Vol.2021-CSEC-94 No.13
Vol.2021-SPT-43 No.13
2021/7/19

ビットコイン利用者の特定・追跡の仕組みに関する考察（２）

才所敏明[1]　辻井重男[2]　櫻井幸一[3]

概要：暗号資産の強い匿名性による不正・不法な取引の決済への利用やマネーロンダリング，テロ資金供与が急増しており，暗号資産の移転に対し国際的に共通のガイドラインによる規制や各国の法規制が強化されつつある．このような社会の要請に基づき，暗号資産の移転にかかわる利用者の特定・追跡のための情報の確認と記録を可能とすることを目指した議論・検討が活発化しており，筆者らも暗号資産システムの利用者の特定・追跡を可能とする具体的な仕組みの考案を目指し，研究を推進中である．本報告では，代表的な暗号資産システムであるビットコインシステムを対象に，資産の提供者・受取者およびトランザクション作成者の特定・追跡を可能とする仕組みを提案する．また，提案方式の，既存のビットコインネットワーク/ビットコインブロックチェーンへの影響の観点，暗号資産に対する規制の内容・動向の観点，規制対応のために提案されている主要な構想との関係の観点，から考察する．

キーワード：暗号資産，匿名性，マネーロンダリング，テロ資金供与，悪用，規制，FATF，FinCEN，OpenVASP，TRISA，ビットコイン，BASP，BUITRA

Consideration on the mechanism of identifying and tracking Bitcoin users (2)

Toshiaki Saisho[1]　Shigeo Tsujii[2]　Kouichi Sakurai[3]

Abstract: Due to the strong anonymity of CryptoAssets, the use for settlement of fraudulent and illegal transactions, money laundering, and terrorist financing are increasing rapidly, and regulation for the transfer of CryptoAssets is being strengthened, by internationally common guidelines and each country's laws. Based on such demands of society, discussions and studies aimed at making it possible to confirm and record information for identifying and tracking users involved in the transfer of CryptoAssets are becoming active. We too are promoting research with the aim of devising a concrete mechanism that enables the identifying and tracking users of CryptoAsset systems. In this report, we propose a mechanism that enables identifying and tracking of BitcoinAsset providers / recipients and transaction creators for the Bitcoin system, which is a typical CryptoAsset system. In addition, we analyze our method proposed from the perspective of the impact of our method on the existing Bitcoin network / Bitcoin blockchain, the perspective of the content and trends of regulations on CryptoAssets, and the perspective of with the main concepts proposed for regulatory compliance.

Keywords: CryptoAssets, anonymity, money laundering, terrorist financing, abuse, regulation, FATF, FinCEN, OpenVASP, TRISA, Bitcoin, BASP, BITFRA

1. はじめに

ビットコインをはじめとする多くの暗号資産は，プライバシーや個人情報の確実な保護の観点から一定レベルの匿名性が確保されている．しかし，暗号資産の匿名性は，マネーロンダリングやテロ資金供与，不正・不法な取引の決済手段としての利用を急増させる原因ともなっており，大きな社会問題となっている．

2019 年の chainalysis のレポート（[15]）によると，不正・不法な取引の決済と想定される比較的少額の決済が急増しており，匿名性の高い決済手段の普及により，不正・不法な取引が蔓延しつつあると考えられる．

2019 年に発表された論文（[16]）によると，2017 年 4 月時点のビットコインブロックチェーンに登録されているトランザクションデータの分析結果，①トランザクションの 32.83%は不正・不法な活動のためのトランザクションであったこと，②ビットコインの全利用者の 5.86%がビットコインの不正・不法な利用者であったこと，③不正・不法な利用者のうち拘束できたのは 0.02%にも満たなかったこと，等が報告されており，ビットコインの匿名性が不正・不法な利用者の拘束を困難とし，結果として不正・不法な利用の急増を招いていると考えられる．

さて，このような暗号資産の不正・不法な利用を防止・抑止すべく，暗号資産サービスの分野でも既存の金融サービス分野と同等の，不正・不法な利用の防止・抑止を目的としたガイドラインや法制度による規制が本格化してきている．2 章にて暗号資産サービス分野における規制の現状・

1 (株)IT 企画
Advanced IT Corporation
E-mail: toshiaki.saisho@advanced-it.co.jp
2 中央大学研究開発機構
Research and Development Initiative, Chuo University
E-mail: tsujii@tamacc.chuo-u.ac.jp
3 九州大学大学院システム情報科学研究院
Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University
E-mail: sakurai@INF.kyushu-u.ac.jp
（株）国際電気通信基盤技術研究所
Advanced Telecommunications Research Institute International

Vol.2021-CSEC-94 No.13
Vol.2021-SPT-43 No.13
2021/7/19

動向について概要を報告する．また，ガイドラインや法律を順守し，社会が求める安心・安全な暗号資産サービスを目指し，複数の団体・企業グループが構想等を提案している．3 章にて，ガイドラインや法律による規制に対応可能な暗号資産サービスを目指した主要な構想の概要を報告する．

筆者らは，2017 年より暗号資産の研究に着手，主要な暗号資産の利用者の匿名性・匿名化技術の調査・分析，匿名性要件の提案とそれに基づく匿名性レベルの評価等を実施してきた．更に 2019 年より，暗号資産の不正・不法な移転の防止・抑止のための暗号資産利用者の特定・追跡の仕組みに関する調査・分析に着手，ビットコインシステムを対象にトランザクション作成者（発行者）の特定・追跡の仕組みを考案し発表した（[1]）．

今回の報告では，トランザクション作成者の他，トランザクションによりビットコイン資産の移転に関与する資産提供者および資産受取者を含めた，3 種のビットコイン利用者の特定･追跡を可能とする，新たな仕組みを提案する．

2. 暗号資産に対する規制の現状・動向

2015 年 6 月の G7 サミットにて，仮想通貨およびその他の新たな支払手段に対する適切な規制の導入が宣言された．同月に早速，FATF（マネーロンダリング・テロ資金対策等に取り組む主要国政府による枠組みとして OECD に事務局を設置し発足した金融活動作業部会：Financial Action Task Force）が，各国の仮想通貨取引所に対して登録・免許制を課すと共に利用者の本人確認を義務付けることなどを各国政府に通達した．日本では，FATF の通達を受け，制度設計や資金決済法の改正が検討され，2016 年 5 月に改正資金決済法を成立させ，仮想通貨取引所の登録制がスタートした．

2018 年 3 月の G20 財務大臣・中央銀行総裁会合にて，CryptoCurrency（日本では仮想通貨）の名称を CryptoAsset（日本では暗号資産）へと名称を変更し，同年 7 月の会合では FATF に対し既存の FATF 基準をどのように暗号資産に適用するかを明確にするよう要請した．FATF は同年 10 月，FATF 勧告 15「新技術」を改訂し，暗号資産交換事業者にはマネーロンダリング等の規制が課されなければならないことを規定した．

更に FATF は 2019 年 6 月，FATF 勧告 16「電信送金」を改訂し，暗号資産の提供者と受取者に関する基本情報の確認・保存を暗号資産関連事業者（VASP : Virtual Asset Service Provider）へ要求している．この改定された FATF 勧告 16 はトラベルルールと呼ばれている（[18]）．トラベルルールの具体的要件は，暗号資産による電信送金の場合も，提供者が利用している VASP は受取者が利用している VASP へ，提供者と受取者に関する以下の情報を，電信送金に含めておくこと，である．

① 資産提供者の名前
② トランザクションの処理に利用される資産提供者のアカウント番号
③ 資産提供者の地理的な住所および国固有の個人識別番号等
④ 資産受取者の名前
⑤ トランザクションの処理に利用される資産受取者のアカウント番号

このようなトラベルルールへの対応に向け，各国政府および暗号資産関連事業者は活動を展開中であるが，2020 年 7 月に公表した FATF のレポートによると，調査を実施した世界の 54 法域（国）のうち 19 法域が暗号資産関連事業者への規制が未実施であった．また，トラベルルール順守のための技術対策は未実施であった．

一方，FATF のトラベルルールは，暗号資産関連事業者への規制であるが，一般に暗号資産は事業者を通さず，直接利用者間で移転が可能なため，現在のトラベルルールでは不正・不法な暗号資産の移転を検知してもその利用者の特定・追跡は難しい．2019 年 10 月に発表された Europol のレポート（[21]）にても，このトラベルルールの問題が指摘されている．

現在のトラベルルールの問題である，個人間の直接の暗号資産移転に対しての規制導入の検討が進められている．スイス政府では，個人の暗号資産ワレットの登録制の導入を検討している模様．また米国でも，財務省の機関である FinCEN（金融犯罪取締ネットワーク：Financial Crimes Enforcement Network）がトラベルルールを強化した個人間の直接の暗号資産移転への規制案を提案し，検討されている（[22]）．

FATF においても，2021 年 3 月，個人間の直接の暗号資産移転への規制を含めたガイドラインへ改定する方針を発表した．このように，個人間の直接の暗号資産移転をも対象とした，マネーロンダリングやテロ資金供与，不正・不法な取引の決済などへの暗号資産の利用に対する包括的な監視・防止および利用者の拘束を可能とする国際的なガイドラインが近々策定・公表される見通しとなった．

3. 規制順守のための構想概要

トラベルルールが公表された後，その順守のための暗号資産取引所向けのソリューションについてベンダーやベンダーグループが検討に着手，まだ構想段階ではあるが複数が提案されている．以下に，代表的な構想，OpenVASP と TRISA，の概要と筆者らの見解をまとめている．

3.1 OpenVASP（[23]）

OpenVASP（Open Virtual Asset Service Provider）は，仮想通貨取引所などの暗号資産関連事業者（VASP）の間で，FATF のトラベルルールで求められている取引情報を送信するためのオープンなプロトコルを確立することを目的として設立された組織である．

Vol.2021-CSEC-94 No.13
Vol.2021-SPT-43 No.13
2021/7/19

VASP の識別コード（VASPcode），VASP が管理する暗号資産アカウント番号（VAAN：Virtual Asset Account Number）の形式の定義，VASP 間のメッセージのやり取りおよびそのメッセージの形式の標準化を進めている．やり取りするメッセージには，FATF で規定されている暗号資産の提供者および受取者の個人情報も含まれている．

OpenVASP の基本原則の一つとして Decentralized Approach を採用している．そのため，VASP が利用者の個人情報のやり取りを行う通信相手の VASP が信頼できるかどうかについては，VASP 自らの責任で確認を求められている．そもそも VASP は各国の法律の規制を受け，認可・登録された事業者であることが前提であるが，VASP がその法域（国）のしかるべき機関により認可・登録されているかを，VASP 自らが通信相手の VASP ごとに確認することが想定されている．しかし，個々の VASP の責任・負担を軽減すると同時に，利用者が利用する VASP への信頼・安心感を増大させる，何らかの仕組みの検討が必要と考えられる．

また，OpenVASP では利用者の個人情報を通信相手の VASP への提供を求める FATF の規定に準じているため，他国の VASP に対しても自国の利用者の個人情報を送信することになり，一方，海外の VASP は他国の利用者の個人情報を記録・管理することになる．このような海外の利用者の個人情報の記録・管理を前提とした仕組みは，各国の法制度に基づき規制されることも想定され，利用者の個人情報の海外流出を必要としない何らかの仕組みの検討が必要と考えられる．

3.2 TRISA（[24]）

トラベルルール情報共有アライアンス(TRISA：Travel Rule Information Sharing Alliance)では，暗号資産システムを構成する中核のブロックチェーンおよびプロトコルを変更することなく，また匿名性を犠牲にすることなく，FATF のトラベルルール準拠に必要な暗号資産の提供者と受取者の情報を共有する VASP をサポートするオープンソースフレームワークである．

TRISA は，OpenVASP と異なり，信頼できる第 3 者機関 TRISA CA（Certificate Authority）の存在を前提とした，通信相手の VASP の信頼性確認が相互に可能な PKI ベースの仕組みを採用している．具体的には，VASP の実在性の確認や法域（国）における認可された VASP であることの確認は，TRISA CA への登録申請時に VASP が提出する情報により，TRISA CA が検証する．確認がとれた VASP へ TRISA CA が公開鍵証明書を発行し，その証明書が VASP の信頼性確認に使用される．

また，TRISA においても利用者の個人情報を通信相手の VASP への提供を求める FATF の規定に準じているため，他国の VASP に対しても利用者の個人情報を送信することになり，一方，海外の VASP は他国の利用者の個人情報を記録・管理することになる．このような海外の利用者の個人情報の記録・管理を前提とした仕組みは，各国の法制度に基づき規制されることも想定され，利用者の個人情報の海外流出を必要としない何らかの仕組みの検討が必要と考えられる．

4. ビットコイン利用者の特定・追跡方式

前章で記載したように，2019 年 6 月に FATF がトラベルルールを発表した後，その順守のための暗号資産取引所向けのソリューションが複数提案されている．しかし，それらはまだ構想段階であり，しかも 2021 年 3 月に FATF が規制の方針を発表した個人間の暗号資産の取引への対応は考慮されていない．

本章では，前章の暗号資産に対する規制の現状・動向を踏まえつつ，代表的暗号資産であるビットコインを対象にした利用者の特定・追跡方式，個人間取引をも含めたビットコイン利用者の特定・追跡方式（BITFRA：Bitcoin User Identifying and Tracking Framework)）を提案する．まず 4.1 にてビットコインシステム概要を，4.2 にて筆者らが提案するビットコイン利用者の特定・追跡方式 BITFRA の具体的仕組みを報告する．

4.1 ビットコインシステム概要

資産（ビットコイン）の移転を示すトランザクションはワレットで生成され，ビットコインネットワークで承認されブロックチェーンに登録される．図 1 にビットコインシステムの構成およびトランザクションの流れを示している．

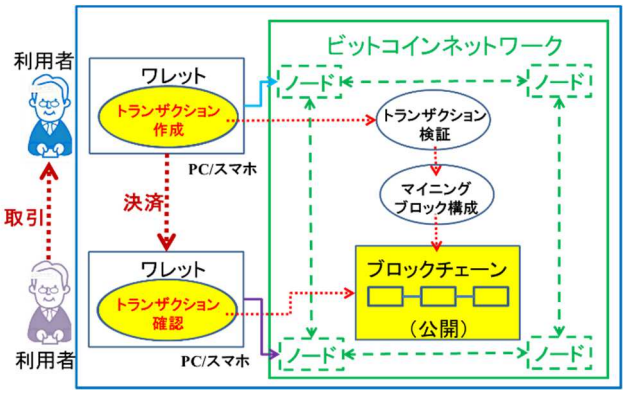

図 1　ビットコインシステム構成概要

トランザクションは，提供に使用される複数の資産の情報と複数の受取者の情報が格納されている．図 2 の新規トランザクションの提供資産の一つである入力資産 1 は，位置情報により提供者が受取者として登録されている既存トランザクションの出力資産 k に対応していることを示し，既存トランザクションの出力資産 k の受取者を示す封印情報に対応する償還情報（所有権の証明）を新規トランザクション内で指定することにより提供者の使用権を第三者も検証可能としている．

Vol.2021-CSEC-94 No.13
Vol.2021-SPT-43 No.13
2021/7/19

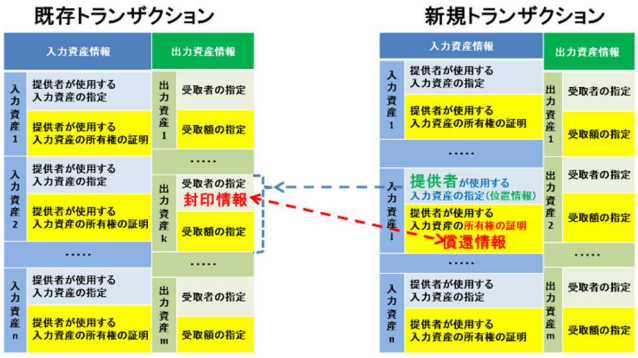

図２　ビットコインにおける封印・償還による資産移転

ビットコインシステムにおける主要な資産移転方式の封印情報および償還情報を図３に示している．封印情報としては，受取者の公開鍵あるいはそのハッシュ値，償還情報としては，封印情報（封印スクリプト）を特定する情報および封印情報に指定された公開鍵に対応する秘密鍵による署名，が指定される．

方式	情報	指定されるスクリプト
P2PKH	封印情報	OP_DUP OP_HASH160 <20-bytes-pubkey-hash> OP_EQUALVERIFY OP_CHECKSIG
	償還情報	<signature> <pubkey>
P2SH	封印情報	OP_HASH160 <20-bytes-multi-sig-script-hash> OP_EQUAL
	償還情報	<signature 1> … <signature M> <multi-sig script>
MultiSig	封印情報	<multi-sig script> OP_CHECKMULTISIG
	償還情報	OP_0 <signature 1> …<signature M>
P2PK	封印情報	<pubkey> OP_CHECKSIG
	償還情報	<signature>

（注）<multi-sig script> = M <pubkey 1> <pubkey 2> ... <pubkey N> N

図３　ビットコインシステムにおける
主要な資産移転方式の封印・償還情報

4.2　特定・追跡方式 BITFRA の提案

ビットコイン利用者には大きく 3 種の利用者，資産提供者，資産受取者，トランザクション作成者に分類できる（図４）．提供者および受取者は複数存在することも多いが，トランザクション作成者は一人であり，提供者の一人が担当することも多い．

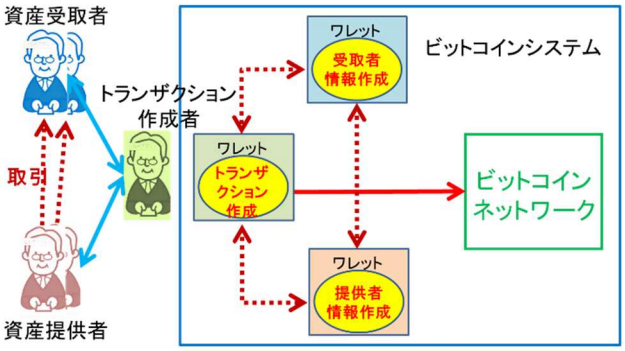

図４　３種のビットコイン利用者

ビットコイン利用者の特定・追跡を可能とするには，利用者の確実な身元確認およびその身元情報の記録が必要となる．また，発行されたトランザクションとそのトランザクションに含まれる資産提供者，資産受取者および作成者との対応の記録が必要となる．

本研究の第一報（[1]）では，トランザクション作成者に限定し考案した複数の特定・追跡の方式，およびそれらの比較・評価について報告した．その結果を踏まえ，本報告では，下記の３点を基本方針とし，トランザクションの作成にかかわる 3 種のビットコイン利用者全員の特定・追跡の方式を考案した．

① ビットコインネットワークへの影響を最小化
② 各国の法制度に準拠した利用者の個人情報保護
③ 複数の暗号資産システムの利用を支援する統合環境への発展の可能性

［提案方式］

提案方式は，ビットコインの資産移転を支援するサービスプロバイダ（BASP：Bitcoin Asset Service Provider）の存在・利用を前提として，ビットコイン利用者の特定・追跡を可能とする提案である．

BASP は，利用者の個人情報保護に関する所属する国の法制度に準拠した，また FATF のガイドラインに準拠した事業者であり，グローバルな BASP 登録制度により，BASP-ID が付与され，BASP 証明書（公開鍵証明書）が交付されることを想定している．

図６にて，利用者の本人確認，トランザクション内の資産の提供者・受取者およびトランザクション作成者とトランザクションの対応の確認・記録の仕組みを示している．

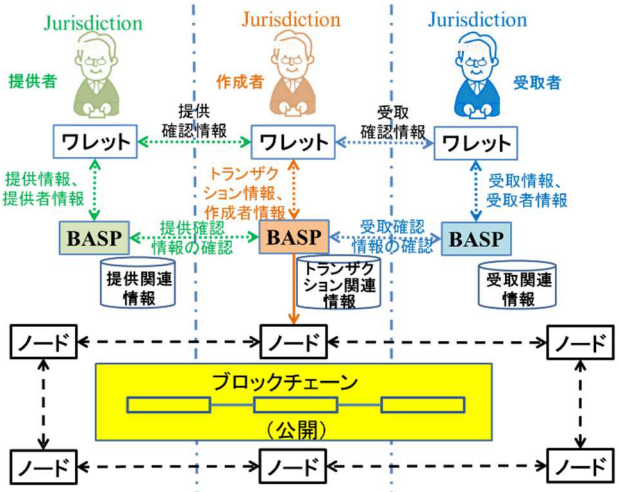

図６　各法域による情報確認と法域間の情報確認

BITFRA で想定している詳細な手順は，ビットコイン利用者の特定･追跡方式を示した図７にて説明することにし，ここでは本方式の基本的な考え方を示す．

ビットコイン利用者がトランザクションの作成にかかわる際には，提供者の場合は提供する資産の所有権を示す情報を提供者が利用する BASP へ送信し妥当性の確認を受

Vol.2021-CSEC-94 No.13
Vol.2021-SPT-43 No.13
2021/7/19

け，受取者は封印情報に示された受取者であることを示す情報を提供者が利用する BASP へ送信し妥当性の確認を受ける．提供者・受取者は，トランザクションの作成に必要な資産情報をトランザクション作成者へ送信する際に，同時にそれぞれが利用する BASP による妥当性確認情報もトランザクション作成者へ送信する．

トランザクション作成者は，発行するトランザクションを作成すると共に，そのトランザクションを構成する提供資産，受取資産のそれぞれの妥当性確認情報を作成者が利用する BASP へ送信する．その BASP は，トランザクションを構成する提供資産，受取資産のそれぞれの妥当性確認情報を検証し，問題なければビットコインネットワークの一つのビットコインノードへトランザクションを送信する．

BASP を利用しビットコイン利用者の特定・追跡を可能とする本方式で管理する具体的な情報，ビットコイン利用者の特定・追跡手順概要を図７に示している．

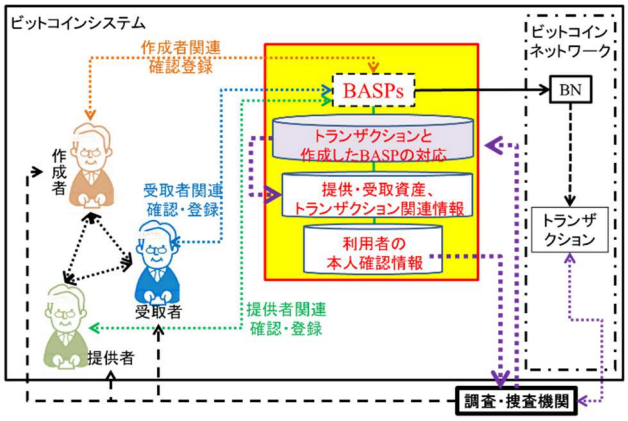

図７　BASP で管理する情報と利用者の特定・追跡方法

以下，本方式における処理概要を示す．

（１）　ビットコイン利用者の BASP への利用者登録

ビットコイン利用者は，それぞれ利用する BASP に利用者登録を行う．登録時には確実な身元確認が実施され，利用者の追跡が可能な身元情報が記録される．また，利用者が実際に作成されるトランザクションに関与する場合に実施される本人確認のための当人確認情報も登録される．

BASP では，登録された利用者の身元情報および当人確認情報は個人情報・プライバシー情報であるため，安全・確実に管理する必要がある．

（２）　提供者・受取者のビットコイン資産の妥当性確認

トランザクション作成者は，トランザクションを構成する資産の提供者・受取者へ必要な情報の送信を求める．

提供者・受取者は，トランザクションを構成する資産情報を作成し利用する BASP へ送信し，提供者・受取者の資産情報の妥当性の確認および提供者・受取者が特定・追跡可能な利用者であることの確認を求める．

BASP は，提供者から資産情報を受信した場合は，資産情報がその提供者の所有資産であることの確認および提供者が身元確認され身元情報が登録された特定・追跡可能な利用者であることを確認し，確認結果を BASP の署名付きで返信する．受取者から資産情報を受信した場合は，受取者が資産情報の受取者であることの確認および受取者が身元確認され身元情報が登録された特定・追跡可能な利用者であることを確認し，確認結果を BASP の署名付きで返信する．

提供者・受取者は，資産情報および BASP による確認結果をトランザクション作成者へ送信する．

（３）　トランザクションの作成

トランザクション作成者は受信したトランザクションを構成する資産情報によりトランザクションを構成する．更に，資産の提供者にはトランザクションのハッシュ値を送信し，対応する提供者の秘密鍵による署名の返送を求め，トランザクションを作成する．

（４）　トランザクションの妥当性確認・発行

トランザクション作成者は，作成したトランザクションと共に，提供者・受取者から受信した資産情報およびその提供者・受取者の確認結果を，トランザクション作成者が利用する BASP へ送信する．

受信した BASP では，ビットコインノードが行っているトランザクションの妥当性検証を実施の上，更にトランザクション内のそれぞれの資産情報および提供者・受取者の確認結果を検証する．このような検証で問題なければ，ビットコインノードへトランザクションに BASP の署名を添付し転送し，ビットコインネットワークへ伝搬する．

なお，当該 BASP では，作成したトランザクションの ID（トランザクション ID）とトランザクション確認情報（トランザクション内の各資産情報に対応する各 BASP による確認結果の集合）の対応を記録する．

更に，監査や調査・捜査対応のために必要なトランザクション ID と BASP の ID（BASP-ID）の対応情報を，監査機関や調査・捜査機関がアクセス可能な形式で記録する．

（５）　ビットコイン利用者の特定・追跡

調査・捜査機関が，怪しげなトランザクションの資産の提供者・受取者・作成者等の特定・追跡が必要と判断した場合，調査・捜査機関はそのトランザクション ID を利用し，トランザクション ID と BASP の ID（BASP-ID）の対応情報からトランザクション確認情報を入手，トランザクション確認情報からトランザクションを構成する各資産を確認した BASP-ID を入手，当該 BASP から各資産の確認結果を入手，各資産の確認結果から各資産に対応する利用者を特定し，登録されている身元情報から，追跡が可能となる，という仕組みである．

Vol.2021-CSEC-94 No.13
Vol.2021-SPT-43 No.13
2021/7/19

5. 提案方式 BITFRA の評価・考察

提案方式 BITFRA はまだ具体的仕様は詰めておらず，検討課題も多いが，現時点で想定している仕組みを前提に，評価・考察結果を報告する．

5.1 提案方式検討における３つの基本方針の観点からの評価・考察

① 「ビットコインネットワークへの影響を最小化」

提案方式は，ビットコインブロックチェーンの構造には影響を与えない．

しかし，各ビットコインノードでは，登録された正規の BASP により利用者の特定・追跡性が確認されたトランザクションであることの確認のため，BASP の署名の検証処理を追加する必要がある．

② 「各国の法制度に準拠した利用者の個人情報保護」

提案方式では，登録された正規の BASP は各国（法域内）での利用者の個人情報の取り扱いに関する法制度に準拠している事業者であることを前提としている．また，法域を超えた個人情報の移転を伴わないことを想定している．

③ 「複数の暗号資産システムの利用を支援する統合環境への発展の可能性」

提案方式で，ビットコインの利用者の特定・追跡の仕組みを，ビットコインネットワークと独立した BASP で実装できることを示した．ビットコインと同様の方式の，資産の移転を示すトランザクションにより資産の移転・残高の管理を行う TCAMS（Transaction based CryptoAssets Management System）方式の暗号資産に適用可能と想定しているが，検証は今後の課題である．

5.2 FATF トラベルルールの観点からの評価・考察

トラベルルールの具体的要件は，提供者が利用している VASP は受取者が利用している VASP へ，提供者と受取者に関する，提供者の名前・アカウント番号・住所・個人識別番号および受取者の名前・アカウント番号等の利用者の情報を，トランザクション（暗号資産移転情報）と共に送付すること，である．

提案方式では，提供者の情報は提供者が利用する VASP と同等の位置づけの BASP にて確認し格納，受取者の情報は受取者が利用する BASP にて確認し格納，トランザクション作成者が利用する BASP にて提供者・受取者の情報へのそれぞれの BASP の署名を収集し，トランザクション内の各資産に対応する署名を格納している．このように，それぞれの利用者が利用する BASP が利用者の情報の確認・格納を担当し確認結果を署名にて通知することにより，BASP 間でのトラベルルールで求められている情報の直接の送受は避け，法域（国）の異なる可能性のある BASP 間での個人情報の送受を回避している．

BASP の信頼性は，FATF のトラベルルールに準じた法制度等が整備されている各国で認可されていることを，BASP のグローバルな登録組織が確認し，BASP-ID が付与され，BASP 証明書（公開鍵証明書）が交付されることを想定している．BASP 証明書および BASP の署名により登録された BASP であることを確認できる仕組みを想定している．

提案方式では，トラベルルールで示されている個人情報を含む利用者の情報の送受を行っていないため，厳密にはトラベルルールには準拠していないが，関係する BASP 間の連携にて，すべての利用者の特定・追跡に必要な情報へアクセス可能であり，また個人情報の法域（国）を超えた送受も不要となる．

5.3 提案されている構想 OpenVASP および TRISA との比較・考察

① 分散型か中央集権型か

OpenVASP と TRISA の根本的な違いは，OpenVASP が通信相手の VASP の信頼性は自己責任で確認するのに対し，TRISA は信頼できる第 3 者機関 TRISA CA（Certificate Authority）の VASP の信頼性確認結果を利用することにある．筆者らの提案方式 BITFRA は，TRISA と同様の，PKI ベースの中央集権型のフレームワークである．

② 個人情報の取扱い

OpenVASP と TRISA は共に FATF のトラベルルール規定の個人情報をそのまま VASP 間で送受する方式を採用している．BITFRA では，個人情報のそのままの VASP 間送受を避け，個人情報を確認し管理していること示す情報を送受する方式を採用している．必要に応じ，トラベルルール規定の情報も VASP 間で共有できる仕組みを目指している．

6. おわりに

暗号資産システムがインターネット社会の金融サービスを担う基盤の一つへ成長するには，マネーロンダリング，テロ資金供与，不正・不法な取引の決済等の不適切な利用の防止・抑止のための仕組みが必要であろう．暗号資産関連業界は，安心・安全な暗号資産システムの実現に向け，大きく変化する必要がある．

暗号資産システムの不適切な利用の防止・抑止のためには不適切な利用者の特定・追跡が必要と考え，本報告ではビットコインを対象にした利用者の特定・追跡方式 BITFRA を提案した．BITFRA により，資産移転時にはビットコイン資産移転にかかわる利用者の特定・追跡性が確認されることになり，それでも不適切な利用が発生時には該当する利用者を特定・追跡でき，法的対応が可能となる．

暗号資産に対す規制内容は現在改定途上であり，規制に対応した仕組みの検討もまだ緒に就いたばかりで，今後さまざまの動きが想定される．筆者らも，提案方式 BITFRA をベースに他の暗号資産への適用可能性検討や，詳細仕様策定等と共に，規制内容の動向，業界側の対応動向を注視しつつ，研究を進める予定である．

謝辞 本研究の一部は，JSPS 科研費 基盤(B) JP18H03240 の支援を受けている．

参考文献

[1] 才所敏明, 辻井重男, 櫻井幸一, “ビットコイン利用者の特定・追跡の仕組みに関する考察”，第 54 回情報通信システムセキュリティ研究会（ICSS）．
[2] 才所敏明，辻井重男，櫻井幸一，“暗号資産の封印・償還における利用者の匿名性および特定・追跡性の考察”，暗号と情報セキュリティシンポジューム（SCIS2021）．
[3] 才所敏明，辻井重男，櫻井幸一，“暗号資産の匿名性要件の整理と対応レベルの比較”, コンピュータセキュリティシンポジューム（CSS2020）．
[4] 才所敏明，辻井重男，櫻井幸一，“暗号資産台帳の匿名性と特定・追跡性についての考察”，2020 年電子情報通信学会ソサイエティ大会.
[5] 才所敏明，辻井重男，櫻井幸一，“DAG 技術ベースの暗号資産の匿名性に関する考察”, 暗号と情報セキュリティシンポジューム（SCIS2020）
[6] 才所敏明，辻井重男，櫻井幸一，” 匿名暗号資産（Monero/Zcash/Grin）ブロックチェーンの匿名性に関する考察 ”, コンピュータセキュリティシンポジューム 2019（CSS2019）．
[7] 才所敏明，辻井重男，櫻井幸一，” 暗号仮想通貨における匿名化技術の現状と展望 ”, 情報処理学会第 81 回全国大会, 2019.
[8] 才所敏明，辻井重男，櫻井幸一，” 仮想通貨の匿名性の現状と課題”，暗号と情報セキュリティシンポジューム（SCIS2019）．
[9] 才所敏明，辻井重男，“インターネット上のサービスにおける利用者の匿名性と特定・追跡性の両立”，暗号と情報セキュリティシンポジューム（SCIS2021）．
[10] 才所敏明，辻井重男，“インターネット時代の本人確認基盤に関する考察ー NAF から GAF へ ー”，コンピュータセキュリティシンポジューム 2020（CSS2020）.
[11] 才所敏明，“NAFJP における本人確認方法に関する考察 ー National Authentication Framework in Japan ー”，コンピュータセキュリティシンポジューム 2019（CSS2019）.
[12] 才所敏明，辻井重男，“日本における本人確認基盤（NAFJA）の考察 ー National Authentication Framework in Japan ー”，情報処理学会・第 85 回コンピュータセキュリティ研究発表会，2019.
[13] 穴田啓晃，櫻井幸一，“ブロックチェーンの暗号論的要素技術の分類”，SCIS2018.
[14] 宇根正志，“暗号資産における取引の追跡困難性と匿名性：研究動向と課題”，金融研究/2019.7.
http://www.imes.boj.or.jp/research/papers/japanese/kk38-3-4.pdf
[15] The Chainalysis 2020 Crypto Crime Report
https://blog.chainalysis.com/reports/darknet-markets-cryptocurrency-2019
[16] Sean Foley, Jonathan R. Karlsen, Tālis J. Putniņš, “Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?”, 2019.
https://academic.oup.com/rfs/article/32/5/1798/5427781
[17] CipherTrace Geographic Risk Report:VASP KYC by Jurisdiction，2020.
https://ciphertrace.com/wp-content/uploads/2020/10/CipherTrace-2020-Geographic-Risk-Report-100120.pdf
[18] INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION（The FATF Recommendations），FATF，2020.
https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/fatf%20recommendations%202012.pdf
[19] GUIDANCE FOR A RISK-BASED APPROACH VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS，FATF，2019.
https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guIDance-rba-virtual-assets.html
[20] DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2018.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843
[21] INTERNET ORGANISED CRIME THREAT ASSESSMENT, EUROPOL, 2019.
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
[22] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, Financial Crimes Enforcement Network, 2020.
https://public-inspection.federalregister.gov/2020-28437.pdf
[23] David Riegelnig, OpenVASP: An Open Protocol to Implement FATF’s Travel Rule for Virtual Assets, 2019.
https://www.openvasp.org/wp-content/uploads/2019/11/OpenVasp_Whitepaper.pdf?cache=1
[24] Travel Rule Information Sharing Architecture for Virtual Asset Service Providers, 2020.
https://trisa.io/trisa-whitepaper/
[25] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. https://bitcoin.org/bitcoin.pdf
[26] Mastering Bitcoin
https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf
[27] Stefano Bistarelli，Ivan Mercanti，Francesco Santini, "An Analysis of Non-standard Transactions", 2019.
https://www.frontiersin.org/articles/10.3389/fbloc.2019.00007/full
[28] Monero：Privacy in the blockchain v1.0
https://eprint.iacr.org/2018/535.pdf
[29] Zero to Monero: First Edition
https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf
[30] Mastering Monero
https://masteringmonero.com/book/Mastering%20Monero%20First%20Edition%20by%20SerHack%20and%20Monero%20Community.pdf
[31] Zcash Protocol Specification
https://www.btrade.co.kr/btrade_res/20180507145055652.pdf
[32] Grin Whitepaper
https://www.allcryptowhitepapers.com/grin-whitepaper/
[33] Serguei Popov，“The Tangle”，April 30, 2018. Version 1.4.3.
https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf
[34] Anton Churyumov，“Byteball: A Decentralized System for Storage and Transferof Value”，2016.
https://obyte.org/Byteball.pdf
[35] Colin LeMahieu，“Nano: A Feeless Distributed Cryptocurrency Network”，2018.
https://nano.org/en/whitepaper
[36] Leemon Baird, Mance Harmon, Paul Madsen，“Hedera: A Public Hashgraph Network & Governing Council”，2019.
https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf
[37] AIDos Kuneen − A Blockless and Anonymous Cryptocurrency for the Post-Quantum Era −，AIDos Developer & AIDos Foundation，2018.
http://www.aIDoskuneen.com/files/adk_whitepaper.pdf

[38] DERO PROJECT WHITE PAPER，2018.
https://dero.io/attachment/Whitepaper.pdf
[39] Tangram: An Introduction，2018.
https://tangrams.io/wp-content/uploads/2018/12/Tangram_An_Introduction-2018-12-19-03-27.pdf
[40] All Cryptocurrencies https://coinmarketcap.com/all/views/all/
[41] Nicolas van Saberhagen, "CryptoNote v2.0", 2013.
https://cryptonote.org/whitepaper.pdf
[42] Andrew Poelstra，“Mimblewimble”，2016.
https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf
[43] Gregory Maxwell，“CoinJoin: Bitcoin privacy for the real world”，2013.
https://bitcointalk.org/index.php?topic=279249.0
[44] Gregory Maxwell，Andrew Poelstra，”Borromean Ring Signature”，2015.
https://raw.githubusercontent.com/Blockstream/borromean_paper/master/borromean_draft_0.01_34241bb.pdf
[45] SHEN NOETHER，“RING CONFIDENTIAL TRANSACTIONS”，2015.
https://eprint.iacr.org/2015/1098.pdf
[46] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer，“From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again”，2011.
https://eprint.iacr.org/2011/443
[47] Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova，“Pinocchio: Nearly Practical Verifiable Computation”，2013.
https://eprint.iacr.org/2013/279
[48] Christina Garman，Matthew Green，Ian Miers，” Accountable Privacy for Decentralized Anonymous Payments”，2016.
https://eprint.iacr.org/2016/061.pdf