参考和訳
元論文 "FATF Travel Rule ’ s Technical Challenges and Solution Taxonomy", IEEE ICBC 2024

FATF 旅行規則の技術的課題とソリューション分類法

Yuto Takei
Mercari, Inc., and
Tokyo Institute of Technology

Kazuyuki Shudo
Kyoto University

概要-仮想資産は、分散型デジタル通貨システムとして世界的に認知されている。また、犯罪収益の移転にも利用されている。2019年、金融行動タスクフォースは、仮想資産サービスプロバイダー(VASP)のための旅行規則を義務付けました。しかし、2024年3月現在、サンライズの問題により、世界的に完全には実施されていない。運用規則に準拠することは、仮想資産アドレスから受信者のVASPを特定すること、アドレスの所有権を証明すること、VASP間の通信プロトコルを確保することなどの課題を提起する。本論文では、これら3つの課題に焦点を当て、それぞれのアプローチの可能性と、追加的な考察を行う。複数の既存プロトコルを分析し、その特徴を分類した。我々の発見は、それらの大部分がVASPのアライアンスに基づいていることを明らかにし、一方、すべてのVASPまたはブロックチェーンについて、通信ハブとしてピアツーピアメッセージを提案するいくつかのソリューションが存在することを明らかにした。さらに、長期的に解決すべき未解決の課題についての洞察を提供する。

索引用語-仮想資産、暗号通貨、FATF、トラベルルール、VASP、アンチマネーロンダリング、コンプライアンス

I. Introduction

仮想資産(VA)は、一般的に暗号通貨とも呼ばれ、世界中に分散型デジタル通貨システムとして認識されています。様々なVAが投資手段として使用されているが、犯罪収益を移転する手段としても使用されている。このような違法行為と戦うために、金融行動タスクフォース(FATF)は、取引所などの仮想資産サービスプロバイダー(VASP)への送り手と受け手に関する情報収集義務であるVA転送のための旅行規則を義務付けています。

VASPの観点からは、VA転送ごとに受信VASPの発見やVASP間の通信プロトコルの確立など、いくつかの技術的な課題が伴います。それでも、VAが広く受け入れられる金融商品となり、VA経済の将来の繁栄を目指すためには、適切なアンチマネーロンダリング/テロ資金調達の戦い(AML/CFT)努力が必要であると言えるでしょう。したがって、あらゆるVASP間の相互運用性と、その実装の効率と有効性が重要である。

ビットコインを皮切りとした2008年以降のVAの歴史全体と比較すると、VAのための旅行規則は2018年に提案された新しいイニシアチブであり、確立された研究文献は限られている。

トラベル・ルールを実施するためのソリューションがいくつかのベンダーによって開発されましたが、その数はいずれも大半を占めていません。ステークホルダーが利用できる領域知識がうまく整理されているとは言い難い。したがって、中立的な視点から体系的に整理された文献が必要である。
我々は、旅行規則全体像を見落とし、VASP、旅行規則のソリューションプロバイダー、規制当局、研究者がエコシステムを理解するのに役立つことを目的としています。本論文における我々の貢献は以下の通りである。

- 公共情報に基づいて、旅行規則に関する知識を集約する。
- 旅行規則の実施において、業界が直面する技術的な課題を列挙する。
- また、2024年3月時点で現在利用可能なソリューションを整理、分析、分類する予定です。

著者らはブロックチェーン解析ソフトウェアを開発した経験があり、現在、VA交換でトラベルルールを実施する立場にある。本論文で描かれた情報は中立であり、一般に入手可能な知識のギャップを埋めるものであると考える。

本論文の構成は以下の通りである。第II章では、VAによるマネーロンダリングのメカニズムと根拠、およびそれを規制するためのFATFの取り組みについて説明する。第III節では、FATFのVAに関する旅行規則の定義を再検討する。また、主要な国における現在の立法状況を説明し、「政府問題」について言及する。セクション IV からセクション VI では、VASP と業界が必然的に Travel Rule の実装で直面する課題について説明します。これらの各セクションでは、問題の概要を説明し、いくつかの可能な解決策を挙げ、各オプションが含むさらなる小さな問題を取り上げます。セクションVIIでは、主要なトラベルルールの解を観察し、解がどのように組み合わされるかを体系化する。第 VIII 章で未解決の課題やその他の一般的な問題について議論した後、第 IX 章で結論を述べる。

技術的な語彙[1]については、FATFの用語に従います。仮想通貨、暗号資産、または類似の金融商品は、仮想資産(VA)と呼ばれます。取引所または類似の事業体を仮想資産サービスプロバイダー(VASPs)と呼びます。

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

参考和訳
元論文 "FATF Travel Rule ’ s Technical Challenges and Solution Taxonomy", IEEE ICBC 2024

II. Background

A. 仮想資産と犯罪行為

ビットコイン[1]やイーサリアム[2]など、多くのVAがブロックチェーン技術[3]を用いて記録されている。ブロックチェーン上の情報は、インターネット上の各参加ノードで管理され、世界中で同期されています。VA保有者は、VAアドレスと金額を指定することで、資産を移転することができます。これらの機能は、目的や受領者に関係なく、支払いを可能にします。特に、行政機関、司法機関、金融機関が腐敗している国や地域では、VAは法通貨と比較して信頼できる金融インフラとして機能しています。支払いが改ざんされたり妨害されたりするリスクはなく、賄賂の要求もなく、送信者と受信者の両方のプライバシーが保護される。
これらの特性は、その利点にもかかわらず、犯罪者にとって便利である。VA保有者は住所から容易に特定できないため、法執行機関に気づかれることなく犯罪収益を送ることが可能である。また、国境を越えた移転が容易であるため、組織的な犯罪やテロに対する違法な資金調達を促進する可能性がある[4]。実際、VAは、Torのような匿名のネットワーク接続上で違法薬物、偽造品識別文書、その他の違法な資料が販売されている場合、売り手と買い手のアイデンティティを隠すために、ダークウェブ市場で支払いを行う手段として使用されています[5]。

ブロックチェーンのトランザクションを匿名化しない技術も知られていますが、基盤となるブロックチェーンにプライバシーを強化する機能を持つVAもあり、そのような分析に対する抵抗力を提供します。例えば、Ben-Sassonらは、zk-SNARKsに関する先行研究[7]に基づいてZcash[6]を開発した。Zcashは、送信側が宛先と、自分以外の人からの金額を隠すことができるシールドされたトランザクションをユーザーが作成することができます。Monero [8]は、リング署名と機密取引を使用して、同様の目標を達成しています。これらのブロックチェーンは、ブロックチェーン分野の利用において、高度な暗号技術の可能性を示している。しかし、これらのブロックチェーン上で違法な収益が交換されるリスクは大きい。FATFはAnonymity Enhanced Coins(AEC)のようなVAを指し、一部の国・地域ではVASPがAECに関連するサービスを提供することが禁止されている。

混合技術は、プライバシーと匿名性を高めることも知られています。CoinJoinは、複数のユーザーからのビットコインの引き出しを1つのトランザクションに集約し、資金の流れを不明瞭にしています[9]。Samourai ウォレットや Wasabi ウォレットのようなプライバシーに特化したウォレットには、以下の機能が組み込まれています[10]。イーサリアム上の分散アプリケーションであるTornado Cashは、zk-SNARKを使用してEtherとERC-20を同じ原理でミックスしています。これらのミキシングサービスは、プライバシーを維持したい正当なユーザーには便利ですが、犯罪者にはよく利用されています。トルネード・キャッシュの開発者は、それが10億米ドルを超えるマネーロンダリングに使用されていることを知り、金融当局から起訴されている[11]。

最近、犯罪者は、異なるブロックチェーン間で資産を移転し、ブロックチェーン上のある暗号通貨から別の暗号通貨へ不正資金を移動させることができるブリッジサービスを利用するかもしれません。Ellipticの分析によると、ブロックチェーン分析を回避するために使用される技術は、2022年8月以降、混合法からクロスチェーン法へとシフトしています[12]。このシフトは、Tornado Cashの制裁に対する反応と言われています。

B. 法執行の取り組み

ブロックチェーン分析ツールは、法執行機関がVAに関わる犯罪行為と戦うために使用されます。これらのツールが採用した最初の手法の1つは、コモンインプット・オーナーシップのヒューリスティックである。この方法は、同じ所有者によって制御される複数のアドレスを推測する[13]。
法執行機関は、違法行為者として特定された既知の住所を含む取引を監視し、資金の流れを追跡する。違法資金がVASPアドレスに預けられた場合、法執行機関は検索ワラントやその他の法的手段を用いて口座所有者を特定しようとする。容疑者が逮捕され、押収された機器に住所の秘密鍵が発見された場合、その事実は逮捕された容疑者の関与の強い証拠として利用される。

しかし、複数の法域にまたがる国境を越えた取引が行われる場合、判例の解決は非常に困難である。例えば、有罪判決の一つは2017年にギリシャで拘束され、Mt.に対してサイバー攻撃を実施した。Goxは、2011年から2014年にかけて日本で開催されたビットコイン取引所である[14]。彼は最終的にアメリカで起訴された。2023年に別の取引所であるBTC-eを運営し、盗まれた資金を洗浄した[15]。

攻撃者が用いる手法は、司法の執行を回避するために、より洗練されたものとなっている。複数のブロックチェーンにまたがる関連トランザクションを分析するためのデータ処理技術は、ますます重要になってきている。

C. FATFの規制の概要

FATFは、各国とその民間セクターのAML/CFT対策を規定するFATF勧告[16]を文書化している。これらの勧告は、FATF会員を通じて直接、またはFATF-Style Regional Bodies（FSRBs)を通じて間接的に、世界中の200以上の管轄区域に適用されます。参加国は、立法上の整合性を確保するため、定期的に相互評価を受け、評価報告書を公開する。各国は提言に沿った法律を制定することが期待される。

マネーロンダリングは3つのステップを含むと理解されています。

1) 犯罪収益が金融ネットワークに預けられる場所。
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.

このうち、(1)配置と(2)レイヤリングの防止はVAにとって特に重要であり、FATFは各国に対し、VASPsに関する規制の制定を要請している。

FATFは、(1)の配置に対する措置として、VASPを含むすべての金融機関に対し、顧客デューデリジェンス(CDD)を実施するよう要求しています。

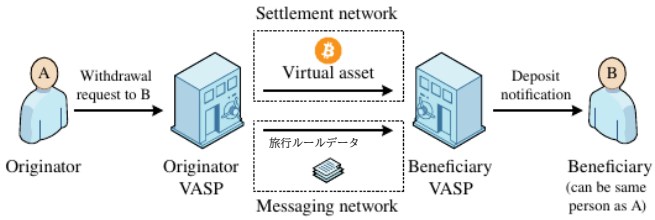


図1. 心臓の旅行ルール

コンプライアントな機関は、顧客を知る(KYC)と呼ばれるプロセスを通じて、リスクの高いユーザーが口座を開設するのを防ぐことができます。これには、合法的な身分証明書とその信憑性を確認し、制裁リスト、刑務所の免責事項、新聞のアーカイブなど、さまざまな情報源で検索を行うことで、顧客の身元を確認することが含まれます。

(2)レイヤリングに対する措置として、FATFは送受信機関の両方に対し、移転に関与する両者の身元を収集し、検証することを要求する。送出機関は、受入機関に顧客情報を伝達しなければならないが、これはトラベルルールと呼ばれる要件である。これにより、受信機関は送信者の身元を確認し、犯罪資金の流入を防ぐことができる。高リスクのユーザーの関与が疑われる場合、機関は疑わしい取引報告書(STR)を提出し、調査当局と協力するため、5年間すべての記録を保持すること。

III. トラベルルルーの現状

A. トラベルルールの詳細

旅行規則は、ユーザーがVASPを他のVASPに引き出すよう要求した場合、発信者VASPから受信者VASPに送信者の情報を伝達する義務として、不正確ではあるが広く知られている。勧告15(新技術)、勧告16(有線転送)、およびそれらの解釈ノートに基づいて、この論文の残りの部分の前提となるため、この規定の詳細を明確にする予定である。

FATF勧告では、送り手を発信者、受け手を受益者と呼んでいる。本稿の残りの部分では、これらに従うことにする。

図1および表Iに示すように、VASPはVAの移管に関して以下の要件を遵守する義務を負っています。

- 発案者VASPと受益者VASPは、送受信者と受信者の両方について、個人を特定できる情報(PII)を取得し、保持しなければならない。
- 発信者VASPは、発信者と受信者の両方のPIIを受益者VASPに送信しなければならない。
- 両VASPは、ユーザー側のPIIの精度を確保する必要があります。

これらは、顧客がVASP口座に保有するVAを、送信側または別の人物や事業体が所有するかどうかに関係なく、他のVASPの口座に送信する際に適用されます。

TABLE I
OBLIGATION OF VASPs

	VASPは受益者はVASPでなければなりません。			
collect	v	v	v	v
ensure accuracy of	√			√
conduct screening with	√	√	√	√
send to other VASP	√	√		
information of	originator	beneficiary	originator	beneficiary

本稿では、仲介VASPは一般的に直接転送されるが、仲介VASPがあれば、クロスボーダー電信送金の対応する銀行と同様の義務を負うため、仲介VASPは考慮しない。さらに、国内と国境を越えた移転の間で義務が若干異なるのに対し、議論を簡単にするために、すべてのVA移転をクロスボーダーと見なします。

PII には以下が含まれていなければならない。

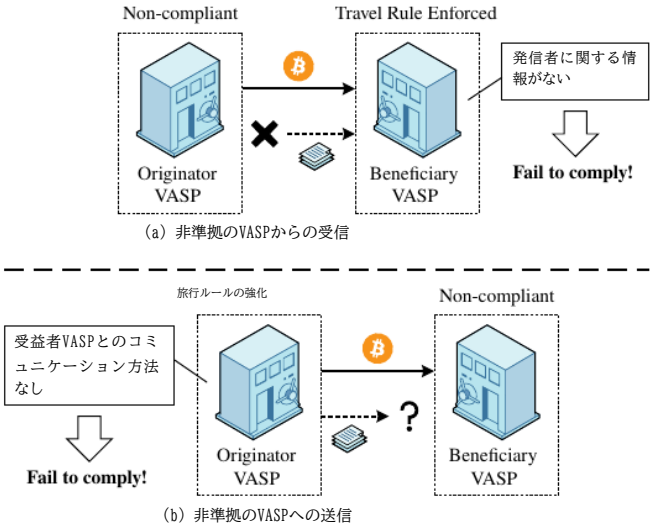
- 名前(通常、自然人の法律名と法人の登録名)。
- VASPまたはVAアドレス内のユーザーIDなど、転送処理に使用されるアカウント番号。
- (For the sender only) Address, national identification number, customer identifier, or date and place of birth.

PIIはVASPからVASPへの転送が1,000米ドル/ユーロを超える前または同時に送信されなければならない。しかし、VASPによって管理されていないアドレス、すなわち、ホスティングされていないウォレット間の転送には、この義務は適用されません。両VASPは、収集したPIIに基づきCDDを実施し、必要に応じて取引を処理または拒否しなければならない。PII は 5 年間保持され、要求に応じて法務当局に開示されなければならない。セクションII-Cで述べたように、FATF勧告は本質的に民間部門ではなく国に適用されるため、各国は上記の要件に沿った立法を行わなければならない。実際には、例外として、非FATF/FSRB加盟国または地域におけるVASPへの移転のための旅行規則の施行を除外することが一般的である。

B. Sunrise Issue

図2に示すように、旅行規則に準拠したVASPは、反対側のVASPに準拠していない場合、必然的に失敗する。これは、トラベルルール規制の実施スケジュールが国によって異なることに起因する。一部の国・地域では、VASP は既に現地法で巡回規則を遵守することが義務付けられており、 また、巡回規則がまだ制定されていないため、PII の送信なしに譲渡が実行される国もあります。この立法時期の違いは、サンライズ問題[17]、[18]として知られている。

サンライズの問題は、移転に関わるカウンターパーティが非準拠の場合、移動ルールに違反する危険性があるため、準拠したVASPに大きな影響を与える。コンプライアントオリジネーターVASPがコンプライアントでない受益者VASPと通信できない場合、オリジネーターVASPはPIIを送信できない。



(a) 非準拠のVASPからの受信

(b) 非準拠のVASPへの送信

Fig. 2. Sunrise Issue

同様に、準拠した受益者VASPは、非準拠の発信者VASPからPIIを受け取ることができないため、送信者に対してCDDを実施することができません。

一方、まだトラベル・ルールを制定していない国の VASP は、遵守することが困難である場合がある。特に巡回規則が複数の当事者を巻き込むことを考慮すると、VASPは法的強制力なしに余分な費用を負担することをためらわれるのは妥当なことである。さらに、VASPがPIIを送信するのを妨げるプライバシー保護法との抵触がある可能性がある。

このような状況に対し、FATFは、サンライズ問題を解決するための立法を促進するために、トラベルルールを実施していない国に対して、次のような働きかけを行っている。彼らは、制定された法律の有効性と運用性を評価するために、積極的に管轄区域と協力している。

C. メッセージングフォーマット

IVMS 101 [19]は、VASP 間メッセージング基準に関する共同作業部会(JWG)が設立し、旅行規則遵守のために VASP 間で交換される情報のスキーマを定義しています。その目的は、世界中のVASPが合意した共通のデータモデルを確立することであった。

JWGは、相互運用性を確保するために、設計プロセスにおいてSWIFTメッセージフォーマット、ISO 20022 [20]、法人識別器 [21]など、さまざまな規格に言及しています。各国のビジネス慣行や文化的背景を考慮し、例えば、ある自然人の名前を表す複数の表現を採用し、欧米諸国で使われているアルファベット以外の文字の音訳をサポートするなど、さまざまな形で採用されています。

IVMS 101では、データモデルとしてシンプルにするために、シリアライズ、エンコーディング、暗号化の方法については規定されていません。具体的なコミュニケーションプロトコルは別途定義する必要があり、実際には各VASPの裁量に委ねられる。

D. 現在の技術的な課題の概要

トラベルルールの実装には、3つの大きな技術的課題がある。これらの課題は、トラベルルールの手順で発生する順序で、以下に概説されています。

1) 宛先VASPの特定。PIIが正しい受信者に送信されるようにするために、発信者VASPは宛先アドレスの制御VASPを識別する必要がある。もし、そのアドレスがホスティングされていないウォレットに属している場合、オリジネーターVASPもそれを知りたいと思うでしょう。この課題を解決するために、中央のアドレスデータベースを利用したり、他のVASPに働きかけてアドレスを管理しているかどうかを問い合わせたりと、さまざまなアプローチが存在します。これについては、セクション IV で説明する。

2) 住所所有の証明 受益者VASPに焦点を当てよう。VASPが、ある特定のVAアドレスを他の人に制御できることを証明したい場合、それは困難な場合があります。これは、多くのVAシステムにおいて、アドレスは公開鍵から派生するが、その逆はできないからである。その結果、他の者、例えばオリジネーターVASPがアドレスに対応する鍵を持っているかどうかを検証することは困難である。この問題は、監査プロセスにおけるVAの所有権を証明するために、トラベルルール以前のVASPによって知られており、Proof of Reserveとして知られている。Hardjonoらは、VASPのウォレットを証明する様々な方法について研究を実施している[22]。

アーキテクチャによっては、受益者VASPは、オリジネーターVASPにリアルタイムで、または集中型VAアドレスディレクトリへの登録により、取引前に、暗号証明が存在する場合、それを提供することができる。VASPはまた、法的保証のような他の手段によって住所のコントロールを確保することができる。VASPが現在使用しているアプローチについては、セクションIVで説明する。

3) PII トランスミッション・インターフェース。発信者VASPが受益者VASPを特定した後、発信者間のコミュニケーション・チャネルを構築するために交渉が必要である。

最も分散化されたアプローチは、各VASPが他のすべてのVASPと直接ピアツーピア通信チャネルを確立することを含む。逆に、最も集中的なアプローチは、共同管理されたVASPディレクトリを維持することで、これによって、発信者VASPは受益者VASPの通信エンドポイントを容易に見つけることができます。しかし、この2つの方法は極端な目的を表しています。実際には、複数のVASPの間でアライアンスを形成することで、よりバランスのとれた解決策を実現することができる。この課題の詳細については、セクション VI で説明する。

IV. 課題1:デスティネーションとデンティフィケーション

図3のようなシナリオを考えてみよう。アリスはVASPであるV aからボブのアドレスaddrにVAを転送することを要求している。撤退要求の際、V aはアリスにボブのPIIとVASPを提供するよう要求する。アリスとボブは同じ人かもしれないことに注意してください。

アリスはV aに誤った情報を、間違いや意図によって提供することがある。したがって、アリスの宣言に関係なく、V aはaddrが以下のいずれかによって制御されているかどうかを判断する必要がある。

V_C) VASPs that comply with the Travel Rule and have a known communication channel,

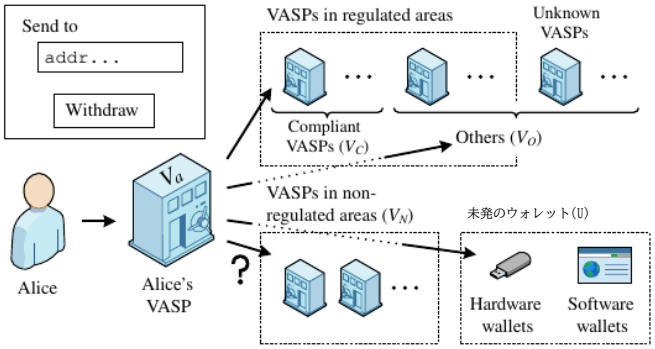


図3. 目的地VASPの特定に関する課題

V_N) VASPs that are neither in a participant country of FATF/FSRB nor in a FATF blacklist country and have no obligation to comply with the Travel Rule, or
V_O) other VASPs with no known communication channel,
or *addr* is one from:

U) 未発着のウォレット。

巡回規則の遵守に従って、V b∈V C 、アリスとボブのPIIを送信する、またはV b∈V N ～ UをPIIを送らずに送信する場合、V aは転送を進めることができる。V a は V O への引き出し要求を拒否しなければならない。

アプローチ1-A. 撤退先を制限する

V aはアリスに引き出しがV NかUのどちらかであることを宣言するよう委任することができる。しかし、この方法は、グローバルな主要なVASPがFATF加盟国に位置していることを考えると、ビジネスの観点から正当化することは困難であろう。さらに、この方法は、アリスが誤宣言をする可能性には対処していない。

アプローチ1-B. ルックアップサービスの利用

addrの制御VASPを見つけるためのルックアップサービスが存在するとする。V aはアリスの引き出し要求に対してルックアップサービスを利用することができる。基本的な考え方として、ルックアップサービスがaddrの制御VASPとして$V_b^\star$で応答する場合、V aはPIIを$V_b^\star$に送信します。そうでなければ、V aはそれを非ホスティングとみなすことができる。図4はそのアプローチを示している。

V aは、可能であれば、さらにブロックチェーン分析ツールを使用することができます。ツールは通常、過去にaddrからの取り下げが行われた場合、ある程度の推測を提供します。一方、新たに生成されたアドレスを特定できない場合があり、不明な点として回答する可能性がある。多くのツールが確率で結果を報告しているが、ここでは簡単のため、最も可能性の高い候補のみを検討する。

アルゴリズム1は、V aが使用できる典型的な決定アルゴリズムを示している。VまたはNilを返すルックアップは、ルックアップサービスへのクエリを表します。Analyze Retning V、U、またはunknownは、ブロックチェーン解析ツールへのクエリを表します。
このアルゴリズムでは、アリスのaddrに関する宣言をV bとし、V C ¦V N ¦V O ¦Uの1つとする。
まず、V a は V b が V O でないか、または転送要求を拒否するかをチェックします。現実には、VASPの中には、Sunriseの問題による妥協案として、準拠ではないものの、PII伝送なしで転送を進めているところがあります。

次に、ルックアップサービスで$V_b^\star$によるaddrの登録が見つかったとします。V b が $V_b^\star$ と一致する場合、V a は V b への PII 伝送に確信を持って進むことができる。その他、カスタマーサポートはアリスに連絡し、転送の目的について追加の検証を行う。状況に応じて、転送を拒否するか、STRをファイルする必要がある場合があります。

addr に関するレコードがない場合、例えば V b がルックアップサービスに登録できない場合、V a は addr の分析を行うことができる。解析結果をV_b^- 、V C ¦V N ¦V O ¦U¦unknown の間で1つとする。

V b = V_b^- または V_b^- = 未知、すなわちアリスの宣言が解析結果と一致するか、ツールが住所に関する洞察を持っていない場合、V a はアリスの宣言に基づいて進行するはずである。すなわち、(V C)であればPIIから$V_b^\star$への伝送で、(V O)であれ(U)であれ、仮想転送を開始する。後者の場合、リスクアセスメントのための追加的な検証が望ましいかもしれないが、それは直ちに旅行規則の違反とはならない。
その他、アリスがVASPで応答した際に未応答と宣言した場合など、V aは可能な解析エラーを考慮し、結果に対するツールの信頼度に応じて応答を調整する必要がある場合があります。

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 it 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) データガバナンスとアクセス制御。2) データガバナンスとアクセス制御:プライバシーの観点から、ルックアップサービスのデータベースへの一般公開は適さない。理想的には、特定の加算器への転送を開始する必要があるVASPだけが、転送プロセス中にのみ、加算器を検索する機能を持つ必要があります。したがって、ルックアップサービスでは、適切なアクセス制御とレート制限を実装することが重要である。

もう一つの懸念は、ルックアップサービスの運営者が、VASPやエンドユーザーの同意なしにデータを使用する可能性があることです。この情報は、ブロックチェーン分析会社がファンドの流れを理解する上で貴重なものとなる可能性があります。解決策としては、登録時にアドレスをハッシュ化することが考えられるが、この場合、所有権を証明することが困難である。これについては、第 VIII-B 章のセクションでさらに説明する。
3) 未登録アドレス。VASPは未登録アドレスを検索できないため、V bが登録に失敗した場合、V aがaddrをUと誤って分類してしまう可能性がある。このことは、AML/CFT[23]のリスクベースアプローチの補助的な補助として、

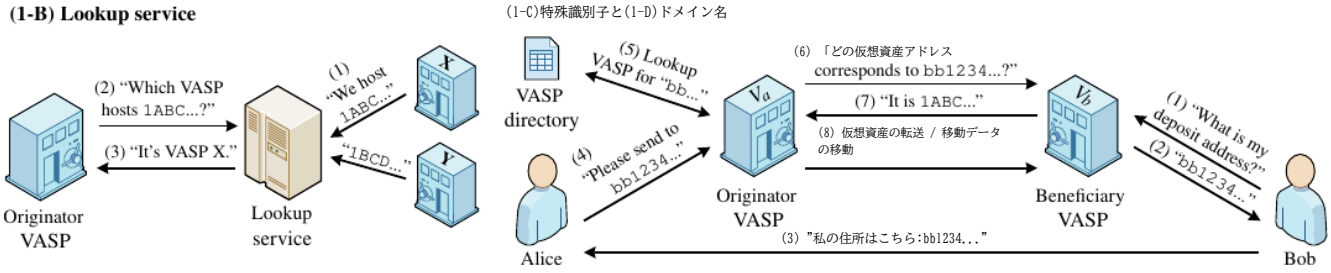


図4. 図4 目的地VASP特定のための可能なアプローチ

アルゴリズム 1 撤退のコンプライアンスと目的地の意思決定フロー

```
V b ←アリスのaddrに関する宣言
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^⋆)                虚偽の宣言の可能性
        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
```

ブロックチェーン分析ツールの重要性を強調しているが、分析に時折エラーが発生する可能性があることを言及する価値がある。したがって、参加VASPは、そのアドレスが生成された後、タイムリーに登録することを推奨することが不可欠である。

4) 複数のルックアップサービス 複数のルックアップサービス。複数のトラベルルールソリューションの出現により、VASPが複数のルックアップサービスに接続できるようになった。このようなシナリオでは、VASPは少なくとも1つのサービスから肯定的な回答を得るまで、またはすべてのサービスから否定的な回答を得るまで、同時にルックアップを行う必要があります。これは、ユーザーの引き出し完了を遅らせる原因となる可能性があります。
決済ネットワークとメッセージングネットワークの時間差による性能の問題は、金融ネットワークの設計時に特定されている[24]。VA転送はメッセージングが完了するのを待たなければならないので、ルックアップのレイテンシを最小にする必要があります。

5) 住所所有の証明。ルックアップサービスが所有権の証明を必要とせずに住所登録を受諾する場合、不正な登録の危険性がある。

これは、VASPが許容しにくい顧客のPIIの開示につながる可能性がある。これを防ぐために、ルックアップサービスは、住所所有の証明を要求する、または、情報の正確性について登録当事者に一定の保証を要求する仕組みを実装する必要があります。

アプローチ1-C. 特別な識別子の使用

特別な識別子の使用は、VASP上のアカウントを表現するためのVAアドレスの代替となります。これにより、ルックアップサービスの必要性がなくなります。図4に描かれた数字に沿った次のステップで、その例を示す。

(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.

特別に符号化された識別子の使用は、国際的な銀行システムにおいて、受取人およびそれぞれの金融機関を識別するための一般的な慣行である。例えば、欧州で広く採用されている国際銀行口座番号(IBAN)[25]は、2文字の国別コードとチェックの数字にしたがって、口座番号と金融機関の両方を Basic Bank Account Number を使って符号化したものである。もう一つの例は、SWIFT Bank Identifier Code (BIC) [26]で、8文字または11文字のコードによって世界中の金融機関とその支店の識別を容易にするものです。

特殊識別子の書式を検討する場合、元のアドレスが含まれないようにシステムを設計することをお勧めします。この方法は、いくつかの理由で有利である。

- 特殊な識別子からアドレスを除外することで、より簡潔でカスタマイズ可能な表現が可能になります。
- これにより、アリスが移動ルールを回避するために偽の識別子を作成する可能性がなくなります。

移動ルールの性質上、V a は PII 伝送のために V b との通信を確立しなければならない。この処理の最初に、V aはaddr⋆をaddrと交換する必要があります。

1) VASPディレクトリの必要性。このアプローチでは、VASPの包括的なリストを維持する必要がある。このリストはVASPディレクトリと呼ばれ、オンラインまたはオフラインで管理することができ、すべてのVASPを集中管理して含めることができ、VASPの内部システム内にキャッシュして定期的に更新することができます。

2) 非ホスティングウォレットとの衝突。2) 非ホスティングウォレットとの衝突:アリスは非ホスティングウォレットに資金を引き出すために、V aは従来のVAアドレスへの引き出し要求を受け入れなければならない。しかし、これは悪意のあるアリスが、旅行規則を回避するために単にaddrを指定することによって、誤った宣言をする危険性をもたらす。その結果、特殊識別子を使用する利点が損なわれてしまいます。

アプローチ1-D. ドメイン名を用いた転送

(1-C)の変形として、VASPのドメイン名は特殊識別子の一部として使用することができます。ルックアップサービスやVASPディレクトリが不要になります。この識別子をDeposit URIと呼ぶ。

アリスがボブにビットコイン転送を行いたいとする。彼はアリスにV asp-b.example/btc/12345の預金を提供し、これには以下が含まれる。

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

V b は与えられた URI 上に特定の API を実装しており、V a はこの API を呼び出して実際の addr を取得することができる。API仕様は、VASPが事前に定義し、合意したものでなければなりません。
実際には、VASPはPIIの送信義務を遵守するために、インターネット上でリーチャブルなドメイン名を持っていると考えるのが妥当である。提供される預託金構造はその一例であり、HTTPSや他のプロトコルと明確に区別するために専用のURIスキームを定義することができます。

1) DNS特有のセキュリティ上の懸念。このアプローチは完全にDNSに依存しており、DNSは異なるアーキテクチャとセキュリティ上の意味を持つ。その結果、VA転送は既存の転送に加え、DNSセキュリティリスクにも脆弱になる可能性がある。例えば、攻撃者は特定のVASPであるV xをターゲットとし、DNS汚染によってV xに寄託されることを意図したすべてのVAを盗む可能性がある[27], [28]。さらに、寄託URIで同様のDNS名を使用したフィッシング攻撃のリスクがある可能性があります。さらに、VASP がドメイン名を変更した場合、古い寄託金 URI は有効でなくなる可能性があります。

V. 課題2:広告の投稿を 早める

受益者VASPは、addrを管理する場合、(1)発信者VASPがセクションIII-D2で述べたように、PII送信を開始する前に特定された受益者VASPの正しさを確認したい場合、(2)ルックアップサービスが(1-B)で述べたように、参加VASPからの新しい登録要求を確認したい場合など、アドレスに対する支配権を主張する必要があるかもしれません。

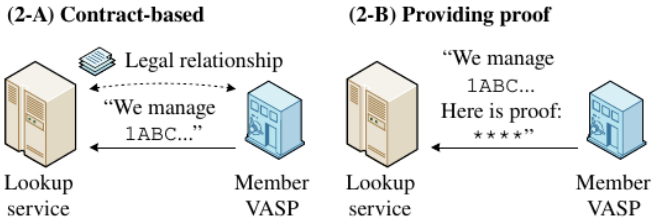


図5. 住所の所有権を主張するための可能なアプローチ

アプローチ2-A. 契約上のコミットメント

一つの可能性は、請求するVASPがaddrに対応する鍵を持つことを法的に保証することである。この保証は、単に契約上の約束である。

この方法は、(1-B)で述べたように、低リスクのプロファイルを持つVASPのみが参加できるアクセス制御型ルックアップサービスを容易にするものである。また、(3-A)で後述するように、VASP間のピアツーピア通信や、(3-C)で言及したアライアンスネットワークの構築にも適合する。
契約上の枠組みは、VASPが支配下にない住所を宣言するリスクを制限するのに役立つが、このリスクを完全に排除するものではない。

Approach 2-B. Cryptographic Proof

もう一つの選択肢は、addrの暗号証明(典型的にはaddrの秘密鍵から生成されるデジタル署名)を生成することである。このプロセスは、addrからの転送のためのVAトランザクションに署名するのと似ています。

V bがV a(あるいはルックアップサービス)に対してaddrの所有権の主張をしていると仮定すると、署名する必要のあるクレームメッセージmsgは以下のフィールドを含むべきである。

- V b の一意な識別子で、V b の法的名称とすることができる。
- *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.
- その他のオプションのメタデータ。例えば、ブロックの高さやタイムスタンプは、addrの有効性をブロックチェーン上の特定の時間に関連付けるものです。

他者による証明の再利用を誤らせるため、プロトコルではV bの一意な識別子またはV aによるチャレンジメッセージのいずれかを必須とする。

V a は、msg のデジタル署名とそのフィールドの有効性を検証する。有効な場合、V a は自信を持って PII の送信を進めることができる、あるいはルックアップサービスは V b による加算器の登録を受け入れることができる。
上記の方法は、単に単一の秘密鍵から addr を生成するだけでよい場合に有効である。また、階層的決定論的(HD)ウォレットでも動作し、1つのマスターシードから異なるキーとアドレスのセットを生成します[29]。しかし、現実には、VASPは他にもいくつかの異なるタイプのVAアドレスを使用しており、それらを考慮する必要があります。

- コールドウォレット。キーはオンラインでは使用できない場合があります。

- マルチシグネチャーウォレット、シークレットシェアリングスキームウォレット、マルチパーティコンピューティングウォレット。鍵や株式の保存は同時にできない場合があります。
- スマートコントラクトウォレットまたは鍵更新機能を持つVA。暗号鍵からアドサーを導出する方法がない場合があります。

それぞれについて詳しく説明します。

1）コールドウォレット V bは、サイバー攻撃から保護するために、addrに対応する鍵をオフラインで保持することができる。これは、V b のデジタル署名 msg の遅延の原因となる可能性があります。最悪の場合、Addrからの離脱が起こるまで証明を延期する必要があるかもしれない。これはV aからV bへの転送とは無関係であり、予測することはできない。その結果、V a は転送時に V b が加算器を持っていることを確認できない。
解として、V bは、最初にコールドウォレット環境で生成されたときに、アドバの証明を事前に生成することができる。

2）マルチシグネチャウォレット。ビットコインのようなVAは、n個のキーのうちm個がトランザクションに署名するために使用されるときに引き出しを許可するマルチシグネチャアドレスを可能にする[30]。多重署名アドレスは、特定の順序でn個の公開鍵とmの値によって一意に識別される。VASPは、セキュリティやバックアップのために、例えば、鍵が異なるオフィサーによって個別に管理される場合や、安全な金庫でオフラインで管理される場合など、マルチシグネチャアドレスを使用することができます。
多署名アドレスの所有権を証明する簡単な方法は、そこから転送するためにトランザクションに署名するのと同じ方法で、m個の鍵を使用して署名することである。しかし、コールドウォレットの場合と同様に、VASPがどのように管理するかによって、すべてのm個の鍵が同時にアクセスできるわけではありません。
一つの可能な解決策は、V bがn個のキーのうち1つだけでmsgに署名するようにプロトコルを変更することである。msgはすべてのn個のキーのリストを含む必要があります。V aがリストされたキーのいずれかによって署名の有効性を確認すると、V aはaddrがV bに属すると判断できる。
しかし、この解決策には注意点があります。セミカストディアン[31]やいくつかのVASP[32]では、マルチシグネチャウォレットを作成するための公開鍵をインポートすることができます。これは、異なるVASP上のn個のキーのうち、いくつかのキーを再利用する結果になる可能性があります。

3）秘密分散型スキームウォレットと複数当事者計算ウォレット。暗号技術により、1つの秘密鍵を回収閾値(m)で複数(n)の株式に分割することができる。この最も初期の方法はShamirの秘密共有[33]であるが、より洗練されたプロトコルも研究されている[34]-[36]。これらのアプローチにより、VASPは秘密分散スキームウォレットやマルチパーティ計算(MPC)ウォレットを作成することができ、マルチシグネチャアドレスのアクセス制御を模倣することができます。
暗号の証明にはn個のうち1個の鍵で十分かもしれないマルチシグネチャーウォレットとは対照的に、実際にm株を使う以外に、アドサに対する制御を実証する一般的な軽量化手法は現在のところ存在しない。

4）スマートコントラクトウォレット、または鍵の更新が可能なVA。VAシステムによっては、アドレスとその署名鍵の間に暗号化関係がない場合があります。これは、アドレスに対応するキーがない場合、またはアドレスが生成された後に、アドレスに関連するキーのセットが変更される場合があることを意味します。
イーサリアムでは、外部所有アカウントと呼ばれる通常のアドレスの代わりに、スマートコントラクトを使用してイーサやERC-20トークンを管理することができます[37]。VASPは、スマートコントラクトウォレット[38]、[39]を利用して、セキュリティの向上を目的としたマルチシグネチャウォレットをシミュレートすることができます。これらのスマートコントラクトウォレットは、ブロックチェーンの状態に基づいてプログラム的に割り当てられたVAアドレスを持っており、これらのアドレスに直接一致する暗号鍵は存在しません。
Flowブロックチェーンは、Flow[40]のアドレスに相当するアカウントのアクセス制御リストを変更することをサポートしています。アカウントアドレスは固定されていますが、アカウントの所有者は、それぞれ異なる重みで、それに関連するキーのリストを変更することができます。トランザクションは、重みの閾値を満たす登録された鍵の組み合わせによって署名される必要がある。

これらの例は、ブロックチェーンノードとタイムスタンプまたはブロックの高さ(msg)を使用して、V a(またはルックアップサービス)がV bが主張するアドラーと公開鍵との関連性を確認する必要性を強調しています。さらに、ルックアップサービスでは、ブロックチェーンの状態の変化を監視し、アドサーの所有権の変化を検出する仕組みを実装する必要があるかもしれません。

VI. 課題3:第二の伝達インタフェース

V a が転送の対応物として V b を特定したと仮定する。PII を送信するためには、V a が V b への通信路を確立する必要がある。しかし、具体的なチャネルは事前にわからないことが多い。コミュニケーションの様々な側面について、以下のような合意が必要である。

- ネットワーク接続性。インターネット経由、VPN経由、または閉じた専用ネットワーク経由か?
- 各当事者のネットワークアドレス。ピアVASPはDNSによって解決されるのか、それともIPアドレスとして提供され、どのように解決されるのか?
- *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?

図6は、様々なアプローチを示したものである。サイバー攻撃は、PIIの開示につながる可能性があるため、各アプローチの設計におけるネットワークのセキュリティは重要である。

アプローチ 3-A. ピアツーピア

最も明白な方法は、VASP間の転送の前に通信プロトコルに合意することです。透過プロセスは、VASPごとにカスタマイズすることができ、柔軟なソリューションを提供します。

例えば、図に示すように、V a と V b は以下の API エンドポイントを公開することがあります。

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 transmits PII to V_b, and vice versa. They may choose to use the IVMS 101 data model over the API.

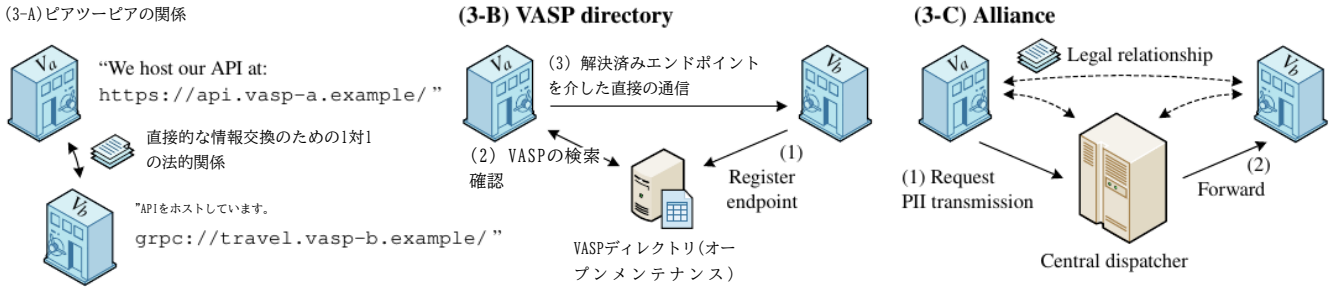


図6. PII伝送のためのVASP間通信の可能なアプローチ

このアプローチの大きな欠点は、すべてのVASPのペアが互いに独立した契約を結ぶことを要求しているため、実用性と実現可能性がないことである。さらに、各VASPで使用される異なるプロトコルやAPIに対応するためには、多大な開発努力と時間が必要である。

アプローチ 3-B. 公開VASPディレクトリ

代替案として、任意のVASPがPII送信のための企業名、ネットワークエンドポイント、管轄区域、およびその他の必要な情報を登録するために参加できるオープンディレクトリを構築することができます。

開いている VASP ディレクトリの管理は柔軟で、様々なアプローチが可能です。このディレクトリには頻繁な更新を必要としない情報が含まれており、各VASPで高速に検索できるようにキャッシュすることができます。(1-D)アプローチと組み合わせることで、DNSインフラを拡張可能なものとして、この方法を実装する可能性が推測される。

1) カバレッジと精度。1)カバレッジと精度:世界中のVASPの包括的なリストを網羅する必要があるため、ディレクトリの品質を確保することが重要です。しかし、このディレクトリを無許可で一般に編集できるようにすることは、その精度にリスクをもたらします。この結果、既存のVASPに関する情報が正しくなかったり、類似の名前の偽リストが含まれていたりして、PIIの盗難につながる可能性があります。

これらのリスクを軽減するために、ディレクトリの編集をVASPのみに限定し、各企業が管轄区域ごとに1つのレコードしか持たないことをお勧めします。そのために、TLSの証明書で使用されている拡張検証と同様の検証プロセスを提案する。このプロセスにより、新規に登録された企業の真正性が確認され、正当な VASP のみがディレクトリに含まれていることが確認されます。また、定期的にディレクトリを更新し、最新かつ正確な状態を維持する必要があります。

2) プロトコルとAPIの標準化。VASP ディレクトリには、VASP のエンドポイント URL や ID を認証するデジタル証明書など、さまざまなパラメータが記載されている場合があります。その場合でも、VASPは通信プロトコルの標準化も検討すべきです。これは、VASP間のシームレスで効率的なインタラクションを保証するために、プロトコルとAPIに関するコンセンサスを得ることを意味します。IVMS 101 メッセージモデル規格は業界で大きな支持を得ているが、標準化を他の層の PII 伝送プロトコルにも拡張することが重要である。

これにより、相互運用性が促進され、ディレクトリの全体的なセキュリティと信頼性が向上します。

アプローチ 3-C. VASPのアライアンス

(3-A)と(3-B)のバランスを取るために、一定の信頼度を持つVASPはアライアンスを形成し、メンバーVASPディレクトリを共同で管理することができます。このディレクトリでは、メンバーのVASPがピアツーピア通信のために互いの情報に簡単にアクセスすることができます。また、アライアンスは、各メンバーにコネクティビティを提供することで、コミュニケーショ ンハブとして機能することもできます。VASPは、アライアンス内にコミュニケーション基準を設けることで、トラベルルールの効率的な実施と運用を確保することができます。

この手法の特筆すべき点は、(1-B)との相性が高いことである。アライアンスはすでにリスクプロファイルを評価したVASPで構成されているため、前述の懸念を払拭しつつ、アライアンスによるルックアップサービスを安全に運営することができる。さらに、アライアンスにとって、適切なVASPを特定するために、ルックアップサービスを提供することは理にかなっている。

このアプローチの潜在的な欠点は、異なるアライアンス間の互換性の問題である。複数の同盟が形成された場合、異なる同盟の境界を越えてVA転送が不相応である場合、その境界を越えることはできない。現実の例として、日本のVASPは、参加するアライアンスによって、事実上2つのグループに分けられる[41]。ユーザーは、異なるアライアンスのVASP間で転送するために、ホスティングされていないウォレットを使用することが要求されます。同様のケースは、スイスでも報告されている[42]。
VASPは、グローバルに多くのVASPと通信するために複数のアライアンスに参加することができますが、これは、参加する各アライアンスの運用とメンテナンスの負荷、および支払うコストを増加させます。これは、クレジットカード商人が複数の決済処理ネットワークに接続されているのと同様です。

There are two ways to solve this issue.

1) 同盟によって提供される橋。1) 同盟によって提供される橋:アライアンスが、他のアライアンスとのアーキテクチャの互換性を確保し、通信を変換する橋を提供することである。各アライアンスにおける潜在的なアーキテクチャの変更により、このアプローチは実装に時間がかかるかもしれないが、実現可能である。
2)仲介型VASP。2)仲介型VASP:複数のアライアンスに参加しているVASPがゲートウェイとして機能し、国際的なフィアット通貨送金のカウンターパートバンクと同様、このVASPを通じた送金を容易にする手法。

TABLE II
COMPARISON OF TRAVEL RULE SOLUTIONS

	Approaches	TRUST (USTRWG)	TRISA	Sygna Bridge	VerifyVASP	Shyft Veriscope	OpenVASP / TRP	Netki / TransactID
課題1)目的地VASPの特定	(1-B) Lookup service	✓	✓			✓		
	(1-C) Special identifier			✓				✓
	(1-D) Domain name						✓	
課題2)住所所有権	(2-A) Contract-based	✓			✓	✓		
	(2-B) Providing proof	✓	✓	✓				
課題3)PII伝送	(3-A) Peer-to-peer						✓	
	(3-B) VASP directory					✓		✓
	(3-C) Alliance	✓	✓	✓	✓			

この方法はよりシンプルであるが、取引手数料、プライバシー、解の複雑さに関する懸念があり、我々の知る限りでは例が観察されていないと思われる。しかし、この方法はクロスチェーンスワップDeFiに有効である可能性があり、スマートコントラクトの使用により複数のブロックチェーン間でVAを交換し、仲介VASPとしての役割に十分に適している可能性があると推測される。

VII. クイントラベルの実装

A. Summary

我々は、一般に公開されている情報を用いて、トラベルルールの複数の解を調査した。これらの多くは、2019年から2021年の間に提案・開発されたものであるが、それ以前に存在した技術も活用したものもある。表 II は、先に説明したアプローチに基づく比較の概要を示している。以下に、主な観察結果をまとめる。

1) アライアンス・ベースのソリューションの優位性 調査したソリューションのうち、USTRWG(現在、TRUST)、TRISA、Sygna Bridge、VerifyVASPはいずれも(3-C)のようなアライアンス・ベースのアプローチを採用している。これらのソリューションは、VASPを採用することで、アライアンスを引き付け、拡大することを目的としています。VASPは、アライアンスに参加する前に徹底的なデューディリジェンスプロセスを受け、その正当性を確保します。これらのソリューションの確立は、ブロックチェーン分析会社によって非常に促進されたことは注目に値します。Sygna BridgeではElliptic、VerifyVASPではChainalysis、TRISAではCipherTraceです。
(3-A)ピアツーピア通信方式には、2つのソリューションがあります。Netki/TransactIDとOpenVASPによるTRPです。これらのプロトコルが現在どの程度VASPに採用されているかは不明である。

最後に、他の2つのソリューションはブロックチェーン技術を活用し、(3-B)オープンディレクトリモデルに分類される。Shyft VeriscopeとEthereumベースのOpenVASP(レガシー)です。Shyft Veriscopeのパブリックブロックチェーンでは活動が限られており、その使用状況を積極的に確認することが困難である。イーサリアムベースのOpenVASPソリューションは、もはやメンテナンスされていません。

2) 様々な住所検索方法。USTRWGとVerifyVASPがアライアンス内でルックアップサービスを提供することを確認した。特に、VerifyVASPは、アライアンス内の各VASPに直接問い合わせ、転送要求を行うというユニークなアプローチをとっています。USTRWGとVARIVASPはともに(2-A)アプローチで暗号証明を義務付けていないようである。

TRISAとSygna Bridgeはブロックチェーン解析の利用を積極的に推進している。前述したように、これらの分析企業の関与は、このことに影響を与えている。

TransactID、OpenVASP、Sygna Bridgeなどの初期のソリューションでは、特別な識別子を使用してメソッドを実装していました。しかし、新しいソリューションは、特別な識別子の使用を積極的に提案するものではありません。このことは、それらを導入するには複数のステークホルダーの協力が必要であり、困難であることを示唆している。

B. トラベル・ルール万能解技術(TRUST)旧米国旅行規則国際法(TRUST)旅行ルールワーキンググループ(USTRWG)

Travel Rule Universal Solution Technology (TRUST) [43]は、2022年2月に設立されたネットワークで、米国のCoinbaseが中心となっている。仮想資産取引所 TRUSTに関する公開情報は限られているが、公式発表ではいくつかの重要な特徴があることが示されている。PII を一元的に保存せずに送信する機能、アドレス所有権検証の仕組み、すべての VASP のデューデリジェンスプロセスなどがある[44]。TRUSTは、2020年10月にホワイトペーパーを発表した米国旅行規則作業部会(USTRWG)に先駆けて行われた[45]。TRUSTについては公開されていないため、主にUSTRWGのホワイトペーパーを基に分析する。

ホワイトペーパーの通り、当初は(1A)を利用し、参加したすべてのVASPが住所を掲載する中央のBulletin Boardを採用した。本システムは、インターネットから分離されたアクセス制御された閉ネットワーク上で動作するように設計されている。USTRWGのホワイトペーパーの時点では、(2-A)住所の証明は提供されていない。TRUSTの発表から、メンバーVASPが証明を要求される(2-B)にシフトしたと考えられる。ホワイトペーパーにあるように、PIIの伝送は以下のように行われます。

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) PIIの送信とVAの転送の時間的な違い。V b がアドの所有権を適時に主張しない場合、V a は先に転送を進め、アドが V b によって主張されると後で PII を送信する。しかし、FATFは後に、取引は送金前または送金と同時に行う必要があると指摘した。このプロトコルは、ネットワーク上のすべての参加者がT以下の時間内にすべての投稿された住所を請求することを保証する時間Tを待つことによって修正することができる。しかし、TRUSTがこれを修正したかどうかは不明である。

2) 他の種類のVAに対するサポート不足。当初、USTRWGは最初のフェーズでBitcoinとEthereumのトランザクションのみをサポートしました。ただし、FATF は、すべての仮想資産にはトラベルルールが適用されると指摘した。
TRUSTがUSTRWGの提案と同じアーキテクチャを持っていると仮定すると、TRUSTについても同様の観察が可能である。

C. 旅行規則情報共有アライアンス(TRISA)

旅行規則情報共有アライアンス(TRISA)[46]は、2019年9月10日に米国のCipherTraceが主導するプラットフォームです。ブロックチェーン解析ツールベンダーTRISAは様々な情報をオープンソースとして公開しています。
TRISAはVASP間の同盟として運営されている。新しいVASPがTRISAに参加する場合、デューデリジェンスのために質問票のチェックリストを提出することが要求される。プロセスが完了すると、VASPはTRISA VASP Directoryにリストされ、検索可能になります。

技術的な観点から、TRISAは厳密なPKIモデルを採用している。アライアンスは、TRISAが運営するTrusted VASP CAからEV証明書を発行しています。VASPは、EV証明書で認証されたmTLSチャネル上のgRPC上でプロトコルバッファにエンコードされたメッセージを介して通信します。

TRISAは今後、住所検索機構や所有権検証を実施する予定であるが、現在のところ、明確な解決策は示されておらず、参加するVASPに選択肢が残されている。彼らは、ユーザーの宣言に基づいて宛先VASPを照会したり、(1-A)で述べたようにアドレスを記録するためにブロックチェーンを使用するなどする方法について言及しているが、最終的にはブロックチェーン分析ツールを使用することを推奨しているようである。
2023年8月、TRISAはOpenVASP / TRP [47]とSygna Bridge [48]との相互運用のための概念実証の完了を発表した。

D. Sygna Bridge

Sygna Bridge [49]は、台湾のブロックチェーンセキュリティ企業であるCoolBitXと英国のブロックチェーン分析ツールベンダーであるEllipticが提供するVASPアライアンスです。

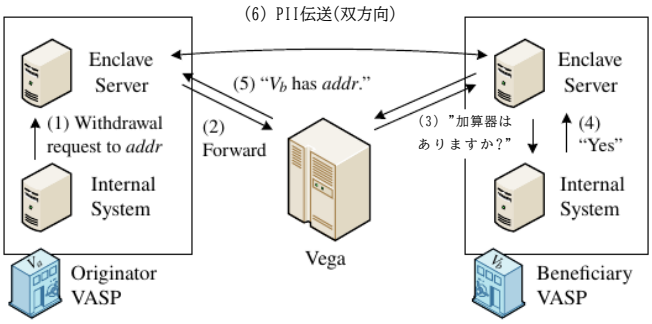


Fig. 7. Architecture of VerifyVASP

Sygna Bridgeは、VASPのデューデリジェンスに参加しています。発信者VASPは受益者VASPに許可を要請し、譲渡が認められた後にのみ譲渡を開始する。Sygna Allianceが運営するBridgeと呼ばれる中央サーバは、メッセージの処理に役割を果たし、高度に集中的なソリューションとして特徴づけられる。Sygna Bridgeは、ユーザースクリーニングやリスクベースの取引分析など、コンプライアンスソリューションに緊密に統合されています。

Sygna Bridgeを使用する場合、各VASPには固有のVASPコードが割り当てられ、各ユーザーはBIP21[50]の拡張フォーマットで説明されるVirtual Asset Account Information(VAAI)というアドレスを持っています。VAAIは、VAアドレス、VASPコード、送信者の名前を符号化する。

発信者VASPがSygna Bridgeを使用してVAAIへの転送を開始すると、VAAI内の受益者VASPコードが参照され、メッセージは自動的にカウンターパーティVASPに中継されます。それ以外の場合、通常のVAアドレスに送信する際、ブロックチェーン分析を行い、White Address Filter API [51]を使用して、どのVASPに属するかを判断します。したがって、アドレスは特別なエンコーディングを取り入れたルックアップやブロックチェーン分析によって、ハイブリッドな手法で識別されることが観察される。所有権の証明は必要ない。

E. VerifyVASP

VerifyVASP [52]は、韓国の仮想資産取引所であるUppitと米国のChainalysisが共同開発したソリューションである。ブロックチェーン解析ツールベンダー提携VASPのクローズド・アライアンスとして運営されている。

図7はそのアーキテクチャを示したものである。VerifyVASPは、各VASPのインフラストラクチャ内で動作するEnclave ServerというDockerイメージを提供します。VASPは、このコンテナをインターフェースとして、VerifyVASPの中央サーバであるVegaに接続します。VASPは、社内システムとエンクレーブサーバーとの間の通信を確立する必要があります。Vegaはルックアップサービスと VASPディレクトリとして機能し、各VASPから住所検索クエリを受け取り、受益者VASPのエンドポイントとともに応答を提供します。

以下の手順は、アリスがV aからV bのボブへの引き出しを要求し、両方のVASPがVerifyVASPに参加する場合のプロセスの概要を示しています。

1) V aの内部システムは、V aのインフラ上でホストされているEnclave Serverの引き出し要求APIを呼び出します。リクエストはVegaに転送されます。
2) Vegaはアライアンスで他のメンバーのVASPに問い合わせ、addrの制御VASPを決定します。
3) V bの内部システムはV bのコンテナからのコールバックに応答し、addrの所有権を通知する。
4) Vega informs V_a's Enclave Server about V_b's ownership.
5) The Enclave Servers of V_a and V_b establish an end-to-end encrypted communication channel to exchange PII.

VerifyVASPでは、V bはaddrの暗号的証明を提供する必要はない。VASPとVegaのネットワークセキュリティは、IPの制限により確保されています。
今回の調査から、VerifyVASPは2つの点でユニークであることがわかりました。

- メンバーVASPから積極的にアドレスを収集する代わりに、転送要求が行われたときにメンバーVASPに問い合わせを行います。
- 受益者VASP(V b)は、受益者情報を発信者VASP(V a)に返送する。これは、旅行規則で義務付けられていないものの、両端のPIIの精度を向上させる。

F. Shyft Veriscope

Shyft Veriscope [53]は、Shyft Networkと呼ばれるプライベートなイーサリアムブロックチェーンを利用しています。VASPはShyft Network上で利用可能な専用トークン(SHFT)を購入する必要があり、これはProof-of-Authorityコンセンサスアルゴリズムによって操作される。シフトネットワークは、(1-A)ルックアップサービス、(2-A)住所証明の必要がない、(3-C)限定アライアンス内で運営される、などの機能を持つ。

発信者VASPに顧客からの引き出し要求があるとき、発信者VASPは送金要求に関する情報を含むトランザクションをShyft Networkに公開する。受益者VASPが取引を検出すると、発信者VASPとのエンドツーエンドのネットワーク接続を開始し、譲渡を許可する。受益者であるVASPは、住所の所有権を証明する必要は特にない。最終的に、彼らはShyft Networkの外側のP2Pを介してIVMS 101フォーマットでメッセージを交換します。

2023年9月現在、公式ブロックチェーンエクスプローラー[54]によると、Shyft Networkメインネットの総取引数は1日あたり10～20件である。スマートコントラクトとドキュメントは一般に公開されている[55]。

G. OpenVASP / 旅行規則プロトコル(TRP)

OpenVASP Association が開発した Travel Rule Protocol (TRP) [56]は、PII 伝送のための最小 API セットとなることを目的としています。情報の多くはオープンソースであり、GitLabで見ることができます。

TRPは、転送先を示すためにTravel Addressという一意の識別子を使用します。移動先住所はtaから始まり、(1-C)で説明したように、Base58と預託URIを用いて符号化される。受信者VASPは各ユーザにTravel Addressを割り当て、送信側は転送要求時にオリジネータVASPにTravel Addressを提供する。

以下は、TRPの仕組みの一例です。

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 u_B, and sends PII and a callback URL u_A to u_B.
4) V_b either responds with an actual VA address *addr* or notifies the rejection.

旅行先住所には受益者VASPのエンドポイントが含まれているため、オリジネーターVASPは受益者VASPを検索する必要はありません。VASPはHTTPS上のピアツーピア(P2P)接続を使用して互いに通信します。

H. Other solutions

Netkiはもともと2015年にBIP70[58]で規定された人間が読める名前[57]を用いてビットコインの支払いを促進した。TransactIDはBIP75[59]で定義されたブロックチェーン外でPIIを交換することを目的とし、Travel Rule[60]に適合させた。
OpenVASPはもともとTRPの前に、イーサリアムブロックチェーン[61]を使用する解決策を提案した。VASPはEthereum上で識別可能なスマートコントラクトを展開する必要がありました[62]。ユーザーは、スマートコントラクトアドレスに基づき、VASPコードを含む独自の仮想資産勘定番号で識別されました。VASPは、非推奨のEthereum Whisper [63]を使用してピアツーピアで通信しました。

Leeら[64]は、VASPアライアンスを構築するために、Corda[65]を用いて許可されたブロックチェーン上の解決策CODEを提案した。デザインでは、PIIはCordaのメッセージングメカニズム上でピアツーピアに送信されます。

VIII. O VIII. トラベルルールとのオペレーション

A. 未公開のウォレットを利用したマネーロンダリング

ホスティングされていないウォレットを中継することで、旅行ルールを回避することができます。現在、この問題に対処するための効果的な解決策は、ホスティングされていないウォレットへの転送とホスティングされていないウォレットからの転送を制限する以外には提案されていない。

この問題は、未発着のウォレットに関わる旅行規則の要件がないことから生じる。この規制の欠如が犯罪者に非ホスティングウォレットの使用を促すのではないかという懸念が指摘されている[66]。しかし、未発着のウォレットに規制を課し、VASP間のみの取引を制限することは、セクション II-A で述べた経済的利益を著しく損ねることになる。例えば、中東の非公式な価値移転システムであるハワラのケースは、地下経済の可能性を強調し、AML/CFTの取り組みの複雑さを増大させている[67]。

運用ルールに未発着ウォレットを統合するための技術的解決策を提案する場合、未発着ウォレット所有者のプライバシーを優先させることが重要である。

B. プライバシー保護によるアドレス所有の証明

調査の結果、多くのアライアンスが住所検索サービスを提供していることが確認された。しかし、ルックアップサービスが集中的にアドレスを収集することは、プライバシーの観点からは望ましくない。

技術的には、以下の2つの要件を満たすことが理想的である。(1) 受益者VASPは、加算器を表示せずに加算器の秘密鍵の所持を証明する暗号コミットメントを登録する、(2) 加算器を知っている人だけがそのコミットメントを検証できる、である。addrの単純なハッシュ値は、要件(1)を満たさない。

我々の知る限り、ビットコインのようなシステムでは、シングルキーウォレットであっても、提案された方式は存在しない。我々は、公開鍵のハッシュ値から加算器を導出するプロセスは、ゼロ知識証明技術と一致しないと考えており、この問題に対処する上で課題となっている。

C. 各種VAへの対応

今回の調査では、ほとんどのソリューションがBitcoinとEthereumをサポートしていることがわかりましたが、サポートのレベルは他のタイプのVAで異なることがわかりました。この矛盾の背景には、他のVAにおけるブロックチェーンのアーキテクチャや暗号に関する支援や基本的な問題の有無にかかわらず、著者らは明確に理解していない。

本号は、2020年以降に出現したNFTや安定コインなどの新しい形態のVAに適用される。これらの中には一定の交換価値を持つものもあり、NFTがマネーロンダリングに利用されているという報告もある[68]。ERC-20や他のトークンのコンプライアンス難易度をさらに調査する必要がある。
さらに、ZcashやMoneroなどのAECは、FATFの定義によりVAに分類される。いくつかのVASPは、現実のAECを扱い、それらは同様にAECのための旅行規則の対象となる。本研究では、AECの詳細な検討は行っていないが、AECを旅行規則に準拠させることの課題については、今後分析する必要がある。

D. その他の一般的な問題点

1) PII 送達のリスク評価。1) PII 送達のリスク評価:起因者 VASP は、受益者 VASP に対する PII 開示のリスクを評価しなければならない。オリジネーターVASPがアライアンスへの参加を検討する場合も同様である。
旅行規則の導入以来、常に議論が交わされてきた。欧州連合におけるVASPは、一般データ保護規則の下で個人情報の保護が厳しく、EU地域外での情報共有に大きな懸念がある[69]。同様に、日本では、PII 開示の禁止の例外として、発信者の同意なしに interVASP PII 伝送を設定する法的修正が行われた[70], [71]。

2) シェル型VASPとマネー・ミュール FATF勧告では、加盟国に対し、VASPを運営するためのライセンス発行や、VASPによる厳格なKYCの実施を合法化することを求めている。しかし、これらの措置をある国や地域で不適切に実施すると、他の国が現地法で旅行規則を規定している場合でも、世界的に旅行規則の有効性が低下する可能性があります。

脆弱な国から不適切に発行されたライセンスによって、シェル型VASPの存在が大きな問題の一つとなっている。このような架空の金融機関は、
シェルバンクと呼ばれる伝統的な金融システムにおける大きな問題であった。VASPディレクトリやアライアンスの信頼性は、架空のVASPがそれらの一部である場合、侵害される可能性があります。
また、VASPを用いたKYCプロセスの厳密性が重要である。多くの金融機関やVASPは、政府発行の身分証明書の偽造コピーを使って架空の口座を作る違法なKYCの試みと戦っている。さらに、正当に作成されたアカウントは、Telegramやその他の高度に匿名化されたチャットで違法に取引されています。これは、経済的に弱い個人が貨幣ラバとして搾取される危険性がある[72]。これらの問題に対処するためには、デジタル識別カードにICチップやスマートカードを使用するなど、堅牢なKYC手順を確立し、実装することが必要である。

IX. Conclusion

仮想資産は、法通貨と並んで重要な金融手段となりつつあり、犯罪目的での悪用を防ぐための措置が必要とされています。そのような手段の一つとして、不正資金の移転を防止することを目的としたFATFのトラベル・ルールがある。渡航規則は、CDDの義務を従来の金融機関からVASPに拡大することにより、AML/CFTの取り組みを強化するものである。

従来の銀行ネットワークとは異なり、仮想資産はユニークな課題を提起している。ユーザーは、転送のためにVASP上の宛先VAアドレスを指定するだけでよく、VASPは本質的にそのアドレスの所有者を知る方法がありません。その結果、与えられたアドレスの制御VASPを特定するために、ルックアップ機構の必要性が強調された。新しく生成された住所は、登録の真正性を高めるために、適時にルックアップサービスに登録され、できれば適切な暗号の証明がなされるべきです。世界中のVASPが、無関係なアドレスの所有権を偽って主張する悪意あるエンティティを除外し、正確な検索のためのメカニズムに積極的に参加することを保証することが不可欠である。これは、参加するVASPの正当性を検証し、認証と認可の仕組みを提供することで実現できます。このような仕組みの有効性は、トラベルルールのグローバルな実施に欠かせないものです。

我々は、様々なトラベルルールの解決策を包括的に検討し、調査から以下の知見を得た。

- 同盟を基盤としたソリューションが最も一般的です。彼らは、ネットワークに参加するために、積極的に新しいVASPを求めている。
- デスティネーション・アドレスから受益者VASPを特定するために使用される方法は、ソリューションによって異なります。ルックアップサービスに依存するものもあれば、ブロックチェーン分析ツールの使用を推奨するものもある。
- ピアツーピアやブロックチェーンベースのソリューションは過去と現在で開発されましたが、これらの代替案の普及は観察されませんでした。

この結果は、VASP間のコミュニケーションプロトコルに関する相互デューデリジェンスとコンセンサスの効率と利便性に起因していると考えられる。しかし、複数のアライアンスが形成されるため、VA経済が分割される可能性があることに懸念がある。

この問題に対処するため、一部のアライアンスは相互運用性を促進し、アライアンスに基づくトラベルルールネットワークをさらに拡大する橋渡しを計画している。

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. 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. 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. 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] Y. Takei, *Complete Guide to the Theory and Practice of NFTs (translated)*. Ohmsha, 5 2023.
[38] BitGo, “Ethereum multisig wallet contract.” [Online]. Available: https://github.com/BitGo/eth-multisig-v4
[39] Safe Ecosystem Foundation, “Safe contracts.” [Online]. Available: https://github.com/safe-global/safe-contracts
[40] 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
[41] 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/
[42] 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
[43] Coinbase, “Travel rule universal solution technology (TRUST).” [Online]. Available: https://www.coinbase.com/travelrule
[44] 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

[45] 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
[46] 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/
[47] TRISA, “TRISA-OpenVASP/ TRP Demonstrate Interoperability,” Aug. 2023. [Online]. Available: https://trisa.io/trisa-trp-interoperability/
[48] 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/
[49] CoolBitX and Elliptic, “Sygna bridge.” [Online]. Available: https://www.sygna.io/bridge/
[50] N. Schneider and M. Corallo, “URI scheme,” Jan. 2012. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0021.mediawiki
[51] Sygna, “Bridge/wallet address filter.” [Online]. Available: https://developers.sygna.io/reference/bridgewallet-address-filter
[52] VerifyVASP. [Online]. Available: https://docs.verifyvasp.com/
[53] Shyft, “Veriscope Docs.” [Online]. Available: https://docs.veriscope.network/
[54] ——, “Poa explorer (mainnet).” [Online]. Available: https://bx.shyft.network/
[55] ——, “Veriscope docs.” [Online]. Available: https://docs.veriscope.network/
[56] OpenVASP Association, “Travel rule protocol (TRP),” Dec. 2020. [Online]. Available: https://gitlab.com/OpenVASP/travel-rule-protocol/-/blob/master/core/specification.md
[57] Netki, “Netki wallet name service.” [Online]. Available: https://www.youtube.com/watch?v=gunA1zBnEcs
[58] G. Andresen and M. Hearn, “Payment protocol,” Jul. 2013. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0070.mediawiki
[59] 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
[60] 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/
[61] 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
[62] OpenVASP Association, “OpenVASP contracts,” Apr. 2020. [Online]. Available: https://github.com/OpenVASP/openvasp-contracts/tree/1.0
[63] Ethereum community, “Ethereum whisper archive.” [Online]. Available: https://github.com/ethereum/whisper
[64] 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.
[65] R. G. Brown, “The Corda platform: An introduction,” May 2018. [Online]. Available: https://www.corda.net/content/corda-platform-whitepaper.pdf
[66] 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
[67] 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.
[68] 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
[69] 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/
[70] 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
[71] 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
[72] 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.
[73] Reuters, “South Korean intelligence says N. Korean hackers possibly behind Coincheck heist,” Feb. 2018. [Online]. Available: https://reut.rs/2BI6Oh1
[74] 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. FATF語彙の略称一覧

表IIIは、本論文で使用したFATFの語彙の略称リストをアルファベット順に示したものである。

TABLE III
Fatfの語彙の概要

AML	アンチマネーロンダリング
CDD	顧客デューデリジェンス
CFT	テロリズムの資金調達に対抗する
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. 旅行規則の歴史

当初の旅行規則は、1996年に米国で銀行証券法(31 CFR 103.33(g))により定義されたものである。この規定は2001年に特別勧告VII(Wire Transfer)としてFATF勧告に組み込まれた。2006年12月までに国際銀行取引に義務付けられるようになった。

2012年、FATFは勧告を全面的に改訂した。運用ルールはレコメンデーション16と改称された。2009年にビットコインのブロックチェーンが開始されたが、その時流版はまだ仮想資産技術を考慮していない。

2017年、ビットコインは約20倍の物価上昇率を記録し、世間の注目を集め、その後、2018年1月に日本の取引所で大規模なネム盗難が発生した。この事件は、2012年からFATFのブラックリストに掲載されている北朝鮮による国家支援型サイバー攻撃[73]、[74]であることが疑われた。

これらの社会運動に対応して、2018年10月にFATFはVAとVASPという用語を定義し、勧告15(新技術)を修正した。補足実用情報を提供する勧告15の解釈ノートは、2019年に修正された。これに伴い、FATFは各国に、VASPがライセンスで規制され、仮想資産への渡航規則義務を拡大する必要があるよう、立法を要請した。

FATFは、調製に12ヶ月の猶予期間を設定し、その後、業界からのフィードバックに基づき、2021年半ばまで別の12ヶ月のウィンドウで調整されました。直近では、2023年4月に、本稿の執筆者でもあるFATFの仮想資産コンタクトグループ(VACG)会議が開催され、FATF、参加者の管轄地域、民間部門間の対話が促進されました。旅行規則の実施状況は、会議中に報告された。また、NFTやその他の仮想資産に対する規制計画についても議論された。