**April 8, 2019**

**To: The Financial Action Task Force**

**Re: Consultation on Virtual Assets**

To whom it may concern,

We are writing in response to the FATF's February 22, 2019, request for public comment on paragraph 7(b) of its Interpretive Note on virtual assets.[1]

As a provider of blockchain forensic and AML/CFT compliance solutions for the cryptocurrency industry, we welcome the FATF's ongoing engagement with the private sector on this specific matter, as well as its broader efforts to ensure the effective monitoring of virtual asset risks and the regulation of virtual asset service providers (VASPs).

We have contributed to a letter submitted to you by Global Digital Finance, an industry body that includes several of our partners and peers, in providing a comprehensive response to the FATF's consultation. You will have received that letter separately. It provides an in-depth consideration of why we, and other industry stakeholders, feel that Recommendation 16 would not be possible for VASPs to implement in full as described in paragraph 7(b) of the Interpretive Note.

While we believe that Recommendation 16 is not technically possible to implement in full with regard to virtual asset transfers, we agree with the FATF that mitigation of money laundering and terrorist financing risks in the virtual asset space is an urgent matter. We are therefore sending the current letter to provide additional information that we believe can assist the FATF in understanding the role that blockchain forensic and AML/CFT compliance solutions can play in mitigating risks related to virtual asset transfers, even if Recommendation 16 is not applied to them directly.

We also set out further below why we feel it is important that the FATF clarify the essential role that blockchain analytics solutions can play in enabling VASPs to apply a risk based approach.

[1] See: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html

**Overview of Blockchain Forensic and AML/CFT Compliance Solutions**

Virtual assets, which include cryptocurrencies and certain other digital payment methods as defined by the FATF, are often described as posing money laundering and terrorist financing risks owing to the level of anonymity they afford users. In June 2014 the FATF noted that "the anonymity provided by the trade in virtual currencies on the internet" presents high AML/CFT risks.[2]

It is true that some virtual assets afford users significant anonymity. For example, anonymity enhancing cryptocurrencies (often referred to as "privacy coins") are a particular subset of cryptocurrencies that rely on obfuscating techniques to conceal information about the sender, recipient, and value of transactions. This subset of virtual assets presents risks similar to those the FATF has highlighted with respect to other products such as cash and anonymous prepaid cards.[3]

However, a high degree of anonymity and transaction obfuscation is not a universal feature of all virtual assets. Indeed, certain types of cryptocurrencies such as Bitcoin and Ethereum, which are among the most widely utilised of all virtual assets, are more accurately described as "pseudonymous". That is, users of these cryptocurrencies are represented by alphanumeric addresses that do not reveal their true identities but are nonetheless highly visible to any observer owing to the public nature of the "blockchains", or ledgers, on which transactions are recorded. The public nature of these blockchains makes it possible for any party to obtain complete information about how counterparties have interacted, including the time, value, and sequence of transactions. As one group of academics has noted, "AML in Bitcoin has to deal with imperfect knowledge of identities, but may exploit perfect knowledge of all transactions."[4]

Despite their pseudonymous nature, the limitation on understanding the identities of counterparties in cryptocurrency transactions is in fact surmountable. Several methods enable the attribution of real-world identities to otherwise pseudonymous addresses. For example, where a VASP conducts KYC on a customer and can associate his or her identity with a specific cryptocurrency address, this has the impact of deanonymizing that address. Alternately, at Elliptic, we undertake a process of data analysis that enables us to attribute specific cryptocurrency addresses to real-world identities, including the identities of addresses known to be controlled by illicit actors, such as cybercriminals, dark web market vendors, terrorist organizations, and persons subject to financial sanctions measures. We then employ heuristics that enable us to assert with confidence

[2] See: http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html

[3] See, for example: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html

[4] See: https://maltemoeser.de/paper/money-laundering.pdf

that a large number of addresses, or "clusters" of otherwise seemingly unidentifiable addresses, are in fact controlled by a single individual or entity.

Therefore, once a real-word identity has been associated with a specific public cryptocurrency address, or set of addresses, it becomes possible to monitor that individual's or entity's transactional activity, and the concurrent audit trail preceding or following on their direct activity involving a VASP, with accuracy across an entire cryptocurrency ecosystem.

Drawing on these techniques, at Elliptic we have provided risk-based AML/CFT monitoring solutions to the cryptocurrency industry since 2013 that rely on the transparency of open-source, public blockchains to enable risk-based transaction monitoring. Our solutions enable VASPs to monitor customer activity on public blockchains to determine whether customer funds may originate from, or are destined for, illicit sources such as drugs marketplaces or wallets associated with sanctioned entities.

Our solutions have been utilised by many of the world's largest cryptocurrency exchanges, as well as banks and other financial institutions, to enable them to identify risks associated with cryptocurrency transactions. They have been implemented by regulated businesses in jurisdictions such as the US that have had AML/CFT requirements in place around virtual assets for more than half a decade – demonstrating that bespoke AML/CFT solutions can enable VASPs dealing in certain types of virtual assets to comply with regulation successfully. We have also worked closely with law enforcement agencies to secure the arrest and successful prosecution of criminals utilizing cryptocurrencies.

**Applicability to the FATF Recommendations**

To this end, the bespoke forensic and transaction monitoring solutions such as those we provide at Elliptic can enable VASPs to satisfy the requirements of certain FATF Recommendations. Specifically, these solutions can enable VASPs to satisfy the requirements of Recommendation 10(d), which provides for:

*[c]onducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.*

Blockchain monitoring solutions can enable VASPs to undertake scrutiny of transactions in detail and ascertain a significant degree of information about customer activity, including:

- the ultimate source or destination of funds, and whether those funds are associated with an illicit actor or prohibited activities;

- an audit trail of those funds' history, including whether funds passed through intermediary addresses on the way to or from a customer's account with the VASP, and whether those intermediary addresses are associated with illicit activity;
- whether a customer's transactions include dealings with other known, identified entities, or involve transactions with unlabelled addresses that have not been clearly attributed to a specific real-world identity, and therefore may require enhanced scrutiny and due diligence.

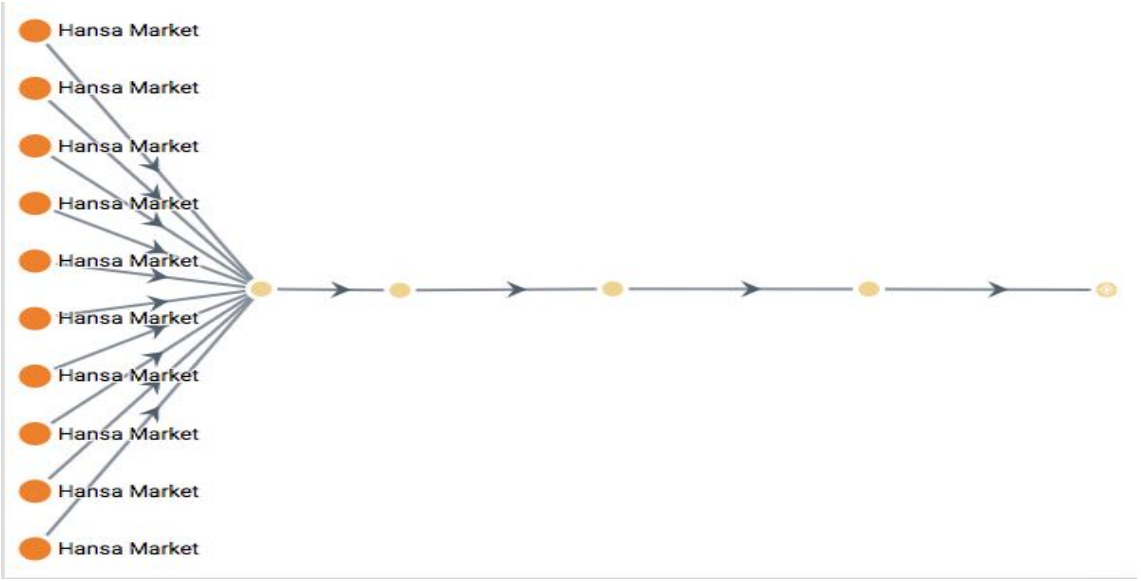
With this information, VASPs can make informed decisions about customer activity, such as whether to close accounts or file suspicious activity reports - just as other financial services providers do when managing relationships with customers using fiat currencies or other products and services.

However, it is important to note that certain features of public blockchains can enable VASPs to engage in a level of scrutiny of transactions that frequently exceeds what is possible in the context of other financial services and activities.

Because public cryptocurrency blockchains provide a complete and chronological record of all activity within a specific cryptocurrency ecosystem, it is possible for a VASP to identify not only the source of funds or ultimate destination involved in a customer's transaction, but to observe the flow of those funds through a large number of intermediary addresses external to their own platform. Blockchain forensic solutions enable VASPs to observe as customer funds "hop" from the customer's known address maintained with the VASP to or from other external cryptocurrency addresses. A VASP can therefore observe, for example, not only that a customer's funds originated from a dark web marketplace, but that those funds passed through several, or even dozens, of intermediary addresses before being deposited at the customer's account with the VASP.

Attempting to conduct this analysis manually would prove enormously time consuming and resource-intensive, but available blockchain analytics software enables VASPs to observe this information about customer transactions as it occurs.

The diagram below provides a simple illustration of this concept.




*This diagram uses sample data drawn from Elliptic's AML monitoring tool to illustrate the hypothetical flow of funds from numerous Bitcoin addresses controlled by an illicit entity (the Hansa Market dark marketplace, represented in orange at left) to a customer's address at a Bitcoin exchange platform (represented by the final yellow circle on the right). The four yellow circles in between represent intermediate addresses, or "hops", through which the bitcoins passed before their final deposit at the exchange. In some cases, the identity of parties controlling intermediate addresses may be known to the VASP. Using this type of information, VASPs can observe the flow of funds to or from a customer's address through even dozens of hops, and can consider how the velocity and timing of intermediate transfers may impact the view of risk associated with those transfers.*

This is a level of transparency and transaction monitoring not possible in other financial services contexts. Unlike standard fiat currency automated transaction monitoring tools, which are limited to providing risk-based indicators of suspicion and information about the *direct* source or destination of a customer's transfers, blockchain analytics tools provide an audit trail of funds flows to or from their ultimate destination or source and through the historical transaction trail, in addition to enabling the detection of risk based "red flags" that may be associated with related parties.

A bank, for example, would not be able to readily observe that its customer's funds originated from an illicit source and passed through dozens of hands or external accounts prior to being deposited in the customer's bank account. VASPs, on the other hand, may not always have complete information about the identity behind every intermediary address associated with a transaction, but, where they employ bespoke blockchain analytic software tools, can glean significant amounts of information about the nature, scale, and velocity of funds flows through an entire transaction trail that may provide indicators of suspicious activity.

Because of this level of visibility afforded to VASPs, the benefits that may be lost from not being able to apply Recommendation 16 in full to virtual asset transfers may ultimately be counterbalanced by the ability of available blockchain forensics and AMl monitoring solutions to enable VASPs to undertake levels of scrutiny in transaction monitoring that would not be possible in many other contexts. As outlined in the

aforementioned letter submitted to you by Global Digital Finance, the visibility and traceability of many open, public blockchains may also therefore facilitate intelligence sharing arrangements that could act as an alternative to Recommendation 16.

In short, while it may not be possible to apply FATF Recommendation 16 to virtual asset transfers, blockchain forensic and bespoke AML/CTF monitoring solutions can provide significant additional benefits in enabling VASPs to identify and assess risks when scrutinizing transactions, and to take action to mitigate associated risks.

We therefore recommend that the FATF provide clarification about the critical role that blockchain analytics play in enabling the application of a risk based approach. This will help to clarify both for regulators, and for VASPs, that solutions exist that can enable effective risk mitigation and AML compliance.

Sincerely,

David Carlisle
Head of Community
Elliptic

Tom Robinson
Chief Scientist and Co-Founder
Elliptic