Travel Rule Research

Suggest Edits

The Verite open source repo includes some code that provides a cursory demonstration of how exchanging verifiable credentials could be a core component of scalable and open ecosystems for financial institutions to comply with Travel Rule reporting obligations with minimal privacy, data leakage, and security risks.

In addition to this high-level "proof of concept," long-tail research in ongoing into FATF use cases forming a cornerstone of Verite in the latter part of 2023.

Please note: TRUST, TRISA, and other protocols that currently do not use Verifiable Credentials as an exchange format for FATF counterparty reporting are in no way incompatible with this group's approach; our goal is to focus on the privacy risks and protocols for mutual discovery and interactions, which can bootstrap any protocol between financial institutions once validated.

The core problems of our FATF research group, aka "The Travel Rule"

The "Travel Rule" refers to the U.S. Bank Secrecy Act rule as well as guidance defined by the international Financial Action Task Force (FATF) Recommendation 16 . The Travel Rule requires Financial Institutions (FIs) and what FATF refers to as Virtual Asset Service Providers (VASPs) to exchange and analyze specific PII data about the originator and beneficiary of a given transaction when such a transaction exceeds a threshold of notional value (the threshold is 3000 USD value for the US BSA version and 1000 USD/EUR value for FATF version). The purpose of these regulations is to police financial crime such as money laundering, block terrorist financing, stop payments to sanctioned entities and countries by requiring intermediaries to report threshold-exceeding transaction and combine those reports with other monitoring to detect and investigate suspicious activities. Since most prosecution and tort discovery of these crimes leans heavily on forensics, this reporting is often archival in nature and format.

Mapping Travel Rule requirements to blockchain transactions poses several challenges. One such problem is "discoverablility" -- knowing when a beneficiary/recipient address is managed by a financial institution and therefore when Travel Rule obligations exist, and furthermore how to contact the recipient institution to execute secure counterparty data exchange. At broadcast time, the originator of a blockchain transaction has no means of knowing whether a recipient address is custodied by a financial institution or VASP, much less which one, and furthermore no means of directly contacting the owner or custodian of that address.

The crypto ecosystem has proposed many potential solutions to this problem over time:

- maintaining registries of known blockchain addresses mapped to VASP network endpoints,
- maintaining a network of VASP nodes which FIs can query/poll prior to transaction broadcasts,
- leveraging analytics services and tools that glean metadata about addresses and make inferences about their level of safety,
- transacting only on permissioned networks or specific chains designed with different identity capabilities,
- introducing new identifier schemes for transacting customers
- many hybrids and combinations of these approaches

Many of these approaches are either greenfield approaches requiring vast, new platforms to be established quickly, or empower dangerously omniscient data barons to be the only possible middlemen regulators and end-users alike can trust to enforce reporting and monitoring. The governance of those platforms and/or middlemen poses, for us, a real challenge to the "opt-in", pseudonymous-by-default ethos of web3, but proposing a cogent, researched, prototyped alternative is worth a thousand eloquent critiques so we have been working on the former rather than stacking up the latter.

The approach

Our design goal in our research and design has been to focus on the privacy problems of discoverability and trust establishment between VASPs and FIs (and perhaps even self-custodied wallets!), imagining an open platform that does not compromise the anonymity guarantees of today's blockchains and marketplaces.

The Verite research group has sketched out a "Verite-maximalist," privacy-preserving architecture for solving these problems by: 1.) using a decentralized bulletin board discovery mechanism for wallet custodians (or, theoretically, a sufficiently sophisticated VC-enabled self-custody wallet!) to discover one another, then 2.) querying public, verifiable information about custodians and/or exchanging private verifiable credentials about self-custody counterparties (if accepted by the former) to mutually authenticate a secure channel, and only then 3.) bootstrapping a mutually-secure connection verifiable credentials exchange about the controllers of both wallets.

Note: The "travel rule" demo in the Verite codebase on github demonstrates one implementation of 1, which we call the "mempool" implementation of a "bulletin board" messaging-based discovery architecture; 2 is still in research phase; and 3 can be achieved today by protocols like TRUST or TRISA, albeit not yet in verifiable credential form.

Discovery and Credentials Exchange Sequence

Note, the following diagram reflects the prototype on github, which predates much of the exploratory/theoretical design work of the FATF working group within Verite's open-source development initiative. The text below presents an expanded, more detailed view; for an understanding of the prototype, refer to the diagram wherever the two differ.

Part 1: Discovery and Proving Control of Blockchain Addresses

Crucial to the design of our system is some kind of bulletin board system which can be conceived of as a miniature "mempool", i.e. a smart contract that hosts ephemeral messages posted publically for the express purpose of being responded to privately by self-authenticating parties.

Before an intended/proposed transaction is broadcast, the sending and receiving FIs use this chain-agnostic "bulletin board" to publish and observe messages establishing and requesting proof of address control.These messages contain no customer data and no specific transaction data other than therecipient address (hashed) and the identity of the sender'scustodian .

Since the transaction amount is not included, observers are unable to determine information about the planned transaction other than its intended origin and destination (this is less information than is available in the EVM-wide mempool, for example, which broadcasts entire transaction ready to be added to blocks). This allows counterparty endpoints to find and connect to one another privatelybefore exchanging counterparty information, and the mutual exchange of proof-of-control credentials for both addresses prevent any other party from spoofing the originator or beneficiary.

1. Alice, the originator, initiates a transfer with her financial institution, which operates a hosted crypto wallet on her behalf.
2. Alice's FI forms a message (referred to here as "M1"), containing:* Request for proof of control of the beneficiary address (e.g. formatted as a Presentation Request or as aCACAO receipt
3.
   - of aSIWX message
4.
   -)
5.
   - One or more identifiers for querying and verifying the identity of the custodian initiating the message (i.e., Alice's)
6.
   - A secure callback URL endpoint for replies (e.g. a Presentation Exchange endpoint for receiving Verifiable Presentations)
7. Optionally, a "Fast mode
8. " variant of this "M1" message could also skip a step by also including:* A Proof-of-control of the originating address (formatted as a Verifiable Credential, for example, or even as a"sign-in with X" off-chain transaction message
9.
   -)
10. Optionally, Alice's FI could elect to support a "Suspicious mode
11. " (i.e. supporting an optional authentication step) by additionally including in M1:* A secure callback URL endpoint for requesting proof-of-control credentials by M1 message identifier after establishing trust (see below)
12. Alice's FI publishes M1 to the decentralized bulletin board.
13. Bob's financial institution observes M1 being emitted in the bulletin board, verifies that the recipient address is in its custody, and responds acordingly.

Part 2: Trust Establishment: i.e. Exchange of Public Credentials

The trust establishment step (which some might think of as an "anti-spam"/"anti-DoS" step to avoid spam or data-collecting crawlers) is not included in the simplified prototype in our repo. There are various prototyping efforts happening in the DIF and elsewhere that may prove adequate for this step, so we are deferring research on it in case open-source specifications get hardened in the meantime for this kind of authentication and public trust registry building.

1. If in "Suspicious Mode
2. ", Bob's financial institution would attempt to authenticate Alice's FI, the author of M1 before responding. If in "Fast Mode
3. , it couldskip to step 3
4. .
5. Bob's financial institution would authenticate Alice's FI by the identifier(s) provided in M1.* In a greenfield world, the simplest identifiers to mandate would be a short list of DID methods that support a given key/value pair in the document, such as a given
6.
   - service
7.
   - type. One simple DID method for this would be
8.
   - did:web

9.
    - , conducive to manual/human-readable fall-backs and auditability without reliance on blockchains or other novel architectures.
10.
    - That said, there are many brownfield registries and identifier networks that could easily be bootstrapped at this step. "Identifier" here refers to any key that can be used to query public registries of regulated financial institutions maintained by trusted intermediaries, competent authorities, or your friendly local trade association and open source standards organization (including a DID registered on-chain or off- with Verite!). Crucially, however, these registries should be multiple and open, to maximize spread and bootstrap an open ecosystem that is inclusive of multiple closed ones and proprietary authorities.
11.
    - This step of authenticating counterparties via registry lookups could be thought of as equivalent to fetching public credentials from authorities; direct exchange of verifiable credentials between FIs could be explored as a more disintermediated/P2P equivalent long-term.
12. Bob's financial institution verifies the originator's proof-of-control.
13. Bob's financial institution constructs message "M2" which contains:* a VC proving control over the beneficiary address or equivalent [off-chain
14.
    -] proof.
15. Bob's FI transmits M2 privately to Alice's FI using the callback URL specified in M1.
16. Alice's FI receives and verifies the VC in M2, leaving both Alice's FI and Bob's FI (a) certain that each controls the designated addresses and (b) with a private secure network connection established through the specified callback URL.

Part 3: Exchange of Counterparty Credentials

If Alice's FI determines the transaction does not meet the threshold required for the Travel Rule after establishing both Alice's and Bob's requirements by jurisdiction, then Part 3 is not necessary and does not apply, as Alice's FI can simply proceed to broadcasting the blockchain transaction.

If the Travel Rule does apply, however, both financial institutions are able to exchange counterparty verifiable credentials over callback URLs that allow for private secure communication. This can happen over any secure channel, and today is mostly done in consortium/network-like platforms that bundle the authentication of step 2 and the secure channel for step 3 (as well as data dictionaries or translation engigges for exchanging the actual information required by applicable reporting requirements, itself a massively complex value-add and rules engine). This research could be called long-tail, as the rapid pace of regulatory change here means the existing protocols will probably be distracted updating their rules engines for some time and not have bandwidth to consider harmonizing on UX and consent flows!

As a prototype of user-centric UX and an architecture that layers consent receipts on top of reporting artefacts, the Verite prototype models how identity-enabled and verifiable-credential-enabled wallets could surface meaningful and direct consent into such a flow. While traditional financial institutions typically require their users to consent to terms and conditions that grant the rights to transfer this kind of private information, this prototype of more proactive and per-interaction consent could pave the way to better support for non-custodial wallet compliance, or conformance to more aggressive regulation about meaningful consent. To address this latter hypothetical requirement, the flow presents notifications as alerts to customers so that they have visibility into when their data is requested, and to provide them the choice to cancel sending or receiving transactions that require such counterparty credentials exchange.

1. If the transaction's value triggers the Travel Rule threshold, Alice's FI responds to Bob's FI by composing a private message "M3" containing:* Transaction amount
2.
    - Alice's originating counterparty verifiable credential
3.
    - Presentation Request for beneficiary counterparty credentials
4. Bob's FI receives M3 and verifies the originator counterparty verifiable credential, and then executes its internal compliance procedures.
5. Once Bob's FI clears the information, it generates message "M4" acknowledging receipt.
6. Bob transmits M4 to the secure callback URL endpoint.
7. Alice's FI receives M4 and verifies Bob's beneficiary counterparty verifiable credential, and then has enough information to decide whether and how to proceed.[Note: this step may include multiple steps, business logic depending on jurisdiction of both parties, bootstrapping into existing travel rule PII exchange protocols, etc.]
8. Once Alice's FI clears the information, it broadcasts the planned transaction to the appropriate blockchain's [actual, public transaction] mempool to execute the exchange of value.
9. [Optional] Depending on the design of the bulletin board, M1 may need to be manually withdrawn to spare resources.

Future Development

Note that this sequence is intended only as ademonstration of how exchanging verifiable credentials may be helpful with Travel Rule requirements. We lean heavily on the expertise of companies already working in this space and protocols already in place to exchange counterparty information securely between Financial Institutions.

Production-level topics such as spam prevention in the bulletin board, cross-chain and multi-swap messaging complications, smart-contract-based wallets and other multisignature counterparties, and private key security protections are beyond the current scope and are among several subjects to address in future development and exploration. Updated3 months ago *