TRISA

Identifying an address as belonging to a VASP.

Stanislav Malyshev
Phillip Seay
Albert Szmigielski
Jelle Vink
Nov 6th 2019
San Francisco

VASPs need to transfer some required data when sending value to another VASP.

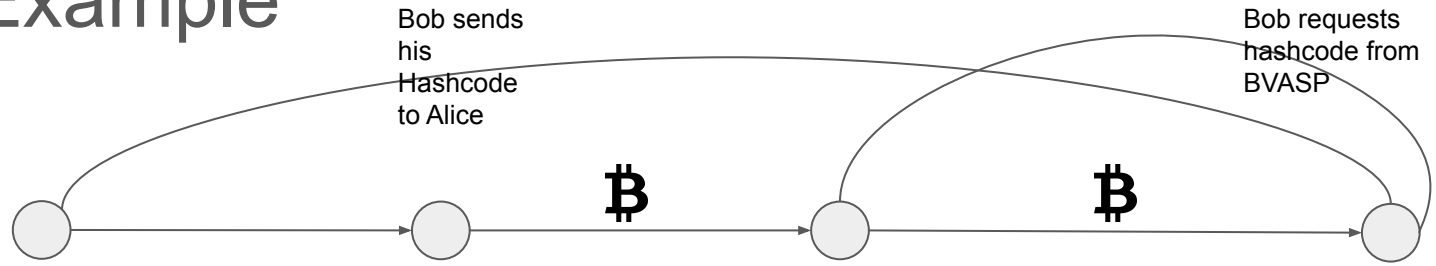
One problem that the current implementation of TRISA does not address is recognizing or identifying an address as belonging to a VASP

Our proposals complement the TRISA protocol.
(They are not a replacement of it.)

Assumptions

- VASPs want to comply. The proposals do not force compliance, just enable it.
- VASPs modify their UI to enable clients to create the required message.
- Sending user may not know if they are sending value to a VASP (or private address).

Example


Bob sends his Hashcode to Alice
Bob requests hashcode from BVASP
Alice
Alice's VASP ("AVASP"). Alice gives AVASP the hashcode she got from Bob along with BVASP's name
SSL/TLS handshake validates BVASP's identity
AVASP either makes API call to BVASP: getTrisaAddress() or looks up BVASP's TRISA address from a directory service
AVASP sends funds to BVASP's TRISA address
Bob's VASP ("BVASP")
If the hashcode validates, send Bob's TRISA information to AVASP and move funds from BVASP's TRISA address to Bob's. If it does not, reject the transaction.
Bob

Proposed solution #1

- Each VASP has designated TRISA wallet address
- This address is well known/published, or returned on demand by the VASP itself (possible mechanisms include an API call to the VASP, or a public lookup service)
- Sending VASP uses its TRISA address to send
- The tx will be sent to the receiving VASP’s TRISA wallet

Proposed solution #1 - Sending

1. Bob gets hash code (HC) from B VASP
2. Bob gives HC to Alice
3. Alice gives HC and B VASP name to A VASP
4. A VASP communicates data to B VASP using TRISA protocol
5. A VASP sends TX from A Wallet to B Wallet including HC
6. A VASP receives Bob’s data from B VASP

Proposed solution #1 - Receiving

1. B VASP receives TX to B Wallet
2. If hash does not validate, freeze funds
3. If hash validates, if TX comes from A VASP AWallet, send Bob's TRISA data to A VASP
4. Transfer funds from B Wallet to Bob's wallet
5. Record Alice's and Bob's data together with TxID and HC

Proposed solution #1 Pros & Cons

- Pro: we can structure the protocol so that B VASP sends Bob's PII only after receiving the tx, which makes phishing for PII prohibitively expensive
- Con: a centralized VASP address lookup service could be prone to attack and corruption.
- Con: having VASPs return their address via API call requires VASPs to implement that API and have it accessible all the time.

Proposed solution #1 notes

- Privacy enhancing, large transactions only between T.R. wallets
- Both A VASP and B VASP have full data, which can be retrieved having TX id and/or Bob’s HC (which is on blockchain)
- Can work on any chain, where a message can be transmitted.
- HC can be a digest of more information (Alice’s details for eg.)

Proposed solution #2

- Vanity Addresses
- Each VASP generates vanity addresses for clients who want to receive value greater than the proposed limit of USD/EUR 1000[1]
- Anytime a VASP is asked to send a value to a vanity address, the travel rule would apply

---

1. https://www.debevoise.com/-/media/files/insights/publications/2019/07/20190712-fatf-recommendations-virtual-assets-eng.pdf

Proposed solution #2 Pros & Cons

- Pro: if the custom component of a vanity address is sufficiently long, the costs of generating a spoofed address would be prohibitive, deterring attackers
- Con: if (vanity) it’s not long enough, attackers could spoof the address

Proposed solution #3

- Create a blockchain where each VASP claims addresses it creates
- VASP would claim the address each time it creates one
- VASP would reject or freeze incoming covered tx when the address is not on the chain
- The chain may be consensus-based (no mining) making its maintenance cheaper
- Only address->VASP link is exposed, getting the PII still needs signed TRISA protocol request
- VASP clients still can have small-money addresses which are not advertised on the chain

Proposed solution #3 Pros & Cons

- Pro: VASPs already have mechanisms to work with existing blockchains - these can be extended to work with this lookup process.
- Con: incentive mechanism to maintain this VASP lookup blockchain is TBD
- Con: mechanism for invalidating addresses that are no longer in use by a VASP is TBD

QUESTIONS?