IEEE ICBC'24 1570982156

FATF Travel Rule's Technical Challenges and Solution Taxonomy

***Abstract*—Virtual assets are globally recognized as a decentralized digital currency system. They are also being used to transfer criminal proceeds. In 2019, the Financial Action Task Force mandated the Travel Rule for virtual asset service providers (VASPs). However, as of 2023, it has not been fully implemented worldwide due to the Sunrise issue. Complying with the Travel Rule poses challenges such as identifying the recipient VASP from a virtual asset address, proving ownership of the address, and ensuring communication protocols between the VASPs. In this paper, we focus on these three challenges and provide potential approaches for each, along with additional considerations. We have analyzed multiple existing protocols and categorized their characteristics. Our findings revealed that the majority of them are based on an alliance by VASPs, while there are a few solutions that suggest peer-to-peer messaging for every VASP or blockchain as a communication hub. Additionally, we offer insights into open challenges that need to be solved in long term.**

***Index Terms*—virtual asset, cryptocurrency, FATF, travel rule, VASP, anti-money laundering, compliance**

I. Introduction

Virtual assets (VAs), also commonly known as cryptocurrencies, are recognized worldwide as decentralized digital currency systems. Various VAs are used as investment instruments, but they are also being used as a means to transfer criminal proceeds. To fight against such illegal activities, the Financial Action Task Force (FATF) has mandated the Travel Rule for VA transfers, which is an information collection obligation about senders and recipients to virtual asset service providers (VASPs), such as exchanges.

From the perspective of VASPs, the regulation comes with several technical challenges, such as the discovery of the receiving VASP for each VA transfer and the establishment of communication protocols between VASPs. Still, it can be said that proper Anti-Money Laundering / Combating the Financing of Terrorism (AML/CFT) efforts must be made so that VAs become widely accepted financial instruments and aim for the future prosperity of the VA economy. Thus, interoperability between any VASPs and the efficiency and effectiveness of the implementation is critical.

Compared to the entire history of VAs since 2008, beginning with Bitcoin, the Travel Rule for VAs is a new initiative proposed in 2018, and the established research literature is limited. Several vendors have developed solutions to implement the Travel Rule, but none of them have become the vast majority. It is hard to say that the domain knowledge available to stakeholders is well organized. Therefore, systematically organized literature from a neutral perspective is necessary.

We aim to overlook the entire picture of the Travel Rule and help VASPs, Travel Rule solution providers, regulatory authorities, and researchers understand the ecosystem. Our contributions in this paper are as follows:

- We will aggregate knowledge about the Travel Rule based on public information sources.
- We will list the technical challenges the industry faces in implementing the Travel Rule.
- We will also organize, analyze, and categorize currently available solutions as of December 2023.

The authors have experience developing blockchain analysis software and are currently in a position to implement the Travel Rule at a VA exchange. We believe the information depicted in the paper is neutral and fills the gap of generally available knowledge.

The composition of this paper is as follows. In Section II, we will explain the mechanism and rationale behind money laundering through VAs and the efforts of the FATF to regulate it. In Section III, we will revisit the definition of the FATF's Travel Rule for VAs. We will also describe the current legislative situation in major countries and mention the "Sunrise issue". From Section IV to Section VI, we will discuss the challenges that VASPs and the industry will inevitably face in implementing the Travel Rule. In each of these sections, we will describe the overview of the issue, list several possible solutions, and delve into further minor issues that each option entails. In Section VII, we will observe major Travel Rule solutions and systematize how solutions are combined. After we discuss open challenges and other general issues in Section VIII, we conclude in Section IX.

We follow the FATF terms for technical vocabulary[1]. Virtual currency, cryptoassets, or similar financial instruments are referred to as virtual assets (VAs). Exchanges or similar entities as virtual asset service providers (VASPs).

II. Background

A. Virtual Assets and Criminal Activities

Many VAs, such as Bitcoin [1] and Ethereum [2], are recorded using blockchain technology [3]. The information on the blockchain is maintained on each participating node on the Internet and synchronized worldwide. VA holders can transfer their assets by specifying a VA address and an amount. These features enable payment regardless of the purpose or recipients. In particular, in countries and regions where administrative, judicial, or financial institutions are corrupt, VAs serve as a trusted financial infrastructure compared to legal currencies. There is no risk of payment being tampered

[1]The list of abbreviations in the paper are available in Appendix A.

with or obstructed, no demands for bribes, and the privacy of both the sender and recipient is protected.

Despite its advantages, these characteristics are convenient for criminals. Since a VA holder cannot be easily identified from their address, it is possible to send criminal proceeds without being noticed by law enforcement agencies. Also, the ease of making cross-border transfers could facilitate illegal funding for organized crime or terrorism [4]. In fact, VAs are used as a means of payment on dark web markets to hide the identities of both sellers and buyers, where illegal drugs, counterfeit identification documents, and other unlawful materials are on sale over anonymous network connections such as Tor [5].

While there are some techniques known to deanonymize blockchain transactions, there are also VAs that have privacy-enhancing features in the underlying blockchain, providing resistance against such analysis. For example, Ben-Sasson et al. developed Zcash [6] based on their earlier work on zk-SNARKs [7]. Zcash allows users to create a shielded transaction, whose sender can hide the destination and the amount from anyone else other than themselves and the recipient. Monero [8] uses ring signatures and confidential transactions to accomplish a similar goal. These blockchains have demonstrated the potential of advanced cryptography in the use of the blockchain field. However, there is a significant risk that unlawful proceeds are exchanged over these blockchains. FATF referrs to such VAs as Anonymity Enhanced Coins (AECs), and VASPs in some jurisdictions are prohibited from offering services related to AECs.

A mixing technique is also known to enhance privacy and anonymity. CoinJoin aggregates Bitcoin withdrawals from multiple users into a single transaction, obscuring the flow of funds [9]. Privacy-focused wallets like Samourai Wallet and Wasabi Wallet have these features built-in [10]. Tornado Cash, a distributed application on Ethereum, mixes Ether and ERC-20 on the same principle using zk-SNARKs. While these mixing services are convenient for legitimate users who want to maintain their privacy, they are frequently used by criminals. The developers of Tornado Cash have been indicted by financial authorities, knowing that it was being used for money laundering exceeding 1 billion USD [11].

Recently, criminals may use bridge services that enable the transfer of assets between different blockchains to move illicit funds from one cryptocurrency on a blockchain to another. According to Elliptic's analysis, the techniques used to evade blockchain analysis have shifted from mixing to cross-chain methods since August 2022 [12]. This shift is said to be a response to the sanctioning of Tornado Cash.

B. Law Enforcement Efforts

Blockchain analysis tools are used by law enforcement agencies to combat criminal activities involving VAs. One of the first techniques employed by these tools is the common-input-ownership heuristic. This method guesses multiple addresses that are controlled by the same owner [13].

Law enforcement agencies monitor transactions involving known addresses identified as illegal entities and track the flow of funds. When the illegal funds have been deposited into a VASP address, law enforcement will try to identify the account owner using search warrants and other legal means. If a suspect is arrested and the private keys for the addresses are found from the seized devices, such a fact will be used as strong evidence of the involvement of the arrested suspect.

However, it is extremely difficult to resolve cases when cross-border transactions are involved across multiple jurisdictions. For example, one of the convicts was detained in Greece in 2017, who conducted a cyber attack against Mt. Gox, a Bitcoin exchange in Japan between 2011 and 2014 [14]. He was eventually indicted in the U.S. in 2023 for laundering the stolen funds by running another exchange, BTC-e [15].

The methods used by attackers have become more sophisticated in order to evade judicial enforcement. Data processing technology for analyzing related transactions across multiple blockchains is becoming increasingly important.

C. Overview of FATF's Regulation

The FATF has documented the FATF Recommendations [16], which dictate AML/CFT measures for countries and their private sectors. These recommendations are applied to over 200 jurisdictions worldwide, either directly through FATF membership or indirectly through FATF-Style Regional Bodies (FSRBs). Participating countries are subjected to regular mutual evaluations to ensure legislative alignment, and the evaluation reports are made public. Each country is expected to enact laws that align with the recommendations.

Money laundering is understood to involve three steps:

1) *Placement* where criminal proceeds are deposited into the financial network.
2) *Layering* where illegal funds are transferred repeatedly or mixed with legitimate funds to obscure the origin and involvement in the crime.
3) *Integration* where the illegal funds are invested in legitimate assets, e.g., real estate, to legitimize them and generate seemingly lawful profits.

Among these, preventing (1) placement and (2) layering is particularly important for VAs, and the FATF urges each country to establish regulations for VASPs.

As a measure against (1) placement, the FATF requires all financial institutions including VASPs to conduct customer due diligence (CDD). A compliant institution can prevent high-risk users from opening accounts through a process known as Know Your Customer (KYC). This involves verifying the identity of customers by reviewing legal identification documents and their authenticity, as well as conducting searches across various sources, such as sanction lists, prison inmate registries, or newspaper archives.

As a measure against (2) layering, the FATF requires both the sending and receiving institutions to collect and verify the identity of both parties involved in a transfer. The sending institution must transmit customer information to the receiving institution, a requirement known as the Travel Rule. This

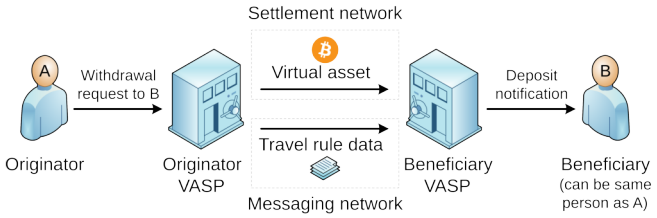

Fig. 1. Travel Rule at its Heart

allows the receiving institution to verify the sender's identity and prevent the inflow of criminal funds. In case of suspected involvement of high-risk users, an institution should file a suspicious transaction report (STR) and retain all records for five years to cooperate with investigative authorities.

III. Status Quo of Travel Rule

A. Details of Travel Rule

The Travel Rule is widely, albeit inaccurately, known as the obligation to transmit the sender's information from the originator VASP to the receiving VASP when a user requests a VASP to withdraw VAs to another VASP. We will clarify the details of the stipulation, based on Recommendation 15 (New technologies), Recommendation 16 (Wire transfers), and their Interpretive Notes, as this will serve as the premise for the rest of this paper.

In the FATF Recommendation, the sender is referred to as the *originator*, the recipient as the *beneficiary*. For the rest of the paper, We will follow these.

As outlined in Figure 1 and Table I, VASPs are obligated to comply with the following requirements regarding the transfer of VAs:

- The originator VASP and the beneficiary VASP must obtain and retain personally identifiable information (PII) about both the sender and the recipient.
- The originator VASP must transmit PII of both the sender and the recipient to the beneficiary VASP.
- Both VASPs must ensure the accuracy of PII for the user on their sides.

These apply when a customer sends VAs held in a VASP account to an account on another VASP, regardless of whether the destination account is owned by the sender or a different person or entity.

We do not consider intermediary VASPs in this paper because VAs are typically transferred directly, although intermediary VASPs, if any, has an obligation similar to a correspondent bank in cross-border wire transfers. Additionally, we consider all VA transfers as cross-border for simplicity of the discussion while the obligations slightly differ between domestic and cross-border transfers.

The PII must include the following:

- Name, typically the legal name for natural persons and the registration name for legal entities.

TABLE I
Obligation of VASPs

	Originator VASP must		Beneficiary VASP must	
collect	√	√	√	√
ensure accuracy of	√			√
conduct screening with	√	√	√	√
send to other VASP	√	√		
information of	originator	beneficiary	originator	beneficiary

- Account number of the account used to process the transfer, such as the user ID within the VASP or VA address.
- (For the sender only) Address, national identification number, customer identifier, or date and place of birth.

The PII must be transmitted either before or simultaneously with VASP-to-VASP transfers exceeding a value of 1,000 USD / EUR. However, this obligation does not apply to transfers involving addresses not managed by VASPs, i.e., unhosted wallets. Both VASPs must conduct CDD based on the PII collected and process or reject the transaction as necessary. The PII must be retained for five years and disclosed to legal authorities upon requests.

As mentioned in Section II-C, each country has to legislate in alignment with the above requirements, as the FATF Recommendations are inherently applied to countries and not private sectors. In practice, as an exception, it is common to exclude the enforcement of the Travel Rule for transfers to VASPs in non-FATF/FSRB member countries or regions.

B. Sunrise Issue

As depicted in Figure 2, VASPs that comply with the Travel Rule inevitably fails, if the VASP on the other side is not compliant. This is due to the fact that the implementation timeline for Travel Rule regulations varies across countries. In some jurisdictions, VASPs are already required to comply with the Travel Rule in their local law, while in others, transfers are executed without the transmission of PII as the Travel Rule has yet to be enacted. This legislative timing difference is known as the Sunrise issue [17], [18].

The Sunrise issue has a significant impact on compliant VASPs as there is a risk of violating the Travel Rule if the counterparty involved in the transfer is non-compliant. When a compliant originator VASP is unable to communicate with a non-compliant beneficiary VASP, the originator VASP fails to transmit PII. Similarly, a compliant beneficiary VASP cannot receive PII from a non-compliant originator VASP and therefore cannot conduct CDD against the sender.

On the other hand, VASPs in countries that have not yet enacted the Travel Rule may find it challenging to comply. It is reasonable for VASPs to be hesitant in incurring extra costs without legal enforcement, especially considering that the Travel Rule involves multiple parties. Additionally, there may be conflicts with privacy protection laws that prevent VASPs from transmitting PII.

In response to this situation, the FATF is urging countries that have not implemented the Travel Rule to expedite legis-

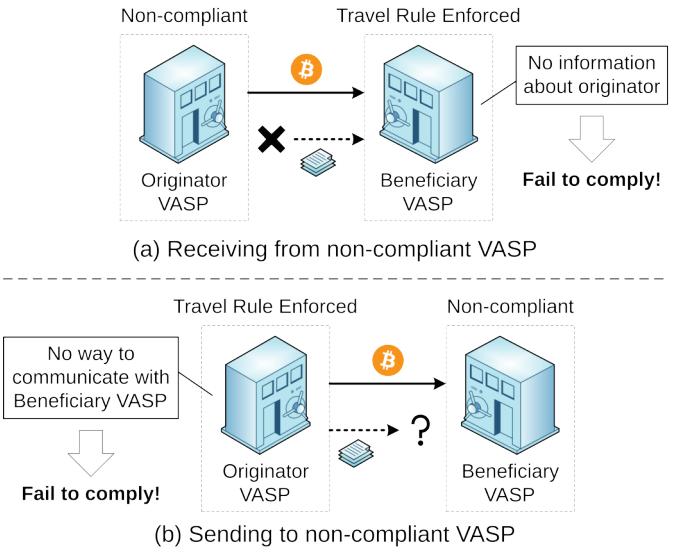

Fig. 2. Sunrise Issue

lation to resolve the Sunrise issue. They are actively engaging with jurisdictions to assess the effectiveness and operationality of the laws that have been enacted.

C. Messaging Format

IVMS 101 [19], established by the Joint Working Group (JWG) on interVASP Messaging Standards, defines the schema of information exchanged between VASPs for Travel Rule compliance. The purpose of it was to establish a common data model agreed upon by VASPs worldwide.

The JWG has referred to various standards, such as the SWIFT message format, ISO 20022 [20], or Legal Entity Identifier [21], during the design process to ensure interoperability. It has considered the business practices and cultural backgrounds of each country, resulting in the adoption of, for example, multiple representations of a natural person's name and transliteration support for characters other than the alphabets used in the western countries.

IVMS 101 does not specify serialization, encoding, or encryption methods to keep it simple as a data model. Specific communication protocols are to be defined separately, and in practice, they are left to the discretion of each VASP.

D. Overview of Current Technical Challenges

There are three major technical challenges in implementing the travel rule. These challenges are outlined below in the order they occur in the travel rule procedure.

1) Destination VASP Identification: To ensure that the PII is transmitted to the correct recipient, a originator VASP needs to identify the controlling VASP of the destination address. If the address belongs to an unhosted wallet otherwise, the originator VASP would like to know it as well. Various approaches exist to address this challenge, such as utilizing a central database of addresses or reaching out to other VASPs to inquire if they manage the address. It will be discussed in Section IV.

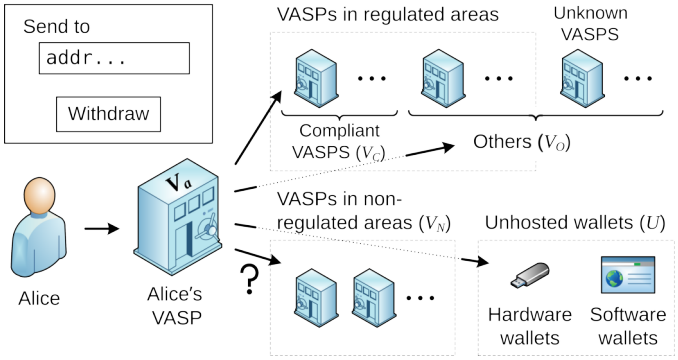

Fig. 3. Challenge on Destination VASP Identification

2) Proof of Address Ownership: Let's focus on the beneficiary VASP. If a VASP wants to demonstrate that they have control over a specific VA address to someone else, it can be challenging. It is because an address can be derived from a public key but not the other way around in many VA systems. As a result, it is difficult for others, e.g., the originator VASP, to verify if the VASP possesses the corresponding key to an address. This issue was known by VASPs before the travel rule, to prove their ownership of VAs during the audit process, known as Proof of Reserve. Hardjono et al. have conducted a study on various methods for attestating VASP's wallets [22].

Depending on the architecture, the beneficiary VASP may provide a cryptographic proof either in real-time to the originator VASP, or prior to the transaction through registration to a centralized VA address directory, if one exists. The VASP may also ensure the control of the address through other means, such as a legal guarante. The current approaches used by VASPs will be discussed in Section IV.

3) PII Transmission Interface: After the originator VASP identified the beneficiary VASP, they need to negotiate to establish a communication channel between them.

The most decentralized approach involves each VASP establishing a direct peer-to-peer communication channel with every other VASP. Conversely, the most centralized approach is to maintain a jointly managed VASP directory, which allows an originator VASP to easily find the communication endpoint for the beneficiary VASP. However, these two methods represent the extreme ends. In practice, a more balanced solution can be achieved by forming alliances among multiple VASPs. Details on this challenge will be discussed in Section VI.

IV. Challenge 1: Destination VASP Identification

Consider a scenario depicted in Figure 3. *Alice* requests to transfer VAs from a VASP, V_a, to *Bob*'s address, *addr*. Upon the withdrawal request, V_a ask *Alice* to provide *Bob*'s PII and his VASP. Note that *Alice* and *Bob* may be the same person.

Alice may provide false information to V_a, either by mistake or deliberately. Therefore, regardless of *Alice*'s declaration, V_a needs to determine whether *addr* is controlled by one of:

V_C) VASPs that complies with the Travel Rule and has a known communication channel,

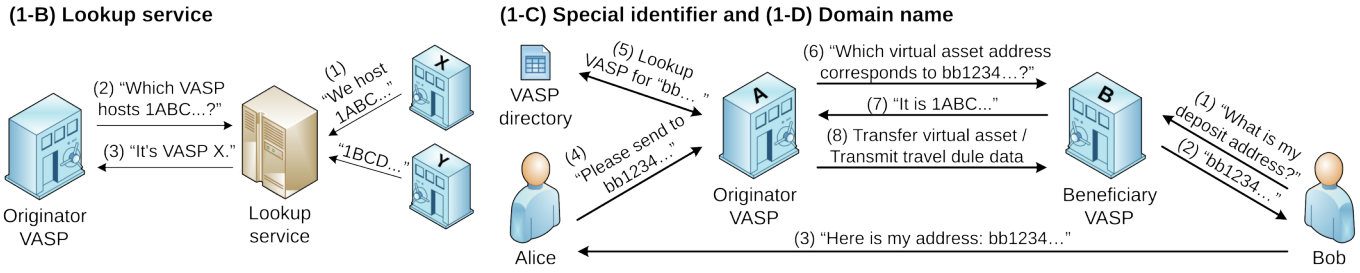

Fig. 4. Possible Approaches for Destination VASP Identification

V_N) VASPs that is neither in a participant country of FATF/FSRB nor in a FATF blacklist country and has no obligation to comply with the Travel Rule, or

V_O) other VASPs with no known communication channel,

or *addr* is one from:

U) unhosted wallets.

As per the Travel Rule compliance, V_a can proceed with the transfer if $V_b \in V_C$, with sending PII of *Alice* and *Bob*, or $V_b \in V_N \cup U$ without sending PII. V_a must reject the withdrawal request to V_O.

Approach 1-A. Restricting Withdrawal Destinations

V_a can mandate *Alice* to declare that the withdrawal is either to V_N or U. However, this method would be difficult to justify from a business perspective, considering the fact that the major global VASPs are located in FATF member countries. Furthermore, this method does not address the possibility of *Alice* making false declarations.

Approach 1-B. Using Lookup Service

Suppose a *lookup service* exists to find the controlling VASP of *addr*. V_a can use the lookup service for *Alice*'s withdrawal request. As a basic idea, if the lookup service responds with $V_b^\star$ as the controlling VASP of *addr*, then V_a transmits PII to $V_b^\star$. Otherwise, V_a may consider it unhosted. Figure 4 illustrates the approach.

V_a may additionally use a blockchain analysis tool if available. Tools typically provide some guess if any withdrawals from *addr* was performed in the past. On the other hand, they may not be able to identify newly generated addresses and may respond as unknown. Many tools report the result with a probability, and we only consider the most likely candidate here for simplicity.

Algorithm 1 illustrate a typical decision algorithm that V_a can use. Lookup returning V or nil denotes the query to the lookup service. Analyze returning V, U or unknown denotes the query to blockchain analysis tool.

In the algorithm, let *Alice*'s declaration about *addr* be denoted as V_b, which is one among $V_C|V_N|V_O|U$.

First, V_a checks if V_b is not V_O, or rejects the transfer request. In reality, some VASPs proceed with the transfer without PII transmission, although non-compliant, as a compromise due to the Sunrise issue.

Algorithm 1 Decision flow of withdrawal compliance and destination

```
V_b ← Alice's declaration about addr
if V_b ∈ V_O then
    return (no, V_b)                          ▷ non-compliant
else
    V_b^⋆ ← Lookup(addr)
    if V_b^⋆ ≠ nil then
        if V_b = V_b^⋆ then
            return (yes, V_b)                 ▷ truthful declaration
        else
            return (no, V_b^⋆)                ▷ possible false declaration
        end if
    else
        V_b^• ← Analyze(addr) || unknown
        if V_b = V_b^• || V_b^• = unknown then
            return (yes, V_b)                 ▷ presumably truthful
        else
            return (no, V_b^•)                ▷ possible wrong analysis
        end if
    end if
end if
```

Next, suppose a registration for addr by $V_b^\star$ is found in the lookup service. If V_b matches with $V_b^\star$, then V_a can confidently proceed with the PII transmission to V_b. Otherwise, customer support will contact *Alice* and perform additional verification regarding the purpose of the transfer. It may be necessary to reject the transfer or file an STR depending on the situation.

When no record is found about *addr*, e.g., in the case where V_b fails to register with the lookup service, V_a may perform an analysis of *addr*. Let the analysis result be denoted as $V_b^\bullet$, one among $V_C|V_N|V_O|U|\texttt{unknown}$.

If $V_b = V_b^\bullet$ or $V_b^\bullet = \texttt{unknown}$, i.e., *Alice*'s declaration matches with the analysis result if available or the tool did not have insights about the address, then V_a should proceed based on *Alice*'s declaration. That is, initiate the virtual transfer with the transmission of PII to $V_b^\star$ if it is (V_C), or without if it is (V_O) or (U). Although additional verification for risk assessment may be preferred in the latter case, it does not immediately constitute a violation of the Travel Rule.

Otherwise, such in the case where *Alice* declared as unhosted while the tool responded with a VASP, V_a may need to consider the possible analysis error, and adjust its response depending on the tool's confidence on result.

Several considerations must be made for this approach.

1) Performance and Security of Lookup Service: Each time VASPs issue a new address to a customer, they are required to register it with the lookup service. The performance of this lookup service is crucial for facilitating any VA transfers for participating VASPs, making it a vital and indispensable system. The implementation of the lookup service does not necessarily need to be centralized; it could also be decentralized, and it is technically feasible to record in the same blockchain as the *addr*. Nonetheless, any architecture needs to be resilient against failure or attacks. For example, we need to consider the possibility of Denial of Service (DoS) attacks through the mass registration of fake addresses.

2) Data Governance and Access Control: From a privacy perspective, it is not suitable to allow public access to the lookup service's database. Ideally, only the VASP that needs to initiate a transfer to a specific *addr* should have the ability to look up *addr*, and only during the transfer process. Therefore, it is important for the lookup service to implement proper access control and rate limiting.

Another concern is that the operator of the lookup service might use the data without the consent of VASPs or end-users. This information could be valuable to blockchain analysis companies for understanding the flow of funds. One possible solution would be to hash addresses when registering, although this would make it difficult to prove ownership. This will be further discussed in the section on Section VIII-B.

3) Unregistered Addresses: VASPs are unable to lookup unregistered addresses, which means that V_a might incorrectly classify *addr* as *U* if V_b fails to register it. This highlights the significance of blockchain analysis tools as a supplementary aid to the risk-based approach for AML/CFT [23], but it is worth mentioning that there can be occasional errors in the analysis. Hence, it is essential to encourage participating VASPs to register their addresses in a timely manner after generated.

4) Multiple Lookup Services: With the emergence of several Travel Rule solutions, it is now possible for a VASP to connect to multiple lookup services. In such a scenario, the VASP needs to conduct lookups simultaneously until it receives a positive response from at least one service, or until it receives negative responses from all services. This might cause a delay in the completion of withdrawals for users.

The issue of performance caused by time differences between the settlement network and messaging network has been identified during the designing of financial networks [24]. The VA transfer has to wait for the messaging to be completed, and therefore, any latency in lookup must be minimized.

5) Proof of Address Ownership: If a lookup service accepts address registrations without requiring proof of ownership, there is a risk of fraudulent registrations. This could lead to the disclosure of a customer's PII, which VASPs are unlikely to tolerate. To prevent this, the lookup service should implement a mechanism to require proof of address ownership or request a certain level of guarantee from registering parties about the accuracy of their information.

Approach 1-C. Using a Special Identifier

The use of a special identifier is an alternative to VA addresses to represent an account on VASPs. This eliminates the requirement for a lookup service. The following steps, aligned with the numbers depicted in Figure 4, illustrate the example.

(1) and (2) *Bob* first requests his deposit address at V_b and receives a special identifier $addr^\star$ (`bb1234...` in the figure) that encodes the issuer V_b.

(3) and (4) *Bob* shares $addr^\star$ with *Alice*, who requests a withdrawal to $addr^\star$ from V_a.

(5) V_a decodes $addr^\star$ to determine V_b.

(6) – (8) V_a queries V_b to obtain the actual address *addr*, and completes the transfer.

The use of specially encoded identifiers is a common practice in international banking systems for identifying recipients and their respective financial institutions. For example, the International Bank Account Number (IBAN) [25], widely adopted in Europe, encodes both the account number and the financial institution using the Basic Bank Account Number, which follows a 2-letter country code and check digits. Another example is the SWIFT Bank Identifier Code (BIC) [26], which facilitates the identification of financial institutions and their branches worldwide through an 8-character or 11-character code.

When considering the format of the special identifier, it is recommended to design the system in such a way that the original address is not included. This approach is advantageous for several reasons:

- By excluding the address from the special identifier, it can be shortened, resulting in a more concise and customizable representation.
- It prevents the possibility of *Alice* creating a false identifier to evade the travel rule.

By nature of the travel rule, V_a must establish communication with V_b for PII transmission. At the beginning of this process, V_a should redeem $addr^\star$ for *addr*.

1) Necessity of VASP Directory: In this approach, a comprehensive list of VASPs needs to be maintained. This list, referred to as a *VASP directory*, can be managed either online, allowing for centralized management and inclusion of all VASPs, or offline, where it can be cached within a VASP's internal system and periodically updated.

2) Conflict with Unhosted Wallets: In order to enable Alice to withdraw funds to an unhosted wallet, V_a must accept the withdrawal request to the conventional VA address. However, this introduces the risk of malicious *Alice* making false declarations by simply specifiying *addr* to evade the travel rule. As a result, the advantages of using the special identifier are compromised.

Approach 1-D. Using Domain Name for Transfers

As a variant to (1-C), the domain name of VASPs can be used as a part of a special identifier. This removes the need for a lookup service or VASP directory. We refer to this identifier as *Deposit URI*.

Suppose *Alice* wants to make a Bitcoin transfer to *Bob*. He provides his deposit URI `vasp-b.example/btc/12345` to *Alice*, which includes:

V_b's domain name	`vasp-b.example`
Type of VA	Bitcoin (`btc`)
Bob's user ID	12345

V_b implements a certain API on the given URI, and V_a can call this API to obtain the actual *addr*. The API specification must be pre-defined and agreed upon by VASPs.

In practice, it is reasonable to assume that VASPs have a reachable domain name on the Internet to comply with the PII transmission obligation. The structure of the deposit URI provided is just one example, and a dedicated URI scheme could be defined to clearly differentiate it from HTTPS or other protocols.

1) DNS-Specific Security Concerns: This approach entirely relies on DNS, which has a different architecture and security implications. As a result, VA transfers may be vulnerable to DNS security risks in addition to existing ones. For instance, an attacker could target a specific VASP, V_x, and potentially steal all VAs that are intended to be deposited to V_x through DNS contamination [27], [28]. Additionally, there is a potential risk of phishing attacks using similar DNS names in the deposit URI. Furthermore, if a VASP changes its domain name, the old deposit URI may no longer be valid.

V. Challenge 2: Claiming Address Ownership

The beneficiary VASP who manages *addr* may need to claim their control over the address, such as in the case (1) when the originator VASP wants to verify the correctness of the identified beneficiary VASP before initiating PII transmission, as mentioned in Section III-D2, or (2) when a lookup service wants to verify a new registration request from a participating VASP, as mentioned in (1-B).

Approach 2-A. Contractual Commitment

One possibility is that the claiming VASP provides a legal guarantee of possessing a corresponding key to *addr*. This guarantee is simply a contractual commitment.

This approach facilitates the access-controlled lookup service where only VASPs with a low-risk profile can participate, as mentioned in (1-B). It is also compatible with peer-to-peer communication between VASPs, as discussed later in (3-A), or in the creation of an alliance network mentioned in (3-C).

Although the contractual framework helps limit the risk of VASPs declaring addresses that are not under their control, it does not completely eliminate this risk.

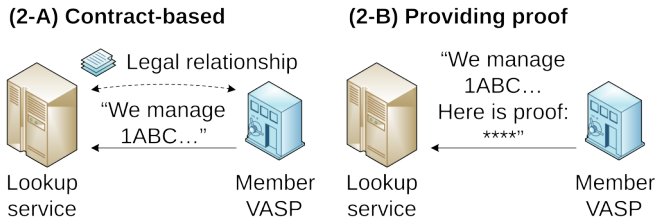

Fig. 5. Possible Approaches for Claiming Ownership of Address

Approach 2-B. Cryptographic Proof

Another option is to generate a cryptographic proof for *addr*, typically a digital signature generated from the private key of *addr*. This process is similar to signing a VA transaction for transfer from *addr*.

Assuming that V_b is making a claim of ownership for *addr* against V_a (or possibly the lookup service), the claim message *msg* that needs to be signed should contain the following fields:

- *Unique identifier* of V_b, which can be the legal name of V_b.
- *Challenge message* to ensure that the proof is generated after V_a's request, which can be random bytes specified by V_a.
- *Public key(s)*, required to derive *addr* and to verify the digital signature.
- Other optional metadata. For example, a block height or a timestamp, to associate the validity of the *addr* to the specific time on the blockchain.

To prevent the proof from being falsely reused by others, either the unique identifier of V_b or the challenge message by V_a should be mandatory in the protocol.

V_a verifies the validity of the digital signature for *msg* along with its contained fields. If valid, V_a can confidently proceed with the transmission of PII, or the lookup service can accept the registration of *addr* by V_b.

The above method works well if *addr* is simply generated from a single private key. It also works with a hierarchical deterministic (HD) wallet, which generates a set of different keys and addresses from a single master seed [29]. However, in reality, VASPs use several other different types of VA addresses which need to be taken into consideration.

- *Cold Wallet*: The key may not be available online.
- *Multisignature Wallet*, *Secret-Sharing Scheme Wallet* and *Multi-Party Computation Wallet*: Consisting key or shares may not be available simultaneously.
- *Smart Contract Wallet* or VAs with key update capability: There may be no method to derive *addr* from cryptographic keys.

We will discuss the detail on each.

1) Cold Wallet: V_b may keep the key corresponding to *addr* offline to protect against cyberattacks. This can cause delays in V_b digitally signing *msg*. In the worst case scenario, the proof may need to be deferred until the withdrawal from *addr* occurs, which is unrelated to the transfer from V_a to V_b

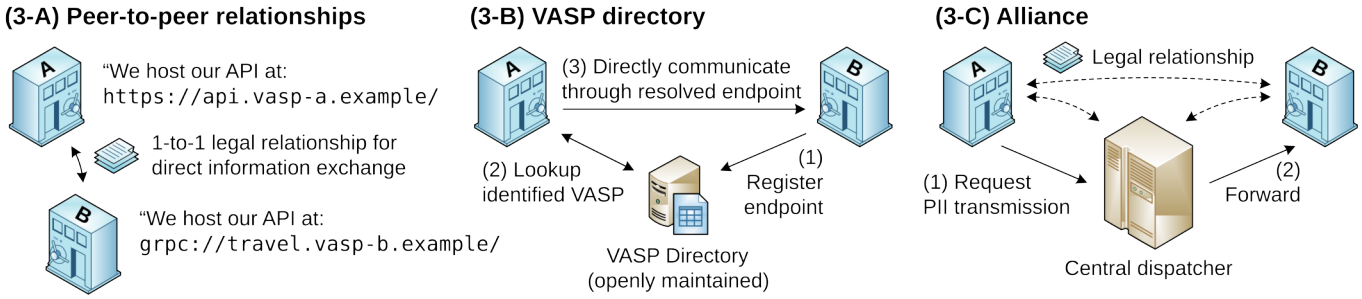

Fig. 6. Possible Approaches for Inter-VASP Communication for PII Transmission

and cannot be predicted. As a result, V_a is unable to verify that V_b possesses $addr$ at the time of the transfer.

As a solution, V_b can generate a proof for $addr$ in advance when it is initially generated in the cold wallet environment.

2) Multisignature Wallet: Bitcoin-like VAs enable a *multisignature address* that allows withdrawals when m out of n keys are used to sign the transaction [30]. A multisignature address is uniquely identified by n public keys in a particular order and the value of m. VASPs may use multisignature addresses for security or backup purposes, for example, where keys are managed individually by different officers, or some are managed offline in a secure vault.

A straightforward method for proving ownership of a multisignature address is to sign using m keys in the same manner as signing the transaction to transfer from it. However, similar to the case of cold wallets, not all m keys may be accessible at the same time, depending on how the VASPs manage them.

One possible solution is to modify the protocol so that V_b signs msg with only a single key out of the n keys. The msg should contain a list of all n keys. Once V_a confirms the validity of the signature by one of the listed keys, V_a can determine that $addr$ belongs to V_b.

Yet, this solution has a caveat. Semi-custodians [31] or a few VASPs [32] allow users to import their public key for creating a multisignature wallet. This can result in the reuse of some keys among the n keys on different VASPs.

3) Secret-Sharing Scheme Wallet and Multi-Party Computation Wallet: A single private key can be divided into multiple (n) shares with a recovery threshold (m) using cryptographic techniques. The earliest method for this is Shamir's secret sharing [33], but more sophisticated protocols have been studied as well [34]–[36]. These approaches enable VASPs to create secret-sharing scheme wallets or multi-party computation (MPC) wallets, which mimic the access control of multisignature addresses.

In contrast to a multisignature wallet, where a single key among n may be sufficient for cryptographic proof, there is currently no general lightweight method to demonstrate control over $addr$ other than by actually using m shares.

4) Smart Contract Wallet, or VAs with Key Update Capability: In some VA systems, there may not be a cryptographic relationship between an address and its signing keys. This means that an address may not have any corresponding keys, or the set of keys associated with an address may be modified after the address is generated.

In Ethereum, instead of a regular address called an Externally Owned Account, smart contracts can be used to manage Ethers or ERC-20 tokens. VASPs can utilize smart contract wallets [37], [38] to simulate multisignature wallets, aiming to increase security. These smart contract wallets have VA addresses that are assigned programmatically based on the state of the blockchain, and there are no cryptographic keys that directly match these addresses.

The Flow blockchain has built-in support for modifying the access control list of an account, equivalent of an address in the Flow [39]. While the account address is fixed, an owner of the account can change the list of keys associated with it each with a different weight. A transaction needs to be signed by a combination of registered keys that meets a weight threshold.

These examples highlight the need for V_a (, or a lookup service) to confirm the association between $addr$ and public key(s) that V_b claims, using the blockchain node along with the timestamp or the block height in msg. Additionally, the lookup service may need to implement a mechanism to monitor changes in the state of blockchain to detect any changes in $addr$'s ownership.

VI. Challenge 3: PII Transmission Interface

Assume that V_a has identified V_b as its counterpart for the transfer. In order to transmit PII, V_a needs to establish a communication channel to V_b. However, the specific channel is often not known in advance. They need to agree on various aspects of the communication, such as:

- *Network Connectivity* Is it over the Internet, over a VPN, or in a closed dedicated network?
- *Network Address of Each Party*: Is the peer VASP resolved by DNS, or provided as an IP address and how?
- *Type of Authentication and Encryption*: Is it provided by TLS, or another protocol? Who issues certificates?
- *Application Layer*: How is the communication done?
- *Encoding*: How are the messages serialized?

Figure 6 illustrates various approaches. The network security in the design of each approach is important, as cyber attacks could lead to the potential disclosure of PII.

Approach 3-A. Peer-to-Peer

The most obvious method is to agree on the communication protocol prior to any transfers between VASPs. The transmission process can be customized for each VASP, providing a flexible solution.

For example, as depicted in the figure, V_a and V_b may publish following API endpoints:

V_a) REST API at `https://api.vasp-a.example/`
V_b) gRPC at `grpc://travel.vasp-b.example/`

V_a and V_b mutually agree that V_a contacts V_b's endpoint and protocol (gRPC) when V_a transmit PII to V_b, and vice versa. They may choose to use IVMS 101 data model over the API.

One major drawback of this approach is its lack of practicality and feasibility in requiring every pair of VASPs to establish independent contracts with one another. Moreover, accommodating different protocols or APIs used by each VASP would demand significant development efforts and time.

Approach 3-B. Public VASP Directory

As an alternative, an open directory can be built that any VASPs can participate in to register their corporate name, network endpoints, jurisdictions, and other necessary information for PII transmission.

The management of the open VASP directory is flexible, allowing for various approaches. The directory contains information that does not require frequent updates and can be cached to facilitate speedy lookups at each VASP. In combination with the (1-D) approach, we speculate the possibility of implementing this method using DNS infrastructure as a possible extension.

1) Coverage and Accuracy: Ensuring the quality of the directory is crucial, as it should encompass a comprehensive list of VASPs from around the world. However, making the directory publicly editable without authorization presents a risk to its accuracy. This could result in incorrect information about existing VASPs or the inclusion of fake listings with similar names, potentially leading to the theft of PII.

To mitigate these risks, it is advisable to restrict the editing of the directory to VASPs only, with each company having only one record per jurisdiction. To achieve this, we propose a verification process similar to the Extended Validation used in TLS certificates. This process would verify the authenticity of newly registered companies, ensuring that only legitimate VASPs are included in the directory. It is also necessary to regularly update the directory to keep it current and accurate.

2) Standardization of Protocols and APIs: The VASP directory may list various parameters, such as the endpoint URLs for VASPs or the digital certificate to authenticate the identity. Even then, VASPs should also consider standardizing the communication protocols. This means reaching a consensus on protocols and APIs to ensure seamless and efficient interactions between VASPs. While the IVMS 101 message model standard has gained significant acceptance in the industry, it is important to extend standardization to other layers of PII transmission protocol as well. This will promote interoperability and enhance the overall security and reliability of the directory.

Approach 3-C. Alliance of VASPs

To strike a balance between (3-A) and (3-B), VASPs that share a certain level of trust can form an alliance and jointly manage the member VASP directory. This directory allows member VASPs to easily access each other's information for peer-to-peer communication. Alternatively, the alliance can act as a communication hub by providing connectivity to each member. By establishing a communication standard within the alliance, VASPs can ensure efficient implementation and operation of the Travel Rule.

The notable advantage of this approach is its high compatibility with (1-B). Since the alliance is composed of VASPs that have already evaluated their risk profiles, a lookup service can be operated by the alliance safely while alleviating concerns described earlier. Furthermore, it makes sense for the alliance to provide lookup services in order to enable the identification of suitable VASPs.

A potential downside of this approach is the issue of compatibility between different alliances. When multiple alliances are formed, VA transfers cannot cross between border of different alliances if they are incompatible. As a real-world example, VASPs in Japan are virtually divided into two groups based on the alliances they join [40]. Users are required to use an unhosted wallet to transfer between VASPs of different alliances. Similar case is also reported in Switzerland [41].

A VASP may participate in multiple alliances to communicate with more VASPs globally, but this increases the operation and maintenance load for each alliance they join, as well as the cost they pay. This is similar to credit card merchants being connected to multiple payment processing networks.

There are two ways to solve this issue.

1) Bridges Provided by Alliances: The first is for an alliance to ensures compatibility in the architecture with other alliances, and to provide bridges which convert communication. Due to potential architecture changes in each alliance, this approach may take time to implement, while feasible.

2) Intermediary VASPs: The second method is for a VASP participating in multiple alliances to act as a gateway, similar to a correspondent bank for international fiat currency transfers, facilitating transfers through this VASP. Although this method is simpler, there are presumably concerns regarding transaction fees, privacy, and complexity of the solution, and no examples have been observed to the our knowledge. However, we speculate that this method has the potential to be effective for cross-chain swap DeFi; they exchange VAs across multiple blockchains through the use of smart contracts, and may be well-suited for serving as an intermediary VASP.

VII. Known Travel Rule Implementations

A. Summary

We conducted a survey of multiple solutions for the Travel Rule using publicly available information. Many of these were proposed and developed between 2019 and 2021, but

TABLE II
COMPARISON OF TRAVEL RULE SOLUTIONS

	Approaches	TRUST (USTRWG)	TRISA	Sygna 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	√	√	√	√			

some also utilized technologies that existed prior to that. Table II illustrates the summary of the comparison based on the previously explained approaches. We outline major observations below.

1) Dominance of Alliance-based Solutions: Among the solutions that were surveyed, USTRWG (currently, TRUST), TRISA, Sygna Bridge, and VerifyVASP all adopt an alliance-based approach as in (3-C). Each of these solutions aims to attract and expand the alliance by recruiting VASPs. VASPs are subjected to a thorough due diligence process before they can join the alliance, ensuring their legitimacy. It is worth noting that the establishment of these solutions was greatly facilitated by blockchain analytics companies: Elliptic for Sygna Bridge, Chainalysis for VerifyVASP, and CipherTrace for TRISA.

There are two solutions in the (3-A) peer-to-peer communication approach: Netki/TransactID and TRP by OpenVASP. It is uncertain how widely these protocols are currently being adopted by VASPs.

Lastly, other two solutions leveraged blockchain technology, which can be categorized as the (3-B) open directory model: Shyft Veriscope and the Ethereum-based OpenVASP (legacy). There is limited activity on the public blockchain of Shyft Veriscope, making it difficult to confirm its active usage. Ethereum-based OpenVASP solution is no longer being maintained.

2) Various Address Lookup Methods: We confirmed that USTRWG and VerifyVASP offer lookup services within the alliances. Especially, VerifyVASP takes a unique approach by directly querying each VASP in the alliance for transfer requests. Both USTRWG and VerifyVASP do not seem to mandate cryptographic proofs, taking (2-A) approach.

TRISA and Sygna Bridge actively promote the use of blockchain analysis. As mentioned earlier, the involvement of these analytics companies has had an influence on this.

Early solutions like TransactID, OpenVASP, and Sygna Bridge implemented methods using special identifiers. However, newer solutions do not actively propose the use of special identifiers. This suggests that introducing them would require cooperation from multiple stakeholders and can be challenging.

B. Travel Rule Universal Solution Technology (TRUST) formerly the U.S. Travel Rule Working Group (USTRWG)

The Travel Rule Universal Solution Technology (TRUST) [42] is a network that was established in February 2022, and it is led by Coinbase, a U.S. virtual asset exchange. While there is limited public information available on TRUST, official announcements indicate that it has several key features. These include the ability to send PII without it being centrally stored, the mechanism for address ownership verification, and a due diligence process for all VASPs [43]. TRUST was preceded by the U.S. Travel Rule Working Group (USTRWG), which released a whitepaper in October 2020 [44]. Since there is no clear public information available on TRUST, we will maily analyze the USTRWG based on their whitepaper instead.

As per the whitepaper, the system initially utilized the (1-A), which involved a centralized Bulletin Board where all participating VASPs posted their addresses. The system was designed to operate on an access-controlled closed network, isolated from the Internet. At the time of the USTRWG's whitepaper, (2-A) proof of address was not provided. We believe from TRUST's announcements that they has shifted to the (2-B), where member VASPs are required to provide proof. As stated by the whitepaper, the transmission of PII is carried out end-to-end through a REST API on HTTP over TLS 1.3, on (3-C) the closed network provided by the alliance.

Here are the steps taken when a withdrawal is requested:

1) V_a posts a message on the Bulletin Board regarding the VA transfer to *addr*.
2) V_b claims ownership of *addr* on the Bulletin Board.
3) V_a confirms V_b's control over *addr*, and initiates the VA transfer to *addr* along with sending PII to V_b.

There are two defects in compliance with the travel rule in USTRWG's specification:

1) Temporal Difference between Transmission of PII and Transfer of VAs: If V_b does not claim ownership of *addr* in a timely manner, V_a proceeds with the transfer first and sends the PII later once *addr* is claimed by V_b. However, the FATF

later pointed out that transactions need to be conducted before or at the same time as the transfer. The protocol can be fixed by waiting for time T, where all participants in the network guarantee to claim any posted address in no longer than T. However, it is unclear whether TRUST has made this fix.

2) Lack of Support for Other Types of VAs: Initially, USTRWG only supported Bitcoin and Ethereum transactions in its first phase. However, the FATF pointed out that all virtual assets are subject to the Travel Rules.

Assume TRUST has the same architecture as USTRWG's proposal, similar observations can be made about TRUST.

C. Travel Rule Information Sharing Alliance (TRISA)

The Travel Rule Information Sharing Alliance (TRISA) [45] is a platform launched on September 10, 2019, led by CipherTrace, a U.S. blockchain analysis tool vendor. TRISA releases a variety of information as open source.

TRISA operates as (3-C) an alliance among VASPs. When a new VASP joins TRISA, they are required to submit a questionnaire checklist for due diligence purposes. Once the process is completed, the VASP is listed on the TRISA VASP Directory and becomes searchable.

From a technical standpoint, TRISA adopts a strict PKI model. The alliance issues EV certificates from the Trusted VASP CA operated by TRISA. VASPs communicate through messages encoded in a protocol buffer over a gRPC on an mTLS channel authenticated with the EV certificate.

While TRISA plans to implement the address lookup mechanism or ownership verification in the future, they do not currently provide an explicit solution, and instead leave the choice to participating VASPs. While they mention a method such as querying the destination VASP based on the user's declaration or using the blockchain to record addresses as mentioned in (1-A), they seem to ultimately recommend using blockchain analysis tools.

In August 2023, TRISA announced its completion of a proof of concept to interoperate with OpenVASP / TRP [46] and Sygna Bridge [47].

D. Sygna Bridge

Sygna Bridge [48] is a VASP alliance provided by CoolBitX, a Taiwanese blockchain security company, and Elliptic, a U.K blockchain analysis tool vendor. Sygna Bridge conducts due diligence for VASPs to participate. The originator VASP requests permission from the beneficiary VASP and initiates the transfer only after being granted. The central server operated by Sygna Alliance, called the Bridge, plays a role in processing the messages, which characterizes it as a highly centralized solution. Sygna Bridge is tightly integrated into their compliance solution, such as user screening and risk-based transaction analysis.

When using Sygna Bridge, each VASP is assigned a unique VASP code, and each user has an address called Virtual Asset Account Information (VAAI), described in the extended format of BIP 21 [49]. VAAI encodes the VA address, the VASP code, and the name of the sender.

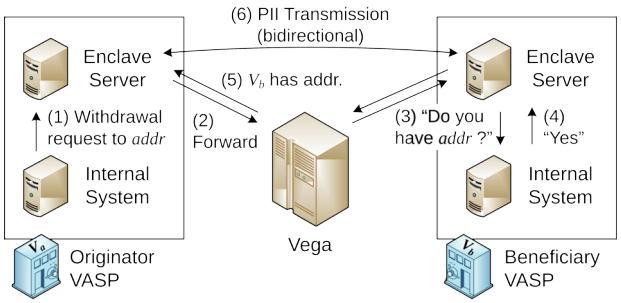

Fig. 7. Architecture of VerifyVASP

When a originator VASP initiates a transfer using Sygna Bridge to a VAAI, the beneficiary VASP code in the VAAI is referenced, and the message is automatically relayed to the counterparty VASP. Otherwise, when sending to a regular VA address, blockchain analysis is performed to determine which VASP it belongs to using the Wallet Address Filter API [50]. Therefore, we observe that the addresses are identified by a hybrid method, either by lookup incorporating special encoding or through blockchain analysis. No ownership proof is required.

E. VerifyVASP

VerifyVASP [51] is a solution co-developed by Upbit, a South Korean virtual asset exchange, and Chainalysis, a U.S. blockchain analysis tool vendor. It operates as a closed alliance for affiliated VASPs.

Figure 7 depicts its architecture. VerifyVASP provides a Docker image called Enclave Server, which runs inside each VASP's infrastructure. VASPs use this container as an interface to connect to Vega, the central server of VerifyVASP. VASPs need to establish communication between their internal systems and the Enclave Server. Vega acts as a lookup service and a VASP directory, receiving address lookup queries from each VASP and providing responses along with the beneficiary VASP's endpoint.

The following steps outline the process when *Alice* requests a withdrawal from V_a to *Bob* on V_b, with both VASPs participating in VerifyVASP:

1) The internal system of V_a calls the withdrawal request API of the Enclave Server hosted on V_a's infrastructure.
2) The request is forwarded to Vega.
3) Vega queries other member VASPs in the alliance to determine the controlling VASP for $addr$.
4) The internal system of V_b responds to the callback from V_b's container, notifying the ownership of $addr$.
5) Vega informs V_a's Enclave Server about V_b's ownership.
6) The Enclave Servers of V_a and V_b establish an end-to-end encrypted communication channel to exchange PII.

In VerifyVASP, V_b does not need to provide cryptographic proof of $addr$. Network security for each VASP and Vega is ensured through IP restrictions.

Based on our investigation, VerifyVASP is unique in two ways:

- Instead of actively collecting addresses from member VASPs, it queries the member VASP when a transfer request is made.
- The beneficiary VASP (V_b) transmits recipient information back to the originator VASP (V_a). This enhances the accuracy of PII on both ends, although it is not required by the travel rule.

F. Shyft Veriscope

Shyft Veriscope [52] utilizes a private Ethereum blockchain called the Shyft Network. VASPs need to purchase dedicated tokens (SHFT) available on the Shyft Network, which is operated by Proof-of-Authority consensus algorithm. Shyft Network functions as (1-A) a lookup service, (2-A) does not require proof of address, and (3-C) operates within a limited alliance.

Whenever there is a withdrawal request from a customer on the originator VASP, they publish a transaction on the Shyft Network that contains information about the transfer request. Once the beneficiary VASP detects the transaction, it starts an end-to-end network connection with the originator VASP to permit the transfer. The beneficiary VASP does not particularly need to prove address ownership. Eventually, they exchange messages in the IVMS 101 format via P2P outside the Shyft Network.

As of September 2023, the total number of transactions on the Shyft Network mainnet is between 10 and 20 per day according to the official blockchain explorer [53]. The smart contracts and documents are publicly available [54].

G. OpenVASP / Travel Rule Protocol (TRP)

The Travel Rule Protocol (TRP) [55], developed by the OpenVASP Association, aims to be a minimum set of APIs for PII transmission. Much of the information is open source and can be found on their GitLab.

The TRP uses a unique identifier called the Travel Address to indicate the transfer destination. The Travel Address starts with `ta` and is encoded using Base58 with the deposit URI, as explained in (1-C). The recipient VASP assigns the Travel Address to each user, and a sender provides it to the originator VASP when a transfer is requested.

Here's an example of how the TRP works:

1) *Bob* obtains his Travel Address $addr^\star$ from V_b.
2) *Alice* requests a transfer to *Bob* by providing $addr^\star$ to V_a.
3) V_a decodes $addr^\star$ to get the deposit URL $\mathsf{u_B}$, and sends PII and a callback URL $\mathsf{u_A}$ to $\mathsf{u_B}$.
4) V_b either responds with an actual VA address *addr* or notifies the rejection.

The Travel Address contains the beneficiary VASP's endpoint, so the originator VASP doesn't need to look up the beneficiary VASP. VASPs communicate with each other using a peer-to-peer (P2P) connection over HTTPS.

H. Other solutions

Netki originally promoted Bitcoin payment using human-readable names [56] specified in BIP 70 [57] in 2015. TransactID aims to exchange PII outside the blockchain, as defined in BIP 75 [58], and adapted to the Travel Rule [59].

OpenVASP originally proposed a solution, before TRP, to use the Ethereum blockchain [60]. It required VASPs to deploy an identifying smart contract on Ethereum [61]. The users were identified by a unique Virtual Asset Account Number, which contains the VASP code, based on the smart contract address. VASPs communicated peer-to-peer using Ethereum Whisper [62], which is deprecated.

Lee, et al [63] suggested the solution CODE over a permissioned blockchain using Corda [64] to build a VASP alliance. In the design, the PII is transmitted peer-to-peer over Corda's messaging mechanism.

VIII. Open Challenges with the Travel Rule

A. Money Laundering using Unhosted Wallets

By relaying through unhosted wallets, the Travel Rule can be bypassed. Currently, there are no effective solutions proposed to address this issue, other than restricting transfers to and from unhosted wallets.

This problem arises from a lack of travel rule requirements involving unhosted wallets. Some concerns have been raised that this lack of regulation may encourage criminals to use unhosted wallets [65]. However, imposing regulations on unhosted wallets and limiting transactions solely between VASPs would significantly undermine the economic benefits mentioned in Section II-A. For example, the case of Hawala, an informal value transfer system in the Middle East, highlights the potential for underground economies and increased complexity in AML/CFT efforts [66].

In proposing technical solutions to integrate unhosted wallets into the Travel Rule, it is crucial to prioritize the privacy of unhosted wallet owners.

B. Privacy Preserving Proof of Address Ownership

From our investigation, we observed that many alliances provide address lookup services. However, it is not desirable from a privacy perspective for the lookup service to centrally collect addresses.

Technically, it is ideal to meet the following two requirements: (1) a beneficiary VASP registers a cryptographic commitment to prove the possession of a secret key for *addr* without showing *addr*, (2) only those who know *addr* can verify the commitment. A simple hash value of *addr* does not satisfy requirement (1).

To our knowledge, there hasn't been any proposed scheme, even for single-key wallets in Bitcoin-like systems. We believe that the process of deriving *addr* from the hash value of the public key does not align with zero-knowledge proof techniques, which poses a challenge in addressing this problem.

C. Support for Various Types of VAs

During our investigation, we discovered that most solutions support Bitcoin and Ethereum, but the level of support varies for other types of VAs. The reasons behind this inconsistency were not clearly understood by the authors, whether the amount of effort required for support, or any fundamental issue related to the architecture or cryptography of blockchains in other VAs.

This issue applies to new forms of VAs such as NFTs and stablecoins that have emerged since 2020. Some of these have a certain exchange value, and there are reports of NFTs being used for money laundering [67]. Further research should evaluate the compliance difficulty of ERC-20 and other tokens.

Furthermore, regarding AECs, e.g. Zcash and Monero, they falls under VA and must be compliant with travel rules according to FATF's definition. There are a few VASPs handling AECs in reality and they are subject for Travel RUles. The authors did not conduct a detailed examination of AECs in this study, but the challenges of making AEC compliant with travel rules should be analyzed in the future.

Furthermore, AECs such as Zcash and Monero are categorized as VAs according to FATF's definition, and they are subject to the travel rules. A few VASPs exist that handle AECs in reality. The authors did not conduct a detailed examination of AECs in this study, but the challenges of making AECs compliant with travel rules should be analyzed in the future.

D. Other General Issues

1) Risk Evaluasion for PII Transmission: An originator VASP must evaluate the risk of PII disclosure against a beneficiary VASP. Same applies when an originator VASP considers joining an alliance.

Since the introduction of the travel rule, there has always been a debate. VASPs in the European Union are subject to strictly protect personal information under the General Data Protection Regulation, and there are significant concerns about sharing information outside of the EU region [68]. Similarly, in Japan, a legal amendment was made to set inter-VASP PII transmission as an exception to the prohibition of PII disclosure without originator's consent [69], [70].

2) Shell VASPs and Money Mules: The FATF Recommendations call for member countries to legislate the issuance of licenses to operate VASPs, and the implementation of strict KYC by VASPs. However, improper implementation of these measures in one country or region may decrease the effectiveness of the Travel Rule globally, even if other countries have stipulated the Travel Rule in their local law.

The existence of Shell VASPs is one major issue caused by the inappropriately issued license by a vulnerable country. Such fictional financial institutions have been a major problem in the traditional financial system, known as shell banks. The credibility of a VASP directory or an alliance could be compromised if a fictional VASP is part of them.

In addition, the strictness of the KYC process with VASPs is crucial. Many financial institutions, as well as VASPs, are fighting against illegal KYC attempts using forged copies of government-issued identification documents to create fictitious accounts. Additionally, legitimately created accounts are illegally traded over Telegram or other highly anonymized chats. This poses a risk to economically vulnerable individuals who can be exploited as money mules [71]. To address these issues, it is necessary to establish and implement robust KYC procedures, such as the use of IC chips or smart cards on digital identification cards.

IX. Conclusion

Virtual assets are becoming important financial tools alongside legal currencies, necessitating measures to prevent their exploitation for criminal purposes. One such measure is the FATF's Travel Rule, which aims to prevent transfers of illicit funds. The Travel Rule enhances AML/CFT efforts by extending CDD obligations from conventional financial institutions to VASPs.

Unlike traditional banking networks, virtual assets pose a unique challenge. Users can simply specify a destination VA address on a VASP for transfers, and the VASP inherently has no way to know the address's owner. Consequently, the need for a lookup mechanism has been emphasized to identify the controlling VASP of a given address. A newly generated address should be registered with the lookup service in a timely manner, preferably with proper cryptographic proof to enhance the authenticity of registration. It is essential to ensure that VASPs worldwide actively participate in the mechanism for an accurate lookup, while excluding malicious entities falsely claiming ownership of irrelevant addresses. This can be achieved by verifying participating VASPs' legitimacy and providing authentication and authorization mechanisms. The effectiveness of such a mechanism is crucial for the global implementation of the Travel Rule.

We conducted a comprehensive review of various Travel Rule solutions and obtained the following findings from our survey:

- Alliance-based solutions are the most prevalent. They are actively seeking new VASPs to join their networks.
- The methods used to identify beneficiary VASPs from destination addresses vary among the solutions. Some rely on lookup services, while others encourage the use of blockchain analysis tools.
- Although peer-to-peer and blockchain-based solutions have been developed in the past and present, we did not observe widespread adoption of these alternatives.

This outcome can be attributed to the efficiency and convenience of mutual due diligence and consensus on communication protocols among VASPs. However, there are concerns regarding the potential division of the VA economy due to the formation of multiple alliances. To address this issue, some alliances are planning to establish bridges that facilitate interoperability and further expand the alliance-based Travel Rule network.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[3] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019.

[4] M. Alnasaa, N. Gueorguiev, J. Honda, E. Imamoglu, P. Mauro, K. Primus, and D. Rozhkov, "Crypto-assets, corruption, and capital controls: Cross-country correlations," *Economics Letters*, vol. 215, p. 110492, Jun. 2022.

[5] K. Kirkpatrick, "Financing the dark web," *Commun. ACM*, vol. 60, no. 3, pp. 21–22, feb 2017.

[6] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from Bitcoin," in *2014 IEEE Symposium on Security and Privacy*, May 2014, pp. 459–474.

[7] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct Non-Interactive zero knowledge for a von neumann architecture," in *23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association, Aug. 2014, pp. 781–796.

[8] S. Noether, "Ring signature confidential transactions for Monero," Cryptology ePrint Archive, Paper 2015/1098, 2015. [Online]. Available: https://eprint.iacr.org/2015/1098

[9] F. K. Maurer, T. Neudecker, and M. Florian, "Anonymous CoinJoin transactions with arbitrary values," in *2017 IEEE Trustcom/BigDataSE/ICESS*, Sep. 2017.

[10] R. Stütz, J. Stockinger, P. Moreno-Sanchez, B. Haslhofer, and M. Maffei, "Adoption and actual privacy of decentralized coinjoin implementations in bitcoin," in *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, ser. AFT '22. New York, NY, USA: Association for Computing Machinery, Sep. 2023, pp. 254–267.

[11] Southern District of New York, U.S. Attorney's Office, "Tornado Cash founders charged with money laundering and sanctions violations," Aug. 2023. [Online]. Available: https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations

[12] Elliptic, "The state of cross-chain crime," p. 9, Oct. 2023. [Online]. Available: https://www.elliptic.co/hubfs/Elliptic_The_State_of_Cross_Chain_Crime_Report_2023.pdf

[13] D. Ermilov, M. Panov, and Y. Yanovich, "Automatic bitcoin address clustering," in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Dec. 2017, pp. 461–466.

[14] A. Feder, N. Gandal, J. T. Hamrick, and T. Moore, "The impact of DDoS and other security shocks on Bitcoin currency exchanges: evidence from Mt. Gox," *Journal of Cybersecurity*, vol. 3, no. 2, pp. 137–144, Jan. 2018.

[15] Office of Public Affairs, U.S. Department of Justice, "Alleged Russian cryptocurrency money launderer extradited to United States," Aug. 2022. [Online]. Available: https://www.justice.gov/opa/pr/alleged-russian-cryptocurrency-money-launderer-extradited-united-states

[16] FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, Feb. 2012. [Online]. Available: https://www.fatf-gafi.org/recommendations.html

[17] ——, *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*, Jun. 2023. [Online]. Available: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html

[18] A. Matsuzawa, "The travel rule challenge: Virtual asset transfers versus wire transfers," *Aspects of APAC*, pp. 88–95, Oct. 2020. [Online]. Available: https://www.fsa.go.jp/frtc/kikou/2020/FSA_article_ACAMSToday2020_Sept-Nov.pdf

[19] Joint Working Group on interVASP Messaging Standards, "interVASP messaging standards," May 2020. [Online]. Available: https://www.intervasp.org/

[20] *ISO 20022-1:2013 - Universal financial industry message scheme*. International Organization for Standardization, May 2013. [Online]. Available: https://www.iso20022.org/

[21] *ISO 17442-1:2020 - Legal entity identifier (LEI)*. International Organization for Standardization, Aug. 2020.

[22] T. Hardjono, A. Lipton, and A. Pentland, "Wallet attestations for virtual asset service providers and crypto-assets insurance," May 2020. [Online]. Available: https://arxiv.org/abs/2005.14689

[23] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Oct. 2021. [Online]. Available: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html

[24] J. Lovejoy, C. Fields, M. Virza, T. Frederick, D. Urness, K. Karwaski, A. Brownworth, and N. Narula, "A high performance payment processing system designed for central bank digital currencies," Cryptology ePrint Archive, Paper 2022/163, 2022. [Online]. Available: https://eprint.iacr.org/2022/163

[25] *ISO 13616-1:2020 - International bank account number (IBAN)*. International Organization for Standardization, Sep. 2020.

[26] *ISO 9362:2022 - Banking telecommunication messages — Business identifier code (BIC)*. International Organization for Standardization, Apr. 2022.

[27] K. Oosthoek and C. Doerr, "From hodl to heist: Analysis of cyber security threats to Bitcoin exchanges," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020, pp. 1–9.

[28] N. Rustgi, "Balancer frontend hit by DNS attack, over $250k stolen," Sep. 2023. [Online]. Available: https://decrypt.co/197953/balancer-frontend-hit-by-dns-attack-over-250k-stolen

[29] P. Wuille, "Hierarchical deterministic wallets," Feb. 2012. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[30] G. Andresen, "Pay to script hash," Jan. 2012. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki

[31] Z. Jaroucheh and B. Ghaleb, "Crypto assets custody: Taxonomy, components, and open challenges," in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023, pp. 1–6.

[32] Blockchain.com, "How do I import a Bitcoin address?" [Online]. Available: https://support.blockchain.com/hc/en-us/articles/8997347711388

[33] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, nov 1979.

[34] R. Gennaro and S. Goldfeder, "Fast multiparty threshold ECDSA with fast trustless setup," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: Association for Computing Machinery, 2018, pp. 1179–1194.

[35] Y. Lindell and A. Nof, "Fast secure multiparty ecdsa with practical distributed key generation and applications to cryptocurrency custody," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: Association for Computing Machinery, 2018, pp. 1837–1854.

[36] J. Doerner, Y. Kondi, E. Lee, and abhi shelat, "Threshold ECDSA in three rounds," Cryptology ePrint Archive, Paper 2023/765, May 2023. [Online]. Available: https://eprint.iacr.org/2023/765

[37] BitGo, "Ethereum multisig wallet contract." [Online]. Available: https://github.com/BitGo/eth-multisig-v4

[38] Safe Ecosystem Foundation, "Safe contracts." [Online]. Available: https://github.com/safe-global/safe-contracts

[39] R. M. Seraj, "Flow's account model offers real ownership to users," Feb. 2023. [Online]. Available: https://flow.com/post/flow-blockchain-news-analysis-ownership-account-model

[40] CoinDesk Japan, "Impact of the travel rule on crypto asset exchanges on remittances, disadvantages, and the response of each domestic exchange," Jul. 2023. [Online]. Available: https://www.coindeskjapan.com/learn/travel-rule/

[41] K. L. Heller and A. Fromm, "The travel rule and its impact on cryptocurrency: A simple explanation of differences between fatf and the swiss approach published by finma," Jan. 2021. [Online]. Available: https://lexcellence.swiss/en/travel-rule-and-its-impact-cryptocurrency-simple-explanation-differences-between-fatf-and-swiss

[42] Coinbase, "Travel rule universal solution technology (TRUST)." [Online]. Available: https://www.coinbase.com/travelrule

[43] TRUST, "Introducing the travel rule universal solution technology ("TRUST")," Feb. 2022. [Online]. Available: https://www.coinbase.com/blog/introducing-the-travel-rule-universal-solution-technology-trust

[44] USTRWG, "Travel rule solution white paper version 1.0," Oct. 2020. [Online]. Available: https://web.archive.org/web/20201101123224/https:

//www.gdf.io/wp-content/uploads/2020/10/USTRWG-Travel-Rule-Solution-V1.pdf
[45] D. Jevans, T. Hardjono, J. Vink, F. Steegmans, J. Jefferies, A. Malhotra, and the TRISA Technical Subcommittee, "Whitepaper version 9," Feb. 2022. [Online]. Available: https://trisa.io/trisa-whitepaper/
[46] TRISA, "TRISA-OpenVASP/ TRP Demonstrate Interoperability," Aug. 2023. [Online]. Available: https://trisa.io/trisa-trp-interoperability/
[47] Sygna, "Trisa and sygna announce interoperability to simplify global travel rule compliance." [Online]. Available: https://www.sygna.io/blog/trisa-sygna-coolbitx-announce-fatf-travel-rule-solution-interoperability/
[48] CoolBitX and Elliptic, "Sygna bridge." [Online]. Available: https://www.sygna.io/bridge/
[49] N. Schneider and M. Corallo, "URI scheme," Jan. 2012. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0021.mediawiki
[50] Sygna, "Bridge/wallet address filter." [Online]. Available: https://developers.sygna.io/reference/bridgewallet-address-filter
[51] VerifyVASP. [Online]. Available: https://docs.verifyvasp.com/
[52] Shyft, "Veriscope Docs." [Online]. Available: https://docs.veriscope.network/
[53] ——, "Poa explorer (mainnet)." [Online]. Available: https://bx.shyft.network/
[54] ——, "Veriscope docs." [Online]. Available: https://docs.veriscope.network/
[55] OpenVASP Association, "Travel rule protocol (TRP)," Dec. 2020. [Online]. Available: https://gitlab.com/OpenVASP/travel-rule-protocol/-/blob/master/core/specification.md
[56] Netki, "Netki wallet name service." [Online]. Available: https://www.youtube.com/watch?v=gunA1zBnEcs
[57] G. Andresen and M. Hearn, "Payment protocol," Jul. 2013. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0070.mediawiki
[58] J. Newton, M. David, A. Voisine, and J. MacWhyte, "Out of band address exchange using payment protocol encryption," Nov. 2015. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0075.mediawiki
[59] N. DiCamillo, "Netki retools digital ID service for FATF's new crypto 'travel rule'." [Online]. Available: https://www.coindesk.com/business/2019/09/09/netki-retools-digital-id-service-for-fatfs-new-crypto-travel-rule/
[60] D. Riegelnig and Bitcoin Suisse, "OpenVASP: An open protocol to implement FATF's travel rule for virtual assets," Nov. 2019. [Online]. Available: https://www.crowdfundinsider.com/wp-content/uploads/2019/11/OpenVasp_Whitepaper-Nov-2019.pdf
[61] OpenVASP Association, "OpenVASP contracts," Apr. 2020. [Online]. Available: https://github.com/OpenVASP/openvasp-contracts/tree/1.0
[62] Ethereum community, "Ethereum whisper archive." [Online]. Available: https://github.com/ethereum/whisper
[63] C. Lee, C. Kang, W. Choi, M. Cha, J. Woo, and J. Hong, "CODE: Blockchain-based travel rule compliance system," in *2022 IEEE International Conference on Blockchain (Blockchain)*, Aug. 2022, pp. 222–229.
[64] R. G. Brown, "The Corda platform: An introduction," May 2018. [Online]. Available: https://www.corda.net/content/corda-platform-whitepaper.pdf
[65] His Majesty's Treasury, "Response to the consultation," p. 28, Oct. 2020, paragraph 6.21. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083351/MLRs_SI_2022_-_Consultation_Response_final.pdf
[66] F. M. J. Teichmann and C. Wittmann, "Challenges resulting from hawala banking for anti-money laundering and anti-terrorist financing policies of swiss banks," *Journal of Money Laundering Control*, 2022.
[67] FATF, *Money Laundering and Terrorist Financing in the Art and Antiquities Market*, Feb. 2023. [Online]. Available: https://www.fatf-gafi.org/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-ArtAntiquities-Market.html
[68] S. B. Neagu, "A sharp turn towards crypto-surveillance: Analyzing implications of the EU's revised transfer of funds regulation," Jul. 2022. [Online]. Available: https://law.stanford.edu/publications/no-64-a-sharp-turn-towards-crypto-surveillance-analyzing-implications-of-the-eus-revised-transfer-of-funds-regulation/
[69] Japan Financial Services Agency, *Publication of the Draft Cabinet Order for Partial Revision of the Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds (translated)*, Feb. 2023. [Online]. Available: https://www.fsa.go.jp/news/r4/sonota/20230203-2/20230203-2.html
[70] Nikkei, *Japan cryptocurrency transfer rules take aim at money laundering*, Sep. 2022. [Online]. Available: https://asia.nikkei.com/Spotlight/Cryptocurrencies/Japan-cryptocurrency-transfer-rules-take-aim-at-money-laundering
[71] M. S. Raza, Q. Zhan, and S. Rubab, "Role of money mules in money laundering and financial crimes a discussion through case studies," *Journal of Financial Crime*, vol. 27, pp. 911–931, 2020.
[72] Reuters, "South Korean intelligence says N. Korean hackers possibly behind Coincheck heist," Feb. 2018. [Online]. Available: https://reut.rs/2BI6Oh1
[73] K. Ji-Young, L. Jong In, and K. Kyoung Gon, "The all-purpose sword: North Korea's cyber operations and strategies," in *2019 11th International Conference on Cyber Conflict (CyCon)*, vol. 900, 2019, pp. 1–20.

APPENDIX

A. List of FATF Vocabulary Abbreviations

Table III illustrates the list of abbreviations from the FATF vocabulary used in this paper, in alphabetical order.

TABLE III
LIST OF FATF VOCABULARY ABBREVIATIONS

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
FATF	Financial Action Task Force
FSRB	FATF-Style Regional Bodies
KYC	Know Your Customer
STR	Suspicious Transaction Report
VA	Virtual Asset
VASP	Virtual Asset Service Provider

B. History of Travel Rule

The original Travel Rule is defined by the Bank Secrecy Act (31 CFR 103.33(g)) in the United States in 1996. The stipulation was incorporated into the FATF Recommendations in 2001 as Special Recommendation VII (Wire transfers). It became mandatory for international banking transactions by December 2006.

In 2012, the FATF entirely revised the recommendations. The Travel Rule was renumbered as Recommendation 16. While the Bitcoin blockchain had started in 2009, the then-current version did not yet consider virtual asset technology.

In 2017, Bitcoin experienced price inflation of about 20 times, gaining public attention, followed by a massive Nem theft in a Japanese exchange in January 2018. This incident was suspected of being a state-backed cyber attack by North Korea [72], [73], which has been listed on the FATF blacklist since 2012.

In response to these social movements, in October 2018, the FATF defined the terms VA and VASP and amended Recommendation 15 (New technologies). The Interpretation Note to Recommendation 15, which provides supplementary practical information, was amended in 2019. Upon this, the FATF asked each country to legislate so that VASPs must be regulated with licenses as well as expand the Travel Rule obligation to virtual assets.

The FATF set a 12-month grace period for preparation, which was later adjusted with another 12-month window

until mid-2021 based on feedback from the industry. Most recently, in April 2023, the FATF's Virtual Assets Contact Group (VACG) meeting, which the author of this paper also attended, was held to facilitate dialogue among the FATF, participant jurisdictions, and the private sector. The progress of the Travel Rule implementation was reported during the meeting. The regulation plans against NFTs or other means of virtual assets were also discussed.