VASPs & The Travel Rule

Information Event – organized by the **Crypto Valley Association**

Zurich University, August 27, 2019

Bitcoin Suisse

VASP Transfer Information Exchange – **Guiding Principles for a Common Protocol**

David Riegelnig

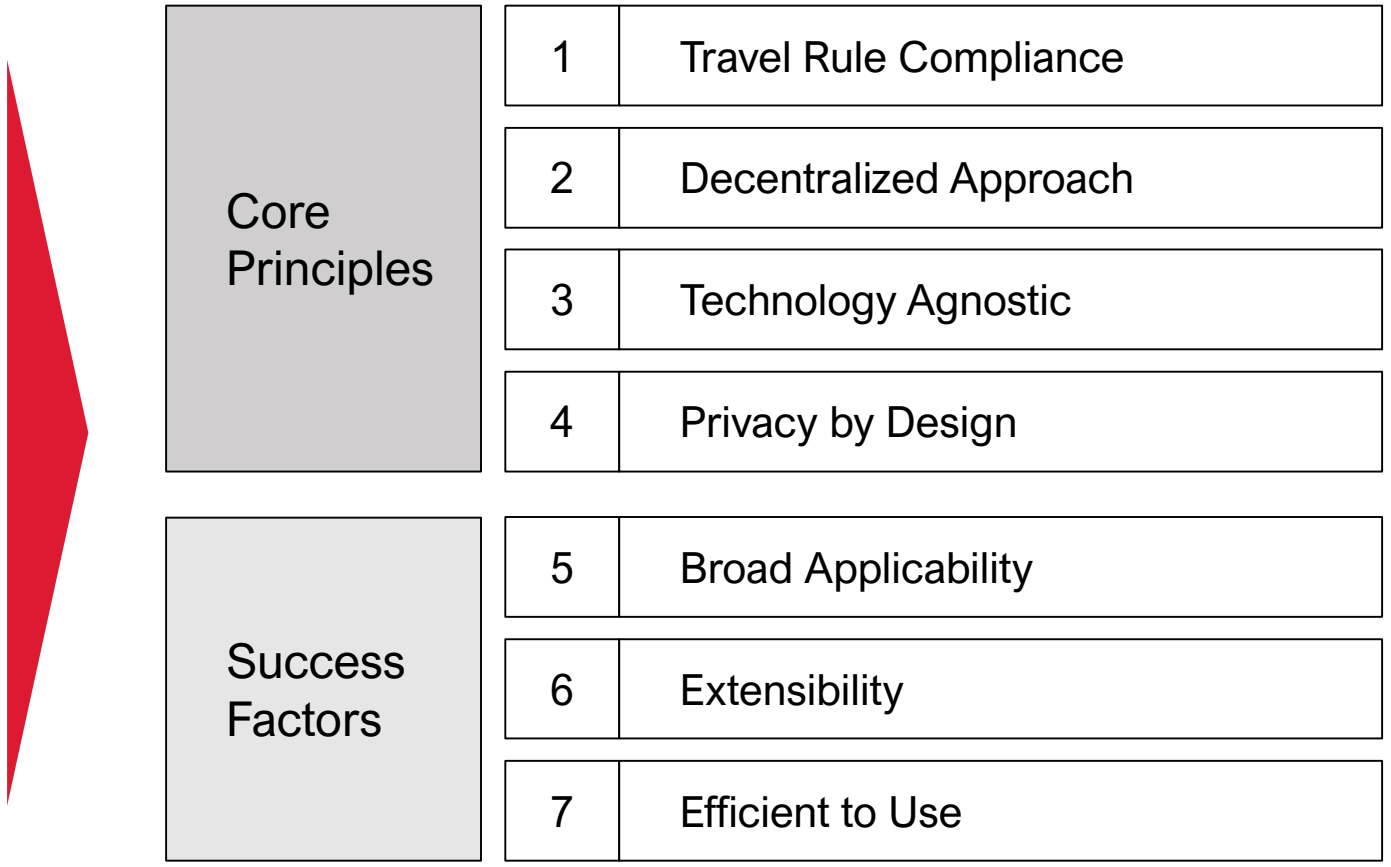
Head Risk Management, Bitcoin Suisse

Bitcoin Suisse

Guiding Principles for a Common Protocol

Bitcoin Suisse proposes a common protocol to facilitate compliance with FATF's travel rule for virtual assets.

Seven principles are proposed as a starting point to guide the community effort.



Bitcoin Suisse

1 – Travel Rule Compliance

Establish a shared communication protocol (“protocol”) for VASPs to exchange VA transfer information as specified in the FATF requirements.

This includes:

a) a common transfer data standard for required originator and beneficiary information;

b) a suitable set of rules to facilitate the data exchange between VASPs.

By this means, the protocol ensures:

- focus on the exchange of VA transfer information (travel rule);
- no interference with other, more country-specific requirements (e.g. VASP registration).

2 – Decentralized Approach

Pursue a decentralized approach that enables any two VASPs to use the protocol without consent or even knowledge of any third party.

This includes that the protocol:

a) does not require a VASP to obtain any form of membership or registration with any third party;

b) does not require the usage of a central component at any time.

By this means, the protocol ensures:

- no central authority can be manipulated or abused;
- no central technical component can be attacked or manipulated, which makes the solution more resilient and secure;
- privacy and economic interests of VASPs are fully protected;
- lock-in of a suboptimal solution is avoided and ongoing innovation is fostered.

3 – Technology Agnostic

Make sure the protocol works with any blockchain or distributed ledger technology (DLT) used for the underlying VA transfer.

This includes that the protocol:

a) requires no changes to the underlying blockchain / DLT;

b) does not assume specific characteristics of the underlying blockchain / DLT (e.g. the existence of a unique identifier or comment field in transactions).

By this means, the protocol ensures:

- no compliance gaps can arise for VASPs due to not supported blockchains / DLTs;
- keeping up to date with the rapid innovation in the field, including emerging technologies such as Layer 2 protocols or “atomic” swaps between blockchains.

4 – Privacy by Design

Make sure the protocol puts privacy of transferred data at the center of its design.

This includes that the protocol:

a) requires robust authentication of the VASPs involved;

b) requires robust end-to-end encryption between VASPs;

c) applies perfect forward secrecy (protecting data transferred in the past against future compromises of the private keys);

d) allows for two VASPs to transfer data without the knowledge of any third party.

By this means, the protocol ensures:

- confidentiality for the VASP and its clients;
- no conflicts with data privacy laws globally.

5 – Broad Applicability

Ensure that the protocol facilitates all applicable usage scenarios where VASPs need to exchange transfer data.

This includes that the protocol:

a) supports VASPs exchanging data as part of a one-off VA transfer;

b) supports VASPs exchanging data for a high number of routine transactions;

c) supports situations where the beneficiary VASP is not known to the sending VASP or where there is uncertainty whether a target address is controlled by a VASP;

d) supports situations where VA transfers between VASPs are initiated or facilitated by smart contracts.

By this means, the protocol ensures:

- neutrality and openness towards all business models;
- ease of integration and therefore better adoption.

6 – Extensibility

Ensure that the protocol allows for custom extensions.

This includes that the protocol:

a) allows for VASPs to add custom data;

b) while doing so, has rules that prevent any weakening of the common core.

By this means, the protocol ensures:

- support for specific business processes;
- support for local regulatory needs;
- efficiency gains while achieving compliance.

7 – Efficient to Use

Ensure minimal cost for VASPs to deploy and maintain the protocol's implementation.

This includes that the protocol:

a) supports straight-through processing capabilities;

b) supports implementations where a single server instance can process VA transfers in all blockchains / DLTs used by the VASP.

By this means, the protocol ensures:

- ease of integration and therefore better adoption.