Royal United Services Institute
for Defence and Security Studies

Occasional Paper

From Intention to Action

Next Steps in Preventing Criminal Abuse of Cryptocurrency

Anton Moiseienko and Kayla Izenman

From Intention to Action

Next Steps in Preventing Criminal Abuse of Cryptocurrency

Anton Moiseienko and Kayla Izenman

RUSI Occasional Paper, September 2019

Royal United Services Institute
for Defence and Security Studies

188 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, September 2019. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

This paper forms part of the Financial Crime 2.0 research programme funded by EY and Refinitiv. The authors wish to thank David Carlisle, Malcolm Chalmers, Yaya Fanusie and Peter Van Valkenburgh for their helpful comments on an earlier version of this paper. Thanks are also due to all those who have generously offered their time to be interviewed for this research, as well as the RUSI Publications team for their work on editing the paper.

Executive Summary

CRYPTOCURRENCIES POSE CHALLENGES for the anti-money-laundering and counterterrorist financing (AML/CTF) regime. In principle, they can lessen reliance on financial intermediaries, such as banks, and enable users to transact pseudonymously or anonymously.

An estimated 99% of cryptocurrency transactions take place through centralised exchanges,[1] which can be subjected to AML/CTF regulation in a manner similar to traditional banks. Capitalising on this opportunity, the Financial Action Task Force (FATF) has mandated that virtual asset service providers (VASPs) should comply with a panoply of financial crime rules reminiscent of those that apply to traditional financial institutions.

As states work on implementing the updated FATF Recommendations, it is not enough to diligently copy the FATF's new requirements in domestic regulations. While the FATF Recommendations provide a framework for addressing cryptocurrency-related financial crime risks, domestic regulators need to make several key choices about the scope of AML/CTF regulation as applied to cryptocurrency businesses; support VASPs' compliance efforts; and provide a credible deterrent for those VASPs that choose to abdicate their AML/CTF responsibilities.

The appetite for engagement on these issues is demonstrated by several consultations launched by national governments over spring and summer 2019, such as those in the UK and Singapore. In the US, the Financial Crime Enforcement Network, the country's regulator and financial intelligence unit, published a detailed guidance on 'certain business models involving convertible virtual currencies' in 2019. It stands out as a helpful example for other countries, but not necessarily the model to follow in all respects.

This paper aims to support domestic authorities that will regulate VASPs and supervise their compliance with AML/CTF regulations in identifying the next steps they should take to effectively prevent criminal abuse of cryptocurrency. This includes action in the following areas:

- **Policing the regulatory perimeter**. Whether a state wishes to regulate VASPs based overseas and, if so, what nexus is required between the VASP and the state in question, is a context-specific decision that should be taken based on:
    - The state's interest in preventing its residents from accessing unregulated VASPs.
    - Its practical ability to enforce AML/CTF regulation against overseas VASPs.
    - Potential regulatory burdens on VASPs required to be registered in multiple jurisdictions.

1. Nathan Sexer, 'State of Decentralized Exchanges, 2018', *Medium,* 31 January 2018.

Once the decision is taken, regulators should use a wide range of intelligence to identify VASPs subject to their regulation, including through liaising with law enforcement agencies and encouraging registered VASPs to report, in confidence, potentially non-compliant peers.

- **Clarifying the definition of VASPs**. While some businesses clearly fall within the five categories of VASP activities listed by the FATF, other business models can present regulators with some uncertainty. This is particularly so in the case of peer-to-peer (P2P) exchanges, which have the potential to weaken the role of centralised VASPs and so blunt the effect of governmental regulation. Although the predominance of centralised VASPs mitigates these concerns for now, drawing a justified line between regulated and unregulated activities is essential both as a matter of principle (to ensure that like activities are treated alike) and to anticipate possible displacement of illicit activity towards unregulated businesses. This paper argues that:
    - Whether a given business holds customers' funds in custody should not be the determinative criterion for deciding whether it is subject to AML/CTF regulation as a VASP. Persons with meaningful control over P2P exchanges should bear AML/CTF obligations even if they do not hold funds in custody. This includes, for instance, persons who can unilaterally restrict access to the exchange or discontinue its operation.
    - Mixers should be subject to AML/CTF obligations and face regulatory or law enforcement action in cases of non-compliance, although such obligations should not extend to persons who merely develop mixing software protocols.
    - Regulators should keep their approach to AML/CTF regulation of cloud-mining companies under review.
- **Supporting compliance efforts**. To facilitate VASPs' AML/CTF efforts, regulators should:
    - Engage with VASPs to devise appropriate arrangements for complying with the 'wire transfer' requirement.
    - With support from law enforcement, consider arrangements for sharing the indicators of suspicion with VASPs to mitigate the inefficiencies of VASPs relying solely on their in-house experience, which inevitably varies across VASPs.
- **Creating a credible deterrent**. To create a credible deterrent from non-compliance, states should take law enforcement and regulatory action against non-compliant VASPs or, when such action is not feasible, consider arrangements for sharing information about non-compliant VASPs with other regulated businesses to protect them from financial crime risks.
- **Addressing developments in anonymity**. In the longer term, states need to consider technological advances that can render cryptocurrency transactions untraceable on a public blockchain, including the potential uptake of privacy coins or mixing protocols. To mitigate their risks, it is important that VASPs collect and analyse sufficient information about their customers' activity, and the type of coin used may indicate the need for higher customer due diligence. Going forward, monitoring of the scale of criminal misuse of privacy coins and mixed transactions would help ensure that VASPs can make informed decisions as to the risks involved and their responses.

Introduction

CRYPTOCURRENCIES CAN POSE challenges for the anti-money-laundering and counterterrorist financing (AML/CTF) regime in two main ways:

- They potentially lessen the reliance on financial intermediaries, such as banks, whom governments require and rely on to detect and report suspicious activity by their customers.
- Some cryptocurrencies, known as 'privacy coins', are designed to enable transactions that, unlike those in Bitcoin, are not recorded on a transparency blockchain. While replicating the anonymity of cash, they can facilitate near-instantaneous transfers, including cross-border transfers, in a manner unparalleled in the offline world.

For now, however, the impact of these potential features of cryptocurrency has been limited:

- Most users purchase cryptocurrency from cryptocurrency exchanges, which have become centralised intermediaries akin to banks.[1]
- Transactions that take place on a transparent blockchain, such as that of Bitcoin, can be traced not only by law enforcement, but also by anyone with access to blockchain tracing capabilities and a dose of curiosity.[2]

In a bid to prevent cryptocurrency from becoming a 'wild west' free from AML/CTF regulation, the global standard-setter in this area, the Financial Action Task Force (FATF), has extended AML/CTF rules to cryptocurrency businesses, which come within the definition of virtual asset service providers (VASPs).[3]

While this is a regulatory milestone, it is not enough for domestic regulators to diligently copy the FATF's new requirements. Within the FATF framework, they need to make several key choices about the scope of AML/CTF regulation as applied to cryptocurrency businesses; support VASPs'

1. Nathan Sexer, 'State of Decentralized Exchanges, 2018', *Medium,* 31 January 2018; TokenInsight, '2019 Q1 Cryptocurrency Exchange Industry Research Report', April 2019, p. 18, <https://tokenin.cn/api/upload/dashboardPdf/TI-Cryptocurrency%20Exchange%202019Q1-Final.pdf>, accessed 9 August 2019.
2. For example, see Blockchain Explorer, <https://www.blockchain.com/explorer>, accessed 23 July 2019; Brenna Smith, 'Tracking Illicit Transactions With Blockchain: A Guide, Featuring Mueller', *Bellingcat*, 1 February 2019.
3. The Financial Action Task Force (FATF) refers to 'virtual asset', defined as 'a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes', which includes cryptocurrency (a type of virtual assets based on cryptography). See FATF Glossary, <https://www.fatf-gafi.org/glossary/u-z/>, accessed 24 July 2019.

compliance efforts; and provide credible deterrent for those VASPs that choose to abdicate their AML/CTF responsibilities.

The appetite for engagement on these issues is demonstrated by several consultations launched by national governments over spring and summer 2019, such as those in the UK and Singapore.[4] In the US, the Financial Crime Enforcement Network (FinCEN), the country's regulator and financial intelligence unit (FIU), published a detailed guidance on 'certain business models involving convertible virtual currencies' in 2019.[5] It stands out as a helpful example for other countries, but not necessarily the model to follow in all respects.

This paper aims to support domestic authorities that will regulate VASPs and supervise their compliance with AML/CTF regulations in identifying next steps they should take to effectively prevent criminal abuse of cryptocurrency. It is based on a workshop convened in London by RUSI on 10 May 2019 with participation from banks, cryptocurrency exchanges, blockchain tracing companies and academia, as well as a further eight semi-structured interviews with subject-matter experts.

4. The Financial Conduct Authority (FCA) consulted on 'cryptoassets' and anti-money laundering/counterterrorist financing (AML/CTF) in 'Transposition of the Fifth Money Laundering Directive: Consultation', April 2019, pp. 14–18, while the Monetary Authority of Singapore consulted on 'digital payment tokens' and AML/CTF in 'Consultation Paper P010 – 2019: Proposed Payment Services Notices on Prevention of Money Laundering and Countering the Financing of Terrorism', June 2019.
5. US Treasury Financial Crime Enforcement Network (FinCEN), 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies', 9 May 2019.

I. AML/CTF Regulation of VASPs

IN OCTOBER 2018, the FATF mandated that states should identify and regulate VASPs that are engaged, as a business, in one or more of the following activities:[6]

- Crypto-to-fiat exchange services.
- Crypto-to-crypto exchange services.
- Transfer of cryptocurrency.
- Safekeeping and/or administration of cryptocurrency.
- Facilitating the issuance of cryptocurrency.

The FATF clarified its expectations in the Interpretive Note to Recommendation 15 and an updated guidance on a risk-based approach, which were published in June 2019.[7] Under the incoming Chinese presidency, the FATF is expected to 'develop the methodology for countries to be assessed against the standard for virtual assets, and … start assessing FATF members for effective compliance with it'.[8] Before considering how domestic regulators should approach implementing the FATF Recommendations, it is helpful to begin by discussing the utility of subjecting VASPs to AML/CTF regulation.

Rationale for Regulation

VASPs' compliance with AML/CTF obligations is indispensable because of the insight they have into the cryptocurrency-related activities of their customers. For instance, in the case of a crypto-to-fiat exchange, a traditional bank will see payments that its customer makes to or receives from such an exchange. But unless the bank invests effort into identifying that customer's cryptocurrency address (with no guarantee of success) and further blockchain tracing, the bank will know little of the customer's cryptocurrency activity.[9] Moreover, transactions between users of the same exchange are likely to take place off-chain. That is to say, the exchange simply reduces the payer's account balance and increases the recipient's balance in its internal records,

6. FATF, 'Regulation of Virtual Assets', 19 October 2018, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html>, accessed 26 June 2019; FATF Glossary, <https://www.fatf-gafi.org/glossary/u-z/>, accessed 16 June 2019.
7. FATF, 'Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers', June 2019. The Interpretive Note to Recommendation 15 is on pp. 55–56.
8. FATF, 'Paper by the Incoming President: Chinese Presidency Priorities for the Financial Action Task Force (FATF)', 2019, <http://www.fatf-gafi.org/media/fatf/content/images/Objectives-FATF-XXXI(2019-2020).pdf>, accessed 28 July 2019.
9. Interventions from a blockchain analysis company representative and a bank financial crime expert, RUSI workshop on money laundering via online businesses, London, 10 May 2019.

without any record of the transaction left on the blockchain.[10] Unlike other regulated businesses, VASPs are therefore uniquely placed to identify illicit financial flows in cryptocurrency, and they are able to glean a substantial amount of information about their customers that can inform suspicious activity report (SAR) filing, for instance by monitoring their customers' deposits and withdrawals and applying blockchain tracing.

Current Compliance Landscape

The AML/CTF landscape among VASPs is varied, partly because many states do not yet regulate them. Research by Coinfirm suggests that as of March 2019, only 58% of 216 exchanges surveyed had AML policies in place, and 69% did not have 'complete and transparent [customer due diligence/know your customer] procedures'.[11] In an experiment published in 2018, researchers were able to use two exchanges to cash out mixed bitcoins into fiat currency without disclosing their identity.[12] Another research paper published in the same year drew a connection between the fact that the EU did not regulate cryptocurrency businesses and the finding that European exchanges 'hosted a disproportionate amount of illicit activity'.[13]

In some jurisdictions where VASPs are regulated, rates of reporting from them are increasing. For instance, the US receives approximately 1,500 cryptocurrency-related SARs per month as of June 2019.[14] In Luxembourg, the number of reports received from VASPs increased from 93 in 2016 to 263 in 2017.[15] Although the public has no way of knowing the quality of SAR reporting emanating from VASPs, on the face of it these statistics suggest that the VASPs' intelligence potential is not negligible.

10. Ross Clayton et al., 'Bitcoin Redux', Cambridge University Computer Laboratory, 28 May 2018, <https://www.cl.cam.ac.uk/~rja14/Papers/bitcoin-redux.pdf>, accessed 9 August 2019.
11. Coinfirm, 'Know Your Exchange Cryptocurrency Exchange Risk Report', March 2019, p. 19.
12. Rolf van Wegberg, Jan-Jaap Oerlemans and Oskar van Deventer, 'Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin', *Journal of Financial Crime* (Vol. 25, No. 2, 2018), pp. 419–35.
13. Yaya J Fanusie and Tom Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services', Foundation for Defense of Democracies Center on Sanctions and Illicit Finance and Elliptic, 12 January 2018, pp. 9, 11.
14. Kenneth A Blanco, 'Prepared Remarks of FinCEN Director Blanco at the NYU Law Program on Corporate Compliance and Enforcement', New York, 12 June 2019, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-blanco-nyu-law-program-corporate-compliance-and>, accessed 16 June 2019.
15. Cellule de renseignement financier, 'Rapport annuel 2017', février 2019, pp. 58–59, <https://justice.public.lu/dam-assets/fr/publications/rapport-activites-crf/rapport-crf-2017.pdf>, accessed 9 August 2019.

II. Policing the Regulatory Perimeter

TO HARNESS THE intelligence potential of VASPs and prevent their criminal abuse, domestic regulators have to first decide who they are aiming to regulate and ensure they identify regulated businesses – in short, they need to 'police the perimeter'.

Requisite Nexus

FATF Recommendation 15 requires that VASPs be 'licensed or registered and subject to effective systems for monitoring and ensuring compliance'. At a minimum, they must be registered in a country of their incorporation (for legal entities) or place of business (for natural persons).[16] Beyond that, states will have to weigh several factors to decide how strong a foreign VASP's presence should be for it to become subject to AML/CTF regulation, including:

- The state's interest in preventing its residents from accessing unregulated VASPs.
- The state's practical ability to enforce its AML/CTF regulation against VASPs located outside its territory.
- The potential regulatory burden on VASPs required to be registered in multiple jurisdictions with which they only have little connection.

For example, in the US, which has been quicker than many other states to regulate VASPs, VASPs are obliged to register and comply with AML/CTF regulations if they carry out activity 'wholly or in substantial part' within the US.[17]

In the UK, it remains to be seen what nexus will be required. By way of comparison, online gambling operators are subject to registration and regulation in Great Britain,[18] if their 'facilities are or will be capable of being used there'.[19]

Neither the US approach nor the current UK one (in relation to online gambling operators) is particularly prescriptive and would require VASPs and regulators to assess, relying largely on common sense and prior enforcement history, whether the threshold is met in any given case.

16. FATF, 'Guidance for a Risk-Based Approach', June 2019, p. 55.
17. Legal Information Institute, '31 CFR § 1010.100 – General Definitions', <https://www.law.cornell.edu/cfr/text/31/1010.100>, accessed 9 August 2019.
18. Northern Ireland has a separate gambling regime.
19. 'Money Laundering Regulations (2017)', Regulation 9(4)(b).

Identification of VASPs

Various approaches can be taken by AML/CTF supervisors[20] to identify VASPs subject to their supervision. For instance, one state's FIU, which also has supervisory functions, relies on a broad range of material, including its own intelligence function, referrals from law enforcement agencies and reports by registered VASPs, who help identify non-registered competitors.[21] Intelligence on non-registered VASPs can also come to FIUs from financial institutions: for instance, a payment-processing company reported identifying a cryptocurrency trader who was holding out to be engaged in a different, non-cryptocurrency-related business.[22]

Recommendation 1: Supervisors should use a wide range of intelligence to identify VASPs subject to their AML/CTF supervision, including through liaising with law enforcement agencies and encouraging registered VASPs to report, in confidence, potentially non-compliant peers.

20. Expected to be the FCA in the UK.
21. Authors' telephone interview with the financial intelligence unit (FIU) of an EU member state, 31 May 2019.
22. Authors' interview with a payment-processing company, 2 July 2019.

III. Clarifying the Definition of VASPs

SOME CRYPTOCURRENCY BUSINESSES clearly fall within the FATF's definition of VASPs, including crypto-to-fiat exchanges and crypto-to-crypto exchanges. Beyond cryptocurrency exchanges, however, there are several business models that pose potential regulatory uncertainty.

Peer-to-Peer Exchanges

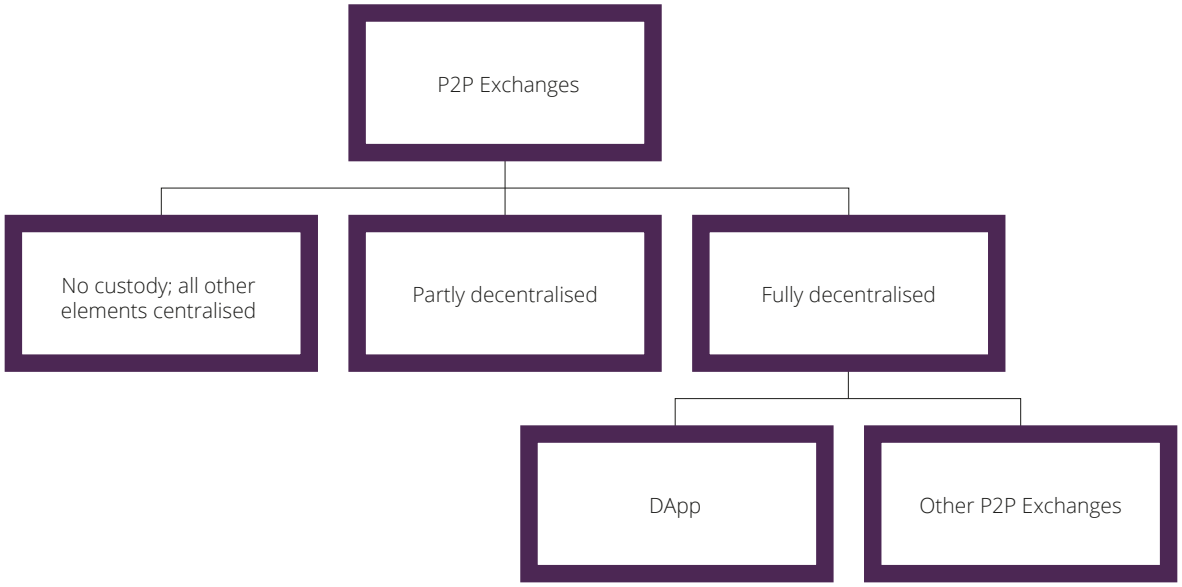
Definition

In the narrowest sense of the term, a peer-to-peer (P2P) exchange does not assume control (custody) over its users' cryptocurrency. Such an exchange may, however, rely on a single administrator for a range of tasks, such as maintaining the platform or matching users' orders.

Some P2P exchanges are akin to a forum where buyers and sellers come together, with the added benefit of an escrow facility to prevent scams.[23] Other exchanges operate on the basis of (self-executable) smart contracts[24] and are often known as decentralised exchanges.[25] In its most ambitious manifestation, a P2P exchange can be maintained by a dispersed community of users and therefore be highly resistant to attempts at regulating or closing it down. This can be potentially achieved through the use of a decentralised application (DApp), a software programme based on smart contracts.[26]

23. For instance, this is how LocalBitcoins works. See Steve Stecklow, 'Making a Fortune from Arranging Private Bitcoin Transactions', *Reuters*, 29 September 2017.
24. A smart contract can be understood as 'computer code that executes on the satisfaction of certain conditions' and, in this context, runs on the nodes of the relevant distributed ledger network (typically Ethereum). See LawTech Delivery Panel, UK Jurisdiction Taskforce, 'Public Consultation: The Status of Cryptoassets, Distributed Ledger Technology and Smart Contracts Under English Private Law', May 2019, p. 30, <https://www.lawsociety.org.uk/news/documents/ukjt-consultation-cryptoassets-smart-contracts-may-2019/>, accessed 9 August 2019.
25. Bennett Garner, 'What is a DEX? Decentralized Exchanges, Explained', *CoinCentral*, 28 August 2018.
26. See the description of decentralised applications in FinCEN, 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies', p. 18.

Figure 1: Taxonomy of P2P Exchanges



Source: Authors' research.

Impact

At present, transaction volumes going through P2P exchanges are minor compared to those processed by centralised exchanges.[27] The same seems to be true for criminal proceeds. According to Chainalysis, a blockchain tracing company, illicit proceeds in cryptocurrency 'flow through either exchanges (65%) or peer-to-peer exchanges (12%), with the rest flowing through other conversion services such as mixing services, bitcoin ATM's [sic] and gambling sites'.[28] The Chainalysis report does not expressly state what kind of P2P exchange it has in mind and whether it covers, for instance, the use of bulletin boards to arrange P2P transactions.[29] At any rate, however, if the use of P2P exchanges increases in the future, their effective regulation will become progressively important.

27. For instance, one source cites 1% even though it defines peer-to-peer exchanges in the broad sense, namely, any non-custodial exchange. See Sexer, 'State of Decentralized Exchanges, 2018'.
28. Chainalysis, 'Crypto Crime Report: Decoding Hacks, Darknet Markets, and Scams', January 2019, p. 24.
29. The authors are grateful to a peer reviewer for pointing this out.

Regulatory Approaches

There are two main related challenges in regulating P2P exchanges:

- The operators of a P2P exchange may have limited insight into the activities of its users, especially if users continue transacting through other communication means.[30]
- A P2P exchange may function in such a way that no single operator would control its activities. For instance, the only way to impact its operation may be to alter its software, which can be maintained by a geographically dispersed group of volunteers.[31]

The FATF is non-committal on whether its rules must apply to P2P exchanges, with the FATF guidance stating:

- *In relation to P2P exchanges*, '[d]epending on a jurisdiction's national legal framework, if a VA [virtual assets] trading platform only provides a forum where buyers and sellers of VAs can post their bids and offers (with or without automatic interaction of orders), and the parties themselves trade at an outside venue …, then the platform may not constitute a VASP'.[32]
- *In relation to DApps*, '[w]hen DApps facilitate or conduct the exchange or transfer of value (whether in VA or traditional fiat currency), the DApp, its owner/operator(s), or both may fall under the definition of a VASP'.[33]

In the US, FinCEN excludes P2P exchanges from AML/CTF requirements if such an exchange 'only provides a forum where buyers and sellers of [convertible virtual currency] post their bids and offers (with or without automatic matching of counterparties), and the parties themselves settle any matched transactions through an outside venue (either through individual wallets or other wallets not hosted by the trading platform)'.[34] This statement seems to imply that, in FinCEN's view, a P2P exchange is only covered by the US AML/CTF rules if it holds a customer's funds in custody. This interpretation is supported by the fact that, unless it also carries out other regulated activities, a cryptocurrency business has to fall within the definition of a 'money transmitter' to bear AML/CTF obligations in the US. A money transmitter 'accepts' and 'transmits' currency, funds or other value, which implies that it has to have funds in its custody.[35]

30. Authors' interview with an investigator in a virtual currency exchange, London, 17 June 2019.
31. Authors' interview with a decentralised exchange (DEX) developer, Signal app, 10 June 2019.
32. FATF, 'Guidance for a Risk-Based Approach', p. 15.
33. *Ibid*.
34. FinCEN, 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies', p. 24.
35. See Peter Van Valkenburgh, 'What Can the EtherDelta Settlement Tell Us About How Decentralized Exchanges are Regulated?', Coin Center, 8 November 2018, <https://coincenter.org/entry/what-can-the-etherdelta-settlement-tell-us-about-how-decentralized-exchanges-are-regulated>, accessed 25 July 2019.

In relation to DApps, on the other hand, FinCEN merely states that 'when DApps perform money transmission, the definition of money transmitter will apply to the DApp, the owners/operators of the DApp, or both'.[36] Despite this being unhelpfully circular, the definition of a 'money transmitter' similarly points to the need for the DApp or its owners/operators to hold users' funds in custody for them to come within the scope of US AML/CTF regulations.

With custody over cryptocurrency being the determinative factor for FinCEN, an exchange that is otherwise fully centralised and has insight into its users' activity would fall outside the regulatory perimeter. Other countries, which are not constrained by the US definition of a 'money transmitter' and may wish to use the intelligence value of P2P exchanges, could take an alternative approach. It could involve extending AML/CTF regulation to those persons, if any, who have meaningful control over a P2P exchange, for instance if they can unilaterally restrict access to the exchange or discontinue its operation.

For example, in the US Securities and Exchange Commission's enforcement action against the founder of a P2P exchange where security coins were traded, that person 'wrote and deployed the EtherDelta smart contract to the Ethereum Blockchain, and exercised complete and sole control over EtherDelta's operations'.[37] While this action did not involve any AML/CTF failings, it dispels the notion that P2P exchanges are necessarily so decentralised that no one can be held responsible for their activity. In instances such as this, the target of regulation is not mere development of software (whose regulation could raise civil liberties concerns and would at any rate be difficult to enforce),[38] but rather its deployment.

Aside from possible regulation, persons controlling P2P exchanges may have reputational incentives to address AML/CTF concerns. Thus, a P2P exchange developer interviewed for this research intimated that their exchange was considering limited customer verification measures to tackle possible criminal misuse.[39]

Recommendation 2: While persons should not be subject to AML/CTF regulation solely on account of developing software used for P2P exchange of cryptocurrency, persons with meaningful control over a P2P exchange platform should be subject to AML/CTF regulation. A person has meaningful control over a P2P exchange if they can, for instance, unilaterally restrict access to the exchange or discontinue its operation.

---

36. FinCEN, 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies', p. 18.
37. United States of America Before the Securities and Exchange Commission, 'Order in the Matter of Zachary Coburn', 8 November 2018, para. 28, p. 9, <https://www.sec.gov/litigation/admin/2018/34-84553.pdf>, accessed 16 June 2019.
38. Authors' interview with a DEX developer, Signal app, 10 June 2019; authors' interview with an investigator in a virtual currency exchange, London, 17 June 2019.
39. Authors' interview with a DEX developer, Signal app, 10 June 2019.

Mixers

Definition

Mixers obfuscate transactions on a transparent blockchain by combining inputs from many users and distributing them among recipients, making blockchain tracing difficult.[40] In addition to custodial mixers that receive and transfer users' cryptocurrency, mixing software has been developed, as discussed in the last part of this paper, but with limited impact to date.

Impact

As per Chainalysis research cited above, mixers appear to be a noticeable but not widespread feature of money laundering in cryptocurrency. This may reflect the fact that in 2017, the two then-biggest mixers – BitMixer and Grams Helix – had gone out of business.[41] As BitMixer's closure was announced, its representative implicitly admitted money-laundering risks of mixers by stating that 'Bitcoin will have a great future without dark market transactions' while mixing 'will be considered as illegal in most of countries [sic]'.[42]

Regulatory Approaches

Views on the legitimacy of mixers differ, with some seeing them as quasi-criminal services and others believing that they safeguard individual privacy.[43] Since they engage in 'transfer of virtual assets' and pose money-laundering risks (as shown, for instance, by the Dutch law enforcement action against Bestmixer.IO, referenced below in Chapter IV 'Creating a Credible Deterrent'), there is force in FinCEN's view that mixers should be subject to AML/CTF obligations.[44]

Recommendation 3: Mixers should be subject to AML/CTF obligations and face regulatory or law enforcement action in case of non-compliance, although such obligations should not extend to persons who merely develop mixing software protocols.

40. Anton Moiseienko and Olivier Kraft, 'From Money Mules to Chain-Hopping: Targeting the Proceeds of Cybercrime', *RUSI Occasional Papers* (November 2018), p. 42.
41. Europol, *Internet Organised Crime Threat Assessment 2018* (The Hague: European Union Agency for Law Enforcement Cooperation, 2018), p. 63.
42. Bitcoin Forum, 'The Lagest Bitcoin Mixer is About to Stop Working', post by Bitmixer.IO's, 23 July 2017, 07:09:15 PM, <https://bitcointalk.org/index.php?topic=2042470.msg20331854#msg20331854>, accessed 28 July 2019.
43. Osato Avan-Nomayo, 'Cryptocurrency Mixers and Why Governments May Want to Shut Them Down', *CoinTelegraph*, 28 May 2019.
44. FinCEN, 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies', p. 19.

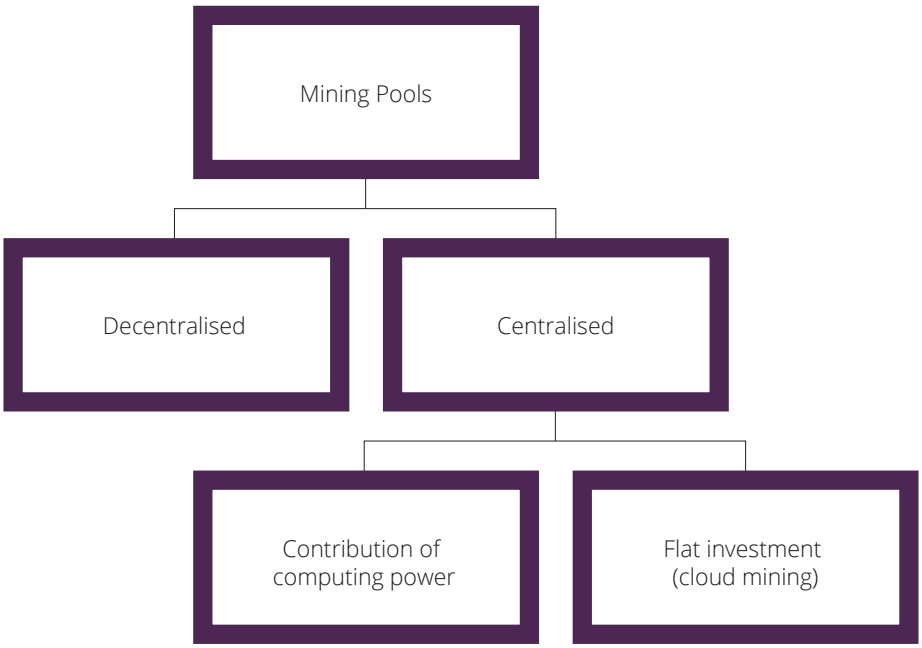
Mining Pools and Cloud-Mining Companies

Definition

To obtain cryptocurrency, users can mine new coins by solving cryptographic puzzles that contribute to the maintenance of the blockchain. To increase their mining revenue, users can unite into mining pools. These can be centralised or decentralised, depending on whether the coins are distributed to users by a central administrator.

While decentralised pools always require users to contribute computing power to the pool, centralised pools can either require contribution of computing power or distribute coins in return for investment of fiat currency (this business model is known as 'cloud mining').

Figure 2: Taxonomy of Mining Pools



Source: Authors' research.

Impact

A VASP whose user claims to have mined cryptocurrency may wish to verify that it was genuinely obtained from legitimate sources.[45] For instance, an alleged Dark Web drug dealer reportedly

45. Giles Dixon, Peter Warrack and Adnan Tahir, 'Front-Running the Traditional "Three Stages of Money Laundering" – Cuckoo Mining, the New Parasite on the Block', *ACAMS Today*, 26 September 2018.

attempted to persuade a cryptocurrency exchange that he had obtained $19 million-worth of Bitcoin through mining (the exchange was not convinced and froze the funds).[46]

The risk of a (sufficiently competent) VASP being successfully deceived is currently limited because only a small number of large pools mine major virtual currencies, especially Bitcoin.[47] Hence a VASP can approach the relevant pool's administrator to verify the information provided by the customer.[48] On the other hand, cloud-mining companies that accept fiat currency and distribute cryptocurrency in effect enable their users to exchange fiat for crypto, which can lead to the conversion of criminally obtained fiat currency. Furthermore, a Chainalysis webinar suggests that some mining pools allow users to make and then receive fiat payments, which provides money-laundering opportunities.[49] In those cases, a question may arise as to whether such a company is a financial institution for AML/CTF purposes regardless of whether it falls within the definition of a VASP.

Regulatory Approaches

While the FATF does not explicitly address the issue, FinCEN states that cloud-mining companies are not subject to AML/CTF regulation because their distribution of virtual currency is 'integral to the provision of [mining] services'.[50] This approach may reflect the fact that (most) cloud-mining companies only enable one-way exchange in a limited set of circumstances. On the other hand, to address potential opportunities for money laundering, regulators should consider keeping their approach to AML/CTF regulation of cloud-mining companies under review.

Recommendation 4: Regulators should keep their approach to AML/CTF regulation of cloud-mining companies under review.

46. US vs. Hugh Brian Haney, 'Sealed Complaint', Southern District of New York, 17 July 2019, p. 7, <https://www.justice.gov/usao-sdny/pr/us-attorney-announces-arrest-and-money-laundering-charges-against-dark-web-narcotics>, accessed 26 July 2019.
47. Interventions from representatives of two different blockchain analysis companies, RUSI workshop on money laundering via online businesses, London, 10 May 2019.
48. Authors' interview with an investigator in a virtual currency exchange, London, 17 June 2019.
49. Chainalysis, 'Webinar: Darknet Markets: Typologies, High Profile Shutdowns, and Where the Funds Go', 27 June 2019, 34:50–35:15, <https://go.chainalysis.com/Darknet-Markets-Webinar.html>, accessed 26 July 2019.
50. FinCEN, 'Application of FinCEN's Regulations to Certain Business Models', p. 38.

IV. Supporting Compliance Efforts

FOR VASPS TO live up to their role as the 'front line' of defence against cryptocurrency-related money laundering, they can benefit from support on the part of regulators and law enforcement agencies, particularly in matters of information sharing.

Wire Transfer Rule

One of the FATF recommendations, known as the 'wire transfer rule', requires originator VASPs to collect certain information[51] about cryptocurrency payers and transfer this information to the VASP (if any) used by the payment's recipient, as well as make such information 'available on request to appropriate authorities'.[52] Some industry participants had expressed misgivings about this rule because users do not need to use a VASP and the payer's or recipient's VASP does not always know whether the cryptocurrency address used by their customer's counterparty is maintained by another VASP.[53]

Recognising this, the FATF makes clear that originator VASPs are not required to pass on the information to individual (non-VASP) users, nor are beneficiary VASPs expected to prevent incoming transfers from individual users.[54] However, the following consequences are likely to result:

- VASPs will need to find a technological solution for complying with the wire transfer rule that does not impose an unreasonable financial burden on VASPs (which, if passed on to their customers, could prompt users to resort to P2P transfers not involving VASPs).
- If a workable solution is implemented, VASPs will have more information about other VASPs' customers with whom they transact, as opposed to transactions with individual (non-VASP) users; therefore, financial crime risks of transactions with individual users may be higher and blockchain analysis, which is discussed later in this paper, may play a greater role in mitigating those risks.

---

51. It is up to regulators to determine what this information should be. For instance, this is one of the questions asked by the Monetary Authority of Singapore in its consultation on 'Proposed Payment Services Notices on Prevention of Money Laundering and Countering the Financing of Terrorism', June 2019, pp. 15–16.
52. FATF, 'Guidance for a Risk-Based Approach', p. 56.
53. Global Digital Finance, 'GDF Input to the FATF Public Statement (the "Public Statement") Dated February 22, 2019', 7 April 2019, <https://www.gdf.io/wp-content/uploads/2018/01/GDF-Input-to-the-FATF-public-statement-of-22-Feb-2019-FINAL.pdf>, accessed 26 June 2019.
54. FATF, 'Guidance for a Risk-Based Approach', p. 30.

Recommendation 5: Regulators and VASPs should cooperate to identify feasible and cost-effective solutions for compliance with the 'wire transfer rule' envisaged in the FATF's Recommendation 16. Such solutions should aim to minimise the risk of customers resorting to less transparent channels (such as direct P2P transfers) if significant additional transaction costs result from the implementation of the 'wire transfer rule'.

Indicators of Suspicion

As soon as VASPs become subject to AML/CTF regulation, they bear the key obligation to report suspicious activity. However, as noted by several authors, 'in the absence of guidance regarding what is suspicious and reportable, practitioners are adrift in a virtual sea of uncertainty and left to their own devices to calibrate the expected regulatory compass'.[55]

Guidance from regulators, such as FinCEN's advisory issued in May 2019, helps redress this knowledge deficit.[56] Yet by and large, VASPs that have been in the business for a prolonged period of time, especially exchanges, tend to rely on risk indicators developed in-house, for instance in relation to risky counterparties.[57] For example, some exchanges employ investigators who open accounts with other VASPs to test the robustness of their AML/CTF controls.[58]

There are also discussions in the industry regarding the sharing of indicators of suspicion with a view to improving participants' understanding of risks they face.[59] Such initiatives can contribute to the collective knowledge of what suspicious cryptocurrency activity looks like, particularly since red flags common in traditional banking cannot always be extrapolated to cryptocurrency.[60]

Recommendation 6: VASPs and law enforcement agencies should continue developing initiatives aimed at sharing cryptocurrency-specific indicators of suspicion.

55. See Peter Warrack and Stephen Brent Sargeant, 'Virtual Assets: Calibrating the Compass of Suspicion', *ACAMS Today*, 28 March 2019.
56. FinCEN, 'Advisory on Illicit Activity Involving Convertible Virtual Currency', 9 May 2019.
57. Authors' telephone interview with a compliance expert in a cryptocurrency exchange in an EU country, 8 May 2019.
58. Authors' interview with an investigator in a cryptocurrency exchange, London, 17 June 2019.
59. Authors' discussions with two financial crime experts (at a cryptocurrency exchange and a blockchain tracing company), by telephone and email, April 2019.
60. For example, rapid multiple fund transfers may be suspicious in some settings but constitute normal activity on cryptocurrency trading platforms. Authors' telephone interview with a compliance officer at a centralised cryptocurrency exchange, 12 April 2019.

V. Creating a Credible Deterrent

A CREDIBLE DETERRENT, INCLUDING regulatory or law enforcement action, must be present to address potential failures to comply with AML/CTF obligations. Notwithstanding potential difficulties of enforcing the law against internet-based businesses that can operate across borders, increasingly often action is being taken against VASPs, as detailed in Table 1.

Table 1: Examples of AML/CTF Enforcement Against VASPs

Year	Name	Jurisdiction	Alleged Misconduct	Outcome
2019	Bestmixer.IO	Netherlands	According to Dutch law enforcement, Bestmixer.io was one of the world's three largest mixers and 'many of the mixed cryptocurrencies on Bestmixer.io had a criminal origin or destination'.	Dutch law enforcement seized the servers and are analysing the mixer's activities.
2019	Reginald Fowler and Ravid Yosef	US	The defendants allegedly opened bank accounts on behalf of unregistered cryptocurrency exchanges while representing to banks that the accounts would be used for the proceeds of real-estate investments.	Case pending.
2019	Eric Powers	US	Eric Powers provided exchange services by entering into P2P transactions with other cryptocurrency users on a regular basis. In doing so, he did not register with FinCEN, nor did he comply with other AML/CTF obligations.	FinCEN assessed a civil penalty of $35,000; he also forfeited $100,000 and 237.5 bitcoin in criminal and civil forfeiture.
2019	'Cryptocurrency laundering' criminal group	Spain	The Spanish Civil Guard arrested eight people and charged eight more for allegedly converting cryptocurrency into fiat currency for other criminal organisations.	Case pending.
2017	BTC-e	US	BTC-e was one of the largest cryptocurrency exchanges from July 2011 to July 2017. According to the US Department of Justice, BTC-e 'lacked basic anti-money laundering controls' and was 'designed to help criminals launder their proceeds'.	FinCEN assessed a civil penalty of $110 million; the alleged operator of BTC-e is detained in Greece pending extradition to France, Russia or the US.
2015	Ripple Labs Incorporated	US	Ripple Labs was issuing the virtual currency it had developed, XRP, in exchange for fiat currency without registering with FinCEN or complying with other AML/CTF obligations.	FinCEN assessed a civil penalty of $700,000; criminal charges were settled out of court.

Sources: Europol, 'Multi-Million Euro Cryptocurrency Laundering Service Bestmixer.Io Taken Down', press release, 22 May 2019, <https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down>, accessed 16 June 2019; US Department of Justice, US Attorney's Office, Southern District of New York, 'Arizona Man And Israeli Woman Charged In Connection With Providing Shadow Banking Services To Cryptocurrency Exchanges', press release, 30 April 2019, <https://www.justice.gov/usao-sdny/pr/arizona-man-and-israeli-woman-charged-connection-providing-shadow-banking-services>, accessed 16 June 2019; US Treasury Financial Crime Enforcement Network (FinCEN), 'FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws', 18 April 2019, <https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money>, accessed 16 June 2019; Europol, 'Cryptocurrency Laundering as a Service: Members of a Criminal Organisation Arrested in Spain', press release, 8 May 2019, <https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain>, accessed 16 June 2019; US vs BTC-e & Vinnik, 'Superseding Indictment', United States District Court, Northern District of California, San Francisco Division, 17 January 2017; FinCEN, 'FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales', 27 July 2017, <https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware>, accessed 16 June 2019; FinCEN, 'FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger', 5 May 2015, <https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual>, accessed 16 June 2019; US Attorney for the Northern District of California, 'Settlement Agreement', <https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/05/05/settlement_agreement.pdf>, accessed 16 June 2019.

Furthermore, in instances when regulatory or law enforcement action against a non-compliant VASP is not feasible (for instance, due to its administrators and assets being outside the state's jurisdiction), it may consider isolating that VASP from its financial system through ensuring that regulated businesses in that state (including financial institutions and VASPs) do not interact with such non-compliant VASPs. This could involve, for instance, the use of information-sharing partnerships such as the UK's Joint Money Laundering Intelligence Taskforce, in countries where such partnerships exist, to share information about non-compliant VASPs, or the introduction of mechanisms analogous to Section 311 of the USA PATRIOT Act, which enables the US Secretary of State to designate foreign financial institutions 'of primary money laundering concern'.

Recommendation 7: Subject to appropriate due process guarantees, regulators should consider mechanisms for disseminating information to regulated businesses about non-compliant overseas VASPs. The relevant financial intelligence unit (FIU) can support the identification of such non-compliant overseas VASPs by analysing SARs received from regulated VASPs or cryptocurrency-related SARs from other regulated businesses.

VI. Addressing Developments in Anonymity

PRIVACY COINS, WHICH the FATF refers to as 'anonymity-enhanced cryptocurrencies', frustrate blockchain tracing capabilities. Specifically, a privacy coin 'allows for peer-to-peer cryptocurrency transactions that leave no plaintext record of sender or recipient addresses and no plaintext record of the amount sent on the blockchain'.[61] To understand their implications, it is convenient to begin with the role of blockchain tracing.

Role of Blockchain Tracing

Blockchain tracing is a key tool in VASPs' compliance armoury. As almost all the most popular cryptocurrencies operate on a visible and transparent blockchain,[62] some companies offer 'blockchain tracing' services to identify coins that are associated with illicit activity, or 'tainted' coins.

Even when the identity of the user of a given cryptocurrency address is unknown, it is still possible, on a transparent blockchain, to trace the details of their transactions and transaction amounts and ultimate destinations of any coins involved in their interactions, along with transaction dates.[63] For instance, a cryptocurrency exchange can use blockchain tracing to:

- Help to potentially establish the identity of persons with whom their customers transact (or, if necessary, trace their customers' more remote connections).[64]
- Establish the legitimate origin of their customer's cryptocurrency by checking that incoming transfers do not originate from illicit sources, such as Dark Web marketplaces.[65]
- Identify transactions taking place between the users of a P2P exchange, which can be treated as suspicious.[66]

---

61. Peter Van Valkenburgh, 'Electronic Cash, Decentralized Exchange, and the Constitution', Coin Center, March 2019, p. 11.
62. According to Coinmarketcap on 17 June 2019, the most popular virtual currencies are: Bitcoin, Ethereum, Ripple, Litecoin and Bitcoin Cash, all of which operate on public ledgers.
63. Smith, 'Tracking Illicit Transactions With Blockchain'.
64. Blockchain tracing can enable 'clustering', namely the identification of cryptocurrency addresses that transact with each other in a way that suggests they are linked to the same person or illicit entity. See Danny Yuxing Huang et al., 'Tracking Ransomware End-to-End', paper presented at the 39th IEEE Symposium on Security and Privacy, San Francisco, CA, 21–23 May 2018.
65. Authors' interview with a blockchain-tracing company representative, London, 12 June 2019.
66. See BISQ Forum, 'Dirty BTC Coins on the XMR Market?', 3 June 2019, <https://bisq.community/t/dirty-btc-coins-on-the-xmr-market/7798>, accessed 16 June 2019.

Overall, the blockchain-tracing capacity is key to mitigating cryptocurrency-related financial crime risks. Yet some privacy advocates argue that blockchain tracing means that cryptocurrencies on transparent blockchains have failed in their privacy aspirations.[67] They contend that Bitcoin's fully transparent blockchain, for example, exposes an unnecessary amount of transaction information to the public and fails to protect users' privacy.[68] For this reason, privacy coins have been developed, which offer users the option of concealing all aspects of their transactions,[69] with significant implications for AML/CTF measures.

Since privacy coins operate based on differing algorithms, their privacy levels vary. This paper examines the three most popular privacy coins: Monero, Zcash and Dash. It then discusses developments that may reduce the traceability of transparent coins, such as Bitcoin.

Lack of Traceability of Privacy Coins

Of the three major privacy coins, Monero is the only one that is private by default, with Zcash and Dash both offering the option to obscure transactions. For example, only 4.5% of all Zcash transactions are shielded and held in private addresses, with 95.5% of the currency remaining transparent.[70] Monero, with its default features, obscures everything, including IP address and geographic location.[71]

Monero

Monero (market cap: $1,665,765,467)[72] uses three primary methods of concealing transaction information and is generally considered the most secure and anonymous privacy coin on the market. Monero hides sender information, stealth addresses and transactions amounts in a manner that is cryptographically private by default, with users' Monero holdings hidden to others.[73] The Monero protocol obfuscates sender information using ring signatures, which make it impossible to determine which address from a group has sent a specific transaction. This,

67. Kirill Shilov, '2019 for Privacy Coins: The Harsher the Regulations, the Higher the Price', *Hacker Noon,* 25 February 2019.
68. Jerry Brito, 'The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society', CoinCenter, February 2019, <https://coincenter.org/entry/the-case-for-electronic-cash>, accessed 24 July 2019.
69. Tom Wilson, '"Privacy Coin" Monero Offers Near Total Anonymity', *Reuters*, 15 May 2019.
70. ZChain, <https://explorer.zcha.in/statistics/value>, accessed 17 June 2019.
71. Monero, 'Monero: Kovri (How Monero Hides IP Addresses)', 16 November 2017, <https://www.youtube.com/watch?v=cxgbLI6IZGs>, accessed 17 June 2019.
72. CoinMarketCap, 'Monero', <https://coinmarketcap.com/currencies/monero/>, accessed 17 June 2019.
73. Monero, 'Moneropedia: Ring Signature', <https://web.getmonero.org/resources/moneropedia/ringsignatures.html>, accessed 17 June 2019; Monero, 'Moneropedia: Stealth Address', <https://web.getmonero.org/resources/moneropedia/stealthaddress.html>, accessed 17 June 2019; Monero, 'Moneropedia: RingCT', <https://web.getmonero.org/resources/moneropedia/ringCT.html>, accessed 17 June 2019.

combined with stealth addresses, which require a user to create single-use random addresses for every new transaction, ensure that transactions are untraceable. In addition, using ring confidential transactions (RingCT) Monero confidential transactions include a cryptographic proof that simply broadcasts that the transaction is true, rather than revealing the numbers involved on the blockchain. It is possible for a user to selectively and voluntarily share Monero transaction information with a view key, which enables the holder of the key to view any incoming transactions.

Dash

Dash (market cap: $1,476,629,914)[74] offers privacy options, but unlike Monero, is not private by default. Dash is also set apart from its competitors as it is not cryptographically private, but private through mixing, relying on a modified version of CoinJoin, a coin-mixing software, to optionally obscure transactions. Dash's PrivateSend, their version of shielded transactions, mixes coins from a given transaction with coins from other transactions using PrivateSend, before sending them to their recipient.

Zcash

Zcash (market cap: $772,142,596[75]), like Dash, is not private by default. However, unlike Dash, Zcash's privacy features make transactions cryptographically private.[76] Zcash, if made private, offers concealment of sender address, recipient address and transaction amount, using Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs), by which a user can prove possession of information without revealing the information itself.[77] However, it has been posited that unshielded Zcash transactions can sometimes leak information about shielded transactions.[78] Interestingly, Zooko Wilcox, the founder of Zcash, has indicated that it may be possible to track Zcash transactions in the future, even those that are shielded.[79]

74. CoinMarketCap, 'Dash', <https://coinmarketcap.com/currencies/dash/>, accessed 28 June 2019.
75. CoinMarketCap, 'Zcash', <https://coinmarketcap.com/currencies/zcash/>, accessed 28 June 2019.
76. Zcash, 'How It Works', <https://z.cash/technology/>, accessed 17 June 2019.
77. Zcash, 'What are zk-SNARKs?', <https://z.cash/technology/zksnarks/>, accessed 12 August 2019.
78. Aziz, 'Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies', *Masterthecrypto*, <https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/>, accessed 17 June 2019.
79. Zooko, 'And by the way, I think we can successfully make Zcash too traceable for criminals like WannaCry, but still completely private & fungible. …' [Twitter post], 6:22pm, 12 May 2017, <https://twitter.com/zooko/status/863202798883577856>, accessed 17 June 2019.

Table 2: Comparison of Privacy Features of Popular Privacy Coins

Coin	Privacy Choice Model	Sender Privacy	Recipient Privacy	Transaction Amount Privacy
Monero	Private by default, some information may be disclosed using a view key	Hidden using ring signatures	Hidden using RingCT/Stealth addresses	Hidden using RingCT
Zcash	Opt-in privacy available	Hidden using zk-SNARKs	Hidden using zk-SNARKs	Hidden using zk-SNARKs
Dash	Opt-in privacy available	Hidden using CoinJoin	Visible	Denomination visible

Sources: Ajay Chandhok, 'Privacy Coins – An Explainer of the Top Anonymous Cryptocurrencies', LedgerOps, <https://ledgerops.com/blog/privacy-coins-an-explainer-of-the-top-anonymous-cryptocurrencies/05/29/2019>, accessed 17 June 2019; Sead Fadilpašić, 'Top 5 Privacy Coins: Features and Differences', CryptoNews, 5 October 2018, <https://cryptonews.com/exclusives/top-5-privacy-coins-features-and-differences-2725.htm>, accessed 17 June 2019; Monero, 'Moneropedia', <https://web.getmonero.org/resources/moneropedia/>, accessed 17 June 2019; Zcash, 'How It Works', <https://z.cash/technology/>, accessed 17 June 2019; Dash, 'How Dash Works', <https://www.dash.org/learning-resources/>, accessed 17 June 2019.

Implications of Privacy Coins

Privacy coins have the following implications for AML/CTF measures:

- It is challenging to distinguish between 'clean' and 'tainted' privacy coins, such as those obtained through cryptojacking[80] or extortion.[81]
- It may be possible to convert cash into privacy coins anonymously, which can be done for privacy reasons but also carries financial crime risks. For instance, privacy coin proponents on Reddit regularly share new strategies for acquiring Monero without ever disclosing their identity, although this appears to be difficult to achieve at scale.[82]

80. Europol, *Internet Organised Crime Threat Assessment 2018*, p. 19.
81. David Canellis, 'Kidnappers in Norway Demand $10M Monero Ransom for Millionaire's Wife', *Next Web*, 9 January 2019.
82. *Reddit*, 'How to Buy Crypto Anonymously', February 2019, <https://www.reddit.com/r/bisq/comments/a84q4f/how_to_buy_crypto_anonymously/>, accessed 12 August 2019; *Reddit*, 'How Do You Buy Monero 100% Anonymously?', January 2019, <https://www.reddit.com/r/Monero/comments/8wya44/how_do_you_buy_monero_100_anonymously/>, accessed 12 August 2019.

Figure 3: Possible Example of Money Laundering Involving Privacy Coins

Source: Authors' research; participant interventions, RUSI workshop on money laundering via online businesses, London, 10 May 2019.

VASPs may be able to mitigate risks posed by privacy coins if they have sufficient information on their customers and those customers' counterparties. However, due to perceived risks, most major exchanges do not operate in privacy coins. Some, such as Coinbase, draw a distinction between shielded and unshielded transactions, accepting, for instance, unshielded Zcash transactions.[83] This can make turning privacy coins into fiat currency very difficult, requiring multiple levels of currency exchange.

Bitcoin Mixing

Aside from the use of privacy coins, efforts are underway to inject greater privacy in Bitcoin transactions. Mixing software, such as CoinJoin or CoinShuffle, can automatically mix Bitcoin inputs.[84] The main challenge to widespread adoption of mixing software is the technical sophistication required of users. Furthermore, due to the nature of mixing, as long as user numbers remain low, privacy benefits of the technology are limited.[85] In addition to mixing, other privacy-enhancing technologies have been developed but not yet integrated in Bitcoin, including the MimbleWimble protocol and Schnorr signatures.[86]

For now, mass adoption of fully private Bitcoin transactions appears a distant possibility, although it would be foolhardy to make confident predictions about the future of cryptocurrency. The newly adopted regulatory approach, which relies on VASPs as the first line of defence against financial crime regardless of what coins their customers transact in, is a sensible response short of regulating privacy coins or software development, which is a highly contentious issue that deserves detailed analysis in its own right. Thus, FinCEN does not extend AML/CTF requirements to the developers of mixing software;[87] nor should other states do so without solid understanding of such regulation's feasibility and civil liberties ramifications.

83. Authors' interview with cryptocurrency expert, London, 16 June 2019.
84. Aaron Van Wirdum, 'Shuffling Coins to Protect Privacy and Fungibility: A New Take on Traditional Mixing', *Bitcoin Magazine*, 14 June 2016.
85. Authors' interview with an investigator in a cryptocurrency exchange, London, 17 June 2019.
86. Simon Chandler, 'Is Bitcoin's Increasing Anonymity a Threat to Privacy Coins?', *CoinTelegraph*, 12 June 2019.
87. Chandler, 'Is Bitcoin's Increasing Anonymity a Threat to Privacy Coins?'.

Recommendation 8: Privacy coins or mixing software are not in and of themselves indicative of criminal activity, but VASPs whose customers use them should ensure they collect and analyse sufficient information about their customers' activity to mitigate financial crime risks.

Recommendation 9: Regulators and law enforcement agencies should monitor criminal misuse of privacy coins or mixing protocols and, when appropriate, share relevant information with VASPs so they can adjust their financial crime mitigation efforts accordingly.

Conclusions and Recommendations

THE REVISION OF the FATF Recommendation to cover cryptocurrency businesses is a necessary step towards addressing cryptocurrency-related financial crime risks. With the ball now in the court of domestic regulators, they must deliver on effectively implementing the FATF's requirements in national systems, in terms of both transposing the rules and ensuring their genuine application. To do so, they should consider the following recommendations, which call for either regulatory action or support of private-sector efforts.

Recommendations

Policing the Regulatory Perimeter

- Supervisors should use a wide range of intelligence to identify VASPs subject to their AML/CTF supervision, including through liaising with law enforcement agencies and encouraging registered VASPs to report, in confidence, potentially non-compliant peers.

Clarifying the Definition of VASP

- While persons should not be subject to AML/CTF regulation solely on account of developing software used for P2P exchange of cryptocurrency, persons with meaningful control over a P2P exchange platform should be subject to AML/CTF regulation. A person has meaningful control over a P2P exchange if they can, for instance, unilaterally restrict access to the exchange or discontinue its operation.
- Mixers should be subject to AML/CTF obligations and face regulatory or law enforcement action in case of non-compliance, although such obligations should not extend to persons who merely develop mixing software protocols.
- Regulators should keep their approach to AML/CTF regulation of cloud-mining companies under review.

Supporting Compliance Efforts

- Regulators and VASPs should cooperate to identify feasible and cost-effective solutions for compliance with the 'wire transfer rule' envisaged in the FATF's Recommendation 16. Such solutions should aim to minimise the risk of customers resorting to less transparent channels (such as direct P2P transfers) if significant additional transaction costs result from the implementation of the 'wire transfer rule'.
- VASPs and law enforcement agencies should continue developing initiatives aimed at sharing cryptocurrency-specific indicators of suspicion.

Creating a Credible Deterrent

- Subject to appropriate due process guarantees, regulators should consider mechanisms for disseminating information to regulated businesses about non-compliant overseas VASPs. The FIU can support the identification of such non-compliant overseas VASPs by analysing SARs received from regulated VASPs or cryptocurrency-related SARs from other regulated businesses.

Addressing Developments in Anonymity

- Privacy coins or mixing software are not in and of themselves indicative of criminal activity, but VASPs whose customers use them should ensure they collect and analyse sufficient information about their customers' activities to mitigate financial crime risks.
- Regulators and law enforcement agencies should monitor criminal misuse of privacy coins and mixing protocols and, when appropriate, share relevant information with VASPs so they can adjust their financial crime mitigation efforts accordingly.

About the Authors

Anton Moiseienko is a Research Fellow at RUSI's Centre for Financial Crime and Security Studies.

Kayla Izenman is a Research Analyst at RUSI's Centre for Financial Crime and Security Studies.