What is a Virtual Asset Service Provider (VASP)?

Any natural or legal person who (...) as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- **exchange between virtual assets and fiat currencies**
- **exchange between one or more forms of virtual assets**
- **transfer of virtual assets**
- **safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets**
- **participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset**

From a regulatory perspective, applying the rule to cryptocurrencies is therefore seen as leveling the playing field between different funds transfer systems.

However, contrary to traditional wire transfers, the rule requires an additional exchange of information that is per se not necessary for blockchain-based transactions. The need for industry participants to agree on standards for such an additional information layer is what makes the requirement difficult.

Peer-to-peer transactions are not affected

Unlike traditional wire transfers, cryptocurrencies are often (or even typically) transferred between parties that are not financial intermediaries or VASPs. These peer-to-peer transfers remain out of scope.

The unequal treatment of transfers among intermediaries versus peer-to-peer transactions has been criticized. It was argued that the travel rule in its current form will be not effective to combat criminal activity, instead putting a burden on the crypto-financial industry. However, service providers which are active in the space will have no alternative but to adhere to the rule.

Possible solutions

Implementing the travel rule is not as easy as it first seems. Imagine you as a VASP receive the instruction from a client to transfer 10 Bitcoin to an unknown blockchain address. How do you know whether the destination address is controlled by another VASP, which triggers the obligation to send originator and beneficiary information? If this can be determined, how is the information transmitted and in what format? What happens if the client refers to the wrong VASP by mistake or even on purpose? Finally, how can it be assured that client data is protected along the way?

Different solutions are currently being discussed by the VASP community. Initial ideas where suggesting centralized approaches, such as global registration of addresses controlled by VASPs, which would obviously undermine the benefits arising from the blockchain. Increasingly, the discussion focuses on decentralized and open protocols. Some ideas suggest the usage of blockchain.

In a recent blog post, Andy Bryant from bitFlyer summarized the different technical solutions across two dimensions: Firstly, whether it follows a centralized or decentralized approach, and secondly whether the solution utilizes a blockchain or not.[1]

	Non-Blockchain	Blockchain
Centralized	Centralized Database Swift-like network	Inter-VASP network Permissioned Ledgers
Decentralized	Off-chain certificate authorities Point-to-point tunnels	Decentralized Trust Networks Cooperative digital storage and data retrieval tool

[1] https://www.andybryant.me/blog/2019/9/25/using-instant-messenger-to-explain-the-fatf-travel-rule-fornbspvasps