

FATF Travel Rule's Technical Challenges and Solution Taxonomy

Yuto TAKEI

(Mercari, Inc. and Tokyo Institute of Technology, JAPAN)

Kazuyuki SHUDO

(Kyoto University, JAPAN)

mercari



Outline of the presentation

1. Research motivation
2. Travel rule explained
3. Challenge 1. Address identification
4. Challenge 2. Address ownership proof
5. Challenge 3. Communication protocol
6. Available travel rule solutions
7. Conclusion

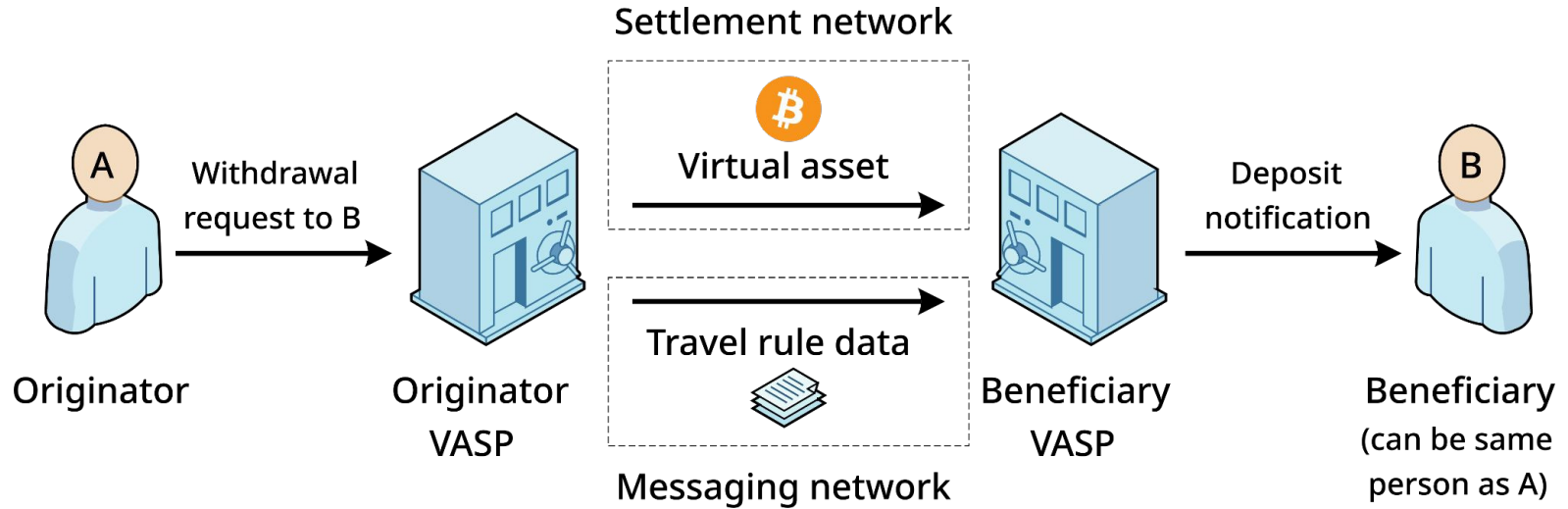
| Research Motivation

- Travel Rule applies to virtual assets starting in 2019.
- By the nature of cryptocurrency, technical challenges exist.
 - High anonymity (or pseudonymity)
 - Instant cross-border transfers
- To establish an understanding of the challenges and solutions, given the limited number of literature available.

Travel Rule Explained

VA = Virtual Asset

VASP = Virtual Asset Service Provider



- Originator VASP must notify beneficiary VASP of PII of originator and beneficiary.
- Both VASP must keep accuracy of their customer's PII.

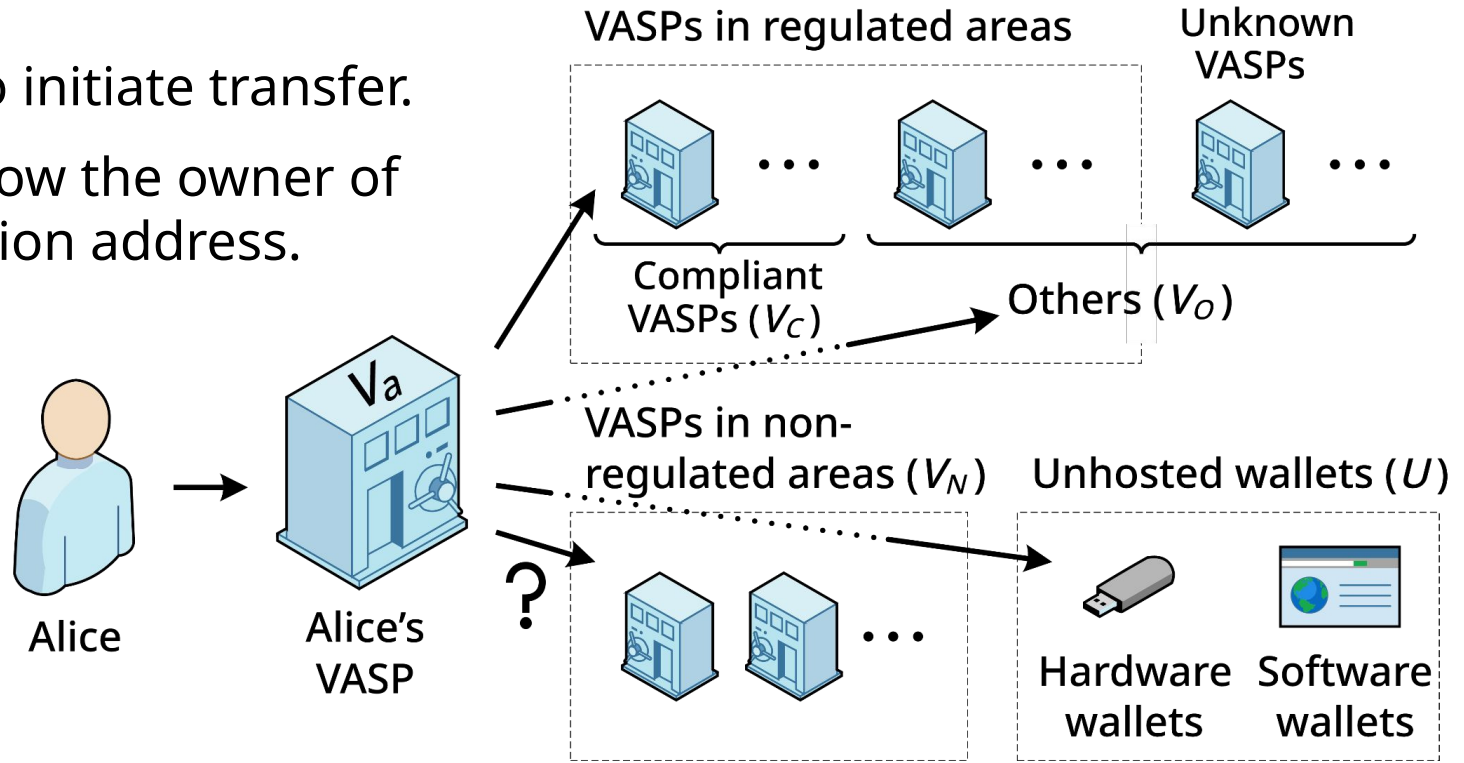
| Challenges in Travel Rule

- 1 Address identification**
The owner of VA address cannot be easily identified.
- 2 Address ownership proof**
Owners cannot be verified easily in some cases.
- 3 Communication protocol**
No common interface is agreed among all VASPs.

Challenge 1. Address Identification

Alice wish to initiate transfer.

V_a has to know the owner of the destination address.



Challenge 1. Address Identification

(1-A) Restricting the transfer

✓ Easy to implement ✗ Not very effective

(1-B) Use of lookup service

✓ Flexible / Scalable ✗ Limited to known addresses / Data governance

(1-C) Special address format

✓ Accurate ✗ VASP directory required / Incompatible with unhosted

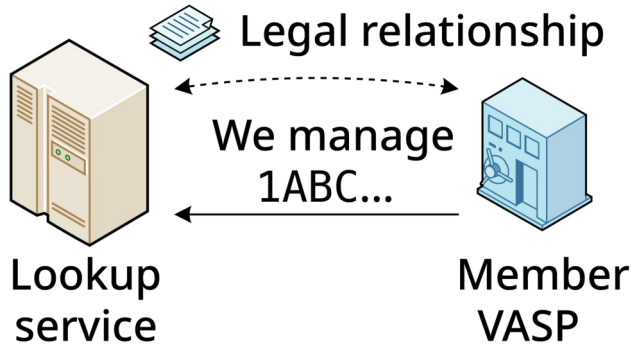
(1-D) Use of domain names of VASPs

✓ Straightforward ✗ Impacted by network security (DNS-specific problems)

Challenge 2. Address Ownership Proof

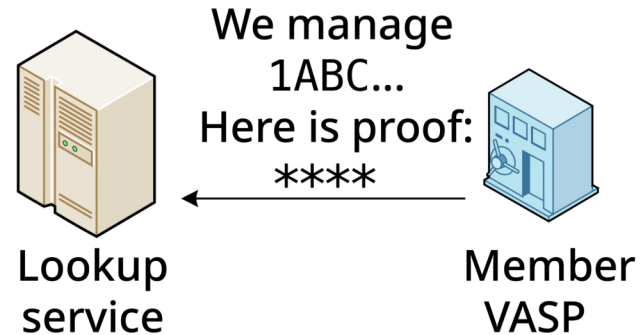
Using lookup services, VASP needs to prove the address ownership.

(2-A) Contract-based



- ✓ Easy to implement
- ✗ Weak guarantee

(2-B) Providing proof



- ✓ Cryptographically secure
- ✗ Not always feasible

Challenge 3. Communication Protocol

VASPs has to establish communication channel between them.

(3-A) Peer-to-peer

✓ Straightforward ✗ Not scalable / Costly

(3-B) VASP directory

✓ Flexible / Scalable ✗ Actively maintained directory + standard required

(3-C) Alliance

✓ Well maintained ✗ Centralized / Closed

Available Travel Rule Solutions

Approaches		TRUST (USTRWG)	TRISA	Syгна Bridge	VerifyVASP	Shyft Veriscope	OpenVASP / TRP	Netki / TransactID
Challenge 1) Identification of Destination VASP	(1-B) Lookup service	✓	✓			✓		
	(1-C) Special identifier			✓				✓
	(1-D) Domain name					✓		
Challenge 2) Address Ownership	(2-A) Contract-based	✓			✓	✓		
	(2-B) Providing proof	✓ ↘	✓	✓				
Challenge 3) PII Transmission	(3-A) Peer-to-peer					✓		
	(3-B) VASP directory				✓		✓	
	(3-C) Alliance	✓	✓	✓	✓			

Alliance-type solutions are the majority.

Blockchain analysis companies are collaborating with many of them.

| Existing Challenges

Unhosted wallets

- Travel Rule may not apply to transfers with unhosted.
- Cannot distinguish between clean VASP addresses and unhosted wallets.

Solution diversity

- Some alliances may not have compatibility.
- Implementation costs increase for VASPs.
- Users cannot initiate transfers across alliances.

| Conclusion

- Effectively, joining alliances is the fastest and prevalent way for exchanges to get on board with the Travel Rule.
- Some implementation issues remain: ownership proof of various types of addresses, or support for new forms of VAs.
- Travel Rule itself continues to have inherent challenges, such as integration with unhosted wallets.