Tatoshi Professional – a tool to meet the "Travel Rule" requirements for Virtual Assets transfers

Providing "proof of wallet ownership" through linking the user's extended public key with his client-ID.

Tobias Kress, Treble Wallet AG, 02.12.2019

Abstract:

In June 2019, the Financial Action Task Force (FATF) released a new guidance for Virtual Asset Service Providers (VASP) making the "Travel Rule" also applicable for Virtual Asset (VA) transactions between VASPs. The FINMA regulation from August 2019 exceeds the FATF requirement by requesting the "Travel Rule" application for all blockchain transaction where a Swiss VASP is involved.

Currently, Swiss VASPs comply to this regulation by limiting transactions to external wallets that belong to their own clients. The wallet ownership is currently proven manually with a "proof of wallet ownership signature".

Tatoshi Professional provides a tool to replace the manual proof signature with a fully automated wallet ownership proof. This is achieved by linking the users' client-IDs with their extended public keys. With Tatoshi Professional, VASPs can easily and efficiently transact with their clients, without any negative impact on the client's user experience. Combined with the Tatoshi Professionals private key recovery functionality, the clients' funds on the non-custodial Tatoshi Professional wallet are as secure as funds on custodial wallets.

If serveral Swiss VASPs should use Tatohsi Professional, the ownership proof via extended public keys could be activated cross-VASP, enabling a seamless and complicant blockchain transactions, as convient as todays domestic bank transfers.

1. Acronyms and Definitions

FATF	**Financial Action Task Force** The **Financial Action Task Force** (on Money Laundering) (FATF), also known by its French name, Groupe d'action financière (GAFI), is an intergovernmental organization founded in 1989 on the initiative of the G7 to develop policies to combat money laundering. In 2001 its mandate expanded to include terrorism financing. It monitors progress in implementing the FATF Recommendations through "peer reviews" ("mutual evaluations") of member countries.[1]
FINMA	**Eidgenössische Finanzmarktaufsicht (FINMA)** The **FINMA** is the Swiss government body responsible for financial regulation. This includes the supervision of banks, insurance companies, stock exchanges and securities dealers, as well as other financial intermediaries in Switzerland.[2]
VA	**Virtual Asset** A **virtual asset** is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.[3]
VASP	**Virtual Asset Service Provider** **Virtual asset service provider** means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i) exchange between virtual assets and fiat currencies; ii) exchange between one or more forms of virtual assets; iii) transfer of virtual assets (In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another); iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[4]

[1] (Wikipedia 2019)
[2] (Wikipedia 2019)
[3] (FATF 2019)
[4] (FATF 2019)

2. Regulatory requirements and the need for a Swiss-specific technical solution

1. FAFT regulation

On June 21, 2019, the Financial Action Task Force (FATF) issued the Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.[5] The new FATF requirements expand the scope of rules on anti-money laundering and countering the financing of terrorism to virtual asset (VA) transactions and to a broad range of providers of crypto-related products and services, including but not limited to custodians and exchanges.

The biggest challenge specified through this new regulation for Virtual Asset Service Providers (VASP), is the application of the so-called "Travel Rule" (Recommendation 16) to VASPs. The "Travel Rule" requires traditional financial institutions to collect and communicate information on the originator and beneficiary of a wire transfer.

This information includes:

(i) originator's name (i.e., the sending customer);
(ii) originator's account number where such an account is used to process the transaction (e.g., the VA wallet);
(iii) originator's physical (geographical) address, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth;
(iv) beneficiary's name; and
(v) beneficiary account number where such an account is used to process the transaction (e.g., the VA wallet).

In line with the FATF's technology-neutral approach, the required information does not need to be communicated as part of (or integrated into) the transfer on the blockchain or other distributed ledger platform itself. Submitting information to the beneficiary VASP could be an entirely distinct process from that of the blockchain or other distributed ledger VA transfer. Any technology or software solution is acceptable, provided that the solution enables the ordering and beneficiary institutions to comply with the requirements of the "Travel Rule"

The FATF expects the application of the "Travel Rule" only for VA transactions between two VASPs. Sending VAs to individual users, who are not obliged entities, does not require to submit the information about originator or beneficiary. VASPs receiving a VA transfer from an entity that is not a VASP or other obliged entity should obtain the required originator information from their customer.

2. FINMA regulation

Swiss FINMA was the first national regulator to implement this new recommendation. On August 26, 2019, they released the FINMA Guidance 02/2019 ("Payments on the blockchain"), specifying the "Travel Rule" application for financial services provider under the FINMA supervision.[6]

[5] (FATF 2019)
[6] (FINMA 2019)

The current FINMA regulation provides a significant deviation from the FATF recommendation by going beyond the FATFs requirements regarding the "Travel Rule" application. In contrast to the FATF recommendation, the FINMA regulation does not provide an exception for payments involving unregulated wallet providers. This means that financial services provider under the FINMA supervision must follow the "Travel Rule" requirements for all VA transactions regardless of whether the counterparty is a VASP or an individual user, who is not obliged entity.

FINMA admits that "no system currently exists at either a national or an international level (such as, for example, SWIFT for interbank transfers) for reliably transferring identification data for payment transactions on the blockchain." To comply with the regulation despite the technically missing capability of sending and receiving the information required for payment transactions on the blockchain, Swiss VASPs are only allowed to do transactions from and to external wallets, if these belong to one of the institution's own customers. "Their ownership of the external wallet must be proven using suitable technical means." Additionally, "transactions between customers of the same institution are permissible"[7]

3. Need for a Swiss-specific technical solution

The fact that the FINMA regulation extends the application of the "Travel Rule" also to payments with non-regulated wallets confronts Swiss VASPs with a major challenge in implementing this regulation. While international software providers and open source organizations are starting to provide first technical solutions for the transmission of originator and beneficiary information, these solutions are designed to work for transactions between two VASPs.

The Swiss-specific requirement to also cover transactions between a VASP and an individual user is currently not covered by any available technical solution. The transmission of origin and beneficiary information is usually carried out via a blockchain independent messaging protocol. The use of such a messaging protocol requires either a registration with the protocol provider and/or the use of technical tools, such as smart contracts. The need to opt-in for such a protocol and the lack of an international standard or market leader means that individual users would have to use a variety of messenger protocols to exchange information with their VASPs while transacting on the blockchain. This is very unlikely going to happen.

The Swiss VASP are currently facing the need of a technical solution that meets the requirements of the "Travel Rule", includes transactions with unregulated individuals and can be used without additional technical know-how or setup on the side of the individual user.

3. Market overview of technical solutions to comply with the "Travel Rule"

1. Second layer messaging protocols

Transactions on most blockchain systems are pseudo-anonymous, meaning that originator and beneficiary are identified through crypto addresses with the natural or juridical persons behind these

[7] (FINMA 2019)

addresses remaining unclear. On the blockchain protocol layer there is currently not technical possibility to transmit additional information as the originator's or beneficiary's details. Due to this restriction, FAFT and FINMA accept an information transmission separately from the original blockchain transaction.

Several second layer protocols currently exist with none of them having a significant market share or providing a market standard. These protocols are either provided by companies and offered as a commercial service (e.g. TRISA[8]) or through an open source community (OpenVASP[9]).

There are some similarities between the different solution. All use public key cryptography to authenticate the participating VASPs. While the commercial solutions mainly use own communication channels and provide the business logic on dedicated hardware, OpenVASP uses the Ethereum blockchain as their IT infrastructure. The whole protocol will be developed as a smart contract, running on the Ethereum Blockchain.

2. Proof of wallet ownership signatures

The idea of using the "proof of wallet ownership signature" as a mean to comply which the "Travel Rule", was indirectly brought up by FINMA. In their regulation they stated, that "as long as an institution supervised by FINMA is not able to send and receive the information required in payment transactions, such transactions are only permitted from and to external wallets if these belong to one of the institution's own customers. Their ownership of the external wallet must be proven using suitable technical means."[10]

The "proof of wallet ownership signature" is a technical mean to proof the ownership of a corresponding crypto address, although it is quite cumbersome and cannot be easily done by every unskilled user.

To proof the ownership of a wallet via a cryptographic signature, the following steps need to be followed:

- Client informs his VASP about his crypto address, that he would like to use to transact with the VASP
- VASP sends client an arbitrary text message via a non-blockchain related communication channel (e.g. email, SMS)
- Client signs this message with his private key, that relates to the given address and sends the signature back to the VASP
- VASP compares the signature with the give address and verifies if the signer used the valid private key related to this address to sign the message
- If the signature is valid, the ownership of this crypto address is proven. The VASP can use the address to interact with his client and meet the "Travel Rule" regulations

Due to security reasons, it is highly recommended to use a crypto address only once. For this reason, all current wallet applications provide a new address for every single transaction. This means that this

[8] (CypherTrace Inc. 2019)
[9] (Riegelnig 2019)
[10] (FINMA 2019)

manual “proof of wallet ownership signature” process must be re-done for every single transaction that a VASP would like to do with his client.

3. Evalution of currently used technical solutions to comply with the “Travel Rule”

Comparing the different approaches to comply with the “Travel Rule”, we see a difference between international and Swiss players. VASPs located outside of Switzerland or VASPs with a mainly international orientation, focus on the development of a second layer messaging protocol.

Swiss based VASPs took note of FINMA’s advice with gratitude and are mainly using external wallets of their client’s as their single point of transactions. This means that they are only transacting with external wallets that technically proven belong to their clients (see Figure 3-1). The technical proof that a wallet belongs to their clients is done with a “proof of wallet ownership signature” prior to every transaction. As most of their clients are not supervised by FINMA they do not need to follow the Travel Rule themselves and can use their external wallet to interact with any other originator or beneficiary.

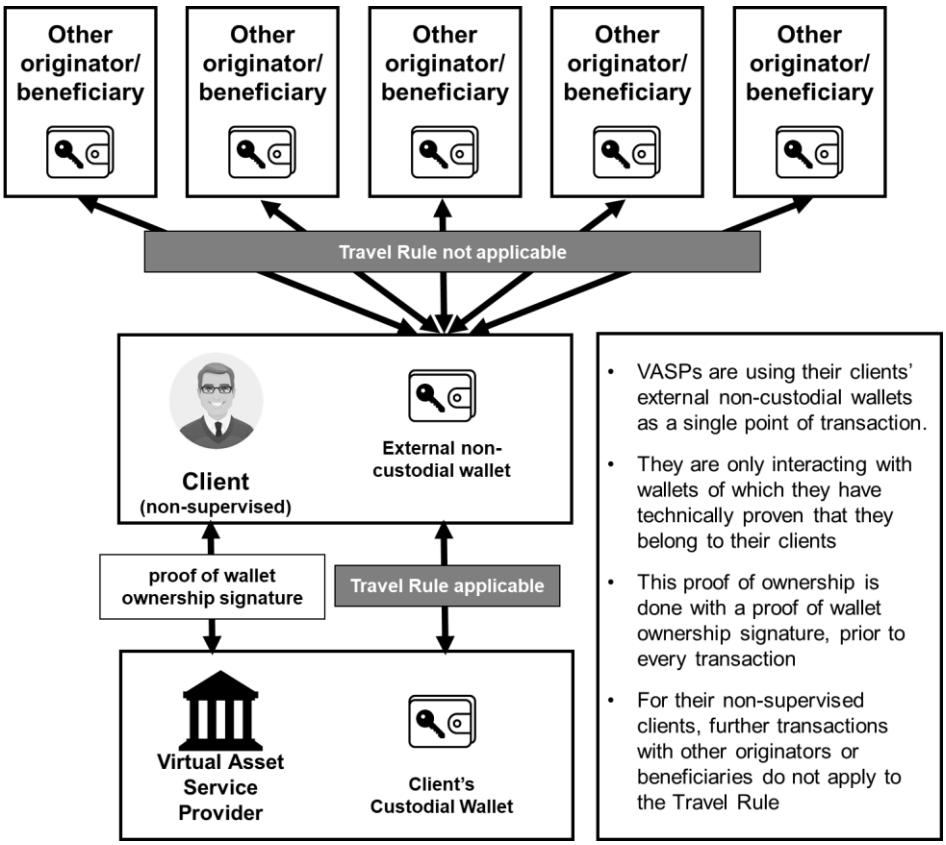

Figure 1: Ownership proven wallets as single point for transaction

We believe that the usage of an ownership proven wallet as single point of interaction is currently the most compliant and feasible way for Swiss VASPs to comply with the “Travel Rule”. On the following pages, we will show a technical solution, how the proof of ownership can be done in a fully automated

way with no manual interaction, neither on VASP-, nor on the client-side. Technical foundation of our proposed solution are extended public keys, which will be introduced in the next chapter.

4. Extended public keys

1. Hierarchical Deterministic (HD) Wallets

As described in chapter 3.2, for security reasons, a crypto address should only be used once for a single transaction, that means users should use a new address for each single transaction. This is a common understanding in the crypto industry and followed be all of today's software and hardware wallets.

While in the early days of crypto currencies, wallets were creating randomly generated private keys and related addresses for every transaction, modern wallets are no longer a bundle of randomly created keys.

Today's wallets are mainly hierarchical deterministic (HD) wallets, as specified in the BIP-39.[11] HD wallets are created from a Master Seed. Every key in the HD wallet is deterministically derived from this Master Seed, which makes it possible to re-create the entire HD wallet from that seed.[12]

If a new address is needed, the wallet will create a new private key as a child key from the previous private key. Using the elliptic curve multiplication process, a related public key is generated, which is the foundation for generating the new crypto address. This methodology was initially developed for Bitcoin but is today widely used in several hundreds of crypto currencies.

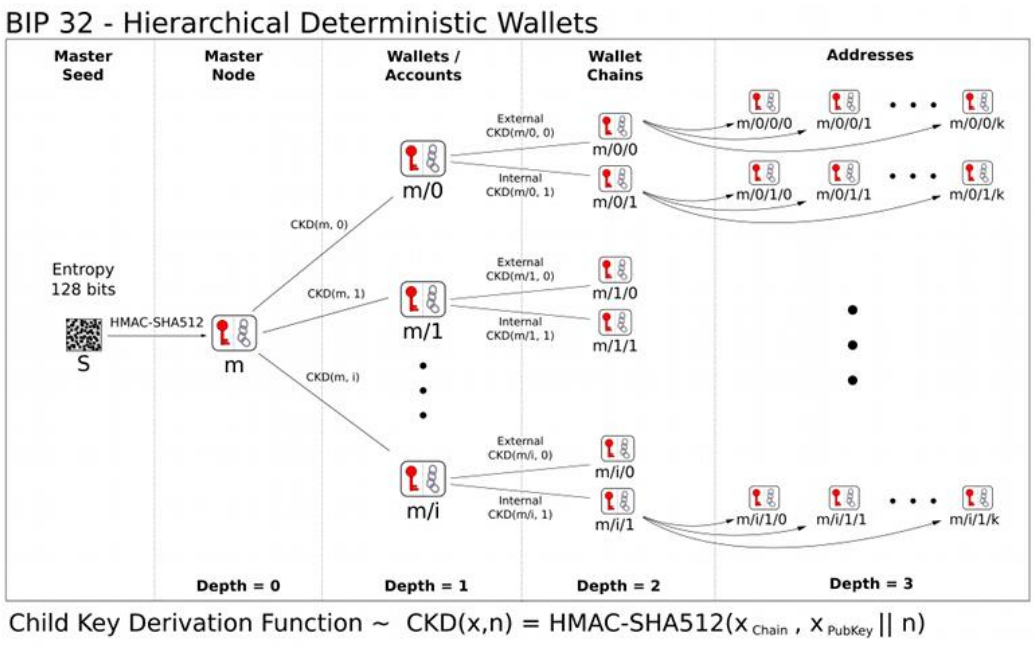

Figure 2: Child Key Derivation Function – Source: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[11] (Wuille 2012)
[12] (Antonopolous 2017)

2. Extended public keys

The extended public key is a special form of public keys, which can be created and used in HD wallets. It contains the master public key, the public key derived from the master private key, as well as deterministic random data, the so-called chain code.

The extended public key has a very useful characteristic. It enables the generation of almost an infinite amount of further public keys, without knowing the related private keys.[13] This enables the owner of an extended public key to generate new crypto address, without having any power of control over the tokens on these addresses.

Having an extended public key does not only enable you to create new addresses out of this key, it also enables you to check if a given address was derived from a specific extended public key. This function is used in the Tatoshi Professional wallet as part of the functionality to proof the wallet ownership and will be detailed in the next chapter.

5. Tatoshi Professional providing proof of wallet ownership through extended public keys

As described in chapter 3.3 “proof of wallet ownership signatures” are the preferred mean of Swiss VASPs to comply with the “Travel Rule”. This manual and cumbersome process that needs to be repeated prior to every single transaction can be automated by using extended public keys to proof the wallet ownership.

Tatoshi Professional is a non-custodial wallet that is provided by Treble Wallet AG. Clients can only use Tatoshi Professional, if their VASP has a contract with Treble Wallet AG. Based on this contract, Tatoshi Professional will be able to link the client’s extended public key with a VASP given client-ID. This allows a permanent and automated proof of wallet ownership.

To set-up Tatoshi Professional, the following steps need to be followed:

1. The VASPs hands-out a personalized activation QR-code to the client. This code contains the client-ID that was given to the client by the VASP
2. The client downloads the Tatoshi Professional app from the Appstore and scans the activation code to activate the app
3. The Tatoshi Professional app send the client-ID and extended public key to the Tatoshi server

To automatically proof the wallet ownership, the VASP can perform the following calls to the Tatoshi server.

Proof of wallet ownership for an incoming transaction:

If the VASP receives a transaction from the client, and wants to ensure that it was sent from the Tatoshi Professional wallet that belongs to his client, he sends the sender address together with the client-ID to the Tatoshi server. The Tatoshi server will check, if the sender address was derived from the extended

[13] (Antonopolous 2017)

public key that is linked to the given client-ID. If this test provides a valid result, Tatoshi server will confirm the wallet ownership.

Proof of wallet ownership for an outgoing transaction:

If the VASP wants to send tokens to the client and needs the proof to interact with a wallet that belongs to his clients, he sends the client-ID to the Tatoshi server. The Tatoshi server will derive a new address form the extended public key that is linked to the given client-ID and return it to the VASP. The VASP can use this address with proven ownership to send tokens to the client.

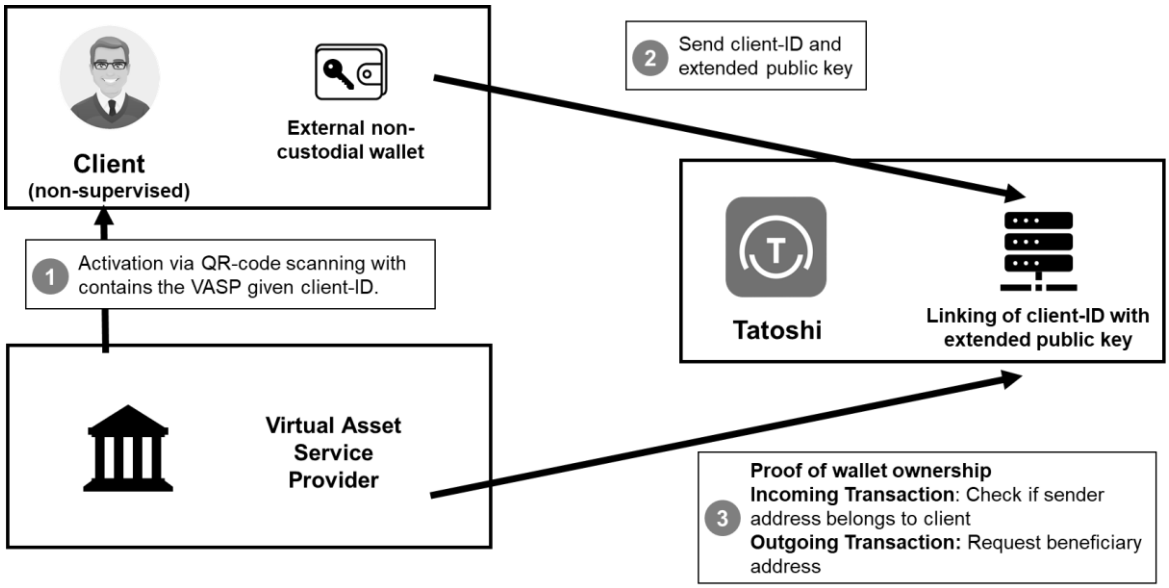

Figure 3:Linking of client-ID with extended public key and automated proof of wallet ownership

This process of proofing the wallet ownership can run fully automated. On the client side, no manual interaction is necessary. For him, the user experience is like using any other non-custodial wallet. For the VASP the wallet ownership proof can be fully automated. Two calls to the proofing webservice can be fully integrated into the VASP's back-end system. The persistent linking of client-ID and extended public key enables a tamper-proof documentation of wallet ownership.

6. Further features of Tatoshi Professional

The use of Tatoshi Professional does not only help VASPs to comply with the "Travel Rule". Tatoshi Professional provides additional features that bring value to the business relation between client and VASP.

1. Private key recovery

One of the reasons, why clients give their VAs into custody with a VASP, is that they do not want to be fully responsible for securing their private keys. With Tatoshi Professional, we can provide this security even for our non-custodial wallets by offering a private key recovery functionality. Based on a

cryptographic secret sharing mechanism, the client's private key is "cut" into 3 "parts". One part is memorable and remains with the client. The other 2 parts are shared between the Tatoshi and the VASP's servers. If the client should lose his private key, he can recover it at any time by re-combining the 3 parts together. The encryption and security features ensure that only the client can recover his private key.

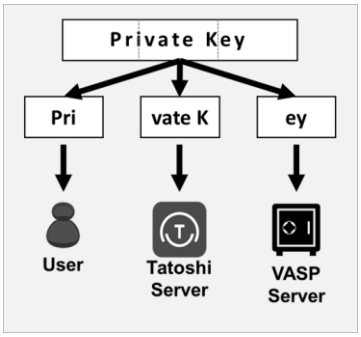

Figure 4: Private key sharing functionality

2. Secure client communication channel

The Tatoshi Professional app has integrated an instant messenger tool that enables a secure and instant communication between client and VASP and can replace other commonly used communication channels as e.g. email or public messenger apps.

3. Read-only access to clients' non-custodial wallet enabling crypto forensic

If the client agrees, Tatoshi Professional can provide a list of all used crypto address to the VASP, enabling a read-only access on the client's non-custodial wallet. This can be used by the VASP to do forensic research on the tokens in the non-custodial wallet. Through these investigations they can ensure not to receive any "tainted coins", tokens that have been involved in any criminal actions. Additionally, this read-only access can be helpful if the VASP would like to integrate the tokens in the non-custodial wallet into his reporting or charge a fee for funds on this non-custodial wallet.

7. Conslusion

Considering the current regulatory framework, the best practice for Swiss VASPs to comply with the "Travel Rule" is to do transactions only with external wallets, which technically proven belong to their clients. Most Swiss based VASPs follow this practice by proofing the wallet ownership with a "proof of wallet ownership signature". This requires a manual, cumbersome verification process that needs to be repeated prior to every single transaction.

The use of extended public keys linked to the client-ID enables a fully automated and integrated wallet ownership proof as well as an electronically and tamper-proof documentation. With Tatoshi

Professional, VASPs can easily and efficiently transact with their clients, without any negative impact on the client's user experience.

Combined with Tatoshi Professionals private key recovery functionality the clients' fund on the non-custodial wallet are as secure as funds on custodial wallets.

8. Outlook

Tatoshi Professional provides a tailor-made solution for Swiss VASPs. If several Swiss VASPs should decide to use Tatoshi Professional, and with given clients' consent, the Swiss VASPs could join their extended public key and client-ID mapping tables. As all clients of Swiss VASPs are identified following the same KYC/AML standards, a Swiss-wide wallet ownership approval function would enable direct transactions between clients of different Swiss VASPs. This would enable transactions as easy and compliant as domestic bank account transfers.

9. References

Antonopolous, Andreas. 2017. *Mastering Bitcoin.* O'Reilly Media Inc. .

CypherTrace Inc. 2019. *Travel Rule Information Sharing Architecturefor VirtualAsset Service Providers(TRISA).* CypherTrace. https://ciphertrace.com/wp-content/uploads/2019/08/TRISA-Enabling-FATF-Travel-Rule-V4.pdf.

FATF. 2019. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.* Paris: FATF. www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html.

FINMA. 2019. *FINMA Guidance 02/2019 "Payments on the blockchain".* Bern: FINMA. https://finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20190826-finma-aufsichtsmitteilung-02-2019.pdf?la=en.

Riegelnig, David. 2019. *OpenVASP:An Open Protocol to Implement FATF'sTravel RuleforVirtual Assets.* OpenVASP. https://www.openvasp.org/wp-content/uploads/2019/11/OpenVasp_Whitepaper.pdf?cache=1.

Wikipedia. 2019. *Financial Action Task Force on Money Laundering.* 12 02. https://en.wikipedia.org/wiki/Financial_Action_Task_Force_on_Money_Laundering.

—. 2019. *Swiss Financial Market Supervisory Authority.* 02. 12. https://en.wikipedia.org/wiki/Swiss_Financial_Market_Supervisory_Authority.

Wuille, Pieter. 2012. *BIP 32: Hierrarchical Deterministic Wallets.* 11. 02. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki.