious perception indicated above: (i) the perceived potential for cryptocurrencies to facilitate financial crime; and (ii) the lack of a robust cryptocurrency regulatory framework.

4. Financial Crime and Cryptocurrencies

85% of survey respondents identified cryptocurrencies' perceived 'potential for facilitating financial crime' as a significant challenge. The majority of FFE members cited money laundering and terrorist financing as the major financial crime risks of cryptocurrencies (Figure II).

Figure II

FinTech-Perceived Financial Crime Risks Related to Cryptocurrencies



Members actively engaging with cryptocurrencies differed significantly in their perceptions of financial crime risks in two areas: terrorist financing and fraud. Those actively engaged in the cryptocurrency space viewed fraud as a significantly greater risk than terrorist financing risk based on the typologies they had identified.

These findings indicate a discrepancy between some of the broader perceptions related to cryptocurrencies and genuine experience of cryptocurrencies and financial crime.

Of the respondents engaging with cryptocurrencies, approximately two-thirds have identified related cases of suspected financial crime. Respondents with more extensive cryptocurrency functions reported experiencing suspected financial crime at rates similar to industry norms within FinTechs and financial institutions more broadly.

FFE members mostly identified financial crime through suspicious customer behaviour or information provided by the customer coming to light during the business relationship. Red flags that alerted members to potential money laundering activity include:

- Suspicions around source of funds. Difficulty confirming source of funds was widely seen as a financial crime risk by FFE members who allowed for cryptocurrency payments. One member reported filing SARs on customers handling cryptocurrencies in response to delayed replies to source of funds checks, triggered when withdrawal limits were hit. In another specific instance, a corporate customer onboarded in order to exchange cryptocurrencies and then attempted to create multiple corporate accounts. The customer displayed evasive behaviour when questioned regarding source of funds and additionally attempted to fund their activity through other businesses under their control.

- Suspicious business activity. One FFE member filed a SAR on the activities of a customer that onboarded for a cryptocurrency service and stated the nature of their business was 'IT consulting,' a type of business not known for high volumes of cash deposits. The company's bank statements showed incoming cash deposits ranging from £2000-£5000 deriving from third parties.

These red flags are similar to those that would cause suspicion in any fiat AML monitoring framework, indicating that solid financial crime risk management frameworks are likely to be effective in the cryptocurrency space.

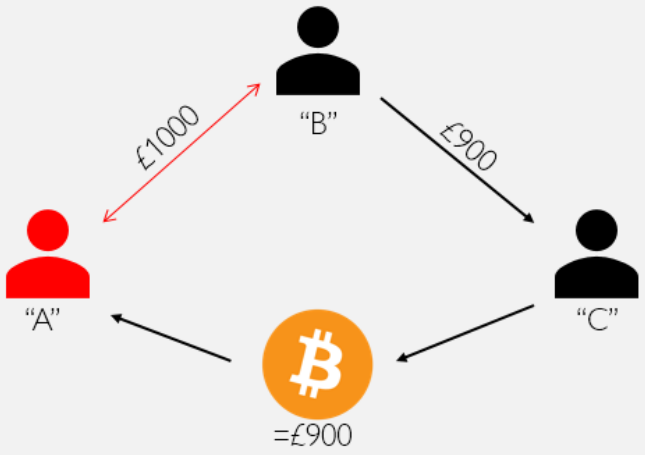
Respondents reported that fraud was a common financial crime related to cryptocurrencies. Two respondents specified that nearly all of the crime typologies they had observed connected to cryptocurrency-linked accounts were fraud-related, which is interesting given the lack of fraud risk highlighted by the respondents. Examples of fraud cases highlighted by respondents include:

- Stolen Card Fraud. One FFE member offering fiat and cryptocurrency linked products stated that fraud occurred far more often in the fiat space. They had seen several cases of stolen card fraud, where profits extracted from the stolen cards were then exchanged for Bitcoin as a way to obscure their origins. However, the compliance officer explained that these fraud instances were easy to track and report.

- Friendly Fraud. One FFE member explained a typical scenario of friendly fraud occurring in the cryptocurrency space. A legitimate cardholder would use their debit or credit card to purchase a cryptocurrency, wait for the cryptocurrency to be transferred to their crypto wallet and would then report their card as stolen. The card issuer would then have to reimburse the cardholder and use the chargeback process to debit funds from the merchant, at a loss to the FinTech.

- Advance Fee Fraud. One FFE member saw fraud cases that affected their customers who sell Bitcoin and accept the profits into their FinTech account (Figure III). One party, 'A,' would arrange the purchase of Bitcoin from the customer ('C'). 'A' would then contact a second party, 'B,' asking them to 'perform a service' by moving funds to a different account and taking a small percentage as payment. 'A' would send the funds (e.g. £1000) to 'B' who would keep a small percentage (e.g. £100) and then transfer the remainder to 'C'. 'C' would in turn release Bitcoin to 'A.' However, 'A' would reverse the payment to 'B,' defrauding them and keeping the Bitcoin purchased by 'B.' The FinTech customer 'C' did not seem aware of the fraud taking place.

Figure III



These fraud typologies identified within the cryptocurrency space mirror those seen by FFE members more generally. Several members referenced common instances of stolen card fraud, particularly for high value goods and cash equivalents, friendly fraud has grown in prominence with the rise of e-commerce and advance fee fraud was identified at the November 2017 FFE meeting as one of the main fraud trends facing the FinTech sector.

It is worthy of note that none of the FinTechs interviewed highlighted any examples of terrorist financing related to cryptocurrencies or cases of sanctions evasion using cryptocurrencies. While FFE members did not perceive or experience sanctions evasion as one of the greatest financial crime risks linked to cryptocurrencies, there are inherent vulnerabilities related to borderless payments that indicate it may warrant greater attention in future research.

No respondents reported seeing cryptocurrency-linked tax evasion, but some acknowledged the difficulty in detecting its occurrence and many respondents engaging with cryptocurrencies provided a warning to customers that explained liability to capital gains tax.

One member reported facing cryptocurrency-related cyberattacks, though they informed us that none of these attacks were successful.

Perceptions of Cryptocurrencies

Respondents highlighted the challenges cryptocurrencies create with banking partners and other stakeholders. One FinTech's compliance team explained, *"we are still trying to think of how we will approach this with our banking partners as well as what [financial crime] controls we will need to establish."*

- One FFE member elaborated, explaining that *"many banking partners will not even be open to trying it"* with cryptocurrencies. The FinTech sector already faces pressure from de-risking policies that treat FinTechs as high risk due to their new business models and at times confusing regulatory status. These problems are amplified in the cryptocurrency space, putting pressure on FinTechs to ensure that any interaction with cryptocurrencies will not affect their relationships with banking partners.
- Another FFE member also noted that, by having a business associated with cryptocurrencies, they struggled with establishing a company bank account or acquiring insurance coverage, even for parts of the company that were not associated with cryptocurrencies.

However, several respondents explained that stakeholders such as banking partners or Payment Service Providers (PSPs) had been supportive of their business plans as long as the stakeholder's rules were followed, and as long as effective controls were in place.

- One respondent highlighted an example of best practice where they spent time with partners, carefully educating them on the details of their business model so that the stakeholders could feel comfortable to support their cryptocurrency-related business developments.
- A respondent offering cryptocurrency-related products explained that the negative opinions and risk aversion toward cryptocurrencies were greater challenges than any actual material obstacles. The compliance officer added, *"It's just the perceived negativity toward cryptocurrencies as a whole."*
- Another FFE member offered a similar take on broader cryptocurrency-related challenges, saying they *"come down to a misunderstanding rather than anything material"*' That is, the reputation of cryptocurrencies as being unregulated, volatile and linked to criminal activity caused greater challenges than the actual practice of dealing

in or supporting cryptocurrencies on a FinTech platform, provided, of course, a sound business model.

Of the ten interviews conducted, all but one member stated that their decisions around whether to engage cryptocurrencies further were not significantly influenced by stakeholders. Instead, decisions tended to be made internally and centred upon a) the commercial opportunities related to cryptocurrencies, b) the capacity or lack thereof for effective AML/CTF controls and c) reputational risks from engaging in the cryptocurrency space.

The general assumption of FinTechs has been that banking partners and other external stakeholders may limit their ability to experiment with cryptocurrencies, given the lack of meaningful cryptocurrency engagement from the financial sector to this point. However, in practice, respondents engaging in the cryptocurrency space tended to report that, through information sharing and adhering to established controls guidance, they were able to better manage their relationships.

It is evident that a number of the difficulties expressed in navigating cryptocurrency opportunities have been driven by issues of public/industry perception more so than issues of practice.

Those interviewed held mixed opinions on the appetite and perspectives of customers. Some respondents explained that there hadn't been as much customer pressure for greater cryptocurrency functionality as may be expected. One FinTech challenger bank, however, explained that cryptocurrency-purchasing customers complained about being unable to trade on the FinTech platform and how it went against their tech-focused nature. *"People forget about regulation and compliance and don't appreciate the risks involved"*.

Reducing Cryptocurrency-Related Financial Crime

While perceptions of financial crime linked to cryptocurrencies may provide more unique challenges for FinTechs, many FFE members still expressed mild to moderate concern over continuing to develop best practice in cryptocurrency financial crime risk management.

Some FFE members reduced exposure to cryptocurrency-related financial crime risks through a narrow product offering. For instance, one member explained that reducing cryptocurrency-related fraud by only accepting bank transfers for cryptocurrency-related payments, as compared to card payments was a viable mitigation. A different member reduced their exposure to fraud by refusing to allow the deposit of profits made from ICOs.

Respondents indirectly engaged with cryptocurrencies raised questions about effective controls to reduce cryptocurrency-related financial crime. One of the greatest challenges identified was the operational difficulty of confirming the source of funds for inbound payments derived from cryptocurrency-related activity. Respondents did not appear

confident in what tools would be necessary, and ultimately effective, for monitoring customer behaviour, instead opting to limit the range of permissible cryptocurrency-linked transactions.

The FFE members with more direct engagement with cryptocurrencies used third party software for their cryptocurrency-related AML/CTF controls. Third party software was used for transaction monitoring, risk scoring and customer due diligence. Despite this, the majority of those interviewed voiced some concern related to their ability to complete assurance on their existing controls' effectiveness due to the technical nature of the solutions.

5. Attitudes Toward Cryptocurrency Regulation

In response to the sudden expansion of cryptocurrencies, international regulators have been working to keep pace, trying to impose order and stability on an ever-changing technological innovation. At the March '18 G20 meeting, a firm deadline of July 2018 was set for establishing concrete recommendations on regulating cryptocurrencies globally, and attendees agreed that standards would be pulled from the Financial Action Task Force (FATF)'s standards on anti-money laundering and counter-terrorist financing[9].

At the end of 2017, the European Union agreed on the revisions to the 4th Money Laundering Directive (5MLD) which bring virtual currency exchanges and custodial wallet providers into scope as obliged entities and require them to maintain effective Know-Your-Customer (KYC) AML policies, monitoring and suspicious reporting standards akin to those held by financial institutions[10]. However, the 5MLD is not due to come into effect until mid-2019, leaving something of a gap in UK and EU cryptocurrency regulation.

When asked to select the greatest risks associated with cryptocurrency engagement, respondents most often identified '*the current lack of a regulatory framework*' - 87.5% of all of those surveyed identified the lack of regulation as one of the 'biggest risks.'

- One compliance officer emphasized their company's risk averse profile and noted that the risks of an unregulated form of currency were *"simply not worth"* any potential business return. This suggests that greater regulatory clarity could bring about further understanding into the AML risks linked to cryptocurrencies and more innovative developments in the cryptocurrency space.

The recent passage of the 5MLD does not appear to have assuaged concerns in the FFE, with 63% of respondents being neither pessimistic nor optimistic about the impact of the 5MLD on cryptocurrency regulations. While FFE members were aware of the 5MLD and its implications, they still showed apprehension toward the impact that the 5MLD would have in practice. For FFE members as a whole, as well as for those participating or considering participating in the cryptocurrency space, the lack of a clear regulatory framework remains a major challenge.

[9] Darryn Pollock, "G20 and Cryptocurrencies: Baby Steps Towards Regulatory Recommendations," Cointelegraph, 21 March 2018.
[10] Francesco Guarascio, "EU agrees clampdown on bitcoin platforms to tackle money laundering," Reuters, 15 December 2017.

6. Takeaways and Final Recommendations

Cryptocurrencies are inextricably linked to complexity, confusion and instability, or at least, they are construed to be. These associations, in addition to the lack of clear regulation and the potential of cryptocurrencies to facilitate financial crime, challenged most of those surveyed in this report. The main findings of this report include:

- Growing engagement with cryptocurrencies. Of those surveyed, nearly half actively engaged with cryptocurrencies or cryptocurrency users, the majority of which are indirectly engaged. As a sector this exposure is not unexpected given the technology focus of most FinTech products and the close relationship with the crypto-development community. One-third of FFE members want to engage more with cryptocurrencies.

- A cautious outlook. FFE members as a whole demonstrated caution regarding the business potential of cryptocurrencies driven by perceived financial crime risks and a lack of regulatory clarity.

- Perceptions of financial crime risks. FFE members highlighted the potential for cryptocurrencies to facilitate financial crime as one of their greatest challenges. However, the perception of risks by the broader FFE was quite different to the realities of actual financial crime typologies identified by members engaged with cryptocurrencies.

- Perceptions are having a negative impact. More generally, many of the challenges FFE members face with expansion or inclusion of cryptocurrency-related products have centred more on perceptions and assumptions of cryptocurrency risks rather than practical cryptocurrency experience or risk exposure. These perceptions can influence stakeholder relations and the ability to obtain banking services, which can stymy innovation or push those engaging with cryptocurrencies into higher risk jurisdictions.

- Similarities in financial crime between fiat space and cryptocurrency space. Effective red flags used to identify suspicious money laundering or fraud typologies in the cryptocurrency space are broadly similar to those used more widely in AML/CTF.

- Concerns over effective controls. Effectively reducing exposure to cryptocurrency-linked financial crime was understandably a concern. Some FFE members achieve this by limiting their overall cryptocurrency exposure, though a robust risk-based anti-financial crime framework can help facilitate responsible engagement.

- A lack of clarity on cryptocurrency regulation. The vast majority of FFE members do not find existing cryptocurrency regulation to be clear and see it as one of the biggest

challenges associated with supporting cryptocurrencies. This is consistent with views expressed anecdotally by other more traditional financial institutions and in the media.

Based on these findings, the following recommendations are given:

- FinTechs. The findings of this paper should not deter FinTechs from exploring opportunities in the cryptocurrency space. If anything, these findings are encouraging and show a more manageable-than-expected experience in dealing with cryptocurrencies. However, it is important, especially from a financial crime perspective, to have in-place risk-based anti-financial crime controls that are tuned to the unique challenges presented by cryptocurrencies.

- FIUs and Law Enforcement. FIUs and law enforcement should be concerned by the discrepancies witnessed between perceived financial crime risks and actual financial crime exposure in the FinTech community. This discrepancy is driving a lack of clarity across the whole financial services sector and has potential to impede the development of innovative crypto-based solutions. FIUs and law enforcement would benefit from engaging in public-private collaboration efforts to improve the wider understanding of cryptocurrency related financial crime within the financial services sector.

- Regulators and Policymakers. Guidance on implementing cryptocurrency regulation like the 5MLD and its implications should be clearly communicated. This is especially important given the desire to improve innovation related to cryptocurrencies. It is also important to ensure that the impact of those regulations is assessed against the full-scope of obliged entities, including FinTech involved in the cryptocurrency space, and not just banks.

Given the scope of this paper, there are several additional avenues of research that should be explored. In particular, there remains some lack of public knowledge on the inherent cryptocurrency risks related to sanctions and tax evasion.

Cryptocurrencies continue to evolve on a daily basis, and perspectives and experiences with them are bound to continue changing as well. And yet, by understanding the avenues of concern held by the FinTech sector, and how this tech-driven sector has adjusted to the growth in cryptocurrencies, we can all gain a more nuanced and insightful understanding to how to best navigate and govern this space.