IMES DISCUSSION PAPER SERIES

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

宇根正志（うね まさし）

Discussion Paper No. 2018-J-20

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

日本銀行金融研究所が刊行している論文等はホームページからダウンロードできます。
https://www.imes.boj.or.jp

IMES Discussion Paper Series 2018-J-20
2018 年 12 月

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

宇根正志（うね まさし）*

要　　旨

ビットコインをはじめとする暗号資産においては、ブロックチェーン上にすべての取引の情報が記録され、取引当事者でなくても取引の流れを追跡できるが、取引当事者である実際の個人や組織まで特定することは困難となっている。もっとも、最近では、暗号資産の取引に付随する情報を用いることなどにより、取引当事者をある程度絞り込むことができるとする研究成果がみられる一方で、取引の追跡困難性を高める新たな手法も提案されている。個々の暗号資産の特性を正確に理解するうえで、その取引の追跡困難性と匿名性について把握することはますます重要になっているといえる。こうした問題意識のもと、本稿では、暗号資産の取引の追跡困難性と匿名性に関する最近の研究動向を紹介する。

キーワード：暗号資産、追跡困難性、匿名性、ビットコイン、ブロックチェーン
JEL classification: L86、L96、Z00

* 日本銀行金融研究所企画役（E-mail: masashi.une@boj.or.jp）

本稿の作成に当たっては、日本電気株式会社特別技術主幹の佐古和恵氏から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目　次

１．はじめに

近年、ビットコインをはじめとする暗号資産（crypto-asset）が注目を集めている[1]。主な暗号資産のシステムは、分散型のネットワーク・インフラによるブロックチェーン上に実装されている。暗号資産の取引が一定のルールに沿って承認されると、取引当事者（送金元や送金先のエンティティ）にかかる情報や取引額等がブロックチェーンにすべて記録され、ネットワーク上のエンティティ（ノード）全体で共有される[2]。その結果、一部のノードが暗号資産の取引にかかる情報を事後的に改変しようとしても、そうした試みが成功する確率を無視できるほど小さくすることができる（耐攻撃性）。

暗号資産にかかる取引の流れは、ブロックチェーン上の情報によって追跡可能である。他方、暗号資産の取引を実行するエンティティ（ユーザー）には、取引について可能な限り第三者に知られたくないというニーズもあるとみられる[3]。そうしたニーズを満たすには、特定のユーザーが関与する複数の取引を関連づけられないようにする（追跡困難にする）とともに、特定の取引に関与しているユーザーの属性（氏名、住所、電話番号、使用する端末等の IP アドレス等、ユーザーの特定や絞込みにつながる情報）を秘匿する（匿名化する）必要がある。ビットコインの場合、基本的には、アドレス（公開鍵のハッシュ値）から取引を追跡可能であるものの、そのアドレスのみから対応するユーザーの属性を特定することは困難である。

こうした暗号資産の追跡困難性や匿名性を評価する研究や、これらの特性を強める手法を提案する研究が、ビットコインを中心に、近年活発となっている（Genkin, Papadopoulos, and Papamanthou [2018]、Henry, Herzberg, and Kate [2018]）。例えば、暗号資産がウェブサイト上での商品・サービス等の支払手段として用いられる場合には、ユーザーの属性にかかる情報が取引関係者に渡ってしまう可能性があるとの研究事例が報告されている（Khalilov and Levi [2018]）。こうした研究も踏まえると、暗号資産による取引の追跡困難性や匿名性を考える際には、暗号資産のシステムの仕組みだけでなく、その利用環境も考慮する必要があるといえる。また、ネットワークにおけるノードの IP アドレスや取引のデータの伝播状況等を手掛りに、取引のアドレスに対応するユーザーの端末を推定する研究事例も知られている。さらに、通常時には暗号資産の取引の追跡困難性を高めつつ、不正な取引の疑いが発生するなどの非常時には追跡が容易にな

---

[1] ビットコイン等は「仮想通貨（virtual currency）」あるいは「暗号通貨（crypto-currency）」と呼ばれてきたが、最近、金融安定理事会（Financial Stability Board）等では、「暗号資産」と呼ばれるようになっている（Financial Stability Board [2018]）。

[2] ブロックチェーンやビットコインの仕組みについては、松尾ほか［2018］を参照されたい。

[3] こうした追跡困難性や匿名性は、他方でマネーロンダリングや脱税等の犯罪への利用を誘発する側面もある（Tziakouris [2018]）。

る暗号資産の仕組みも提案されている。このように、さまざまな観点から数多くの研究成果が発表されているなかで、個々の暗号資産の特性を正確に理解するためには、その追跡困難性と匿名性について把握しておくことがますます重要となっている。

こうした問題意識のもと、本稿では、暗号資産の取引の追跡困難性や匿名性の評価、追跡困難性を高める手法について、最新の研究動向をサーベイする。既存の研究成果の多くはビットコインを対象としていることを踏まえ、ここでもビットコインにかかる研究成果を中心に取り上げる。以下、2 節では、取引の追跡困難性や匿名性を評価する最近の主な研究を紹介する。3 節では、追跡困難性や匿名性を高める主な手法を説明する。4 節では、最近の研究動向や今後の課題等について考察し、締め括りとする。

２．ビットコインにおける取引の追跡困難性や匿名性の評価

（１）概念と評価の視点

ビットコインの取引の追跡困難性や匿名性を考える場合、まず、これらの概念を明確にしておく必要がある。追跡困難性（unlinkability あるいは untraceability）については、研究論文によって区々の定義がなされているものの、概していえば、「特定のユーザーによる複数の取引やその流れを把握すること（取引の追跡）の難しさの度合い」と表現できる。また、匿名性（anonymity）は、「特定の取引にかかる当事者の属性を推定することの難しさの度合い」と定義できる。

まず、追跡困難性についてみると、ビットコインでは、ブロックチェーンから、任意の取引におけるアドレス（公開鍵のハッシュ値）を識別し、そのアドレスが用いられる取引を抽出することができる[4]。もっとも、アドレスの生成に制限はなく、同一のユーザーが複数のアドレスを使用可能であるため、例えば、取引の度に新しいアドレスを使用することによって、追跡困難性を高めることができる。また、そのアドレスのみから対応するユーザーの属性を推定することも困難であるといえる。

匿名性については、どのような属性を推定することを目的とするかによって、推定の難しさが変化しうる。推定対象となる（ユーザーの）属性としては、例えば、Khalilov and Levi [2018]では、①当事者の個人や企業を一意に特定可能な情報（氏名、電話番号、メールアドレス、住所・所在地等）、②個人や企業が使用しているモバイル端末・PC・サーバー等の IP アドレス、③モバイル端末等の

[4] 本稿では、ビットコインでのアドレスを単に「アドレス」と記述する。例えば、IP アドレスについて言及する場合には「IP アドレス」と記述して区別することとする。なお、ブロックチェーン上に記録されているデータを利用するためには、それらのデータが（ブロックの確定後に）改変されていないことが前提となる。本稿では、ブロックチェーン上に記録されているデータが一貫性を確保しているという想定のもとで議論を進める。

位置情報が挙げられている。位置情報については、IP アドレス等によって特定可能な地域から GPS による位置情報まで、さまざまな粒度が想定される。このように、推定の対象となる属性にはさまざまなバリエーションが想定される。

さらに、取引の流れやユーザーの属性を推定するうえで、ブロックチェーンに記載されている情報のほかに、どのような情報が利用可能であるかが重要となる。例えば、インターネット上で寄付を募るためのサイトを開設し、そのサイト上でアドレスを公開した結果、そのアドレスがサイトの主催者のものであるという手掛りから、主催者が有していた他の（非公開の）アドレスも推定可能となったという事例が知られている（Ron and Shamir [2013]）。このように、アドレスの使用・管理の形態も属性の推定に大きな影響を与えることから、匿名性を評価する際に留意が必要である[5]。

（２）追跡困難性や匿名性の評価にかかる主な研究事例

本節（1）で示した 2 つの視点を考慮しつつ、ビットコインの取引の追跡困難性や匿名性を評価した最近の主な研究事例を説明する。ユーザーの属性の推定に用いられる情報の観点から、①ブロックチェーンの情報を用いるケース、②ネットワークのレイヤーで生成・交信される情報を用いるケース、③ブロックチェーンやネットワーク以外の情報も用いるケースに分けて整理する。

イ．ブロックチェーンの情報を用いるケース

ビットコインでは、ユーザーである個人や企業が異なる複数のアドレスを生成・使用することができる。実際に、1 件の取引のデータ（transaction）における入力と出力にそれぞれ複数の送金元のアドレスと送金先のアドレスが存在するケースが多い。同一のユーザーが数多くのアドレスを使用して取引を行う場合には、特定のアドレスに対応するユーザーの属性を推定することはより困難になると考えられる。そこで、取引やアドレスの関係を示すグラフやクラスタリングの手法等を活用し、ブロックチェーン上の複数の取引のデータから、同一のユーザーのものとみられるアドレスを抽出・グループ化する（いわゆる、アドレスの名寄せを行う）試みが数多く行われている。

[5] アドレスの管理については、暗号資産の交換や現金化においても同様に問題となる。例えば、仮想通貨交換業者を通じてビットコインを他の暗号資産等に交換するときに、当該業者は、そのビットコインのアドレスに対応するユーザーの身元や属性を把握することがマネーロンダリング規制等との関係から求められる。この場合、仮想通貨交換業者における取引の記録が安全に保管されている（第三者の手に渡らないように管理される）ことが、各ユーザーの身元等を秘匿するうえでの前提となる。逆に言えば、仮想通貨交換業者から、アドレスとユーザーの属性を対応づける情報が流出する可能性を前提とする場合には、ユーザーの身元等を秘匿したいというニーズを満たすことが困難となる。

代表的なものとしては、複数の取引間の関係（ある取引の出力のアドレスが別の取引の入力のアドレスとなっていることなど）や複数のアドレス間の関係（ある取引の入力のアドレスとその出力のアドレスとの間に関係があることなど）をグラフで表現し、それらを分析する手法が広く知られている（Reid and Harrigan [2012]）[6]。Ron and Shamir [2013]では、ブロックチェーンの情報（2012 年 5 月 13 日時点）から取引間の関係を示すグラフを生成し、約 370 万件のアドレスを、それぞれ各ユーザーに対応するとみられる複数のグループに分類している。そのうえで上記のグラフを解析し、約 2.5 万のユーザーが取引を実施していたと推定したほか、そのなかには、約 16 万件のアドレスを有する（単一の）ユーザーが存在していた可能性が高いことを示した。

ビットコインの取引において一定の仮説を立て、それに基づきアドレスの名寄せ等を試みる研究も盛んに行われている。Meiklejohn *et al.* [2013]では、次の 2 つの仮説のもとでアドレスをグループ化している。すなわち、①複数のアドレスが同一の取引のデータの入力に存在する場合、同一のユーザーがそれらを使用しているという仮説と、②「おつりアドレス」（change address）を出力とする取引では、入力のアドレスはすべて同一のユーザー（おつりアドレスの所有者）によって使用されているという仮説である[7]。これらに基づいて分析した結果、約 1.2 千万件のアドレス（2013 年 4 月 13 日時点）を、各ユーザーに対応するとみられる約 330 万のグループに分類することができた。

また、Androulaki *et al.* [2013]では、次の 2 つの仮説がアドレスのグループ化に用いられている。すなわち、①複数のアドレスが同一の取引の入力に存在した場合、同一のユーザーがそれらを使用しているという仮説と、②取引に複数の出力が存在し、それらのなかに新規のアドレスが存在した場合、それはおつりアドレスであるという仮説である。これらに基づいて分析した結果、約 14 万件のブロック（2011 年 9 月時点）に含まれる約 160 万件のアドレスを、各ユーザー

[6] ビットコイン以外の暗号資産においても、少数ではあるが類似の研究成果が発表されている。例えば、Moreno-Sanchez, Zafar, and Kate [2016]では、Ripple をインフラとして利用して暗号資産の取引を行うケースを対象に、台帳（Ripple Ledger）に記録された情報（ウォレットの情報、送金の送受信先等）を用いることによって、同一のユーザーが使用している複数の（異なる）ウォレットを抽出しグループ化している。「ある取引における送金元のウォレットと送金先のウォレットを同一のユーザーが使用している」という仮説を設定したうえで、約 17 万件のウォレットの識別情報と約 1.3 千万件の取引の記録（2015 年 12 月 1 日時点）を分析し、959 個のウォレットの識別情報を（各ユーザーが使用しているとみられる）561 のグループに分類しているほか、（各ユーザーが使用する）Ripple ウォレットとビットコイン・ウォレットのペアを 241 のクラスタに分類している。

[7] おつりアドレスは、ビットコインの取引において発生する「おつり」（入力の総額から実際の送金額等を差し引いたもの）の送金先を指定するものである。おつりは送金元のユーザーに戻ってくるものであることから、おつりアドレスは、通常、入力のアドレスに対応するユーザーによって生成・使用されると考えられる。

に対応するとみられる約 69 万のグループに分類することができた。

このように一定の仮説を立てることによって、アドレスの名寄せ等が可能になることが知られている。もっとも、個々の仮説の妥当性は研究途上の段階にあり、必ずしもコンセンサスが得られているわけでもない。また、時間の経過とともにユーザーの行動が変化し、仮説の妥当性が低下する可能性がある点にも留意する必要がある。

ロ．ネットワークのレイヤーの情報を用いるケース

ビットコインは P2P（Peer-to-Peer）ネットワークにおいて取引される。P2P ネットワークにおいて、各ノードが他のどのノードと通信するかは、各ノードが有する他のノードの IP アドレスのリストに依存する。通常、各ノードは、一定の通信プロトコルに則って他のノードとのコネクションをまず確立する。そのうえで、自分が有している他のノードの IP アドレスのリストを自分の近隣のノードに適宜転送するとともに、他のノードから、同様の通信によって IP アドレスのリストを受信し自分のリストを更新していく。ビットコインの取引を行う場合には、ノードは、上記のリストに基づいて他のノードを選択し、それらに対して取引のデータ等をブロードキャストする。そのデータを受信した各ノードは、別の複数のノードにそれをさらにブロードキャストする。こうした処理が順次繰り返されてデータがリレーされることによって、取引のデータは P2P ネットワーク全体に拡散されていくことになる。

このようなプロトコルに着目して、特定の（送金元の）アドレスに対応するユーザーの端末やそれが接続しているノードの IP アドレス等をどの程度特定できるかを評価する研究が多数発表されている[8]。

Koshy, Koshy, and McDaniel [2014]では、P2P ネットワークにおける通信経路やそのパターン（リレー・パターン）を手掛りに、取引のアドレスとそれに対応するユーザーの端末（ウォレットやサーバー）の IP アドレスを探索する手法が提案されている。まず、多くのノードに接続して通信データを収集・分析し、特殊なリレー・パターンをみつける。次に、そうしたパターンにかかる仮説をいくつか設定し、それらに基づいてアドレスと IP アドレスとの対応関係を推定する。例えば、「特定の取引のデータにかかる通信を、あるノードから 1 度だけ受信した」というパターン（全取引の約 3.2%）については、「このノードが取引を開始した可能性が高い」という仮説を設定している。こうした手法を用いて、

[8] こうした研究成果をベースとして、ネットワークの情報を分析して取引の流れを追跡するツール（例えば、BitConeView）やそうした分析を支援するサービスを提供する企業（例えば、Elliptic、Chainalysis、Numisight、Skry）が既に存在している。上記のツールの 1 つである BitConeView は、ビットコインの送金の流れ（送金元と送金先のアドレス、特定のアドレスにおけるビットコインの滞留時間等）を可視化しグラフとして表示するツールである。

2012 年 7 月から約 5 か月間、ビットコインのネットワーク上のノード（約 2,700 個）と通信して約 550 万件の取引のデータを収集・分析したところ、約 1,200 件のアドレスにそれぞれ対応する IP アドレスを推定することができたとしている。

また、Biryukov, Khovratovich, and Pustogarov [2014]では、ビットコインの P2P ネットワークへのアクセス時に最初に接続するノード（エントリー・ノード）を手掛りに、特定のアドレスに対応するユーザーの端末（ビットコイン・クライアントを搭載）の IP アドレスを特定する手法が提案されている。まず、①P2P ネットワーク上の既知のノードと通信を行い、各ノードが有する IP アドレスのリストを収集する、②推定したいアドレスに対応する端末が接続しているとみられるノード（エントリー・ノード）群を絞り込む、③推定対象のアドレスを含む取引のデータがどのような経路で転送されているかを観察し、最終的に、上記②のエントリー・ノードのリストと突合しつつ IP アドレスを推定する。この手法によれば、ユーザーの端末の IP アドレスが NAT（Network Address Transformation）やファイアウォールによってインターネットから直接観察できない場合でも、一定の確率でその端末を識別できるとしている。提案手法の効果を確認するために、60 日間で約 6 万件の取引のデータを収集して分析したところ、攻撃者が観察しているノード群に送信された取引のデータの約 11%について、送金元アドレスに対応するユーザーの端末の IP アドレスを特定できるとの試算結果を示している。

ハ．ブロックチェーンやネットワーク以外の情報も用いるケース

ビットコイン等の暗号資産は、商品・サービスの購入時における支払手段として用いられるケースがある。例えば、ユーザーがインターネット上のオンライン・ショップのサイトにアクセスしてデジタル・コンテンツを購入する際に、そのショップのアドレスにビットコインを送金して支払いを行う場合がある。このときショップ等は、そのユーザーのアドレスに加え、さまざまな属性情報（ユーザーが利用しているインターネット・サービス・プロバイダー、メールアドレス、関連するコンテンツの購買履歴等）を入手できる場合がある。これを踏まえて、ブロックチェーンやネットワーク自体から得られる情報に加え、それ以外の情報も利用してユーザーの属性を推定する手法も研究されている。

Androulaki *et al.* [2013]では、ビットコインの取引にかかる処理を模倣するツールを用いて、商品購入の履歴やアドレス等からユーザーのプロファイルの推定を試行している[9]。まず、ユーザーのプロファイルとして、大学教官、大学事務員、学生の 3 種類をまず設定し、これらの属性を有するユーザーの実際の取引行動（購入対象の商品・サービスの種類、購入店舗、購入頻度、支払代金の多

[9] こうした分析手法は behavior-based analysis と呼ばれる。

寡等）を調査してプロファイルを作成する。模倣ツール上の（仮想の）各ユーザー（100 名、200 名、400 名の 3 パターン）には 3 種類のプロファイルの 1 つがそれぞれ割り当てられ、各ユーザーによる取引のデータがブロックチェーン上に記載されるようにする。こうして生成された取引のデータにおけるアドレスを名寄せするとともに、取引行動のパターンを抽出・分類し、各アドレスに対応するユーザーの属性を推定した。その結果、約 40%のユーザーの属性を約 80%の確率で正しく判定できたとしている。

Goldfeder *et al.* [2018]では、ウェブサイト上で商品を購入する際にビットコインで支払いを行った場合、その情報がどのように処理・管理されているかを調査した結果を示している。ウェブサイトの管理者以外の第三者が商品購入やビットコインの取引等にかかる情報を入手するケースでは、当該第三者が、特定の商品購入にかかる情報から（ビットコインにおける取引の）アドレスに対応するユーザーの属性を特定できる場合が考えられる[10]。ビットコインで支払いが可能な 130 件のウェブサイトを調査したところ、53 件のウェブサイトにおいて、商品購入等にかかる情報（購入日時、購入者の識別情報、支払金額、支払先の識別情報等）がショッピング・カートのサイトを通じて 40 社以上の（第三者の）企業に提供されていたとしている[11]。また、130 件のうち 17 件のウェブサイトでは、ビットコインによる取引のデータが第三者に提供されていたとの結果も示している。さらに、複数の商品購入等の支払いにビットコインを使用し、商品購入等にかかる情報を分析する場合、匿名性を高める手法の 1 つであるミキシング（詳細は後述）を適用したケースでも、取引のアドレスに対応するユーザーの属性を約 80%の確率で特定可能であるとしている[12]。

３．追跡困難性や匿名性を高める手法

2 節のとおり、これまでの研究によって、暗号資産にかかる取引が追跡可能となるケースも、一定程度存在することが示されている。そこで、ビットコインの追跡困難性や匿名性を高めるための手法の研究も活発に行われている。これまでに提案されている主な手法は、ネットワークに対して実施するものと、ブロックチェーン上のデータに対して実施するものとに分けることができる（Khalilov and Levi [2018]）。

[10] サイバー攻撃等によって、第三者から商品購入等にかかる情報が流出した場合、それらの情報が悪用される可能性がある。

[11] 商品購入等にかかる情報を入手した企業は、それらの情報を、当該商品にかかるマーケティングや広告戦略の検討に利用していたとみられる。

[12] ビットコインの取引の追跡困難化ツール（Ghostery や uBlock Origin）を適用したとしても、複数のウェブサイトにおいて商品購入等にかかる情報が流出することになるため、属性の推定防止が困難となる場合があると評価している。

（１）ネットワークに対して実施する手法

イ．匿名通信技術 Tor

ネットワークにおける対策は、取引のデータにおけるアドレスと、そのアドレスに対応するユーザーの（端末等の）IP アドレスとの間の関係性を推定しづらくすることを企図している[13]。そうした手法としては、Tor（The Onion Routing）が広く知られている（Dingledine, Mathewson, and Syverson [2004]）[14]。

Tor は、ウェブ・ブラウジング（web browsing）やインスタント・メッセージのように、比較的サイズの小さなデータを高速で通信することを主眼に開発された匿名通信技術である。ユーザーが、自分の IP アドレスや通信内容を秘匿しつつ、インターネット上の特定のサーバーにアクセスしたい場合、そのサーバーにアクセスするルート（ストリームと呼ばれる）をまず設定する。そのうえで、ストリーム上の各ノードとセッション鍵を共有するための情報を入手し、それを用いて通信データ（アクセスしたいサーバーのアドレスやサービスの種類を特定するデータ等を含む）を暗号化して送信する[15]。ストリーム上に位置する各ノードは、暗号化された通信データを受信すると、自分が共有しているセッション鍵で復号したうえで、それを次のノードに転送する[16]。この処理を各ノードが順次実施し、ストリーム上の最後のノードは、当初のユーザーのデータ（平文）を、ユーザーがアクセスしたいサーバーに送信する（図表 1 を参照）。その結果、最終的に通信データを受信したサーバーが、当初それを生成したユーザーを特定することは困難となる[17]。

---

[13] IP アドレスをユーザーの属性情報の 1 つと考えれば、こうした対策は匿名性の高まりにつながるものと位置付けられる。

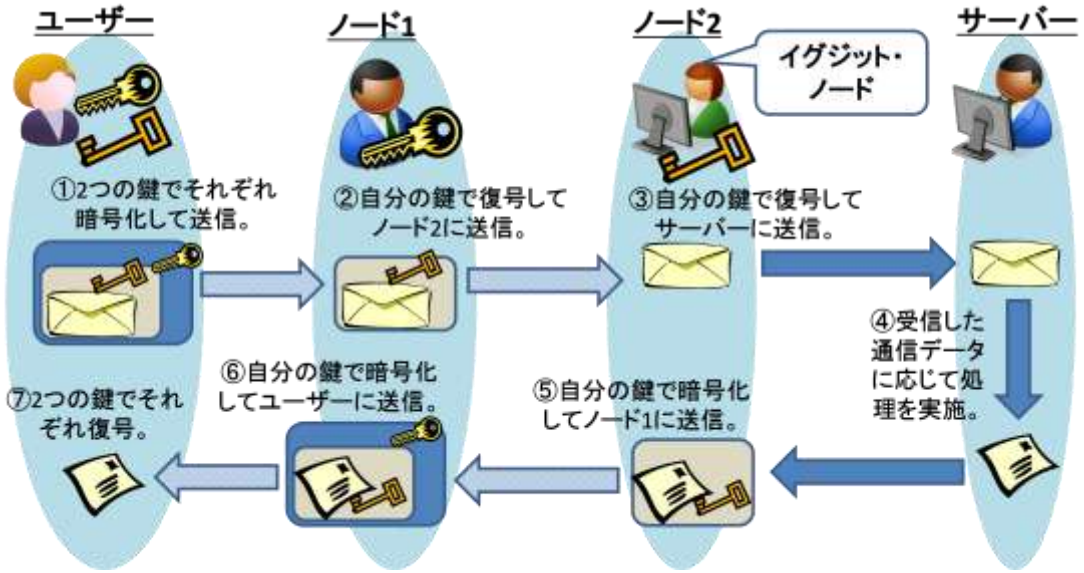
[14] Anoncoin、BitTor、Torcoin、Stealthcoi 等の暗号資産は、Tor の利用をサポートする機能を有している。

[15] ユーザーと各ノードは、公開鍵暗号を用いて事前にセッション鍵をそれぞれ個別に共有する。このとき、ユーザーは、各ノードの公開鍵証明書を入手して、セッション鍵を生成するためのデータの一部を（各ノードの公開鍵で）暗号化して送信する。このように、各ノードはユーザーの認証を実施しておらず、その意味で、ユーザーは各ノードに対して一定の匿名性を確保している。

[16] ノード間の通信は暗号通信プロトコル TLS（Transport Layer Security）で暗号化される。

[17] Henry, Herzberg, and Kate [2018]では、①Tor の通信をブロックする企業が一部存在しているほか、政府による国家レベルの検閲の対象となっている場合もある、②Tor がランサムウェアの配布やボットネットのコマンド送信等に悪用されるケースがあることなどから、暗号資産等の取引の通信に利用することに懐疑的な見方が示されている。

図表 1. Tor による通信の流れ（2 ホップのケース。概念図）



ロ. Tor の効果

ビットコインのユーザーが Tor を利用してビットコインのノードと通信する場合でも、取引の追跡やユーザーの属性の推定を企図した攻撃には留意する必要がある[18]。

Biryukov and Pustogarov [2015]では、ビットコインの DoS（Denial-of-Service）攻撃対策（ノードのペナルティ・スコア＜penalty score＞を用いるもの）を逆手にとって、特定のユーザーの通信経路を対象として、攻撃者が準備した Tor 上のノードを経由するように操作し、同一のユーザーによる通信や取引を探索する手法を提案している[19]。その手法の流れは以下のとおりである。

① 攻撃者は、Tor 上のノードとビットコインの（P2P ネットワーク上の）ノードを攻撃用に準備する。
② 攻撃者は、Tor 上の攻撃用ノードから、特定の（正常な）ノードをイグジット・ノード（exit node）とする不正な通信をビットコインのノードに対して

[18] 暗号資産についてではないが、P2P ネットワーク上の特定のアプリケーションへのアクセスに Tor を用いた場合、通信データから通信当事者の IP アドレスを推定可能であることを指摘する研究成果がある（Manils *et al.* [2010]）。

[19] ビットコインの P2P ネットワークでは、不正なメッセージを受信した場合、それを送信したノードのペナルティ・スコアを加算していく仕組みを備えている。各ノードは、他のすべてのノードについてペナルティ・スコアのリストを保有しており、このスコアが 100 に達したノードに対しては、24 時間、接続を受け付けないという対応をとる。この仕組みが DoS 攻撃対策にも利用されている。

繰り返し送信する[20]。この通信は、正常なノードのペナルティ・スコアを引き上げて、ビットコインの他のノードが上記のノードと通信しないようにするために行われる。

③ 攻撃者は、上記②を他のノードに対しても繰り返し行い、それらの（正常な）ノードがビットコインの通信を行うことができないようにする。この結果、Tor 上の攻撃用ノードがビットコインの取引におけるイグジット・ノードに選ばれる確率が高まる。

④ ユーザーが攻撃用ノードをイグジット・ノードに指定してアクセスしたときに、ユーザーからの通信データ（ビットコインの取引のデータ。平文）の内容を攻撃者が知ることができる（中間侵入が成功）。

さらに、上記④において、攻撃者のノードは、自分が保有している IP アドレスのリストをユーザーに送信する（ユーザーはそれを自分のリストに追加）。このとき、ユーザーに送信するリストに、そのユーザーを追跡するための偽のアドレス（アドレス・クッキー）を含めておく。また、同時に、そのユーザーが保有しているリストの送信も要求する。攻撃者は、ユーザーからリストを受信すると、それをビットコインの取引のデータと対応づけて保有しておく。こうした準備により、攻撃者が別のセッションで同様のデータを受信した際に、過去に受信したデータ（リストと取引のデータを対応付けしたもの）と照合し、一致するものがあれば、同一のユーザーによる通信であることが判明する。これを手掛りとして、取引のアドレスの名寄せや特定のユーザーの IP アドレスを推定可能になる。

提案手法の理論的な評価では、攻撃者が、Tor 上のイグジット・ノード全体の 1～3%のノード、および、1,000～1,500 個のビットコインのノード（ボットネット等を利用）を操作できれば、大多数の Tor の通信を攻撃者のノードに誘導可能であるとの試算結果を示している[21]。また、アドレス・クッキーについては、ユーザーが保有するアドレスのリストのうち、約 76%のアドレスが 10 時間後も保持されていた（24 時間後に保持されていたアドレスの割合は約 55%）ことなどから、取引やユーザーを追跡する手段として有効であると評価している。こうした攻撃への対策としては、①ビットコインの DoS 対策手法の見直し、②ビットコインの取引にかかる通信の暗号化と相互認証の実施、③信頼できる（Tor 上の）ノードのリストの作成・共有とメンテナンスが挙げられている。

[20] イグジット・ノードは、Tor の通信路の末端のノードであり、Tor 上で多重に暗号化された通信データは、このノードにおいて平文となるほか、ユーザーへの「戻り」の通信データ（平文）も、このノードが最初に受信することになり、その内容を知ることができる。

[21] 攻撃の準備にかかる費用は、1 か月あたり約 2.5 千米ドルと試算されている。

（２）ブロックチェーンに対して実施する手法

2 節（2）で紹介したように、ブロックチェーンに記録される取引のアドレスを名寄せしたり、IP アドレス等の属性との対応関係を推定したりすることが、ある程度可能である。これらは、暗号資産の送金における追跡困難性や匿名性を低下させうる要因となる。主な対策としては、ビットコイン等の既存の暗号資産にミキシング（mixing）の手法を組み合わせるものと、高度な暗号技術を利用するものに分けられる（Genkin, Papadopoulos, and Papamanthou [2018]）。

イ．ミキシング

ミキシングは、暗号資産の取引のデータにおける入力や出力に、他の無関係なアドレスを記入し本来のアドレスと混在させることによって、第三者による取引の追跡やアドレスの名寄せをより困難にする手法である。この手法のメリットは、対象となる暗号資産の仕様やシステムに影響を与えることなく利用可能という点である。ミキシングの手法としては、それを実行する単一のエンティティ（ミキサー＜mixer＞）が中央集中的に処理するものと、各ユーザーがそれぞれ分散して処理するものが提案されている。

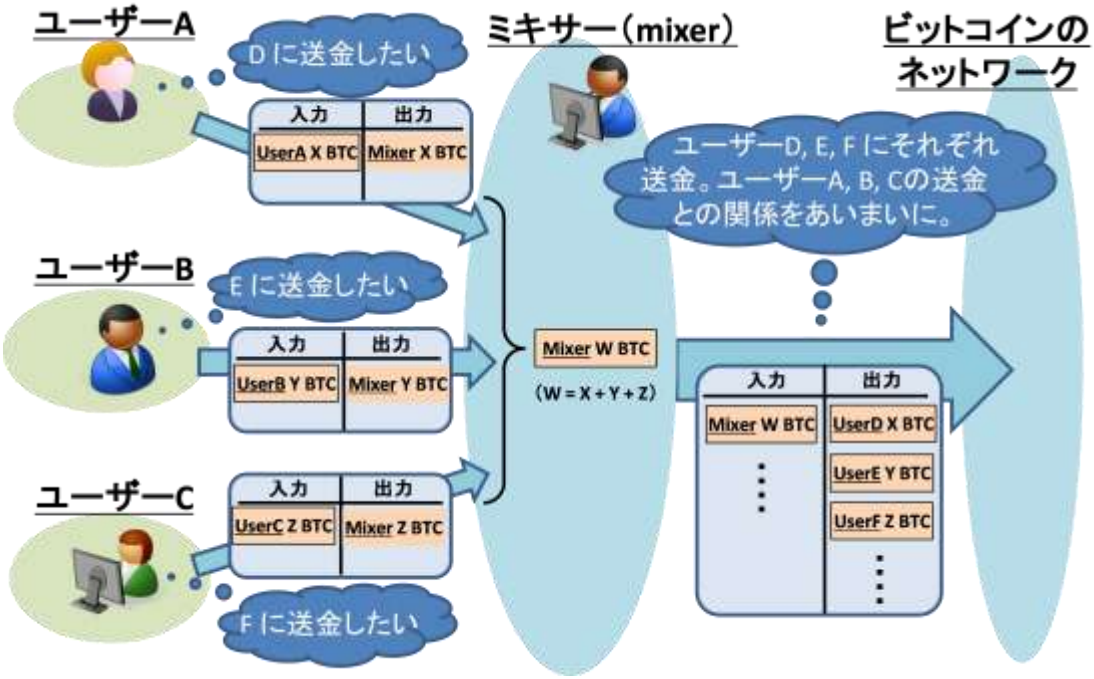
（イ）中央集中型のミキシング

ミキサーは、複数のユーザーからの送金依頼を受け付けた後、（ミキサーが所有する）ユーザーとは無関係のアドレスにそれらの送金を繰り返し行って取引の流れを複雑にしたうえで、最終的に、各ユーザーによって事前に指定された送金先に一定の金額をそれぞれ送金するというものである。既にいくつかのサービスが提供されており、後述する分散型のミキシングに比べて手軽に利用できる[22]。シンプルな例としては、ミキサーが、受け取った暗号資産の送金を特段再送金することなく、同一のアドレスから（事前に指定された）各アドレスにそれぞれ送金するというものが挙げられる（図表 2 を参照）。

実際のミキシングのサービスにおける取引の追跡困難性を評価した最近の研究として、廣澤・上原［2018］が挙げられる。この研究では、ミキシングのサービスを利用してビットコインの送金を自分で行い、自分の取引がブロックチェーン上のデータを用いて追跡できるか否かを評価している。ミキシングのサービスの 1 つである「BitcoinCloak」に対して 0.016BTC の送金を依頼したところ、まず、BitcoinCloak において複数の金額に分割され、BitcoinCloak が保有している未使用アドレス等にそれぞれ送金が行われた。この処理が複数回繰り

[22] ミキサーのサービスは「タンブラー」「ランドリー・サービス」とも呼ばれており、Bitmixer、Bitlaunder、Coinmixer、BitcoinCloak、Helix 等、その提供を行うサービスが存在する。

図表 2. ミキサーによるミキシング：シンプルな例（概念図）



（備考）Genkin, Papadopoulos, and Papamanthou [2018]の Figure 1 を基に作成。

返し実施され、当初送金された 0.016BTC は、数千個のアドレスを経由して、最終的には、指定したアドレスに集約された。ブロックチェーン上の情報を用いて取引の流れを分析したところ、複数のアドレスの名寄せが成功しない限り、第三者がブロックチェーンの情報のみから取引の流れを追跡することは困難であると評価している。

もっとも、中央集中型のミキシングには、ミキサーが暗号資産を不正に盗取するリスクがあるほか、その主体は取引の流れを把握できるという問題もあり、ミキサーが信頼できる第三者であることが求められる（Ben-Sasson *et al.* [2014]、Biryukov and Pustogarov [2015]、長沼ほか［2017］）[23]。

（ロ）分散型のミキシング

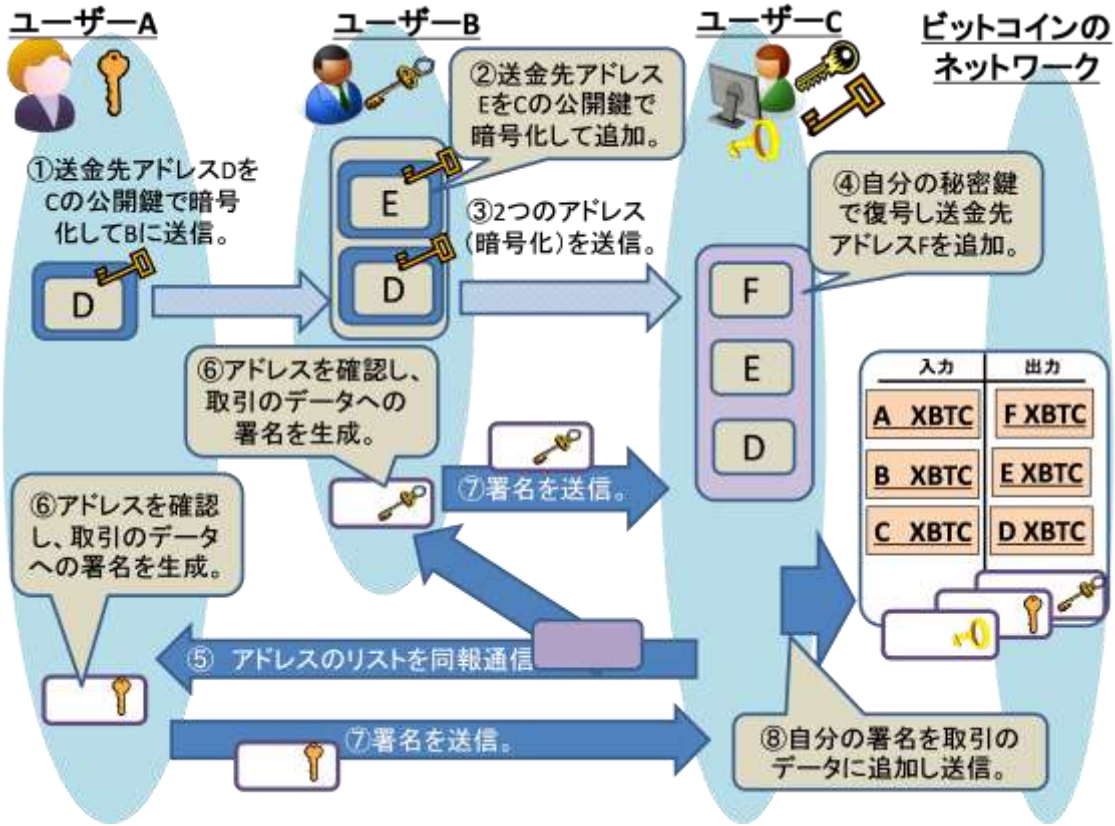
上記のような中央集中型のミキシングの問題への対応として、複数のユーザーが協力して実行するミキシングの手法（CoinJoin、CoinShuffle、CoinParty、Xim 等）も提案されている。ここでは、代表的な手法の 1 つである CoinShuffle の概要を紹介する（Ruffing, Moreno-Sanchez, and Kate [2014]）。3 つのユーザー（アドレスをそれぞれ A、B、C とする）がそれぞれアドレス D、E、F の各ユーザー

[23] こうした問題への対策を考慮した手法（例えば、CoinSwap、TrumbleBit、Blindcoin）も提案されている（Heilman *et al.* [2017]）。

にビットコインを送金する場合を考える。これらの取引におけるアドレスの関係を推定困難にするために、CoinShuffle では、各ユーザーが他のすべてのユーザーに対してそれぞれの取引のデータをブロードキャストする。以下の説明では、理解しやすくするために、ユーザーA からユーザーB、次に、ユーザーB からユーザーC という順番での通信に限定して説明する。まず、各ユーザーが自分の公開鍵を生成して他のすべてのユーザーに送信した後、以下の処理が実行される（図表 3 を参照）。

① ユーザーA は、ユーザーC の公開鍵を用いて送金先アドレス D を暗号化し、ユーザーB に送信する。
② B は C の公開鍵を用いて送金先アドレス E を暗号化し、A から受信した暗号化データにそれを追加して（2 つの暗号化済みアドレスを）シャッフルする。
③ B は、シャッフルした結果（暗号化済みアドレス D と E）を C に送信する。
④ C は、受信した暗号文を復号して（平文の）アドレス D と E を得た後、自分の送金先アドレス F を加えてシャッフルする。

図表 3. CoinShuffle における処理（A→B→C の場合）の流れ（概念図）



⑤ C は、上記④の 3 つのアドレスを A と B にブロードキャストする。
⑥ A と B は､受信したデータに自分の送金先アドレスが含まれていることを確認し、取引のデータを生成したうえで署名をそれぞれ生成する。
⑦ A と B は、上記⑥で生成した署名をそれぞれ C に送信する。
⑧ C は、A と B の署名、および、（取引のデータに対する）自分の署名を取引のデータに追加し、ビットコインのネットワークに送信する。A と B は、送信された取引のデータを取得し､自分の送金先アドレスが間違いなく含まれていることを確認する。

CoinShuffle の処理性能については、50 名のユーザーによって上記のプロトコルを LAN 環境上で動作させる実験が行われており、一連の処理にかかる時間が少なくとも 40 秒以上かかる旨が報告されている[24]。

CoinShuffle では、各ユーザーが事前に他のユーザーと通信を行って鍵を共有するなどの準備作業も必要になる。また､CoinShuffle には､参加可能なユーザー数に上限が存在するという問題が知られている。取引のデータには各ユーザーの署名が付与されることから、ユーザー数の増加とともに、取引のデータのサイズが大きくなる。取引のデータのサイズには上限が存在する（ビットコインでは 100 キロ・バイト）ことから、ユーザー数が制限されることになる。こうした問題への対応として、マルチパーティ計算を利用し、ユーザーの数によらず取引のデータに付与する署名の数を一定とする手法（CoinParty）が提案されている（Ziegeldorf *et al.* [2015]）[25]。

ロ．高度な暗号技術（リング署名やゼロ知識証明）の利用

高度な暗号技術、特に、リング署名（ring signature）やゼロ知識証明（zero-knowledge proof）を利用することによって､取引の追跡困難性や匿名性を高める仕組みを暗号資産に実装する手法が提案されている（ただし、ビットコイン等の既存の暗号資産に実装するには、当該暗号資産のシステムの仕様変更が必要となる)。こうしたリング署名やゼロ知識証明等を利用する手法は、信頼できる第三者を用いないものと用いるものに分けることができる。

（イ）信頼できる第三者を用いない手法

まず、暗号鍵等のセットアップ時に信頼できる第三者を利用しない主な手法

[24] CoinShuffle の処理性能を向上させる改良版（CoinShuffle++）も提案されている（Ruffing, Moreno-Sanchez, and Kate [2017]）。
[25] マルチパーティ計算（multi-party computation）とは、複数のエンティティが自分の（秘密の）データを他のエンティティに秘匿したままで、それらのエンティティが連携して一定の計算を実行するプロトコルの総称である。

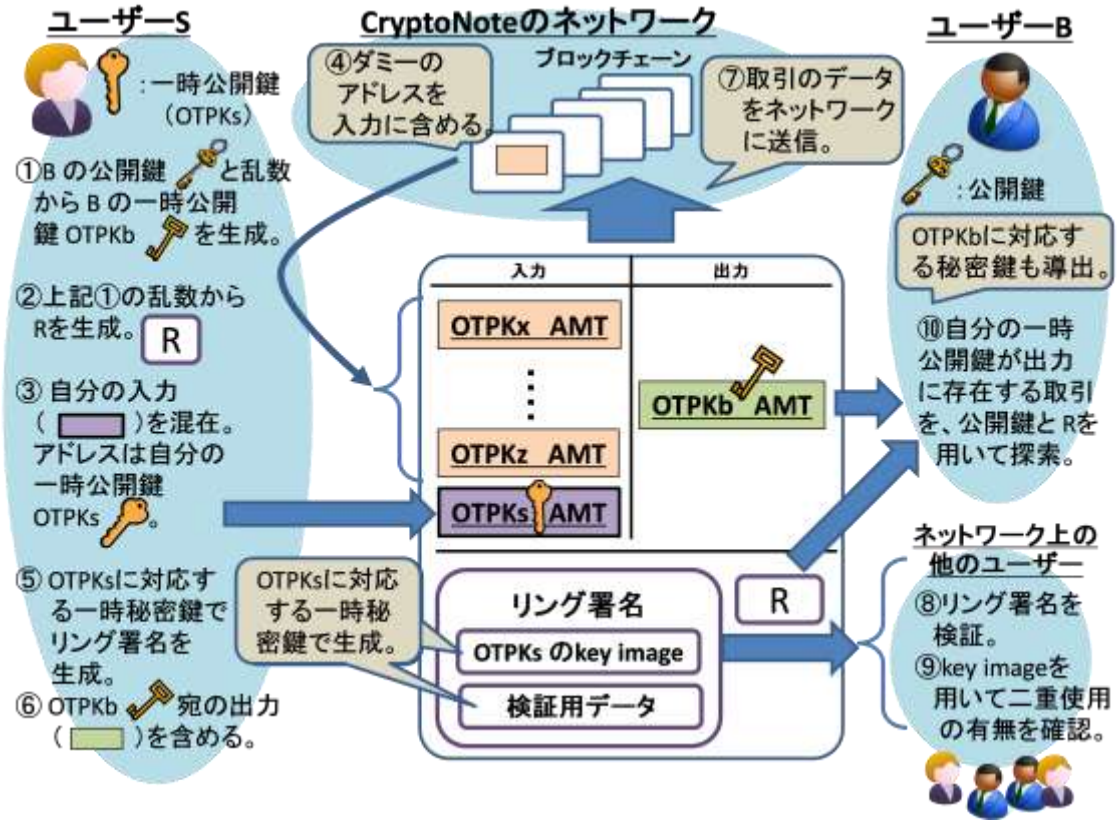
として、CryptoNote、Monero が挙げられる。これらの手法における取引の追跡困難性を高めるうえで、リング署名が重要な役割を果たす[26]。リング署名は、「署名の生成者があるグループに属するメンバーの一人であることを検証できるものの、それがどのメンバーかを特定することが困難である」という特性をもつ署名方式の総称である。ここでは、CryptoNote を取り上げて、処理の概要を説明する。

CryptoNote では、(i) 送金先のアドレスの使用回数を 1 回だけとして、送金先のアドレスの名寄せを困難にする（どのアドレスも 1 回のみの利用であることから、このアドレスを一時公開鍵と呼ぶ)、(ii) ダミーのアドレスを混在させ、複数の入力のアドレスのなかから真の送金元アドレスを推定しづらくする、(iii) リング署名によって、取引のデータをどのアドレスのユーザーが生成したかを秘匿する（van Saberhagen [2013])。送金者のユーザーS が送金先のユーザーB に一定額（AMT）を送金する場合を想定すると、処理の流れの概要は以下のとおりとなる（図表 4 を参照)。

① ユーザーS は、ユーザーB の公開鍵（楕円曲線暗号）を入手するとともに、乱数を生成し、これらを用いて B の一時公開鍵（OTPKb）を生成する。この一時公開鍵は、B が送金を受け取るときのアドレスとなり、送金を行う都度生成される（1 回限りの使用)。
② S は、上記①で生成した乱数から、ある値 R（公開可能）を生成する。この R は、B が自分宛の取引（その出力に OTPKb がアドレスとして含まれているもの）をみつけるときに用いられる。
③ S は、自分の送金元アドレス（まだ他のユーザーに送金していないもの）を取引のデータの入力に含める[27]。この送金元アドレスには、一時公開鍵 OTPKs が対応する。
④ S は、既存のブロックチェーンの別のブロックから、同じ送金額の送金先となっている複数のアドレス（OTPKx, …, OTPKz）を取得し、ダミーとして取引のデータの入力に含める。

[26] 具体的には、「traceable ring signature」と呼ばれるリング署名が利用されている（Fujisaki and Suzuki [2007])。これによって、暗号資産の二重使用（同一の暗号鍵によって生成された異なる 2 つの署名を送金に利用すること）を防ぐことができる。
[27] この送金元アドレスについては、今回の B への送金額と同額が別のアドレスにより既に送金されており、未使用であることが前提となっている。

図表 4. CryptoNote における処理の流れ（概念図）



⑤ S は、取引の入力のアドレスすべてを対象に、自分の一時公開鍵 OTPKs に対応する一時秘密鍵によってリング署名を生成する。リング署名の生成では、取引の入力に含まれるすべてのアドレス（一時公開鍵）や、OTPKs のキー・イメージ（OTPKs のハッシュ値に一時秘密鍵を乗じたもの）も使われる。このキー・イメージは、暗号資産の二重使用の検知に使用される。

⑥ S は、送金先の（B の）アドレス OTPKb と送金額を取引のデータの出力に含める。

⑦ S は、取引のデータにリング署名や R を含めた後、そのデータを CryptoNote のネットワークに送信する。

⑧ ネットワーク上の他のユーザーは、取引のデータを検証する。まず、リング署名を検証する。ここでは、取引のデータの入力に含まれるすべての一時公開鍵が使用される。このため、リング署名を生成したユーザーに対応するアドレスは推定困難となる。

⑨ ネットワーク上の他のユーザーは、リング署名からキー・イメージを抽出し、過去の取引のデータを探索しつつ、同一のキー・イメージのリング署名が存在しているか否かを確認する。存在していた場合、この取引を二重

使用とみなして破棄する。ここでキー・イメージから、それに対応する一時公開鍵を生成することは困難であり、S の取引であることは秘匿される。

⑩ B は､検証対象となっていた取引が自分宛の送金か否かを確認するために、自分の秘密鍵、公開鍵、R を用いて一定の処理を行い、その結果が OTPKb と一致するか否かを確認する。これは（特定の秘密鍵を有する）B のみ実行可能である。一致すれば、B は、OTPKb が自分宛のアドレスであることを認識し、OTPKb を別の送金に使うことができる。OTPKb を別の送金で使用するときに必要な一時秘密鍵は、B が自分の秘密鍵等から生成できる。

上記のとおり、CryptoNote では、真の送金元のアドレス（OTPKs に対応）は、取引のデータの入力に含まれる他の複数のアドレスと混在しており、取引の追跡困難性はそれらのアドレスの数に依存する。追跡困難性を高めるためには、ダミーのアドレスの数を増やす必要がある。その場合には、リング署名等にかかる計算量が増加するというデメリットがある。また、送金額は秘匿されないことになる。

CryptoNote の仕組みをベースとしつつ、取引における送金額を秘匿するとともに計算量を削減することが可能な暗号資産として、Monero が提案されている（Noether, Mackenzie, and the Monero Research Lab [2016]）。Monero では、リング署名に加えて、準同型暗号を利用している。準同型暗号は、データを暗号化したまま加算や乗算を実行できるという特長を有している。これにより、取引のデータにおける送金額をマスクしたうえで、（各送金額の特定はできないものの）入力と出力において各送金額の合計が整合的であることを確認できる。

Monero については、実際のブロックチェーン上のデータを分析し、真の送金元アドレスをどの程度特定できるかを評価した結果が報告されている（Kumar *et al.* [2017]）。Kumar *et al.* [2017]では、まず、約 42 万個を超えるブロック（2014 年 4 月～2017 年 2 月のデータ）を分析したところ、送金額のマスクを実施していたブロック数が全体の約 11%にとどまっていたほか、約 65%のブロックにおいてダミーの入力が使用されていなかった（取引の入力のアドレスは 1 つのみであった）ことが報告されている。このように、上記のデータ取得期間における取引では、匿名性を高める手法が十分に活用されておらず、ダミーのアドレスを混入しないブロック（約 65%）については、取引の流れが追跡可能となっていた。また、直前のブロックの出力のアドレスが直後のブロックにおいて入力のアドレスとして登場する場合、そのアドレスは約 98%の確率で実際に費消されていた（ダミーではなかった）としている。

（ロ）信頼できる第三者を用いる手法

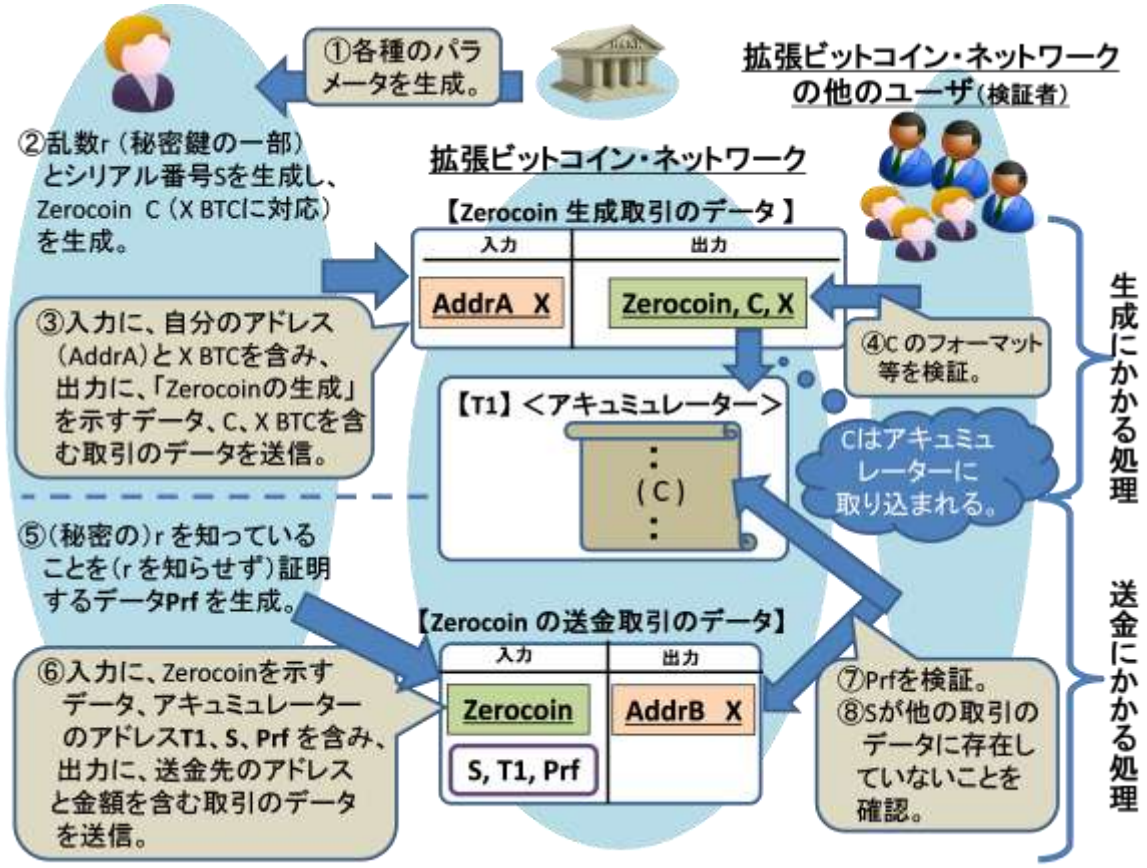
暗号技術とともに、暗号鍵等のセットアップ時に信頼できる第三者を用いる暗号資産として、Zerocoin、Zerocash、Zcash 等が提案されている（Miers *et al.* [2013]）。これらは、ビットコインの基本的な仕組みをベースとしたうえで、ゼロ知識証明を利用している。ゼロ知識証明は、ある秘密の情報について、その内容を相手（検証者）に知らせることなく、「自分がそれを知っている」ことだけを証明する手法の総称であり、追跡困難性や匿名性を高めるうえで重要な構成要素となっている。以下では、代表的なものの 1 つである Zerocoin の取引の処理の流れを説明する。

例として、ビットコインの仕組みを拡張して Zerocoin を構成する場合において、その拡張されたネットワーク（以下、拡張ビットコイン・ネットワーク）上のユーザーA がユーザーB に X BTC を送金するケースを想定する。処理の流れは、Zerocoin の生成と送金に分けることができる（図表 5 を参照）。

【Zerocoin の生成】

① パラメータ準備者（信頼できる第三者）は、取引で使用する各種のパラメー

図表 5. Zerocoin における処理の流れ（概念図）



タを生成し、各ユーザーに配信する。

② ユーザーA は、乱数 r（A の秘密鍵の一部）を生成するとともに、生成する Zerocoin（C とする）のシリアル番号 S を生成したうえで、これらのデータを用いて C を計算する。ここでは、C から r を求めることができないように、離散対数問題の困難性を利用する。

③ A は、ビットコイン（X BTC）を C に対応づけるために、ビットコインの取引のデータを生成する[28]。入力には、自分のアドレス（AddrA）とビットコインの送金額（X）が含まれ、出力には、「Zerocoin の生成」を示すデータのほかに、C と X が含まれる。生成した取引のデータを、ビットコインのネットワークに送信する[29]。

④ 拡張ビットコイン・ネットワークの他のユーザーは、検証者として、C の値のフォーマット等を検証する。それが成功すると、ビットコインのプルーフ・オブ・ワークを経て、上記③のブロックは、拡張ビットコイン・ネットワークでのブロックチェーンに取り込まれる。その後、C は「アキュミュレーター（accumulator）」と呼ばれる、Zerocoin のリスト（特定のブロックに格納される）に「未使用の Zerocoin」として記載される。

【Zerocoin の送金】

⑤ A は、Zerocoin を用いて X BTC を B（アドレスは AddrB）に送金する場合、まず、「秘密の r の値を開示せず、それを確かに知っていること」だけを第三者に証明するためのデータ Prf（ビットコインにおける取引のデータへの署名に相当）を生成する。このとき、A は、アキュミュレーターから未使用のすべての Zerocoin の値（C）を収集して署名生成に使用する。

⑥ A は、入力に、Zerocoin を示すデータ、アキュミュレーターを含むブロックを特定するデータ（T1）、S、Prf を含み、出力に、AddrB と X BTC を含む取引のデータを生成する。次に、この取引のデータを、拡張ビットコイン・ネットワークに送信する。

⑦ 拡張ビットコイン・ネットワークの他のユーザー（検証者として行動）は、T1 で示されるブロックから収集した（アキュミュレーターに含まれる未使用の）Zerocoin の系列（C を含む）や S 等を用いて Prf を検証し、送金元のユーザーが（Prf に対応する）秘密鍵を有していることを確認する。

⑧ 上記⑦の他のユーザーは、二重使用でないことを確認するために、同一の S を含むブロックがほかに存在しないことを、ブロックチェーンを参照しつつ

[28] ここで、Zerocoin（C）に対応づけるビットコインの金額（X BTC）は、システムで固有の値となる。

[29] この処理を、Zerocoin における預託（escrow）と呼ぶ場合がある。

確認する。

上記⑦の確認において使用されるデータには A のアドレスを特定する情報が含まれていないほか、Prf の検証からも、支払いに利用される Zerocoin が C であることを知ることができない。こうしたことから、取引の流れは追跡困難となる。ただし、その追跡困難性は、アキュミュレーターに記載される Zerocoin の数(C の系列の数)に比例することから、一定の追跡困難性を確保するためには、アキュミュレーターに含まれる Zerocoin のリストが相応に大きくなっている必要がある。また、当初の送金元と最終的な送金先のアドレスは公開されることになる。

Zerocoin の改良版として、Zerocash や Zcash が提案されている。Zerocash は、Zerocoin における追跡困難性に加えて、最初の送金元と最後の送金先のアドレスを秘匿する機能を有しているほか、ゼロ知識証明の手法等を改良することでより高速での処理を実現している（Ben-Sasson *et al.* [2014]）[30]。こうした実用性の高さを利用して開発された暗号資産が Zcash である。Zcash は、Zerocash をベースとしつつ、ビットコインと類似のマイニング手法を採用した暗号資産であり、2016 年 10 月から稼働している（ビットコインのフォークの 1 つ）[31]。

Kappos *et al.* [2018]では、Zcash における取引のデータ約 2 百万件（2018 年 1 月 21 日時点）を対象に、各取引の入力に含まれるアドレスと出力に含まれるアドレス（アドレス数は全体で約 1.7 百万件）を対応付けしてグラフを作成し、その分析結果を報告している。Zcash は、アドレスを秘匿して送金を行うモードに加えて、通常のビットコインのように、アドレスを開示するモードが準備されている。分析対象となった取引のデータ全体についてみると、約 74%がアドレスを開示するモードであり、取引の追跡を困難にする機構が利用されていなかったとしている。また、取引のデータにおける入力のアドレスと出力のアドレスの関係をグラフ化し、対応付けされたアドレスの系列（約 56 万件）をそれぞれ識別できた（取引の流れを把握できた）としている。

[30] Zerocash では、ゼロ知識証明として zk-SNARK（zero-knowledge succinct non-interactive argument of knowledge）と呼ばれる手法等を利用しており、（Zerocoin に比べて）取引のデータのサイズ（約 45 キロ・バイト→約 1 キロ・バイト）や、ビットコインを費消する取引のデータの検証にかかる処理時間（約 45 秒→約 1 秒）を大きく削減可能であるとしている（Ben-Sasson *et al.* [2014]）。

[31] Zcash では、（ユーザーのアドレスとは異なる）隠されたアドレス（hidden address）やダミーのアドレスとの間での送金（取引の入力と出力が共に隠されたアドレスとなるもの）が可能となっている（「シールド・プール＜shielded pool＞内の取引」と呼ばれる）。これによって、取引の追跡困難性がより高まると期待される（Kappos *et al.* [2018]）。

４．結びに代えて：考察と今後の課題

ここまで説明してきたように、暗号資産の取引の流れをブロックチェーン上の情報等からどれだけ追跡できるか、また、各取引のユーザーの属性を推定できるかについて、近年、数多くの研究結果が発表されている。それらの評価結果を横並びで比較することは困難であるものの、ナイーブなビットコインはもとより、匿名通信路 Tor やミキシング等の手法を利用したとしても、取引のデータに含まれるアドレスの系列をグラフ化したり、ビットコインの取引の行動パターンを利用したりすることによって、取引の流れやアドレスの名寄せがある程度可能なことが示されている。

こうした状況を踏まえ、ミキシングや高度な暗号技術を利用した手法が提案されている。リング署名やゼロ知識証明を用いる手法では、取引等を実施するときの処理量やデータ量をいかに削減していくかが実用化するうえでの課題であるほか、信頼できる第三者を用いる手法においては、そうした第三者（エンティティ）の存在をどのように実現していくかも重要な課題となる[32]。

また、取引の追跡困難性や匿名性を考えるうえで、各暗号資産の技術的側面に注目するだけでなく、それらの取引がどのように利用されているかを考慮することが重要といえる。これは、暗号資産がインターネット上での商品の購入等の支払いや寄付活動における送金に利用される場合、そうした、暗号資産のシステムの外側でやりとりされる情報によって、暗号資産のユーザーの属性にかかる情報が第三者に推定される可能性を指摘する研究成果からも明らかである。また、カラードコインやスマートコントラクトのように、ブロックチェーン上で暗号資産と別のアプリケーションが相乗りしている場合、他のアプリケーションにおける処理や情報が暗号資産の取引の追跡困難性等に影響を与える可能性も想定される。こうした点を踏まえると、暗号資産のアプリケーションや利用環境を特定し、第三者がどのような情報を得ることができるかを明確にしたうえで、暗号資産のエコシステム全体を俯瞰しつつ、個々の暗号資産の追跡困難性や匿名性を議論することが求められる。

ユーザーの視点からは、各種の手法によって取引の追跡困難性や匿名性がどの程度確保できるのかが理解しづらいという課題がある。実際に、Monero や Zcash にかかる研究では、取引の追跡を困難にする手法を利用していない取引がかなり多いことが指摘されている。新しい手法の普及が遅れているのは、それに対するユーザーの信頼が十分に得られていないためではないかという指摘もある。追跡困難性や匿名性等の用語の統一も含め、各種の手法の効果を横並び

[32] 信頼できる第三者を利用するという考え方は、ブロックチェーンを利用する暗号資産の基本的なコンセプト（分散型のシステム）とは本質的に相容れないものである。こうした双方の考え方を統合したシステムを考案していくことができるかは今後の検討課題である。

で評価する手法を開発することに加え、一般のユーザーが理解できるようなかたちで評価結果をいかに示していくかも検討する必要がある。

暗号資産による健全な取引という観点では、サイバー攻撃等によって暗号資産が不正送金されたり盗取されたりした場合に、そうした取引の追跡が困難になる可能性があるほか、マネーロンダリングに利用される可能性も問題として指摘されている（Tziakouris [2018]）。取引の追跡を効率化するために、例えば、2018 年 1 月に発生したコインチェック事件では、流出した NEM の換金や交換を阻止するために、それを保有しているとみられるウォレットに対してトークン（モザイク）を付与してマーキングするという対応が行われた。佐藤・今村・面［2018］では、モザイクの付与や時系列での拡散状況を調査し、取引の追跡の効果について評価を行っている。また、Zerocoin について、不正な取引を追跡する監査人の機能を追加した手法の研究も行われている（長沼ほか［2017］）。これは、ユーザーが送金を行う際に、信頼できる第三者である監査人に対して、ゼロ知識証明を解くための情報を渡し、送金の流れを追跡する必要が生じた場合に限り、監査人が上記の情報を使用して送金元等を特定できるというものである。こうした手法についても研究が活発化しており、法執行の有効性を確保する観点から、取引の追跡困難性等の研究とともに、引き続き、研究動向をフォローしていくことが重要である。

以　上

【参考文献】

佐藤哲平・今村光良・面和成、「コインチェック事件における流出 NEM の追跡に関する実態調査」、『信学技報』118 (30)、電子情報通信学会、2018 年、35～41 頁

長沼健・吉野雅之・佐藤尚宜・鈴木貴之、「監査機能付匿名送金」、『2017 年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2017 年

廣澤龍典・上原哲太郎、「ビットコインのミキシングにおける資金移動の分析」、『情報処理学会研究報告』2018-CSEC-81 (9)、情報処理学会、2018 年 5 月

松尾真一郎・楠正憲・崎村夏彦・佐古和恵・佐藤雅史・林達也・古川諒・宮澤慎一、『ブロックチェーン技術の未解決問題』、日経 BP 社、2018 年

Androulaki, Elli, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun, "Evaluating User Privacy in Bitcoin," *Proceedings of International Conference on Financial Cryptography and Data Security (FC) 2013*, Lecture Notes in Computer Science, 7859, Springer-Verlag, 2013, pp.34-51.

Ben-Sasson, Eli, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," *Proceedings of IEEE Symposium on Security and Privacy (SP) 2014*, IEEE, 2014, pp.459-474.

Biryukov, Alex, Dmitry Khovratovich, and Ivan Pustogarov, "Deanonymisation of Clients in Bitcoin P2P Network," *Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS) 2014*, Association for Computing Machinery, 2014, pp.15-29.

———, and Ivan Pustogarov, "Bitocoin over Tor Isn't a Good Idea," *Proceedings of IEEE Symposium on Security and Privacy (SP) 2015*, IEEE, 2015, pp.122-134.

Dingledine, Roger, Nick Mathewson, and Paul Syverson, "Tor: The Second-Generation Onion Router," *Proceedings of Conference on USENIX Security Symposium (SSYM) 2004*, Vol.13, Advanced Computing Systems Association, 2004.

Financial Stability Board, "Crypto-Assets: Report to the G20 on Work by the FSB and Standard-Setting Bodies," Financial Stability Board, 2018.

Fujisaki, Eiichiro, and Kotaro Suzuki, "Traceable Ring Signature," *Proceedings of International Workshop on Public Key Cryptography (PKC) 2007*, Lecture Notes in Computer Science, 4450, Springer-Verlag, 2007, pp.181-200.

Genkin, Daniel, Dimitrios Papadopoulos, and Charalampos Papamanthou, "Privacy in Decentralized Cryptocurrencies," *Communications of the ACM*, 61 (6), Association for Computing Machinery, 2018, pp.78-88.

Goldfeder, Steven, Harry Kalodner, Dillon Reisman, and Arvind Narayanan, "When the

Cookies Meets the Blockchain: Privacy Risks of Web Payments via Cryptocurrencies," *Proceedings on Privacy Enhancing Technologies*, 2018 (4), De Gruyter, 2018, pp.179-199.

Heilman, Ethan, Leen Alshenibr, Foteini Baldimtsi, Alessandra Scafuro, and Sharon Goldberg, "TumbleBit: an Untrusted Bitcoin-Compatible Anonymous Payment Hub," *Reeports of Annual Network and Distributed System Security Symposium (NDSS) 2017*, Internet Society, 2017.

Henry, Ryan, Amir Herzberg, and Aniket Kate, "Blockchain Access Privacy: Challenges and Directions," *IEEE Security and Privacy*, 16 (4), IEEE, 2018, pp.38-45.

Kappos, George, Haaroon Yousaf, Mary Maller, and Sara Meiklejohn, "An Empirical Analysis of Anonymity in Zcash," *Proceedings of USENIX Security Symposium 2018*, Advanced Computing Systems Association, 2018, pp.463-477.

Khalilov, Merve Can Kus, and Albert Levi, "A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems," *IEEE Communications Survey and Tutorials*, 20 (3), IEEE, 2018, pp.2543-2585.

Koshy, Philip, Diana Koshy, and Patrick McDaniel, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," *Proceedings of International Conference on Financial Cryptography and Data Security (FC) 2014*, Lecture Notes in Computer Science, 8437, Springer-Verlag, 2014, pp.469-485.

Kumar, Amrit, Clément Fischer, Shruti Tople, and Prateek Saxena, "A Traceability Analysis of Monero's Blockchain," *Proceedings of European Symposium on Research in Computer Security (ESORICS) 2017*, Part II, Lecture Notes in Computer Science, 10493, Springer-Verlag, 2017, pp.153-173.

Manils, Pere, Chaabane Abdelberi, Stevens Le Blond, Mohamed Ali Kaafar, Claude Castelluccia, Arnaud Legout, and Walid Dabbous, "Compromising Tor Anonymity Exploiting P2P Information Leakage," *HAL*, inria-00471556, Institut National de Recherche en Informatique et en Automatique, 2010.

Meiklejohn, Sara, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage, "A Fistful of Bitcoins: Characterizing Payments among Men with no Names," *Proceedings of Conference on Internet Measurement Conference (IMC) 2013*, Association for Computing Machinery, 2013, pp.127-140.

Miers, Ian, Christina Garman, Matthew Green, and Aviel D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," *Proceedings of IEEE Symposium on Security and Privacy (SP) 2013*, IEEE, 2013, pp.397-411.

Moreno-Sanchez, Pedro, Muhammad Bilal Zafar, and Aniket Kate, "Listening to

Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network," *Proceedings on Privacy Enhancing Technologies*, 2016 (4), De Gruyter, 2016, pp.436-453.

Noether, Shen, Adam Mackenzie, and the Monero Research Lab, "Ring Confidential Transactions," *Ledger*, Vol.1, University of Pittsburgh, 2016, pp.1-18.

Reid, Fergal, and Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System," in Yaniv Altshuler *et al*., eds. *Security and Privacy in Social Networks*, Springer-Verlag, 2012, pp.197-223.

Ron, Dorit, and Adi Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," *Proceedings of International Conference on Financial Cryptography and Data Security (FC) 2013*, Lecture Notes in Computer Science, 7859, Springer-Verlag, 2013, pp.6-24.

Ruffing, Tim, Pedro Moreno-Sanchez, and Aniket Kate, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin," *Proceedings of European Symposium on Research in Computer Security (ESORICS) 2014*, Lecture Notes in Computer Science, 8713, Springer-Verlag, 2014, pp.345-364.

———, ———, and ———, "P2P Mixing and Unlinkable Bitcoin Transactions," *Reports of Annual Network and Distributed System Security Symposium (NDSS) 2017*, Internet Society, 2017.

van Saberhagen, Nicolas, "CryptoNote v 2.0," 2013.（URL: https://cryptonote.org/whitepaper.pdf、アクセス日：2018 年 9 月 18 日）

Tziakouris, Giannis, "Cryptocurrencies – A Forensic Challenge or Opportunity for Law Enforcement? An Interpol Perspective," *IEEE Security and Privacy*, 16 (4), IEEE, 2018, pp.92-94.

Ziegeldorf, Jan Henrik, Fred Grossmann, Martin Henze, Nicolas Inden, and Klaus Wehrle, "CoinParty: Secure Mult-Party Mixing of Bitcoins," *Proceedings of ACM Conference on Data and Application Security and Privacy (CODASPY) 2015*, Association for Computing Machinery, 2015, pp.75-86.