ブロックチェーンを用いた金融取引のプライバシー保護と追跡可能性に関する調査研究報告書（参考資料）

2019 年 3 月 20 日

金融庁
Financial Services Agency

[1] [2]

株式会社三菱総合研究所
社会 ICT イノベーション本部

[1] 本参考資料作成にあたっては、立命館大学・上原哲太郎教授、米ジョージタウン大学・松尾真一郎研究教授から有益な助言やコメントを得た。

[2] 本参考資料の内容は、金融庁の公式見解を示すものではない。また、本参考資料で記載している過去または現在の事実以外の内容については、本稿執筆時点で入手可能な情報に基づいた見通しであり、実際の動向等は種々の不確定要因によって変動する可能性がある。

目 次

図 表 目 次

用語の一覧

本報告書での表記	正式名称・意味など
AML/CFT	Anti-Money Laundering / Combating the Financing of Terrorism：マネー・ローンダリング及びテロ資金供与対策
FATF	Financial Action Task Force：金融活動作業部会
KYC	Know Your Customer：本人確認
DApps	Decentralized Applications：分散型アプリケーション ブロックチェーン上のスマートコントラクトを介してサービスを提供するアプリケーションの総称
DEX	Decentralized Exchange：分散型取引所
ファンジビリティ	Fungibility：等価交換性、代用可能性 過去の取引内容や移転経路によらず、同じ種類で同額であれば、財や資産が等価で交換可能であるという性質（代表的な例として通貨が挙げられ、1 万円は他の 1 万円と区別されることはなく、相互に代用可能といえる）
オフチェーン	Off-Chain：ブロックチェーン以外の手段（専用サーバやメール/SNS 等）
クリプトロンダリング	Crypto-Laundering：暗号資産を用いた資金洗浄
匿名セット	Anonymity set：匿名化したいものと同質な集合体（匿名とは匿名セットの中で識別ができないことであると考えられる）
再識別	Re-Identification、De-anonymization：匿名化された主体を、他のデータソースと組合せることなどにより、特定すること ※本資料では追跡と同義として扱う
カストディリスク	Custody Risk：暗号資産の秘密鍵の預託先（カストディアン）の破産、ハッキング被害、過失、不正使用、詐欺、不適切な管理などの結果として、預託中の暗号資産に損失が発生するリスク
FATF 未遵守国	FATF 勧告で推奨されているガイドラインに対して、本稿執筆時点で対策を徹底していない国 ※本資料でのみ用いる略称
ダークマーケット	Dark Market：Tor 秘匿サービスなどを用いたダークウェブ上のマーケットプレイス
プライバシー	Privacy：個人情報をみだりに公開されない権利や能力
セキュリティ	Security：犯罪等からの保護や保安
検閲耐性	Censorship Resistance：公権力による強権的な差し止め等に対抗する性質
匿名性	Anonymity：ある行動の主体が識別不能であること
仮名性	Pseudonymity：本来の名前とは異なる識別子を用いること
機密性	Confidentiality：情報へのアクセス制限が適切に確保されていること
非連結性	Unlinkability：イベントや主体同士が関連するか識別不能であること
追跡不能性	Untracerbility：ある情報から他を追跡不能であること
非検知性	Undetectability：あるイベントが発生したか検知不能であること
非観測性	Unobservability：匿名性と非検知性を含む性質

要 約

暗号資産は、電子的・分散的に処理されるという特性から、実世界上の本人情報と紐付かず、また実態把握が困難となる危険性が存在する。さらに、近年では、プライバシー保護等の考えに紐付けられつつ、その取引に関する各種匿名化技術の開発が積極的に進められている。近年の暗号資産経済圏の拡大に伴い、暗号資産関連犯罪のリスクが高まる一方で、こうした各種匿名化技術の急速な進展により、暗号資産を用いたマネーロンダリングやテロ資金供与の防止は困難な状況になりつつある。今後、暗号資産経済圏が拡大し、匿名化技術も進展していく中では、暗号資産を用いた資金洗浄等のリスクはさらに拡大・深刻化していくことが懸念される。これは、適切な利用者保護や取引の適正化などを阻害し、安全、公平で信頼できる暗号資産経済圏の実現を困難にさせるものであると考えられる。こうした問題意識を踏まえ、本調査研究は、政策立案の前提となる現状を正しく評価・認識することを目的として実施されたものである。

まず、暗号資産経済圏の状況を概観すると、未だ規模は小さいものの、個人利用を中心に世界的に拡大している。その用途も広がりを見せており、物品購入、法定通貨との取引や資本逃避以外に、暗号資産同士の取引やサービス利用手段としての利用も増加している。他方で、暗号資産を用いた犯罪リスクも増加している。ビットコインは匿名ネットワーク上での違法な電子商取引で既に広く利用されているが、近年はビットコイン以外の暗号資産の利用も拡大している。さらに、暗号資産に関連したサイバー犯罪も増加傾向にあり、暗号資産取引所を狙うサイバー犯罪や一般人を狙うクリプトジャックなど手法の多様化とあわせて、被害額の増大を招いている。

- こうした暗号資産建て犯罪収益は(1)規制遵守が徹底されていない暗号資産取引所、暗号資産決済代行業者や DEX、(2)ミキシングサービス、(3)ギャンブルサイトなどを通して、資金洗浄が行われる。資金洗浄に最も多く用いられる暗号資産取引所については、AML/CFT 規制の効果が報告されているものの、FATF 勧告の未遵守国に所在する取引所や KYC 未対応の取引所が相当数存在することなどから、暗号資産建て犯罪収益の資金洗浄経路を塞ぐことには困難が予想される。

次に、様々な匿名化技術や再識別技術の動向について、アプリケーションレイヤー、P2P レイヤー/インターネットレイヤー、実世界レイヤーの三層に分けて整理を行ったが、総じて匿名化技術の方が優勢であると考えられる。

- アプリケーションレイヤーのブロックチェーンにおいては、ミキシングやリング署名などの従前からある技術に加え、近年はライトニングネットワークやアトミック・クロスチェーン・スワップ、ゼロ知識証明、ミンブルウィンブルなどの技術が積極的に開発されている。こうした技術を組み入れた匿名通貨以外に、ビットコインにおいても匿名性はさらに強化される方向にある。ここでは、ファンジビリティの確保やプライバシーの保護といった観点以外に、スケーラビリティの確保やデータ量の削減等の観点からも、技術開発が行われている。

- アプリケーションレイヤーの DEX は、中央集権型取引所のカストディリスク解消を目指したものだが、未だ取引量は僅かであり、技術的にも安全性と効率性のバランスを模索している段階に留まる。今後は技術的に最適なバランスに加えて、DEX でしか実現できないユースケースの開発が進むと考えられる。

- P2P レイヤー/インターネットレイヤーの匿名通信においては、利用の裾野が拡大しつつあり、今後はビットコインやセキュアチャットツールなど他のアプリケーションと組合せた場合の全体としての匿名性の確保などが図られていくと考えられる。

- 実世界レイヤーでは、フリーWifi、プリペイド SIM、中古デバイスなどで、本人情報なしにインターネットに接続することが既に可能な状況になっている。

- こうした状況に対し、再識別技術は(1)各層毎の技術的な推測、(2)外部のデータを用いた特定という二通りのアプローチを組合せて行われるが、基本的には犯行者のミスをつく等の対応に留まる。KYC 情報や EC 購入履歴情報、ログ情報やレジストリ情報などの外部データは重要な役割を果たすが、一定期間後に廃棄される場合、精度が悪い場合やプライバシー保護の観点から収集されない場合などがあり、事後的に再識別を行うことには技術的な困難が考えられる。

さらに、現在および近い将来における技術の進展が暗号資産取引における AML/CFT 上の重大な懸念に繋がり得る点を実際に検証することを目的として実証実験を行った。具体的には、暗号資産建て犯罪収益を資金洗浄する場合を想定し(1)ライトニングネットワークを用いた資金洗浄、(2)ミキシングサービスを用いた資金洗浄、(3)リスクスコアリングツールによる評価という 3 シナリオを実施した。

- ライトニングネットワークを用いたクリプトロンダリングでは、四種類のライトニングネットワーク基盤を用いたが、いずれにおいても、ブロックチェーン上のデー

タやネットワーク上のパケットデータから移転経路を把握することは困難であることを確認した。今後の開発動向からは、さらに匿名性が強化されることが見込まれる。

- ミキシングサービスを用いたクリプトロンダリングでは、こうしたサービスは容易に利用可能である一方、ブロックチェーン上のデータから移転経路を把握することは困難であることが分かった。

- リスクスコアリングツールによる評価では、複数のツールを用いて実際のビットコインアドレスを評価したが、多くのツールにおいて、そのリスク評価は必ずしも適切ではないことを確認した。

本調査研究で得られた結果を踏まえると、巧妙に匿名化された場合、事後の犯行者特定は技術的には極めて困難と言わざるを得ず、その意味で極めて匿名性の高い暗号資産の資金洗浄は既に可能であると言える。また、その利用にあたっての技術的・心理的なハードルも低くなっている。各種匿名化技術の進展は急速であることから、今後はこうしたリスクが拡大・深刻化する懸念がある。他方で、自律分散性に代表される暗号資産経済圏固有の特性により、従来の規制アプローチは必ずしも有効でなく、規制の強化は意図せざる結果（脱法行為でなく適法行為のみを減少させるリスク濃縮など）を招く懸念があると考えられる。

そのため、適切な利用者保護や取引の適正化など、安全、公平で信頼できる暗号資産経済圏の実現へ向けて、当局は様々なステークホルダーと今後議論を深めていく必要があると考えられる。

本調査研究の結果を踏まえると、対策にあたっては現時点で以下の方針が考えられる。①まず、極めて進展が早い分野であることや法令等の実効性確保が技術的に難しい部分があることなどを踏まえると、対策にあたっては、予め法令等で明確に定める部分とそれ以外の部分に分けて、柔軟かつ機動的な対応を図ることが望ましい。②また、法令等で定める部分についてはその実効性を確保しつつ、境界を含むそれ以外の部分については、当局と様々なステークホルダーの相互理解を深め、社会的厚生の増大という共通の目標へ向けた協力関係となるよう取り組むことが望ましい。

1. 背景

近年、Fintech の代表的な技術の一つとされるブロックチェーンの利活用が急速に広がりつつある。ブロックチェーンの代表的なユースケースである暗号資産には、既に一般からの多大な関心と多額の資金が流入しており、金融システムの安定や利用者保護、マネーロンダリング・テロ資金供与防止（AML/CFT）等の観点からの適切な対応が必要とされている。国際的にも、金融活動作業部会（FATF）による仮想通貨交換業規制の見直しの表明[3]など、暗号資産を巡る AML/CFT の観点からの議論は今後益々重要となることが考えられる。

現在までに、暗号資産の売買・交換等のサービスを提供し、暗号資産と法定通貨ないし異なる暗号資産同士をつなぐ接点の役割を果たす、仮想通貨交換業者に対して、顧客の本人確認（KYC）、疑わしい取引の当局への届出等の制度対応が講じられている。

他方、暗号資産の世界では、通貨（すなわち、交換媒体）としての利便性向上を目指す中で、ファンジビリティ（等価交換性、Fungibility）[4]の確保が重要な課題と認識されており、利用者のプライバシー保護などの考えにも紐付けられつつ、積極的にファンジビリティの向上（すなわち匿名性や追跡困難性の向上）へ向けた取組が進められており、基盤レベルで匿名化技術が組み込まれた各種の匿名通貨も開発されている。また、ブロックチェーンの特性を活かし、特定の管理主体を必要とせずにサービスを提供する分散型アプリケーション（Dapps）の高度化・普及へ向けた取組も進められており、具体的なユースケースとして分散型取引所（DEX）なども開発されている。

このような中、暗号資産関連犯罪は近年増加傾向にあり、詐欺的な事案、ランサムウェア、クリプトジャック、仮想通貨交換業者を狙ったサイバー犯罪やブロックチェーン再編成を悪用した犯罪など、攻撃頻度や被害額の増加、手法の多様化が見られる。こうした犯罪者グループが各種匿名化技術を悪用し、不正に得た暗号資産の資金洗浄を図る危険性が懸念されている[5]。

今後は、暗号資産に関する様々な取引において、匿名化技術が分散型のサービ

---

3 Financial Action Task Force, "FATF Report to the G20 Finance Ministers and Central Bank Governors", http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf, 2019/1/7

4 財や資産が同じ種類の財や資産と等価で交換され得ることを指す。例えば、ファンジビリティのあるものとして通貨が挙げられる。一万円はそれぞれ区別されることがなく、同一の通貨であれば相互に代用可能といえる。

5 取引種別ごとに危険度等を記載した犯罪収益移転危険度調査書においては、マネーロンダリング等の危険度は、暗号資産は他業態よりも高いという旨が記載されている。国家公安委員会，警察庁ウェブサイト，"犯罪収益移転危険度調査書", https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/risk/risk301206.pdf, 2019/1/9

スとして広く普及していく可能性が考えられる。この場合、特定のサービス提供主体が存在しないため、制度対象先の特定や制度対応状況の監査等が困難となり、制度の実質的な有効性が低下することが懸念される。たとえサービスとして広く提供されずとも、複数の条件を満たせば既に実現可能な状況になりつつあり、これは暗号資産に対する制度の有効性に対して大きな脅威となりつつある。

上記を踏まえ、本調査研究では、ブロックチェーンを活用した金融取引におけるプライバシー保護技術と分散化技術を巡る開発状況や今後の見通しについて調査および実証実験を行い、理論的考察および実証実験を通じて把握された当局としての課題への対応策を、技術面・制度面の両面から考察した。本報告書はこれまでの検討結果をまとめたものである。

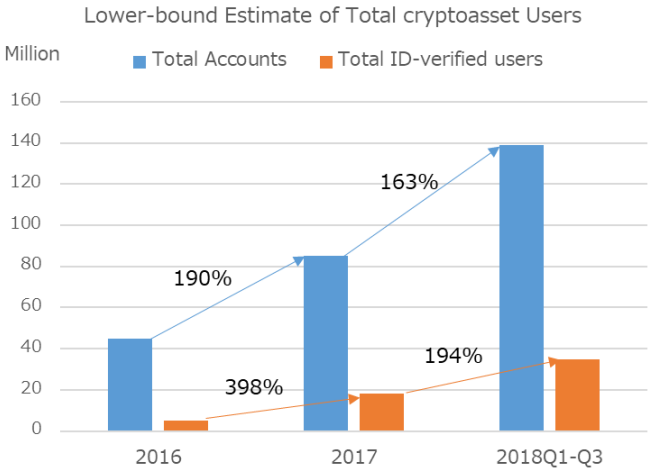
本報告書の構成は以下の通りである。第二章では暗号資産を取り巻く状況について概観した後、第三章では暗号資産取引を巡る匿名化技術等にかかる調査結果およびそこから導かれる AML/CFT 上の課題について理論的に考察する。第四章では理論的考察で挙げた課題について実証実験で実際に確認した結果を記載し、第五章ではこれらの課題に対する技術面・制度面での対応策を記載する。

2. 暗号資産を取り巻く状況

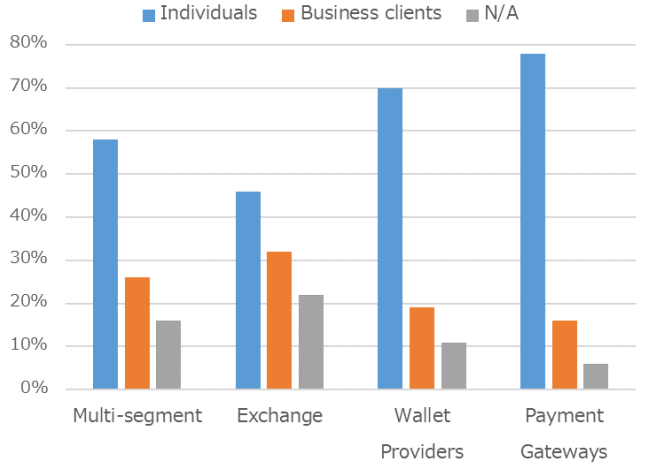
2.1 暗号資産経済圏の拡大

代表的な暗号資産であるビットコインは、当初は、キプロスでの金融危機における資本逃避手段や高インフレ国における資本逃避手段、さらにシルクロードなどに代表されるダークマーケットでの決済手段として一般の注目を集めた。現在では、47 ヶ国を調査した調査[6]によると、暗号資産利用者の口座数は全世界で凡そ 1.4 億弱に拡大し（図表 1）、利用者の多くが個人であると推定される（図表 2）。

図表 1 暗号資産利用者の口座数の推移 [6]



図表 2 事業種別毎の暗号資産利用者の内訳 [6]

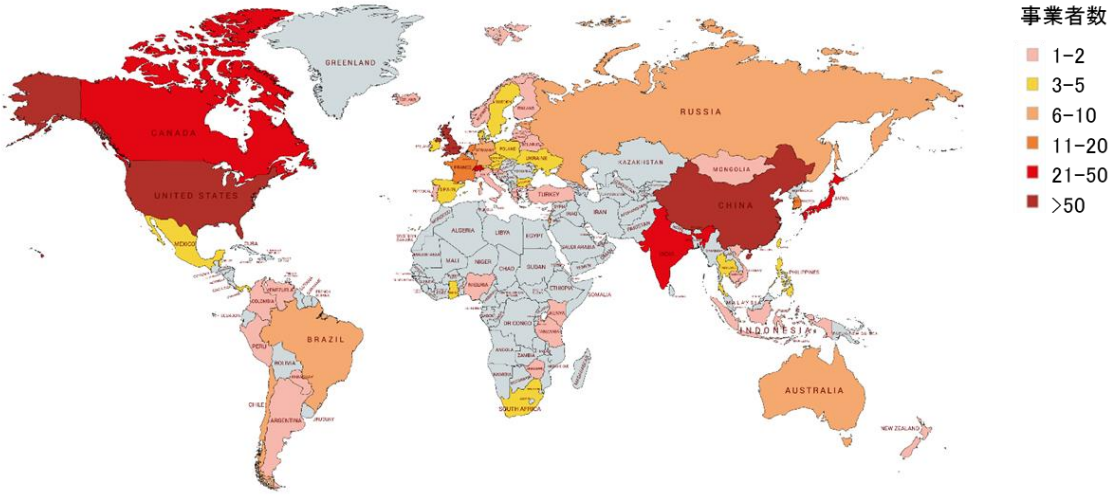


また、同調査によると、暗号資産関連サービスを提供する事業者も世界的な広がり

6 Rauchs, M., et al., University of Cambridge Judge Business School, “2nd Global Cryptoasset Benchmarking Study”, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf, 2019/1/9
図表 3 ・・・・・ p.28 Figure 10 より三菱総研作成
図表 17 ・・・・・ p.45 Figure 22

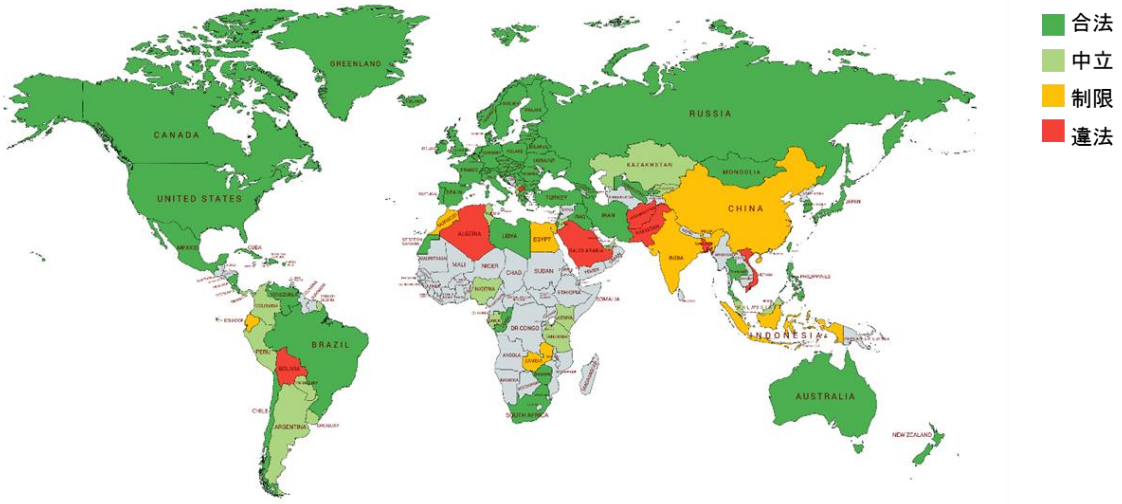
を見せており（図表 3）、日本・米国・欧州・カナダにおいては国民の凡そ 2-9%が仮想関連事業者を介すなどして暗号資産を保有していると推定している。

図表 3 暗号資産関連事業者数の世界的分布（調査対象企業数は 561 社）[6]



代表的な暗号資産であるビットコインの法的な扱いに関する暗号資産コミュニティの調査[7]では、約 4 割強の国々（110 ヶ国）において暗号資産は合法ないし中立とされているが、（図表 4）、それらの国々においても、ビットコインの法的な位置付けは、通貨（Currency）以外にも財（Property）やコモディティ（Commodity）など分かれており、国ごとに適用される規制内容も異なることが考えられる。

図表 4 ビットコインの法的な扱い[8]



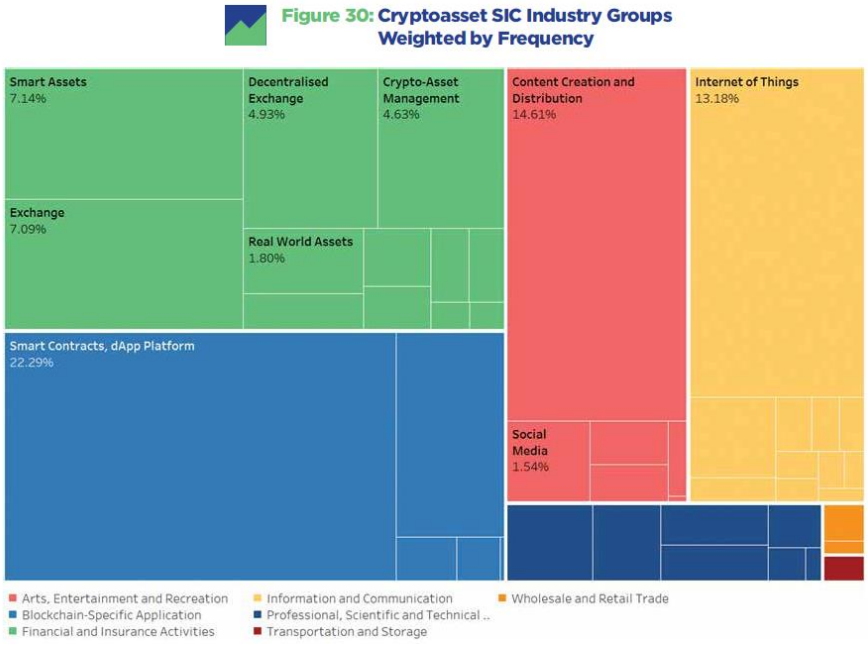
暗号資産の用途としては、現在までに、（1）交換手段（Exchange Token）、（2）投

7 Coin Dance, coin.dance, "Bitcoin Legality By Country", https://coin.dance/poli, 2019/1/11
8 Coin Dance, coin.dance, "Bitcoin Legality by Country", https://coin.dance/poli/legality, 2019/1/11 より三

資・資金調達手段（Security Token）、（3）サービス利用手段（Utility Token）の三種類に大別されると指摘されており[9]、同様の三分類は他の資料でも指摘される[10]。

- 交換手段としては、電子的であるという暗号資産の特性から情報商材との親和性が高く、初期ではアンダーグラウンドマーケットでの脆弱性情報、マルウェアや不正に取得したアカウント情報などが取引の中心であったが、近年では EC サイトでの物品やゲームアイテム等のデジタルコンテンツなども取引されるようになってきている。
- 投資・資金調達手段としては、投資目的での暗号資産の購入や ICO（Initial Coin Offering）など、特に 2017 年末にかけて大きな盛り上がりを見せた。
- サービス利用手段としての用途は近年増加しており[11]、例えば、SNS、ゲーム、コンテンツ配信、デバイス間送金など多様な用途が提案されている（図表 5）。

図表 5 暗号資産の用途の内訳（件数ベース）※色分は英国標準産業分類を参考 [11]



菱総研作成

9 The joint HM Treasury-Financial Conduct Authority-Bank of England Cryptoassets Taskforce, "Cryptoassets Taskforce: final report", https://www.gov.uk/government/publications/cryptoassets-taskforce, 2019/1/9

10 Swiss Financial Market Supervisory Authority, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en, 2019/1/11

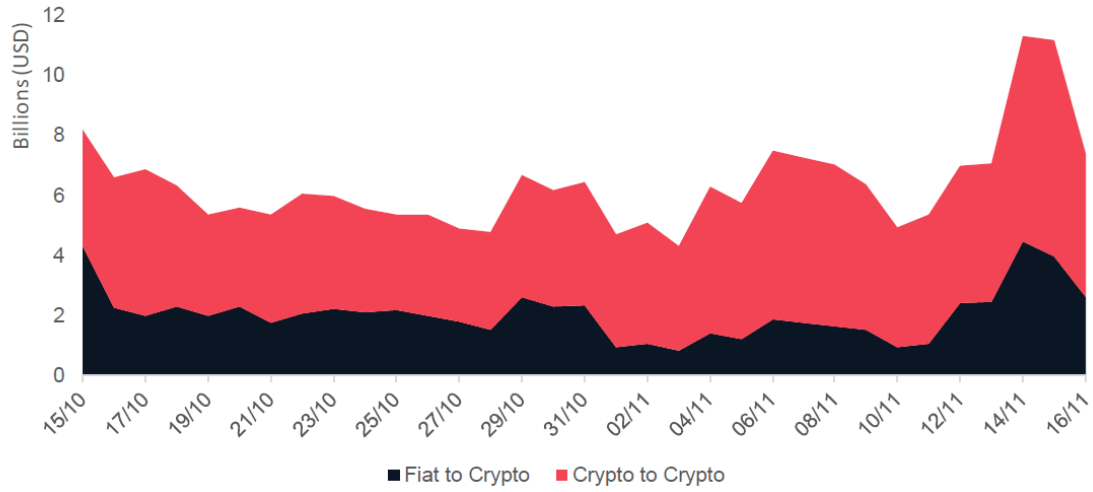
11 CryptCompare, Crypt Coin Comparison LTD, "Cryptoasset Taxonomy Report 2018", https://www.cryptocompare.com/media/34478555/cryptocompare-cryptoasset-taxonomy-report-2018.pdf p.58 Figure 30, 2019/1/11

ビットコイン以外にも様々な暗号資産が提案されており、ある調査では暗号資産の種類として 1,900 種類以上[12]が挙げられ、また、他の調査ではイーサリアム上でやり取りされる暗号資産として約 16 万種類以上[13]が挙げられている。

こうした暗号資産の種類の増加や暗号資産分野への資金流入の増加に伴い、暗号資産同士の取引も増加している。70 以上の仮想通貨取引所のデータを用いた調査[14]では、現物取引において、暗号資産同士の取引額は、暗号資産と法定通貨の取引を含む全体の取引額の約 2/3 を占めると報告されている（図表 6）[15]。同調査において、暗号資産のみ扱う取引所が全体の 4 割強を占めるということと併せて、暗号資産同士の取引が活発に行われていることが伺える。

図表 6 現物取引における暗号資産取引額の内訳（2018 年 10 月～11 月）[14]

Figure 6 – Historical Crypto to Crypto versus Fiat to Crypto Exchange Spot Volumes



今後の動向としては、ブロックチェーンは、様々なアプリケーションが利用できる共有データや共有トークンを提供するプロトコル層自体の経済的価値（例．時価総額）がアプリケーション層よりも高い仕組みであり、従来のインターネットのビジネスモデルを変える可能性があると期待されている（図表 7）[16]。これは個々のアプリケーショ

12 正確には本稿執筆時点で 1985 個。CoinLore, "Cryptocurrency List", https://www.coinlore.com/all_coins, 2019/1/14

13 正確には本稿執筆時点で 16 万 2377 個。Etherscan, "Token Tracker - Ethereum Token Market Capitalization", https://etherscan.io/tokens, 2019/1/14

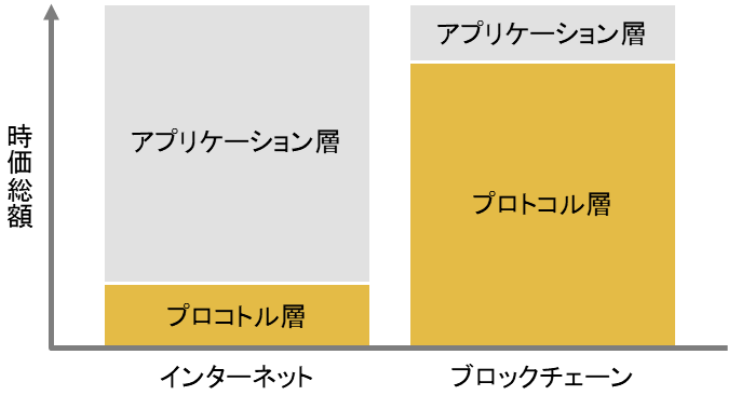
14 CryptoCompare, Crypt Coin Comparison LTD, "CCCAGG Exchange Review, November 2018", https://www.cryptocompare.com/media/35308846/cryptocompare_exchange_review_2018_11.pdf p.11 Figure 6, 2019/1/14

15 ただし、他の調査[6]では、暗号資産同士の取引額は全体の約 1/3 に留まると報告しており、調査により結果が異なるという点で、正確な統計の整備が待たれる。

16 Monegro, J., UNION SQUARE VENTURES, "Fat Protocols", http://www.usv.com/blog/fat-protocols, 2019/1/11

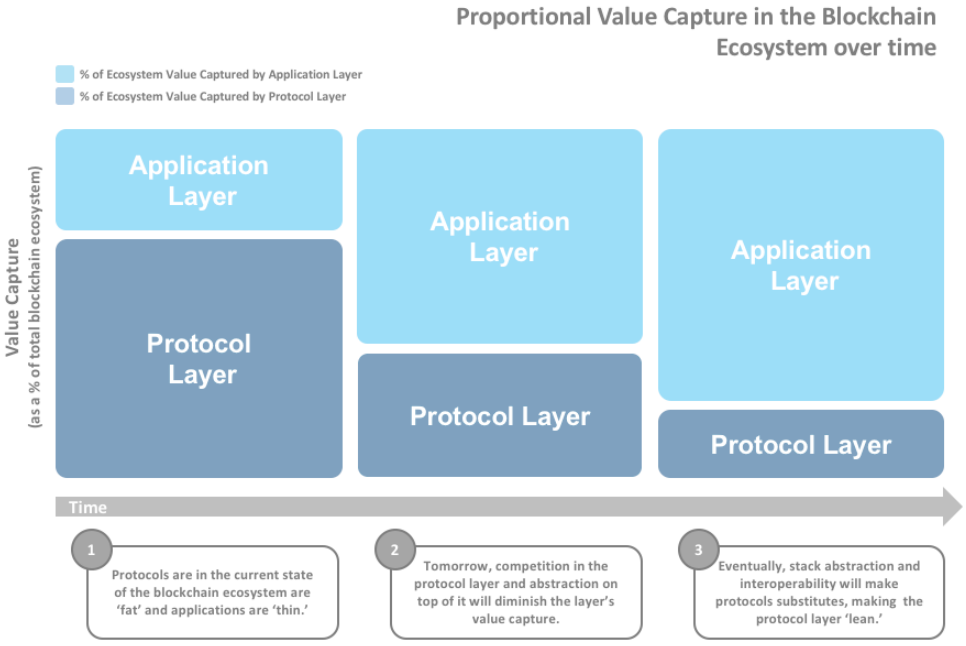
ンの成功が、そのアプリケーションを利用するのに必要なトークンの需要や投機を呼び、プロトコル層の時価総額を上昇させ、プロトコル層の方が早く成長するという想定に基づく。

図表 7 インターネットとブロックチェーンの比較[17]



図表 7 は著名な指摘だが、この指摘の妥当性については現在までに見解が分かれており、ブロックチェーンエコシステムの成熟とともに、アプリケーションの価値が高まっていくだろうとの指摘もなされている（図表 8）。

図表 8 ブロックチェーンの成熟に伴う構造変化のイメージ[18]

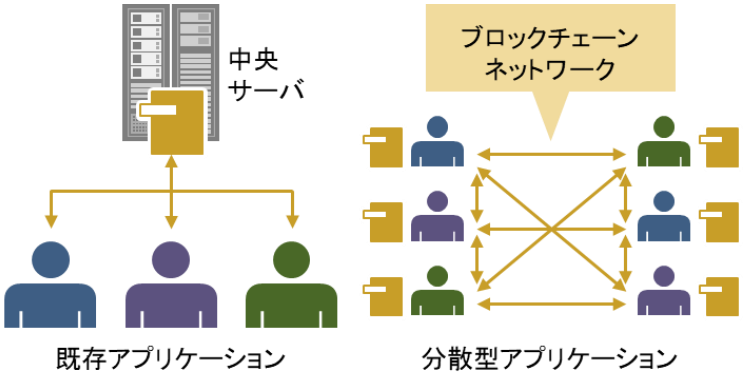


17 Monegro, J., UNION SQUARE VENTURES, "Fat Protocols", http://www.usv.com/blog/fat-protocols, 2019/1/11 より三菱総研作成

18 Jonhnson Nakano, Medium, "https://cdn-images-1.medium.com/max/1500/1*DkyoT1dHsURGTUeZfm-a_g.png", 2019/3/20

また、ブロックチェーン上のスマートコントラクトを用いて構築されるアプリケーション、分散型アプリケーション（DApps）は、①特定の管理主体を必要としないこと、②（ブロックチェーンが稼働する限り）常時利用可能であること、③プログラムロジックが公開されて透明性が高いこと（一部の関係者が秘密裏に変更することはできず、変更した場合は変更の履歴が公開されること）、④支払いと組合せて「プログラム可能な支払い」を実現できることなどの特徴があり、その可能性には大きな期待が寄せられている（図表 9）。

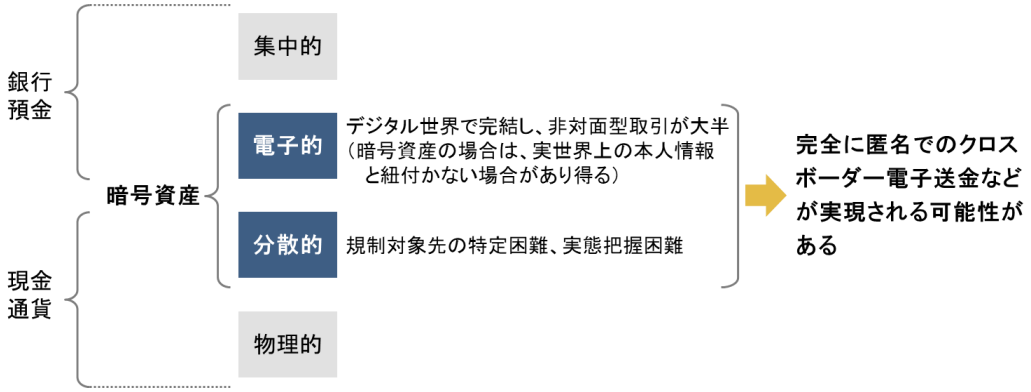
図表 9 既存アプリケーションと分散型アプリケーションの比較



2.2 暗号資産関連犯罪の拡大

暗号資産は、物理的・分散的に処理される現金通貨の特性（常時支払い可能であり、当局や既存金融システムの影響を受けにくく、匿名性が高く、口座開設不要で誰でも利用可能等）と、電子的・集中的に処理される銀行預金（インターネットを介して処理され、サイバーセキュリティ対策が施されており、取引履歴が常時記録される等）の特性の両者をそれぞれ部分的に兼ね備えた、電子的・分散的に処理されるという独自の特性があると指摘される（図表 10）[19]。したがって、暗号資産は、その特性から、実世界上の本人情報と紐付かず、また実態把握が困難となる危険性が存在すると考えられる。

図表 10 法定通貨と比較した場合の暗号資産の通貨としての特性



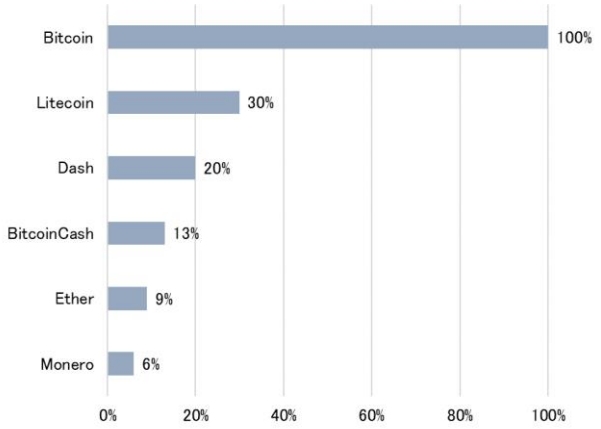
暗号資産のうち、特にビットコインはダークマーケットで行われる違法な電子商取引の決済手段として広く利用されており、近年ではビットコイン以外の暗号資産の利用も拡大している。ダークウェブ上のマーケットプレイスや掲示板など 150 サイトを調査した民間調査[20]によると、ビットコインは全てのサイトで利用可能であり、2 番手はライトコインであった（図表 11）。なお、英語圏ではモネロの利用が多い一方、東欧ではダッシュの利用が多いなど、地理的な偏りも見られた。

---

19 BitMEX Research, BitMEX, "Would Bitcoin's mass adoption fundamentally transform the financial system?", https://blog.bitmex.com/thetimes/, 2019/1/9
分散型や集中型の分類は以下の資料でも指摘されている。柳川範之，日本銀行ウェブサイト，東京大学金融教育研究センター・日本銀行決済機構局共催コンファレンス「フィンテックと貨幣の将来像」"通貨・仮想通貨の未来像", https://www.boj.or.jp/announcements/release_2016/data/rel161201a1.pdf, 2019/1/9

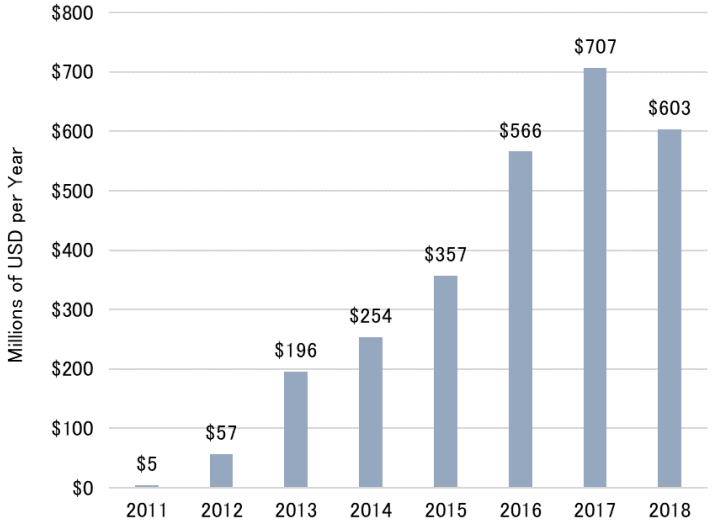
20 Barysevich, A., et al, Record Future, "Litecoin Emerges as the Next Dominant Dark Web Currency", https://www.recordedfuture.com/dark-web-currency/, 2019/2/23
図表 11 は本資料に基づき三菱総研作成

図表 11 ダークマーケットでの暗号資産の取扱状況（2018 年）[20]



また、ダークマーケットへの暗号資産の流入量はビットコインに絞った場合 2017 年に 7 億ドルを超えたと見られている（図表 12）。ここで、2017 年中頃からは、ビットコインの認知が広まるに連れ、手数料の増大や処理遅延の拡大等が顕著になったため、他の暗号資産の利用が増えたと推測されている。

図表 12 ダークマーケットへのビットコインの流入量（2011～2018 年）[21]



暗号資産の利用が拡大していくにつれ、暗号資産に関連した犯罪事例も増加傾向にあり、仮想通貨交換業者を狙ったサイバー犯罪、ランサムウェア、フィッシング詐欺、クリプトジャック、ブロックチェーン再編成を悪用した犯罪など、攻撃頻度や被害額の増加、手法の多様化が見られる。我が国では、特に暗号資産取引所 MtGox、Coincheck や Zaif を巡る事件をきっかけとして、暗号資産に関連したサイバー犯罪

21 Chainalysis Team, Chainalysis, "Crypto Crime Report - Decoding increasingly sophisticated hacks, darknet markets, and scams January 2019", https://blog.chainalysis.com/2019-cryptocrime-review, 2019/2/23 より三菱総研作成

へ社会的な関心が高まった（図表 13）。

図表 13 暗号資産を巡る不正事件の例[22]

発生時期	取引所／事件の名称	被害額
2014 年 2 月	MtGox（日）	約 470 億円
2016 年 6 月	The DAO	約 65 億円
2016 年 8 月	Bitfinex（香）	約 65 億円
2017 年 6 月	Wanacry	約 1600 万円（身代金額）
2017 年 11 月	Thether（米）	約 50 億円
2017 年 12 月	NiceHash（スロベニア）	約 68 億円
2018 年 1 月	Coincheck（日）	約 580 億円
2018 年 2 月	BitGrail（伊）	約 181 億円
2018 年 6 月	Coinrail（韓）	約 40 億円
2018 年 6 月	Bithumb（韓）	約 33 億円
2018 年 7 月	Bancor（瑞西）	約 26 億円
2018 年 9 月	Zaif（日）	約 70 億円

例えば、民間の調査[23]では、暗号資産の高騰した 2017 年末から、ランサムウェアからクリプトジャックへ攻撃手法が移行したことが指摘されている（図表 14）。ランサムウェアの場合、必ずしも身代金が得られるとは限らず、また、一般にはビットコインなどの暗号資産で身代金を受け取るが、受け取りに用いるアドレスが広く周知されることで犯行者の身元が露呈する危険性も考えられる。他方で、感染先のマシンリソースを用いて暗号資産の採掘を行うクリプトジャックでは犯行社の身元が露呈する問題点がないことなどにより、クリプトジャックが使われるようになったと考えられる。

民間の調査[24]では、仮想通貨取引所等の被害額は、2018 年の第三四半期までに 2017 年の約 3.5 倍にあたる 9.27 億ドルに増加し（図表 15）、2018 年内に 10 億ドルを超えると推定されている。

---

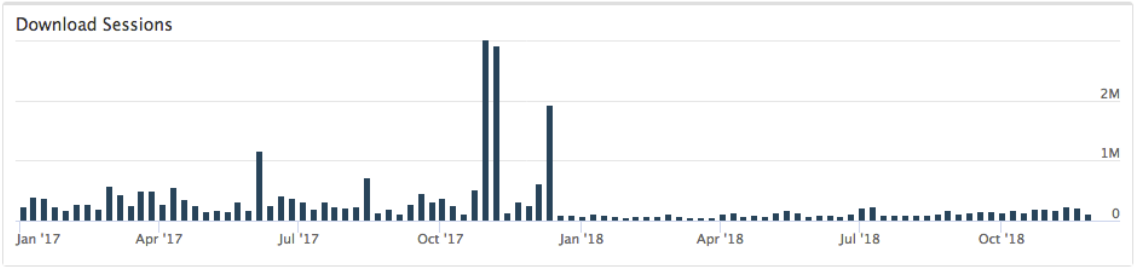
22 以下の資料を参考に三菱総研にて社会的影響の大きい事例を追記。楠 正憲, 情報処理学会 特別解説, "Zaif からの暗号資産流出 ～仮想通貨交換業者はアントローラブル？～", https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=191952&item_no=1&page_id=13&block_id=8, 2019/1/7

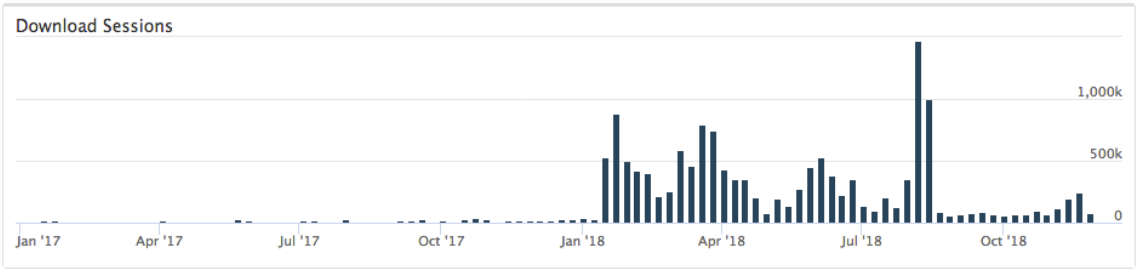
23 林 薫, Palo Alto Networks, Inc., "2018 年のサイバー脅威の振り返りと 2019 年の予測", https://www.paloaltonetworks.jp/company/in-the-news/2018/2018-playback-2019-prediction, 2019/1/30

24 CipherTrace, CipherTrace, Inc., "Cryptocurrency Anti-Money Laundering Report - Q3 2018", https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf, 2019/1/11

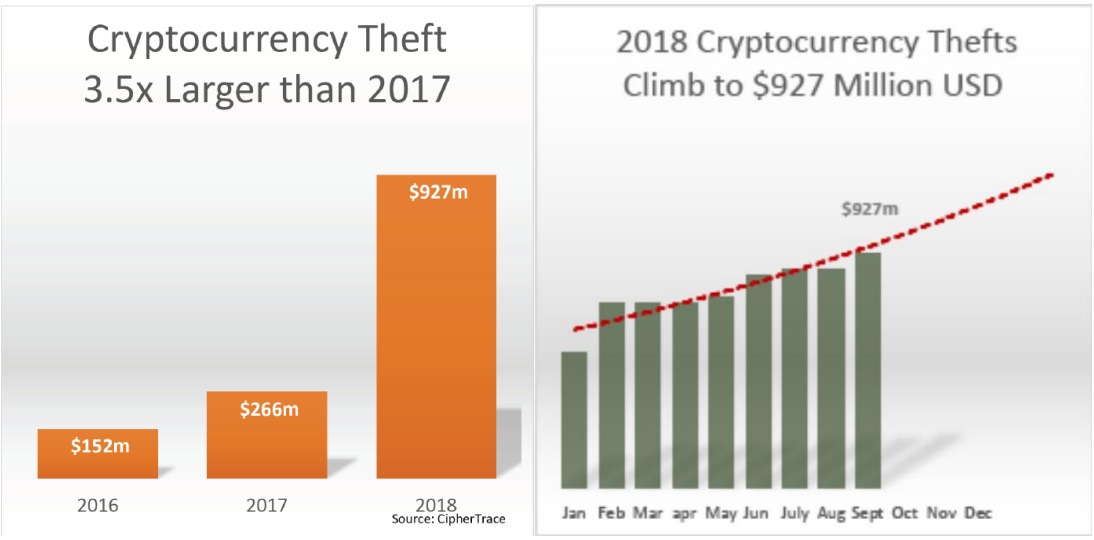
図表 15（左）・・・・・ p.10 Fig 8
図表 15（右）・・・・・ p.9 Fig 7
図表 20（左）・・・・・ p.5 Fig 3
図表 20（右）・・・・・ p.3 Fig 2

図表 14 ランサムウェア検出数（上図）とクリプトジャックマルウェア検出数（下図）の推移[25]





図表 15 仮想通貨取引所等の被害額の状況（左：年別、右：2018 年の月別）[24]

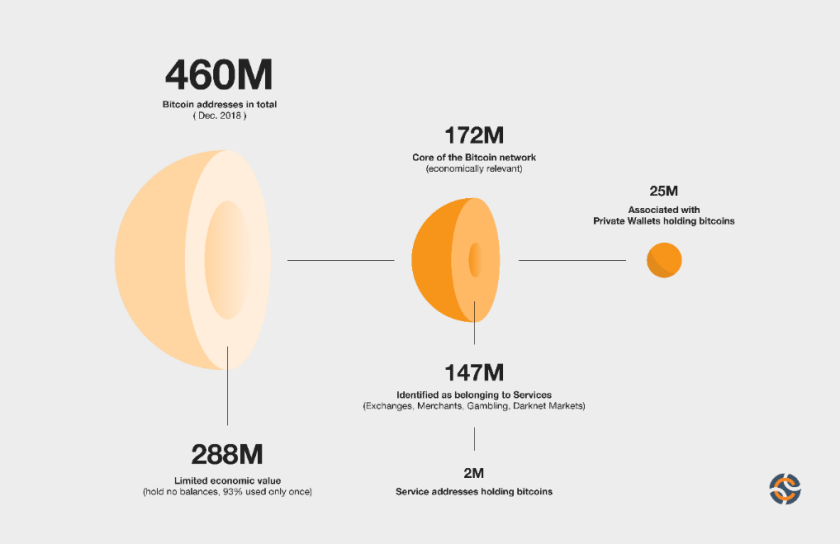


暗号資産経済圏に関わるプレーヤーを考えると、個人以外に、仮想通貨取引所、カストディ事業者や決済代行業者などのサービス事業者も多く関与している。例えば、2018 年 12 月までのビットコインのアドレス（約 4.6 億アドレス）を対象にした民間の調査[26]では、残高のあるアドレス（約 1.72 億アドレス）のうち 86%（約 1.47 億アドレス）は何らかのサービス事業者が保有するアドレスであり（図表 16）、このことから

25 （上図）林 薫, Palo Alto Networks, Inc., "2018 年のサイバー脅威の振り返りと 2019 年の予測", https://www.paloaltonetworks.jp/content/dam/pan/ja_JP/Images/blog/2018/126525/picture-02.png, 2019/1/30
（下図）林 薫, Palo Alto Networks, Inc., "2018 年のサイバー脅威の振り返りと 2019 年の予測", https://www.paloaltonetworks.jp/content/dam/pan/ja_JP/Images/blog/2018/126525/picture-03.png, 2019/1/30
26 ChainAnalysis Team, Chainalysis, Inc., "Mapping the Universe of Bitcoin's 460 Million Addresses", https://blog.chainalysis.com/reports/bitcoin-addresses, 2019/1/14

も、暗号資産の取引にはサービス事業者が深く関わっていることが推測される。

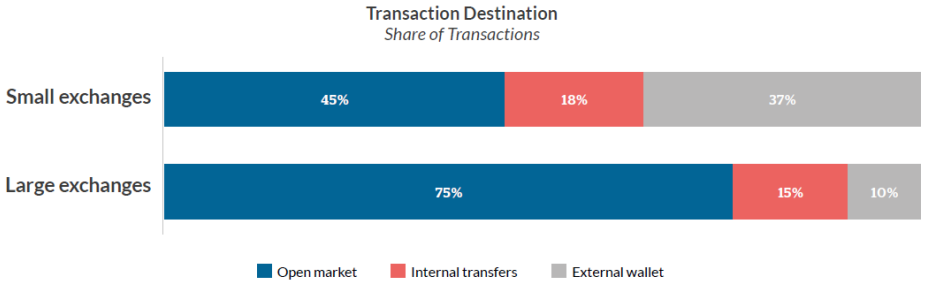
図表 16 ビットコインにおけるアドレス所有者の内訳[27]



特に仮想通貨取引所は、一般投資家から見て、暗号資産取引の窓口となる存在であり、多くの顧客の秘密鍵の管理も行っている。近年では、仮想通貨取引所内で完結する取引も増えており、ある調査では大半のトランザクション（大手取引所では 90%、小規模取引所では 63%）は取引所内で処理されると報告されている（図表 17）。仮想通貨取引所等を中心とするエコシステムが拡大する場合、エコシステムの核となる取引所等は今後もハッキングなどの犯罪の対象になりやすいことが考えられる。

図表 17 仮想通貨取引所からの送金先の内訳（件数ベース）[6]

Figure 22: Small exchanges have a larger relative share of outgoing transactions than large exchanges



27 ChainAnalysis Team, Chainalysis, Inc., "Mapping the Universe of Bitcoin's 460 Million Addresses", https://uploads-ssl.webflow.com/5a95e929b010650001bae4c6/5c1a7d564195de5b2388a17c_400m%20addresses%20full%20infographic.png, 2019/1/14

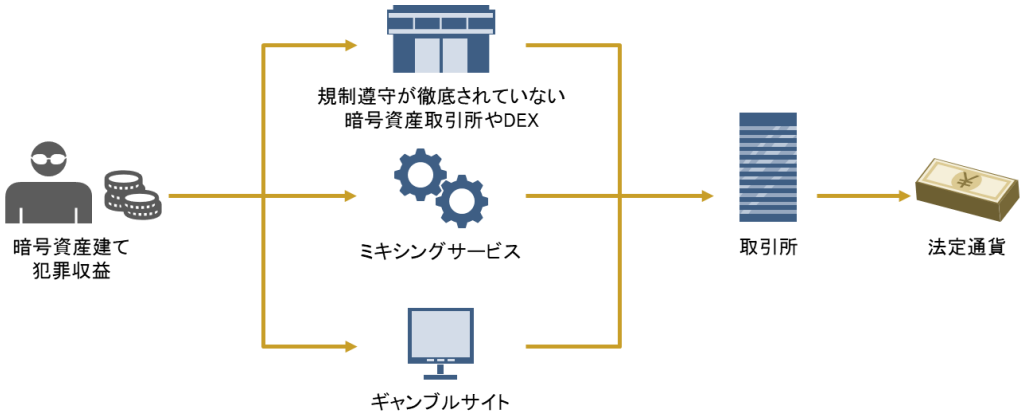
2.3 暗号資産を用いた資金洗浄

AML/CFT の観点からみると、暗号資産関連犯罪等で不正に取得された暗号資産は、その後何らかの形で資金洗浄が行われると考えられる。資金洗浄に用いられる代表的なサービス事業者として、(1)規制遵守が徹底されていない仮想通貨取引所や仮想通貨決済代行業者、(2)ミキシングサービス、(3)オンラインギャンブルサイト等が挙げられる[24]。こうした資金洗浄が行われて犯罪の痕跡が除去された上で、当該暗号資産は一般の仮想通貨取引所等へ移動すると考えられる(図表 18)。

ここで、仮想通貨取引所、販売業者や決済代行業者は、以下の特徴などから資金洗浄に用いられやすいと考えられる。

- 法定通貨や異なる暗号資産に変換できること
- 取引所に入った後の資金の移動経路は第三者からは分からないこと

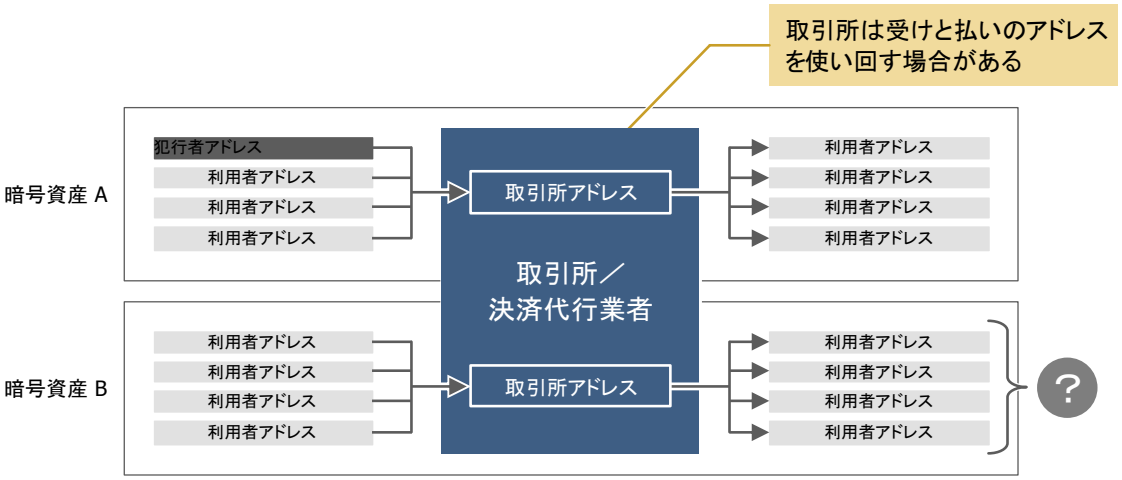
図表 18 暗号資産の資金洗浄のイメージ



仮想通貨取引所では、顧客からの入金を受け付けるアドレスや顧客へ暗号資産を引き出すアドレスを顧客毎に分けずに使い回す場合がある。そのような場合には、ある暗号資産 A で入金したユーザが、どの暗号資産のどのアドレスで引き出したか、取引所外の第三者が把握することは極めて困難である(図表 19)。

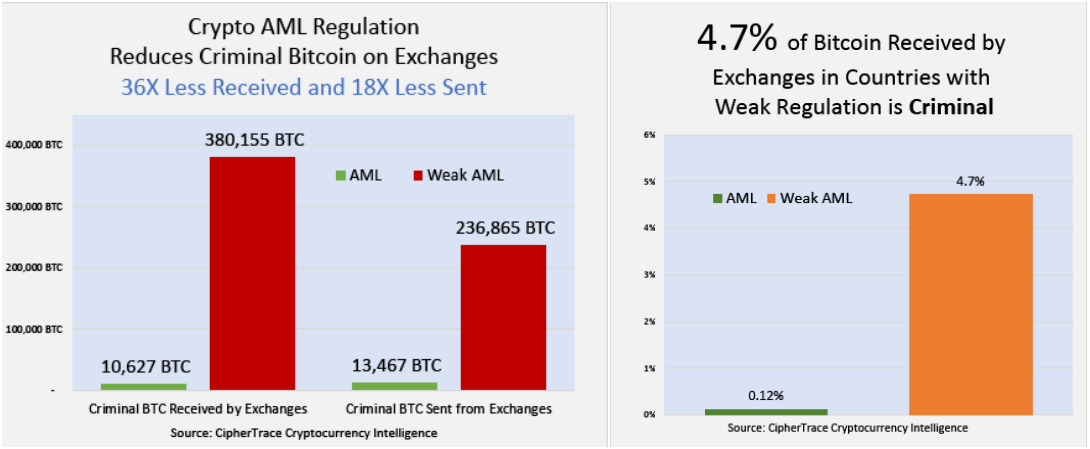
実際、主要な 20 取引所を対象にした調査[24]では、犯罪やダークマーケット等に関係するビットコインのうち、主要取引所を経由して資金洗浄が図られた額は、2009 年 1 月から 2018 年 9 月までに約 25 億ドルに上ると推定されている。

図表 19 取引所が資金洗浄に用いられるイメージ



資金洗浄には、特に AML/CFT の対応が徹底されていない仮想通貨取引所が利用されると考えられている。民間の調査[24]では、AML 規制が徹底されていない国の取引所は、規制が徹底されている国の取引所に比べて、暗号資産関連犯罪に関わるビットコインを 36 倍多く受け取り、そうした先へ 18 倍多く送金すると推定されている（図表 20）[28]。特に最近は、規制対応の弱い国の取引所へ、不正な取引が集中する傾向が指摘されている（図表 21）。

図表 20 AML 規制の強弱と仮想通貨取引所を経由する不正な取引額の比較 [24]



これらの事実は、仮想通貨取引所への AML/CFT の規制の効果が確かにあるということも意味すると考えられる。

28 当該調査では、AML 規制が弱い国として、アメリカ合衆国国務省国際麻薬・法執行局の公表する"Money Laundering and Financial Crimes Country Database"に基づき、KYC や疑わしい取引の届け出などを義務付けていない 79 ヶ国を定義した。

図表 21 AML 規制の強弱と仮想通貨取引所を経由する不正な取引額の 2018 年における推移（上段：AML 規制の強い国の取引所、下段：AML 規制の弱い国の取引所）[24]

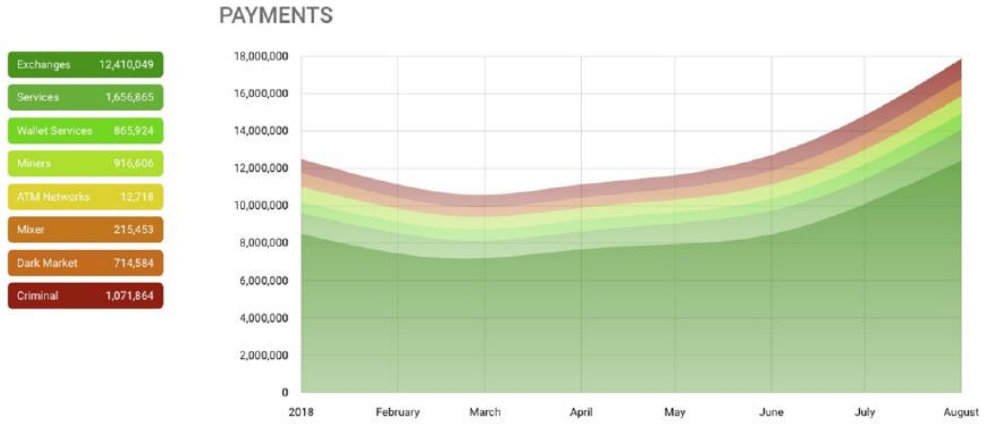


Fig 5. Transaction Analysis of a Top 10 Global Cryptocurrency Exchange with Strong AML

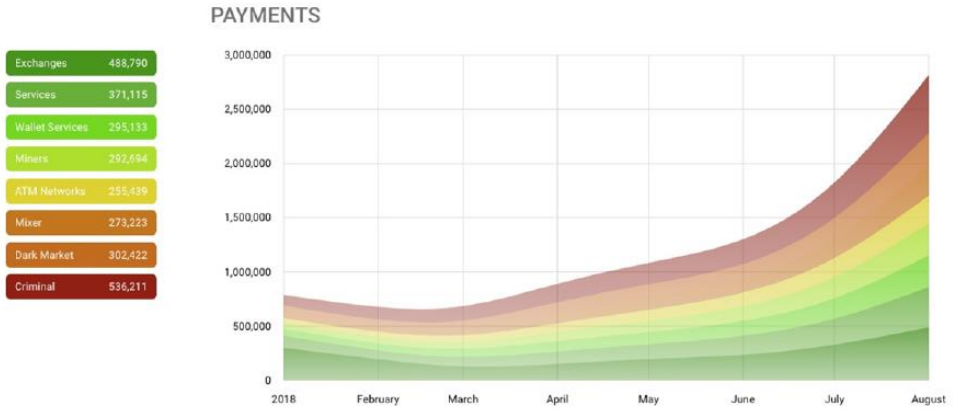


Fig 6. Transaction Analysis of a Top 10 Global Cryptocurrency Exchange with Weak/No AML

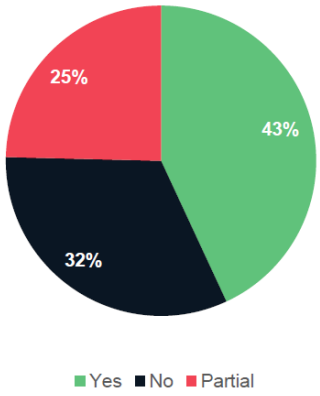
しかしながら、2018 年 4 月～5 月にかけて、欧州・米国等の 25 の仮想通貨取引所・ウォレット事業者を対象にした民間の調査[29]では、全体の 7 割弱において、KYC が徹底されていなかったと報告しており、他の調査 [14] では、全体の約 1/3 の取引所は KYC を行っていないと報告されている（図表 22）。

また、FATF 未加盟国に本拠地を置く仮想通貨取引所も多く（図表 23）、こうした取引所へ規制遵守を徹底させることには困難も予想される。

29 Mitek, "The Cryptocurrency Identity Crisis: An Industry Scorecard for Digital ID Verification for KYC and AML", https://www.miteksystems.com/resources/cryptocurrency-paid-strategies, 2019/1/7

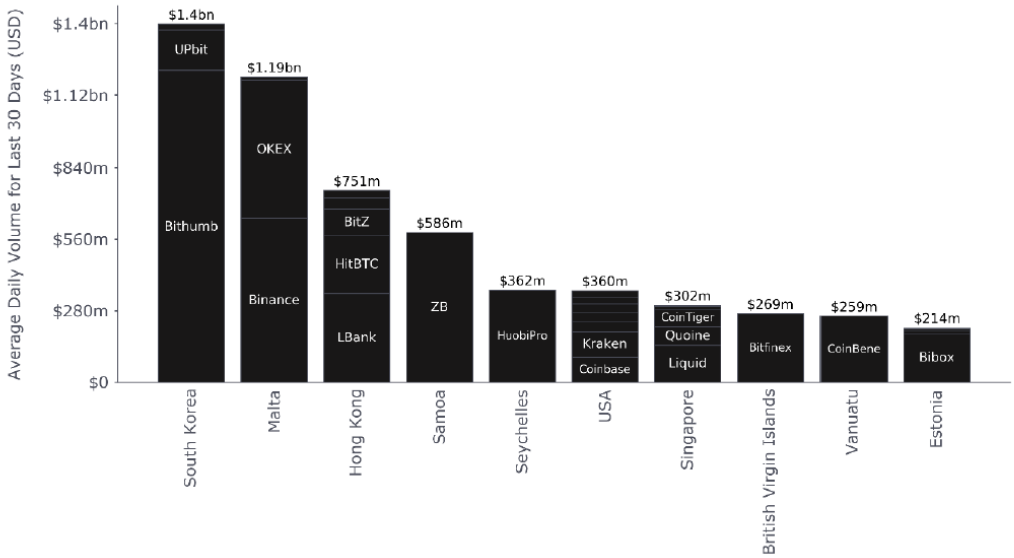
図表 22 仮想通貨取引所（130 取引所）に対する KYC 対応状況の調査結果 [14]

Figure 28 – KYC Requirements Among the Top 130 Exchanges



図表 23 主要な仮想通貨取引所の所在国の内訳（取引高は 2018 年 10 月 15 日～2018 年 11 月 15 日までが対象）[14]

Figure 14 – Top 10 Exchange Legal Jurisdictions - Constituent Exchanges by Impact on Volume



また、既存の取引所以外に、DEX を介して暗号資産の交換が行われる可能性が考えられる。この場合、ブロックチェーン上に既にデプロイされたスマートコントラクトが一連の取引処理を行うため、利用者にとっては KYC を経ずに取引が可能であることが懸念される。反対に、当局にとっては規制の対象先が事後的に変更や修正できないプログラム（スマートコントラクト）になる可能性があり、エンフォースメントの有効性を確保できない点などが懸念される。

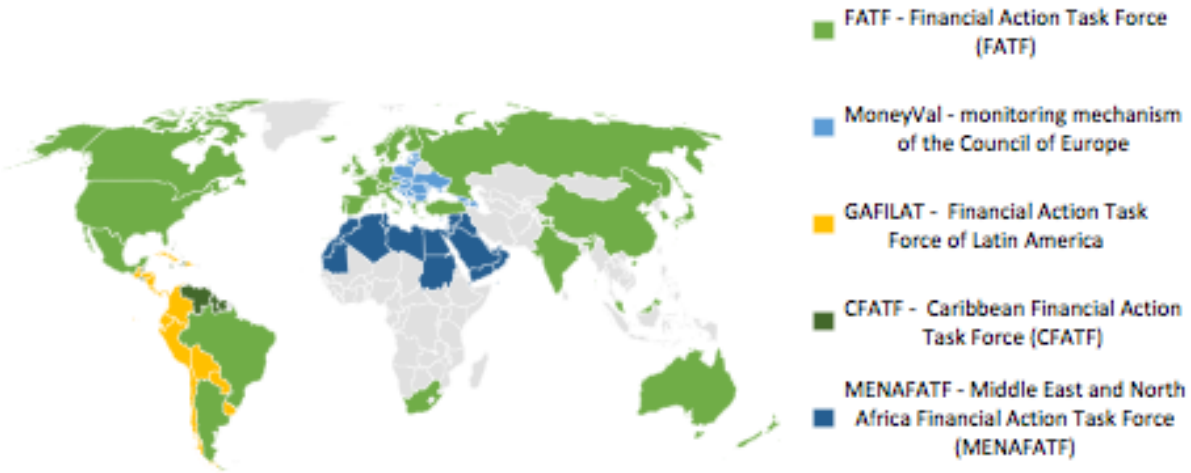
他に、暗号資産経済圏が拡大すること（2.1 節）により、不正に取得された暗号資産が法定通貨に交換されずに暗号資産のまま保持されていくことも考えられる。この場合、仮想通貨取引所等を経由しないため、KYC などの規制対応がなされるポイント

が無いことが懸念される。

さらに、図表 6 の通り、暗号資産同士の取引が活発化するにつれ、DEX などを介して不正に取得された暗号資産が匿名性の高い暗号資産（所謂、匿名通貨）に交換される可能性が考えられる。匿名通貨においては、ビットコインの場合よりも追跡がさらに困難となることが懸念される。これは、ライトニングネットワークなどのブロックチェーン外の取引技術（一般にレイヤー2 技術と呼ばれる）が普及した場合も同様であり、例えばライトニングネットワークでは中継ノードを介した送金が行われることで、通常のビットコインの送金の場合よりも追跡がさらに困難になることが懸念される。

本節では、暗号資産経済圏における資金の移動と、特に仮想通貨取引所の役割について焦点をあてたが、AML/CFT 上は、国毎に取引所の対応が分かれているのは望ましくなく、全体を底上げしていく必要がある。また、取引所以外のプレーヤーについても対策を行う必要がある。そして、グローバルに行われるという暗号資産の性格上、国際的に歩調を揃えて対策を進めていく必要がある。その意味で、暗号資産の AML/CFT は、今後、FATF 等の多国間の枠組みで積極的に対策が図られていくことが望ましいと考えられる（図表 24）。

図表 24 AML/CFT に関する政府間機関 [24]



3. 暗号資産取引を巡る匿名化技術等にかかる調査結果

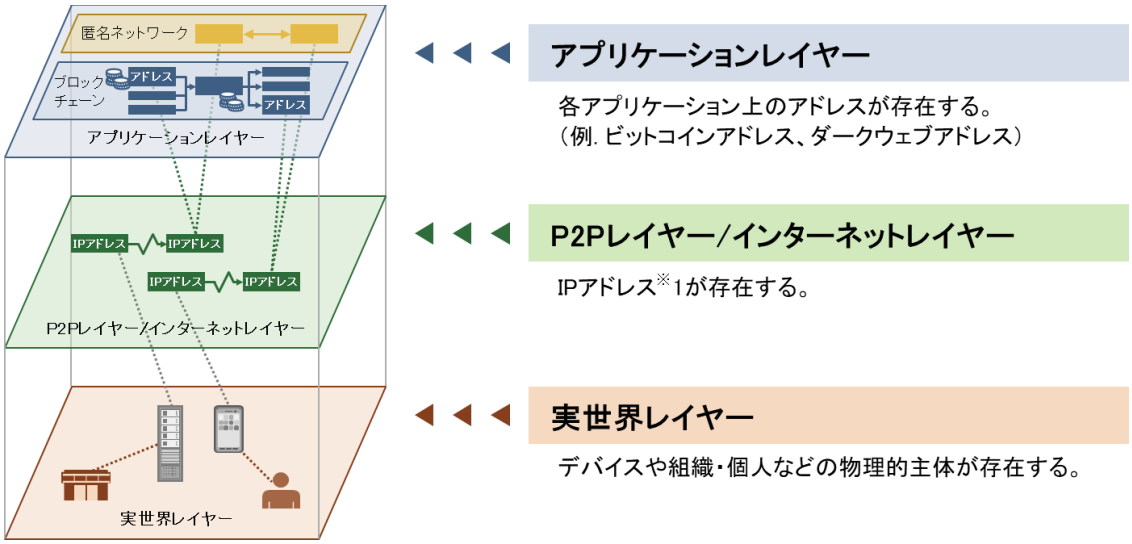
本章では、「プライバシー保護技術及び分散化技術を巡る開発状況の調査」におけるブロックチェーン要素技術の開発状況について記載する。

3.1 調査結果の全体像

暗号資産取引を巡る様々な匿名化技術や再識別技術を調査するにあたり、本調査研究では、アプリケーションレイヤー、P2P レイヤー/インターネットレイヤー、実世界レイヤーの三種類に大別して整理した（図表 25）[30]。

- アプリケーションレイヤーとは、例えば、ビットコインアドレス、ダークウェブサイトのアドレスやチャットツールの ID など、各アプリケーションにおけるユーザの識別子（アドレス）が存在するレイヤーである。例えば、ビットコインネットワークや匿名ネットワークなどがアプリケーションレイヤーに含まれる。
- P2P レイヤー/インターネットレイヤーとは、IP アドレスが存在するレイヤーである。このレイヤーには、エンドツーエンドの通信を実現する仕組みが含まれる。
- 実世界レイヤーとは、デバイスや組織・個人などの物理的主体が存在するレイヤーである。

図表 25 追跡可能性を巡る全体像を整理するためのレイヤー図

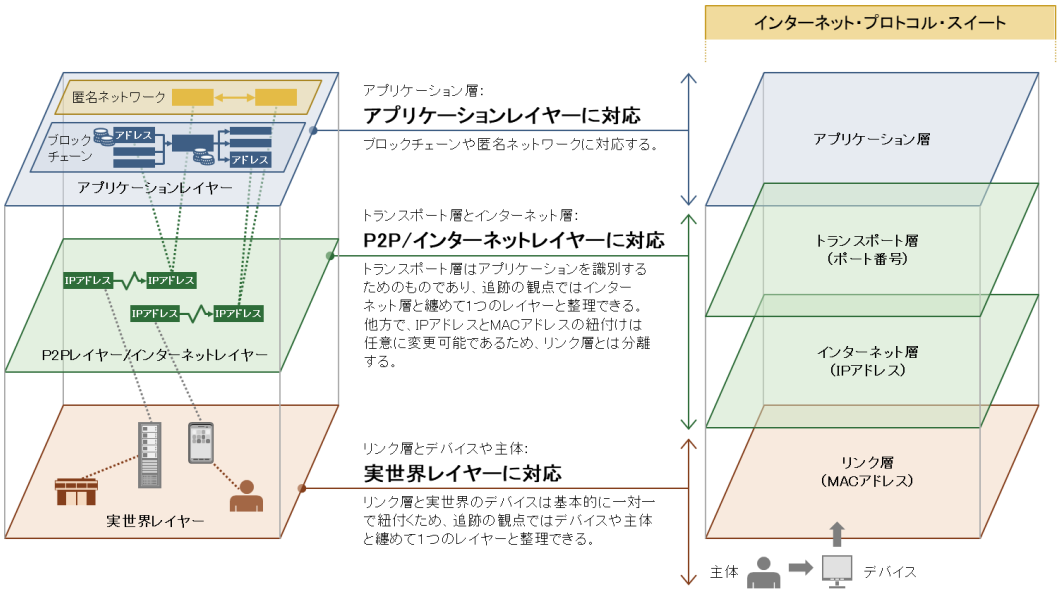


インターネットにおける通信機能の階層構造を表現したインターネットプロトコルス

30 匿名化技術や再識別技術の動向については以下の文献が良くまとまっている。宇根正志，日本銀行, "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", http://www.imes.boj.or.jp/research/papers/japanese/18-J-20.pdf, 2018/12/21

イートと、本調査研究で整理するレイヤーとの対応関係は図表 26 のようになる。

図表 26 インターネットプロトコルスイートとの比較



- アプリケーション層はアプリケーションレイヤーに対応する。
- トランスポート層ではポート番号を用いてプログラム間でデータ送受信を行う。ポート番号はアプリケーションを識別するためのものであり、ブロックチェーンのポート番号は一意に定まる[31]。そのためトランスポート層とインターネット層を纏めて P2P レイヤー/インターネットレイヤーとした。
- インターネット層とネットワークインタフェース層について、IP アドレス（インターネット層、論理アドレス）と MAC アドレス（ネットワークインタフェース層、物理アドレス）の紐付け関係は任意に変更可能であるため、両者は別のレイヤーとして分けることとした[32]。
- ネットワークインタフェース層では MAC アドレスとデバイスは原則として一意に識別される[33]。そのため、本調査研究ではネットワークインタフェース層とデバイスや主体を纏めて実世界レイヤーとした。

31 ポート番号は任意の番号に変更することが可能であるが、ブロックチェーンネットワーク上で相互に通信するためにはお互いに一意の番号を把握している必要がある。そのため、ここでは広義の意味で「一意に定まる」と記載した。

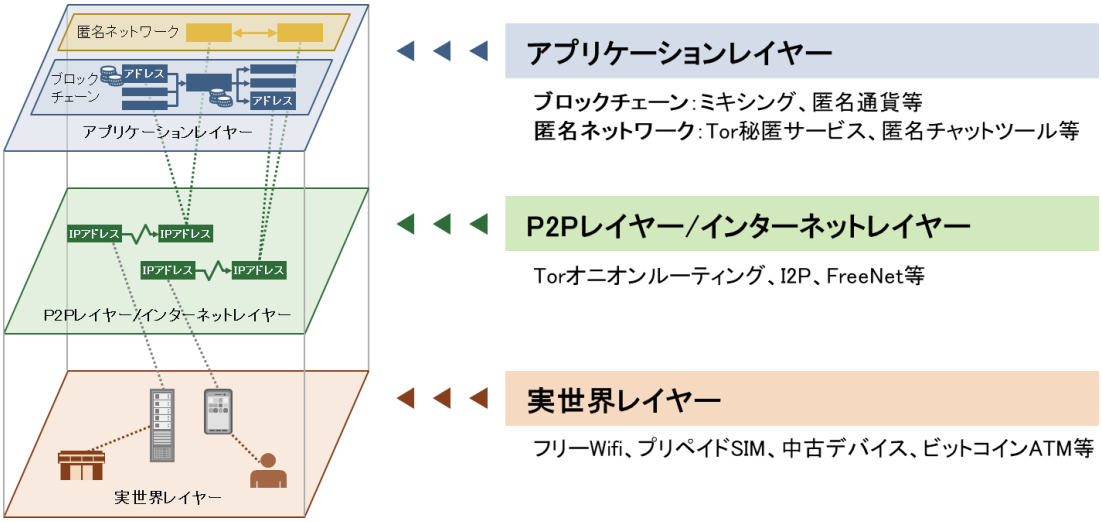
32 IP アドレスと MAC アドレスの関係は時間とともに変わり得ると考えられる。ある時刻の ARP（Address Resolution Protocol、IP アドレスから MAC アドレスを紐付けるプロトコルのこと）のログを参照することで、その時刻での IP アドレスと MAC アドレスを紐付けることが可能となる。

33デバイスによっては MAC アドレスを書き換えることが可能な場合もあるが、原則として、MAC アドレスはデバイス毎にユニークな番号が振り分けられるものであり、同一ネットワーク内で重複してはいけない。

3.1.1 匿名化技術

匿名化にあたっては、レイヤー毎の匿名化技術を組み合せることが考えられる（図表 27）。

図表 27 匿名化技術の全体像

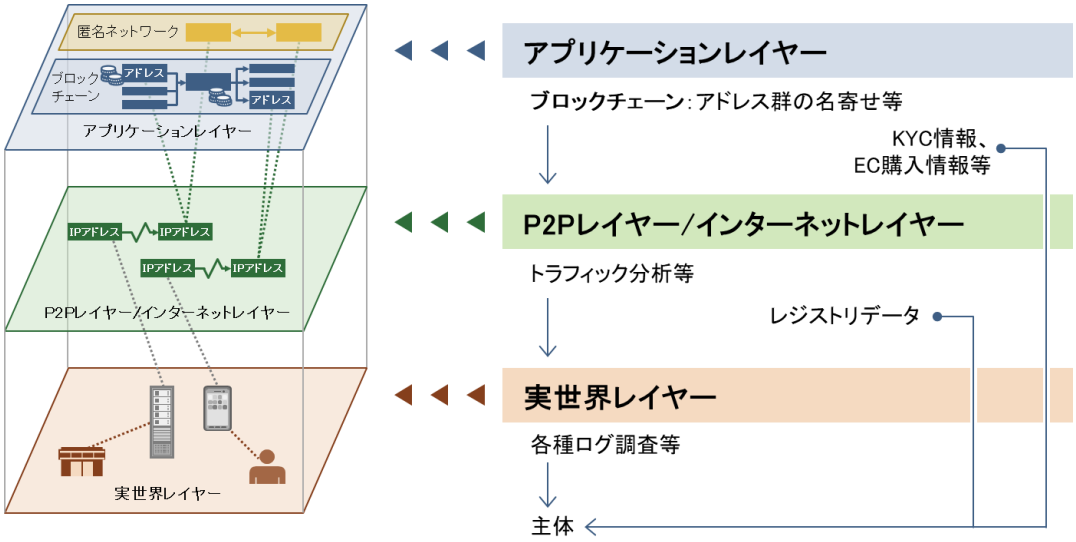


- アプリケーションレイヤーでは、ブロックチェーンであればミキシングサービスや匿名通貨などを用いることで、取引内容等の匿名化を図ることができる。他に、Tor 秘匿サービスを用いて、送信者・受信者双方の身元や通信内容の秘匿化を図ることや、セキュアチャットツールで通信内容の秘匿化を図ることも考えられる。
- P2P レイヤー/インターネットレイヤーでは、Tor オニオンルーティングや、I2P、Freenet 等を用いることで、ブロックチェーンやセキュアチャットツールなどを使う際に、送信元 IP アドレスの秘匿化を図ることができる。
- 実世界レイヤーでは、フリーWifi、プリペイド SIM や中古デバイスを用いることで、インターネットへの接続にあたって本人情報の秘匿を図ることができる。他に、ビットコイン ATM 等を用いることで、仮想通貨と法定通貨の交換にあたっての本人情報の秘匿を図ることも考えられる。

3.1.2 再識別技術

再識別化（追跡）にあたっては、大きく（1）レイヤー毎のプロトコルに基づく追跡、もしくは（2）外部のデータベース（以下、外部 DB）に基づく追跡という二通りのアプローチが挙げられ、これらを組み合わせて再識別が行われる（図表 28）。

図表 28 再識別技術の全体像



- プロトコルに基づく追跡

  - ✓ アプリケーションレイヤー（ブロックチェーン）では、ブロックチェーンデータを用いて、ブロックチェーン上のアドレスの名寄せ等を行い、暗号資産の移動経路を推測する。

  - ✓ P2P レイヤー/インターネットレイヤーでは、（ブロックチェーン上のアドレスに対応するトランザクションの発信元 IP アドレスが得られたとして）ネットワークトラフィックを監視すること等により、実際の発信元 IP アドレスを推測する。

  - ✓ 実世界レイヤーでは、（実際の発信元 IP アドレスが得られたとして）追跡対象のトランザクションが発信された時刻の ARP ログ等により、IP アドレス（論理アドレス）から MAC アドレス（物理アドレス）を特定し、MAC アドレスからデバイスや主体の推測を行う。

- 外部 DB に基づく追跡

  - ✓ アプリケーションレイヤー（ブロックチェーン）では、KYC 情報や第三者機関から提供される情報、暗号資産による決済が行われたブラウザのクッキー [34]を用いて収集された情報等により、ブロックチェーン上のアドレスから主体を直接特定する。

34 クッキーとはサーバ側からクライアント側に送信されるクライアントを識別する情報である。クッキーはクライアント側に保存され、当該サーバにアクセスする際にクライアントのブラウザからサーバ宛に送信される。サーバは受信したクッキーからクライアントを識別することができる。

- ✓ P2P レイヤー/インターネットレイヤー：我が国では日本ネットワークインフォメーションセンター（Japan Network Information Center、以下 JPNIC）など、各国の IP アドレスを管理する国別インターネットレジストリ（National Internet Registry、以下 NIR）が提供している WHOIS サービス[35]や地理的な位置情報を推測するジオロケーション情報等により、IP アドレスから主体を直接特定する。

35 インターネットレジストリがインターネット資源の登録情報を提供するサービスである。
日本ネットワークインフォメーションセンターウェブサイト, "WHOIS とは", https://www.nic.ad.jp/ja/whois/, 2018/12/17

3.2 ブロックチェーン要素技術にかかる調査

本節では、「プライバシー保護技術及び分散化技術を巡る開発状況の調査」におけるブロックチェーン要素技術の開発状況について記載する。

3.2.1 概要

3.2.1.1 背景

ブロックチェーンではトランザクションの内容は全ての参加者に公開される。ここで、送金元アドレス、送金先アドレス、送金金額、ブロックに格納された時刻等の取引内容がそのままトランザクションの内容として記録される場合、取引経路等を再識別される可能性がある。また、ブロックチェーンではトランザクションは P2P ネットワーク上を伝播していくが、十分な数のセンサーノードなどを用いてその伝播経路を推測されることで、発信元ノードの IP アドレスを推測される可能性もある。

こうした点を踏まえて、ブロックチェーン上でプライバシー保護を目指す多くの取り組みが進められている。ここで、ビットコインなどの暗号資産取引の匿名化対象としては、トランザクションの内容、およびトランザクションの発信元の二つが挙げられる

- トランザクションの内容は全員に公開されるため、匿名化にあたっては「実際の資産移動経路」 、「取引内容（送金元、送金先、送金金額等）」や「取引の存在自体」を如何に特定できなくするかがポイントになる。この際、送金元アドレス、送金先アドレス、送金金額などを秘匿化しつつ、取引データの検証をマイナーノードが正しく行えるようにすることが重要となる。
- トランザクションの発信元（ここでは必要な秘密鍵の保有者を指す）の匿名化にあたっては、伝播経路を複雑にすることや、ダミーの発信元を用意することなどにより、「実際の発信元」を如何に特定できなくするかがポイントになる。

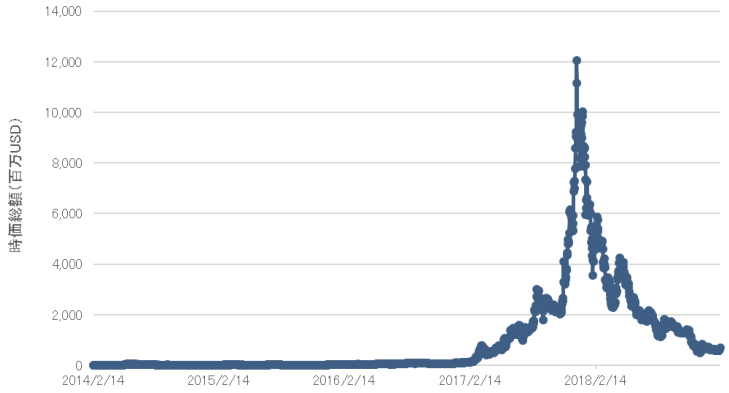
3.2.1.2 活用事例

様々な暗号資産において、次節以降に記載する匿名化技術が用いられており、例えば、ビットコインでは、送金元と送金先のつながりを秘匿化するミキシングサービスが容易に利用可能である。他に、匿名化技術をブロックチェーン基盤に組み込んだ暗号資産も存在し、これらは一般に匿名通貨と呼ばれる。代表的な匿名通貨として、Dash、Monero、Zcash が挙げられるが、これらの概要について以下に記載する。

3.2.1.2.1 Dash（ダッシュ）

Dash はビットコインのコードベースを元に、取引の即時承認機能（インスタントセンド）と取引履歴の難読化機能（プライベートセンド）を持つ暗号資産である（単位は DASH）。マイニングにはビットコインとは異なる X11[36]というハッシュアルゴリズムを利用した Proof of Work を採用しており、ネットワークは 2014 年 1 月 19 日に稼働した[37]。なお、コインの総発行量は 2200 万 Dash で、時価総額は約 859 億円（2018 年 12 月 21 日時点）である（図表 29）。Dash のマイニング報酬は、他の暗号資産とは異なり、報酬の 45%をブロックをマイニングしたマイナーに、45%をマスターノードと呼ばれるノードにそれぞれ分配し、残りの 10%は Dash の運営資金となる[38]。

図表 29 Dash の時価総額の推移[39]



(i) マスターノード

ビットコインではトランザクションやブロックの検証、伝播をするフルノードは無報酬で稼働しているが[40]、Dash では一部のフルノードに対してブロック報酬の 45%を与えることで、フルノードを一定のサービスレベルで提供するインセンティブを与えている。このノードをマスターノードと呼び、ブロックやトランザクションの検証、伝播以外にもイ

36 11 種類のハッシュ関数（blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo）を組み合わせて1つのハッシュ値を計算するハッシュ関数で、11 種類のハッシュ関数を同時に破らなければ攻撃ができないため堅牢性が高いとされている。

37 稼働当初は XCoin（XCO）と呼ばれており、同名の会社が存在したため、その後 Darkcoin（DRK）に変更され、さらにその後 2015 年 3 月に現在の Dash(DASH)に変更された。

38 Dash DAO と呼ばれる DAO の予算となり、コミュニティから提出される予算案を元に用途が決まる。マスターノードの所有者には予算案を決定するための一票の投票権が与えられ、賛成票から反対票を引いたものがマスターノードの総数の 10%を超える場合、予算案は可決され、提案者の指定したアドレスに要求額が支払われる。

39 CoinMarketCap, coinmarketcap.com, "Dash Chart", https://coinmarketcap.com/currencies/dash/, 2019/2/21 より三菱総研作成

40 2018 年 12 月 20 日時点で 9,207 のフルノードが稼働している。

ンスタントセンド、プライベートセンドなどの機能を提供する[41]。誰もがマスターノードになることはできるが、マスターノードになるためには 1,000DASH の所有を証明する必要がある。この 1,000DASH は担保では無いが、自身の残高を使いすぎて 1,000 DASH の所有を証明できなくなるとマスターノードからは除外される。

(ii) インスタントセンド

ビットコインを利用したペイメントサービスでは、決済スピードを早めるために、決済のトランザクションがまだブロックに格納されていない未承認の状態でも、トランザクションがネットワークを伝播してきた段階で決済を承認するゼロ承認（0-confirmation）を採用する場合もあるが、この場合コインの二重使用のリスクが存在する。

このような即時決済が求められるケースにおいて Dash では、マスターノードが提供するインスタントセンドというサービスにより、トランザクションを数秒でロックし決済を完了させることができる。インスタントセンドのフラグがセットされたトランザクションが送信されると、インスタントセンドトランザクションで使用される各インプットに対して、マスターノードのリストから決定論的に 10 個のノード（Quorum）が選択される[42]。その内、少なくとも 6 ノードがそのトランザクションを承認し、インプットをロックし、他の取引で使用できなくすることで決済は完了する（ロックされたインプットは、ブロックチェーン上で 6 承認されるまでロック状態が続き、その間ロックされたインプットを使用する競合トランザクションや競合ブロックが送られてきても、それらはリジェクトされる）。また、インスタントセンドのトランザクションのアウトプットは、インプットがロックされた時点で、後続の別のインスタントセンドトランザクションのインプットとして利用可能になる。上記の仕組みにより Dash では二重使用のリスクなく即時決済をサポートしている。

(iii) プライベートセンド

プライベートセンド[43]もマスターノードが提供するサービスの1つで、Dash における送金のプライバシー及びコインの代替可能性を向上させるための機能で、CoinJoin を改善したミキシングベースの匿名性を提供する。ユーザがプライベートセンドを利用する場合、以下のプロセスでコインがミキシングされる。

---

41 2018 年 12 月 20 日時点で 5,013 のマスターノードが稼働している。
42 マスターノードのリストから対象ノードを選択する際は、各ブロックの Proof-of-Work のハッシュを使い、そのブロックにおけるマスターノードの疑似順序付けを行うことで決められる。
43 2016 年 5 月以前はダークセンドと呼ばれていた機能である。

(1) プライベートセンドを利用するユーザは、トランザクションで使用するインプットとして使用できるよう、まず所持している DASH を 4 つの金種（0.01 DASH, 0.1 DASH, 1 DASH, 10 DASH）に分割する。ミキシングはこの金種毎に行われる。

(2) ユーザのウォレットは、マスターノードに対してプライベートセンドの要求を送る。この時、ユーザを識別するような情報はマスターノードには送られない。

(3) 同様のメッセージを送信したユーザが他に 2 人集まると、ミキシングセッションが開始される。マスターノードはインプットをミックスし、計 3 人のユーザのウォレットに対し、各コインの送金先を指定するよう求める。この時各ユーザのウォレットが送金先として自身のアドレスをセットするが、これは既存のアドレスではなく新しいアドレスが指定される。

(4) 各ウォレットは金種毎にこのプロセスを何度も繰り返す（この1回のプロセスをラウンドと呼ぶ）。ラウンドを重ねるごとに取引履歴の特定が指数関数的に難しくなる。ユーザは2～8回のミキシングラウンドを選択する。

(5) 上記のミキシングラウンドはバックグラウンドで実行され、全ラウンドが終了するとミキシング済みのトランザクションが入手できる[44]。

プライベートセンドはミキシングによりインプットとアウトプットの関連を難読化するもので、それ以外のアドレスや送金額の秘匿化を行うことはない。これらの情報はビットコインと同様にブロックチェーン上で誰もが確認可能であるため、他の匿名通貨と比較すると匿名化のレベルは高くないと言える。

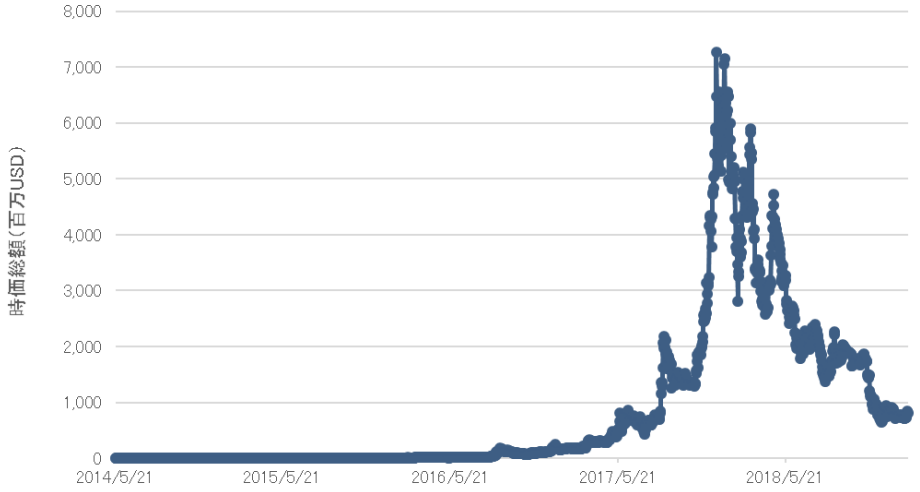
3.2.1.2.2 Monero（モネロ）

Monero は、匿名性を向上させるための仕組みを提案する CryptoNote プロトコル[45]を実装した暗号資産（単位は XMR）で[46]、Bytecoin のコードベースを元に作られた。2014 年 4 月 18 日にネットワークが稼働し、送金元を難読化するプライバシー機能を求めるユーザを中心に利用が進む。マイニングには CryptoNight v2 アルゴリズ

44 なお、プライベートセンドで送金可能なコインの量は 1 セッションあたり 1,000 DASH に制限されており、多額の資金を匿名化する場合は複数のセッションを必要とする。
45 Saberhagen, N., "Crypto Note v2.0", https://cryptonote.org/whitepaper.pdf, 2018/12/21
46 CryptoNote プロトコルは Monero 以外にも、Bytecoin、Dashcoin、Fantomcoin など多数の暗号通貨で採用されている。

ム[47]を利用した Proof of Work を採用しており、コインの総発行量は定義されておらず上限は無い。またビットコインと異なり、ブロックサイズの制限がない。但し、過剰なブロックサイズの拡大を防ぐため、新しいブロックのサイズは直近 100 ブロックのブロックサイズの中央値（以下、M100）と比較され、M100 の 2 倍を超えるブロックサイズは許可されず、新しいブロックサイズが M100 を超えた場合、超過サイズ分だけブロック報酬が削減されるペナルティが存在する[48]。時価総額は約 990 億円（2018 年 12 月 21 日時点）である（図表 30）。Monero では、ステルスアドレス、リング署名、リング CT（Confidential Transaction）という3つの機能で匿名性を確保する。

図表 30 Monero の時価総額の推移[49]



(i) ステルスアドレス

Monero でアカウントを作成すると、以下の 3 つのデータが生成される。

- private spend key … コインを送金する際に使用する鍵。
- private view key … アカウント宛の送金（着金）を検知するための鍵。
- 公開アドレス … private view key と private spend key から生成されるアドレス。

47 CryptoNight はもともと CrypteNote の一部として 2013 年に設計されたアルゴリズムである（CryptoNight v0）。Monero ではその後オリジナルの CryptoNight v0 に変更を加えた、CryptoNight v1, CryptoNight v2 を開発しており、ハードフォークにより ASIC 耐性を持つアルゴリズムへ移行している。

48 超過サイズが M100 の 10%の場合は 0.1×0.1 = 0.01（1%）、50%の場合は 0.5×0.5 = 0.25（25%）、80%の場合は 0.8×0.8=0.64（64%）が標準の報酬額から減少する。

49 CoinMarketCap, coinmarketcap.com, "Monero Chart", https://coinmarketcap.com/currencies/monero/, 2019/2/21 より三菱総研作成

Monero では送金先のアドレスを、受取人の公開アドレスと送金人がランダムに選択した nonce を使って導出する。このため送金の都度、ランダムなワンタイムアドレスが生成されることになり、このアドレスをステルスアドレスと呼ぶ。ステルスアドレスと受取人の公開鍵を関連付けることはできず、誰宛の送金であるかは取引の当事者以外には分からない。但し、private view key を第三者と共有することで、該当するアカウントへの着金の内容を第三者に公開することが可能である。

(ii) リング署名

Monero ではリング署名を利用して、送金元のコインの匿名化を行う。送金トランザクションを作成する際に、自身の UTXO の他にブロックチェーン上から同じ量を持つ TXO（Transaction Output）を、未使用・使用済み関係なく集めてダミーのインプットとする。各 TXO はそれぞれステルスアドレス（公開鍵）にロックされている。送金人は自身の UTXO（Unspent Transaction Output）に対応する private spend key を使ってインプットの TXO のセット（公開鍵のセット）に対して有効なリング署名を作成する。リング署名は鍵を持つユーザグループ内の任意のユーザが生成できるデジタル署名で、その署名はユーザグループ内の誰の鍵で行われたものかは分からないという特性を持つ。つまり、自身の UTXO とブロックチェーン上から集めた TXO の内、どのコインを使用したのか外部からは分からないということになる。このリング署名の特性を利用して、送金元のコインの匿名化を行っている。

(iii) リング CT

Monero はビットコインの開発者である Gregory Maxwell が発表した Confidential Transaction を採用し、トランザクションの送金額を秘匿するための仕組みを 2017 年 1 月に導入した。この Confidential Transaction では、コインの量を秘密の値とし、ブラインドファクターと共に Commitment[50]と呼ばれるデータに変換する。Commitment は楕円曲線上の点（公開鍵）で、Commitment からその生成に使われたコインの量を計算することはできないため、これをトランザクションの送金額として扱うことで取引の当事者以外は送金額を知ることができない。また、トランザクションのインプットとアウトプットでコインの量が変化していないか（不正をしていないか）は、このインプットのコインの点の合計値（点）からアウトプットのコインの点の合計値（点）を減算することで、コインの量を知らずとも検証が可能になる。この導入に合わせてリング署名も

50 Commitment = (ブラインドファクター) * G +(コインの量) * H
ここで、G は楕円曲線のベースポイント、H は G から G とは異なるベースポイントである。

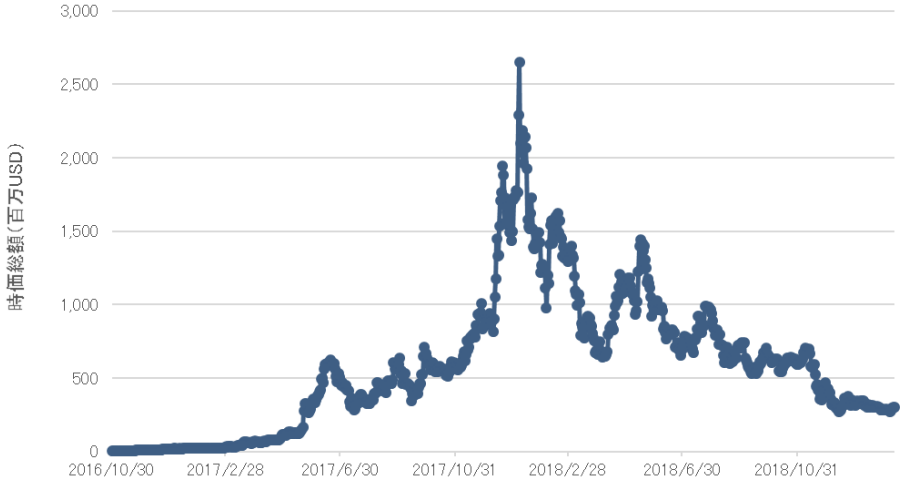
Confidential Transaction に対応した改良版に更新されている。そして 2017 年 9 月以降、この機能はネットワーク上の全てのトランザクションで必須の機能となった。

Monero では、上記の機能により送金元の難読化および送金額の秘匿化を行うことで、暗号資産の送金の匿名性を強化している。送金先のアドレスはステルスアドレスにより、アドレスとユーザの関連性は難読化されるものの、アドレス自体は識別可能である。さらにこのアドレス自体も秘匿するのが Zcash の匿名化技術であるが、暗号資産の中では Monero も匿名化レベルの高い通貨と言える。

3.2.1.2.3 Zcash（ジーキャッシュ）

Zcash はビットコインのコードを元に、ゼロ知識証明を中心とした暗号技術を導入することによりユーザのプライバシーを強化することを目的とした暗号資産（単位は ZEC）である。2016 年 10 月 28 日にネットワークが稼働して以来、秘匿性とプライバシーの特性を望むマイナーやユーザからの関心が高い。マイニングには Equihash アルゴリズム[51]を利用した Proof of Work を採用しており、コインの総発行量はビットコインと同様に固定で 2100 万 ZEC である。時価総額は約 384 億円（2018 年 12 月 21 日時点）である（図表 31）。

図表 31 Zcash の時価総額の推移[52]



51 ルクセンブルグ大学で開発されたメモリ指向の Proof of Work アルゴリズム。
Biryukov, A., et al., "Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem", https://eprint.iacr.org/2015/946.pdf, 2018/12/13

52 CoinMarketCap, coinmarketcap.com, "Zcash Chart", https://coinmarketcap.com/currencies/zcash/, 2019/2/21 より三菱総研作成

(i) アドレスと秘匿スコープ

Zcash のアドレスは z から始まるシールドアドレス（Z アドレス）と、t から透過アドレス（T アドレス）のいずれかになる。透過アドレスを使用した場合、何も情報は秘匿されないため、アドレスや送金額を秘匿したい場合はシールドアドレスを使用することになる。この 2 種類のアドレスを利用した送金トランザクションの組み合わせは以下の 4 通りになる。

- 透過アドレスから透過アドレスへ送金する場合

  ビットコインと同様に動作し、送信元、送金先、送金額はすべてブロックチェーン上で公開される。

- 透過アドレスからシールドアドレスへの送金する場合

  送金元のコインの量は公開されるが、送金先のアドレスの数と各アドレスが所持するコインの量は秘匿される。

- シールドアドレスから透過アドレスへの送金する場合

  送金元の数、送金元のアドレスやそのアドレスが保持するコインの量は秘匿されるが、送金先のアドレスとそのアドレス宛のコインの量は公開される。

- シールドアドレスからシールドアドレスへの送金の場合

  送金元の数、送金元のアドレスやそのアドレスが保持するコインの量に加え、送金先の数、送金先のアドレスやそのアドレス宛のコインの量のすべてが秘匿される。このコインの受取人は受信したコインの量は確認できるが、送金元のアドレスを確認することはできない。

シールドアドレスへ送金する場合は、さらに追加のメモフィールドが利用可能になる。メモフィールドには請求書番号や口座番号、払い戻しアドレスなどその支払いに関する任意のデータを設定でき、受取人はこのデータを元に送金を識別することが可能になる。このメモフィールドは暗号化され、受取人以外に内容は分からない。

(ii) ゼロ知識証明（zk-SNARKs）を利用した検証と送金

Zcash のシールドアドレスを利用したトランザクションでは、送金元・送金先の数、アドレス、コインの量が秘匿されるが、これらが秘匿された場合に各ノードがそのトランザクションが有効なトランザクションかどうか（すなわち、コインの二重使用や増殖がさ

れてないかなど）をどのように判断するかが課題となる。Zcash では、プライバシーを維持したまま、ネットワークのコンセンサスルールに従ってトランザクションの有効性を検証する必要があり、秘匿情報を明らかにすることなく取引の検証を行うのにゼロ知識証明を利用する。これは有効なトランザクションを決定するためのルールを zk-SNARKs にエンコードすることで行われる[53]。

ビットコインでは未使用のトランザクションアウトプット（UTXO）を追跡することで、未使用のコインを識別するが、Zcash のシールドトランザクション[54]でシールド化された UTXO は Commitment と呼ばれる。Commitment はコインを受信したアドレスと、コインの量、ユーザが独自に生成する固有の文字列、ランダムな nonce で構成されるハッシュ値である。

Commitment = Hash(受信アドレス ｜ コインの量 ｜ 固有文字列 ｜nonce)

Commitment が使用済みであるかどうかは、Commitment 内の固有文字列から生成したハッシュ値である Nullifier を使ってチェックする。Zcash の各ノードは全ての Commitment のリストと Nullifier のリストを管理しており、Commitment に対応する Nullifier が既に存在する場合その Commitment は使用済みと判断される。

シールドトランザクションの作成者（送金人）は、自身が所持している未使用の Commitment に対応する Nullifier を公開することで自身の Commitment を無効化すると同時に、新しい受取人によって生成された新しい Commitment を用意するシールドトランザクションを作成することでコインを送金する。この時、未使用の Commitment を使用する権限があることを示すゼロ知識証明を一緒に提供する。このゼロ知識証明は以下を証明する。

- 署名が Commitment の受信アドレスに対応した鍵による署名であること。
- 公開された Nullifier は確かに使用する Commitment の固有文字列から生成されたものであること。

53 zk-SNARKs はセットアップ時に公開パラメータを生成する必要があり、このパラメータの生成元の情報が明らかになると検証者に有効と判断させることができる誤った証明が生成できるという問題がある。Zcash の場合は、コインの増殖が可能になってしまう。このため公開パラメータ生成時の情報は誰も知り得ない状態にすることが求められる。Zcash では 2016 年 10 月のネットワーク稼働前と 2018 年 10 月のハードフォーク（Sapling）の際に、公開パラメータが生成されており、その際は独自に設計されたマルチパーティ計算により、以下のように公開パラメータを生成するセレモニーを開催している。
Zcash ウェブサイト, "Parameter Generation", https://z.cash/technology/paramgen, 2018/12/14

54 シールドアドレスを利用したコインの送信、受信を行うトランザクションをシールドトランザクションと呼ぶ。

- インプットのコインの量はアウトプットのコインの量となること。

上記のように送金先のアドレス（公開鍵）および量は Commitment により誰にも分からない形式で保持され、その所有権と量の整合性をゼロ知識証明によって担保することで Zcash の匿名性は維持される仕組みとなっている。

(iii) viewing-key を用いた取引内容の公開

通常シールドアドレスが所持するコインはそのアドレスの所有者にしか取引の内容が分からないよう秘匿されているが、viewing-key と呼ばれる鍵を共有することで、監査人など信頼できる第三者に取引の内容を開示することが可能である。ただし、viewing-key で可能なのは情報の参照のみであって、viewing-key を使ってコインを使用することはできない。

(iv) パフォーマンスの向上

Zcash がリリースされた当初のゼロ知識証明は、シールドトランザクションの作成に 40 秒以上かかり、約 3GB のメモリを必要とした。検証はミリ秒単位で済むので高速であるが、シールドトランザクション作成者のコストが大きかった。このパフォーマンス問題を解消するため、新しい楕円曲線をベースとしたアルゴリズムが設計され、2018 年 10 月 29 日のハードフォーク（Sapling）でアクティベートされた。Sapling で有効になった zc から始まる新しいシールドアドレスを使用した場合、そのシールドトランザクションの作成は数秒で完了し、必要なメモリ量も約 40MB で済む。こおの大幅なパフォーマンス改善の結果、シールドトランザクションの作成の敷居は下がりモバイルウォレットでの利用も考慮できるレベルとなった。他の匿名通貨と同様 Zcash でも匿名性を維持するシールドトランザクションの増えるほどその匿名性は強化される。

Zcash では上記のようにシールドトランザクションにより送金元、送金先、送金額の秘匿化が可能で、匿名通貨の中でも匿名化のレベルは最も高い。一方、ユーザが第三者に viewing-key を共有することで、秘匿情報を開示するオプションも兼ね備えている。

3.2.2 要素技術

本節では、専門家等の意見を踏まえ、ブロックチェーンにおいて匿名性を高める代表的な技術として図表 32 に挙げる 9 つの技術について記載する。

図表 32 匿名性に関係するブロックチェーンの要素技術

No	匿名化の対象	要素技術	対応している暗号資産名（カッコは技術の名称）	概要
1	トランザクションの内容	ミキシング	ビットコイン（CoinJoin、Tumblebit 等）、ダッシュ（PrivateSend）ビットコインキャッシュ、ライトコイン、イーサリアム等	コインをプーリングすることで、送金元アドレスと送金先アドレスの関係を第三者から隠蔽する。
2		ステルスアドレス	モネロ	受取人のワンタイムアドレスを生成することで、受取人の情報を第三者から隠蔽する。
3		リング署名	モネロ（Ring CT）	ダミーの送金元を含めることで、実際の送金元を第三者から隠蔽する。
4		ゼロ知識証明（zk-SNARKs）	ジーキャッシュ、イーサリアム	ブロックチェーンデータに、取引内容（送金元、送金先、送金金額等）を一切記録しないことで、これらを第三者から隠蔽する。
5		ライトニングネットワーク	ビットコイン（Lightning Network）、イーサリアム（Raiden Network）、ライトコイン	オフチェーン（ブロックチェーン外）で取引を行い、中継ノードを介して取引を行うことで、実際の送金元と送金先の関係を第三者から隠蔽する。
6		アトミック・クロスチェーン・スワップ	ビットコイン、イーサリアム、ライトコイン、ディクレッド	第三者を介さずに、異なるブロックチェーンネットワーク間でのコインの受渡を行うことで、取引ペアとなるコインの受け渡しの関係を第三者から隠蔽する。
7		ミンブルウィンブル	グリン、ビーム	取引額を第三者から秘匿するとともに、不要なトランザクションをブロックチェーン上に記録しないことで、取引の存在自体を第三者から秘匿する。
8		シュノア署名	グリン、ビーム	署名集約機能により、ブロックチェーンのデータ量を削減するとともに、取引当事者の数や取引内容を第三者から隠蔽する。
9	発信元	ダンデリオン	グリン、ゼットコイン	ランダムに選んだノードをランダムな回数中継した後に、トランザクションをブロードキャストすることで、実際の発信元を第三者から隠蔽する。

3.2.2.1 ミキシング

3.2.2.1.1 背景

ビットコインを送金する際は、トランザクションを作成し、P2P ネットワークに送信、その後マイナーによりブロックに取り込まれることでブロックチェーンに送金内容が記録される。このブロックチェーン上の取引データには基本的に個人情報は含まれず、匿名性が高いと言われることもあるが、ブロックチェーンの送金記録はどのアドレスからどのアドレスにいくら送金されたか記録されており、送金記録を誰もが追跡することができる。ビットコインが提供するのは完全な匿名性ではなく、あくまで仮名性[55]である。このためプライバシーを強化するためのさまざまな提案が行われている。

ビットコインにおける匿名性を向上させる仕組みの1つがミキシングである。ミキシングでは、多数のユーザの送金を1トランザクションにまとめて行うことで、どのインプットがどのアウトプットへ送金しているのか判りづらくし、匿名性を向上させる。

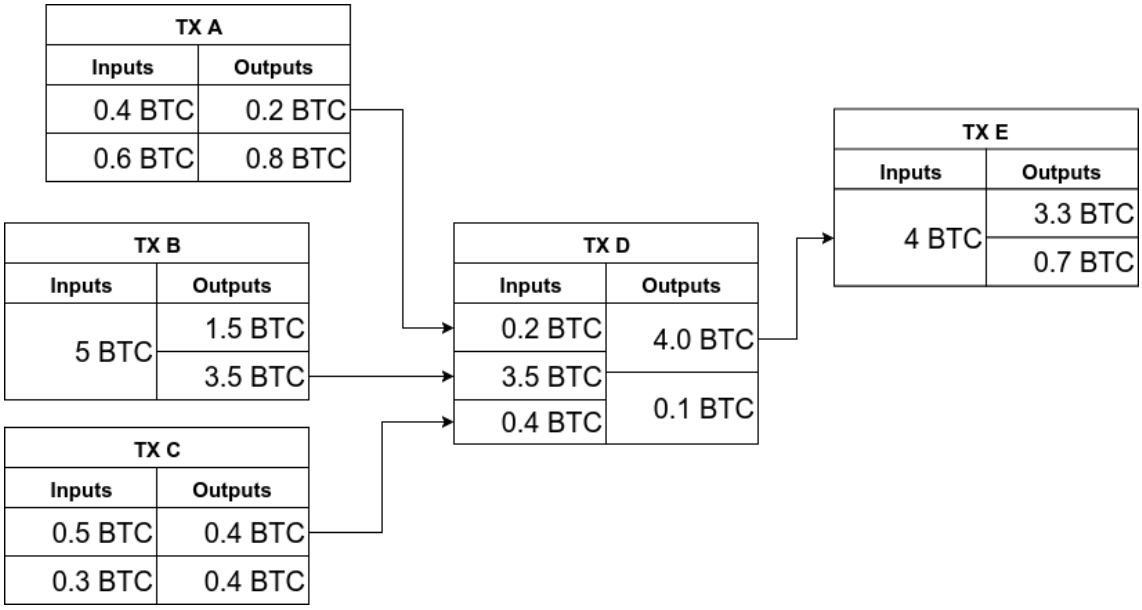
具体的な仕組みの説明の前に、ビットコインのトランザクションの構造について説明する（図表 33）。ビットコインのトランザクションは1つ以上のインプットと1つ以上のアウトプットを持ち、インプットのコインがアウトプット宛に送金される。各インプットは、それより前のトランザクションのアウトプットを参照している。そして、各インプットにはそれぞれそのインプットを使用することが可能であることを証明するためのデジタル署名が付与されている。通常ビットコインを送金する場合は、自身が所有するアウトプットのセットから送金額を満たすアウトプットを選択し（1つのアウトプットで送金額に満たない場合は、送金額を満たすまでアウトプットを選択する）、それをインプットとし、アウトプットは送金先のアウトプットと、お釣りを受け取るアウトプットで構成されることが多い。

上記のようなトランザクションが大半であるため、インプットが参照するアウトプットのアドレスが別々のアドレスであったとしても、一般的に、それらは同じ所有者のアウトプットであると推測することもできる。しかし、必ずしもトランザクションの全インプットが同じ所有者のものである必要はなく、多数のユーザへの送金のインプットとアウトプットを混ぜ合わせて1つのトランザクションにすることも可能である。そのようなトランザクションを作ることでコインの元の所有者が誰か判断できないようにする仕組みをミキシングと呼ぶ。

---

55 所有者は正当なアイデンティティを持つ実際の名前を所有しているが、その名前を使用せずに偽名を使用し、その偽名に基づいて識別される状態を指す。ビットコインにおいてはアドレスが偽名として作用する。

図表 33 ビットコインのトランザクション構造



3.2.2.1.2 仕組み

(i) 中央集権型のミキシングサービス

初期からサービスを提供しているのが中央集権型のミキシングサービスである。これには運営者が存在し、ユーザは運営者が管理するプールにコインを送り、運営者が他のユーザのコインと混ぜ合わせ、希望する宛先に送金することでミキシングを代行する。ミキシング時にどのようなトランザクションを構成して匿名性を高めるかは、運営者によって異なる。

このようなミキシングサービスの利用にあたっては、運営者によるコインの持ち逃げや、ハッキング等による情報漏洩（利用情報や送金情報）がユーザにとってのリスクとなる。また、ミキシングの処理を運営者が代行するため、手軽に利用できるのが便利な反面、匿名性の観点では、運営者には送金情報が全て分かってしまうという課題が残る。また規制という意味では、2017 年 8 月、当時世界最大であったミキシングサービス Bitmixer.io が、今後の規制の強化に伴うサービス継続の困難さからサービスの終了を発表しており[56]、他社のサービスも継続して利用可能な状態がいつまで続くかは不透明な状況である。

なお、ミキシングをサービスとして提供する事業者への法的規制について考察した

56 BITMIXER.IO, Bitcoin Forum, "The lagest Bitcoin mixer is about to stop working", https://bitcointalk.org/index.php?topic=2042470.0, 2018/11/18

研究[57]では、国内法の下ではミキシングサービス事業者は信託会社[58]として考えるのが適切であり、この場合、犯罪による収益の移転防止に関する法律（犯罪収益移転防止法）における特定事業者に該当するため、本人確認記録や取引記録の保持が義務付けられると整理している。

(ii) CoinJoin

中央集権型のミキシングサービスが運営者への信頼を必要とするのに対して、CoinJoin は 2013 年に Gregory Maxwell によって提案された管理者無しでミキシングトランザクションを構成する P2P のミキシングプロトコル[59]である。CoinJoin のプロトコルはシンプルで、以下のルールでトランザクションを構成する（図表 34）。

「N 人の参加者がある量のコインをアウトプットにすることに合意した場合、各ユーザはその量を満たすインプットを提供する。そしてトランザクションは合意したコインの量のアウトプットを N 個持ち、ユーザの一部が指定されたコイン量を超過するインプットを提供した場合にお釣り用のアウトプットをアウトプットに余分に追加する。」

各ユーザは送金に必要なインプットと、送金先のアウトプット、必要に応じてお釣り用のアウトプットを提供する。参加者全ての情報が揃うと、参加者のいずれか、ないし、第三者が送金用のトランザクションを作成する。このトランザクションについて、参加者はそれぞれ署名を行い[60]、作成されたトランザクションがブロックチェーンネットワーク上にブロードキャストされる。

中央集権型のミキシングサービスと比べて、持ち逃げされるような心配はなく、他者を信頼することもなく、ミキシングを行うことができる。そして、（お釣りを除いて）送金先のコインの量が全て同じであるため、どのインプットのコインがどのアウトプットのコインに流れているのかは判別できなくなる。CoinJoin はブロックチェーンのスペース効率の良い簡単なミキシング技術だが、ビットコインの最大標準トランザクションサイズ（100KB）の制限から、匿名セットのサイズ（インプットの数）は 350～470 に制限さ

57 廣澤他, "ビットコインのミキシングにおける資金移動の分析", 研究報告コンピュータセキュリティ（CSEC）, 2018-CSEC-81(9), 1-8 (2018-05-10), https://ipsj.ixsq.nii.ac.jp/ej/index.php?active_action=repository_view_main_item_detail&page_id=13&block_id=8&item_id=189339&item_no=1, 2018/11/18

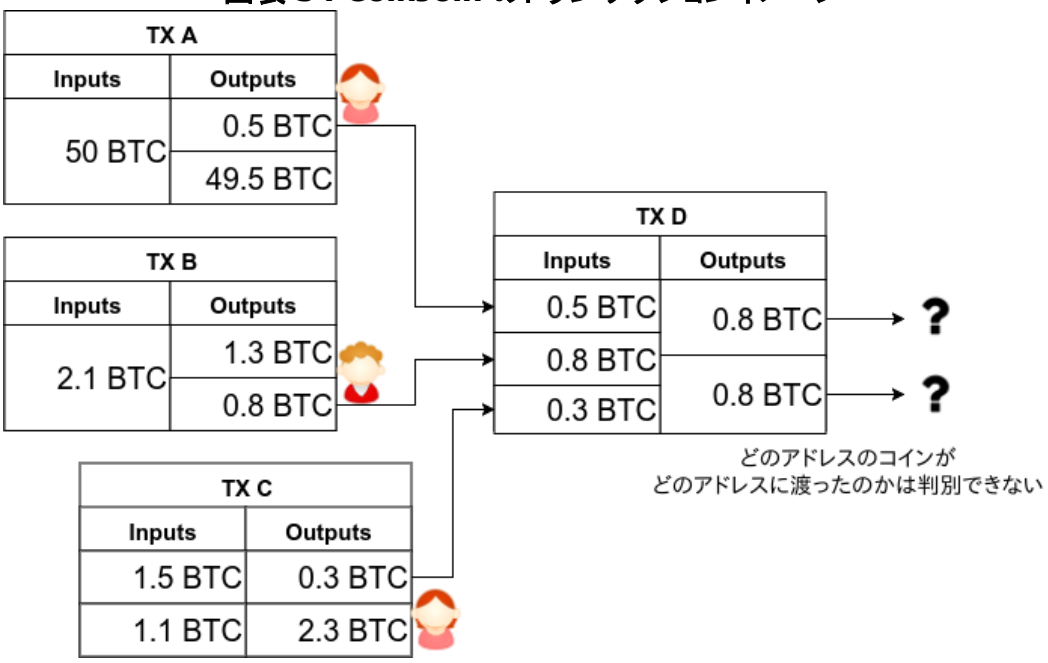
58 ビットコインを用いた暗号資産取引におけるプライバシーを保護することを目的とした目的信託（受益者の定めのない信託の一種）と整理している。

59 gmaxwell, Bitcoin Forum, "CoinJoin: Bitcoin privacy for the real world", https://bitcointalk.org/index.php?topic=279249, 2018/11/18

60 参加者全員の署名が集まらないと、当該トランザクションは有効とならない。

れる。

図表 34 CoinJoin のトランザクションイメージ



CoinJoin を利用する際の理想的なトランザクション構成はインプットとアウトプットの数が同じで、各インプットの量と各アウトプット量が全て等しい（手数料は全て均等に各インプットに分散している）状態である。当然そういったトランザクションを多人数でタイミングよく構成するのは難しく、これが CoinJoin の課題になる。ウォレットサービス等でユーザ向けに CoinJoin サービスを提供する場合、ユーザの利便性を向上させるため、インプットの量は均一ではなく、アウトプットの量も均一で無くなる等、CoinJoin の前提条件を崩すことを許容することも考えられる。このようなサービスで作成された CoinJoin トランザクションはアドレスの名寄せを行うことで、ある程度インプットとアウトプットのつながりが明らかになることが報告されており[61]、期待したレベルの匿名性が得られないという結果になる。

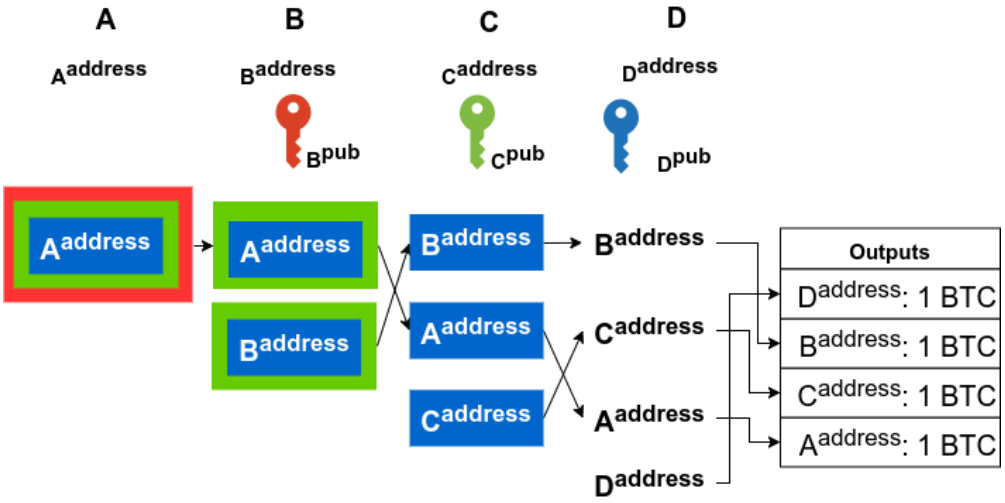
(iii) CoinShuffle

CoinJoin により複数の参加者のコインを混ぜ合わせても、インプットとアウトプットのアドレスの順序に相関関係があると（例えば、n 番目のインプットと n 番目のアウト

61 CoinJoin と似た技術で、Blockchain.info が提供していた SharedCoin というミキシングサービスについて、トランザクションインプットの 69%とトランザクションアウトプットの 53%がグループ化可能で意図された匿名性が得られないという脆弱性が報告されている。Atlas, K., "Weaknesses in SharedCoin", http://www.coinjoinsudoku.com/, 2018/11/19

プットが常に対応する、など）、そこから匿名性が損なわれる可能性がある。CoinShuffle は、2014 年に公開された CoinJoin ベースのミキシングプロトコルの1つで[62]、ミキシングトランザクションのアウトプットの順序をシャッフルする方法について規定している（図表 35）。CoinShuffle では、1.鍵交換、2.シャッフル、3.トランザクションの作成という3つのフェーズで、トランザクションアウトプットの順序をシャッフルする。A, B, C, D の 4 人の参加者がいる場合、以下のような各フェーズを経て、コインがシャッフルされる。

図表 35 CoinShuffle の公開鍵暗号を使ったコインのシャッフル



(1) 鍵交換フェーズ

全ての参加者は最終的なコインの受取先のアドレス $A^{address}$、$B^{address}$、$C^{address}$、$D^{address}$ を作成する。但しこのアドレスは他の参加者には公表しない。続いて A 以外のユーザは、それぞれ公開鍵暗号方式の鍵ペアを生成する。B, C, D が生成した鍵ペアの内、公開鍵を B^{pub}, C^{pub}, D^{pub} とする。各参加者は自身の公開鍵と、その公開鍵に対する署名（自分が所有するコインのインプットアドレスに対応する秘密鍵で作成したもの）を送る。

(2) シャッフルフェーズ

A は、他の全員の公開鍵（B^{pub}, C^{pub}, D^{pub}）を使って順番に自身のアドレス $A^{address}$ を暗号化する。具体的には最初に D^{pub} を使って $A^{address}$ を暗号化し、暗号化したデータをさらに C^{pub} で暗号化し、さらにそれを B^{pub} で暗号化する。そのようにして作成した

62 Ruffing, T., et al., "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin", http://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/coinshuffle.pdf, 2018/11/20

暗号データ enc(B^{pub}, enc(C^{pub}, enc(D^{pub}, $A^{address}$)))を B に渡す。

B は、A から受信したデータを B^{pub} に対応する秘密鍵で復号し、データ enc(C^{pub}, enc(D^{pub}, $A^{address}$))を得る。さらに A と同様に自身のアドレス $B^{address}$ を C^{pub}, D^{pub} を使って暗号化して enc(C^{pub}, enc(D^{pub}, $B^{address}$))を得る。この時点で B は 2 つの暗号データを所持しているが、その順番をランダムにシャッフルして、C に渡す。

C は、B と同様に B から受信した 2 つのデータを C^{pub} に対応する秘密鍵で復号し、自身のアドレスを D^{pub} で暗号化し、他の 2 つのデータを合わせてランダムにシャッフルする。シャッフルした3つのデータ enc(D^{pub}, $B^{address}$), enc(D^{pub}, $C^{address}$), enc(D^{pub}, $A^{address}$)を D に渡す。

D も同様に D^{pub} に対応する秘密鍵で復号し、$B^{address}$, $C^{address}$, $A^{address}$ を入手し自身のアドレス $D^{address}$ を加えシャッフルし、シャッフル後のリストを全員に送る。

(3)トランザクションの作成フェーズ

D からアドレスのリストを受信した各参加者は、その中に自身のアドレスが存在するか確認し、存在する場合は自身のインプットを D に送付し、トランザクションを作成する。その上で、生成されたトランザクションに参加者それぞれが署名し、参加者全員の署名が集まれば当該トランザクションは有効となる。もし自身のアドレスが存在しなかった場合は、署名をしなければコインを失うことはない。参加者のアドレスが存在しない場合は、誰かが不正を働いていることになるが、これについては別のステップを実行することで誰が不正をしたのか明らかにされる仕組みとなっている。

上記のように CoinShuffle では、各参加者の公開鍵暗号の鍵ペアを使って各参加者の送信先アドレスを暗号化することで、自身以外のアドレスについてはどのアドレスが誰のアドレスなのか誰も紐付けができない状態で、全参加者のアドレスをシャッフルすることが可能になる。

さらに、公開鍵暗号を使用したシャッフルフェーズを、食事する暗号学者の問題[63]に置き換えることで、ミキシングを並列処理できるようにした改良版の CoinShuffle++

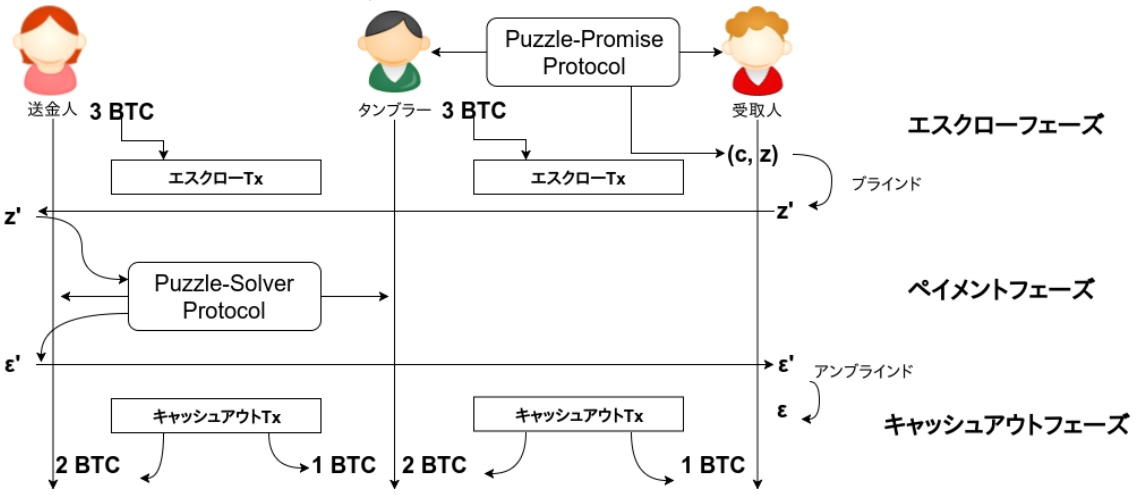
63 Wikipedia, "食事する暗号学者の問題", https://ja.wikipedia.org/wiki/%E9%A3%9F%E4%BA%8B%E3%81%99%E3%82%8B%E6%9A%97%E5%8F%B7%E5%AD%A6%E8%80%85%E3%81%AE%E5%95%8F%E9%A1%8C, 2018/11/20
3 人以上の暗号学者が食事中に支払われた食事代金が学者の 1 人が支払ったのか、雇い主が支払ったのかについて、暗号学者が支払っていた場合にその学者を特定することなく知る方法を問う問題。参加者の各組み合わせでコイントスをし、その結果表が出た回数を全員に宣言するが、もし支払いをした学者がいた場合はその学者だけ反対の結果を宣言することで答えが分かるというもの。DC ネットとも呼ばれる。

が同じ研究者らによって提案され、処理時間が大幅に向上している[64]。

(iv) Tumblebit

TumbleBit[65]は 2016 年に発表された、仲介者（以下タンブラーと呼ぶ）が存在するタイプのミキシングサービスである。CoinJoin などが 1 つのトランザクションで多数の参加者のコインをミキシングするのに対し、TumbleBit は送金人がタンブラーを経由してコインを受取人に送金することでブロックチェーン上の送金元と送金先の関連を削除するという異なるアプローチをとっている。その際、中央集権型のミキシングサービスであれば管理者のみは送金元と送金先の関連を知っているが、TumbleBit ではタンブラーもユーザの送金元と送金先のアドレスの関連を知ることができないという特徴がある。この TumbleBit を利用したミキシングは以下の 3 つのフェーズで構成される（図表 36）。以下タンブラーを利用して、送金人が受取人に 1 BTC を送金するフローについて記述する。

図表 36 TumbleBit の決済フロー



(1) エスクローフェーズ

ミキシングに参加する送金人と受取人は、それぞれタンブラーとの間にペイメントチャネルを開く。送金人は自身の 3 BTC[66]をタンブラーとの 2-of-2 のマルチシグ[67]にデ

64 参加者 50 人のミキシングを行う際、CoinShuffle では処理に約 3 分かかるのに対し、CoinShuffle では約 15 秒で処理が完了する測定結果が論文に記載されている。Ruffing, T., et al., "P2P Mixing and Unlinkable Bitcoin Transactions", https://crypsys.mmci.uni-saarland.de/projects/FastDC/paper.pdf, 2018/11/20

65 Heilman, E., et al., “TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub”, https://eprint.iacr.org/2016/575.pdf, 2018/12/4

66 金額は、総金額以上であれば、任意の値を指定できるが、ここでは 3BTC とした。

67 M-of-N マルチシグとは、そのマルチシグへ送金されたコインを利用するにあたって、N 個のうち M 個の秘密鍵が必要となるということを指す。

ポジットするエスクロー^{Tx}を作成しブロードキャストする。同様に、タンブラーは自身の 3 BTC を受取人との 2-of-2 のマルチシグにデポジットする、別のエスクロー^{Tx}を作成しブロードキャストする。

各エスクロー^{Tx}には 2-of-2 のマルチシグ以外にタイムアウトが設定されており、設定された時刻を過ぎると資金の供給元が資金を取り戻すことができるようになっている。そして受取人は Puzzle-Promise Protocol と呼ばれる手順[68]を実行し、タンブラーからパズルzを手に入れる。最終的に、このパズル z の解答と引き換えに受取人はコインを入手することになる（後述）。

(2) ペイメントフェーズ

パズルの解答はタンブラーが知っているため、受取人はパズルを送金人に渡し、送金人がコインと交換でタンブラーからパズルの解答を購入するのがペイメントフェーズになる。この時、受取人がパズル z をそのまま送金人に渡し、それがタンブラーに渡るとタンブラーに送金人と受取人の関係が漏れてしまうため、受取人はパズル z をそのまま使わず、z をブラインドファクターを使ってブラインドした z′に変換してから送金人に渡す[69]。送金人はこのパズルの解答をタンブラーに要求するため Puzzle-Solver Protocol と呼ばれる手順を実行し、タンブラーから解答 ε′を受け取る。送金人はこの答えが正しいか検証し、正しければ解答 ε′を受取人に渡す。

(3) キャッシュアウトフェーズ

受取人はパズル z′の解答 ε′をブラインドファクターを使ってアンブラインドし、パズル z の解答 ε を計算する。この ε を使ってタンブラーから 1 BTC 入手するキャッシュアウトトランザクションを完成させ、ブロードキャストする。

TumbleBit では上記のように送金人とタンブラー、タンブラーと受取人の2つのペイメントチャネルを利用して送金するため、他のミキシングプロトコルと異なり、送金人と受取人の送金がオンチェーン上で直接結びつくことが無い。CoinJoin などの 1 トランザクションでミキシングするタイプのプロトコルと異なり、ユーザ毎にオンチェーントランザクションが作られるため、匿名セットがトランザクションのサイズ上限の制限を受けることもない。また、上記のようなパズルとそのブラインド/アンブラインド処理を利

68 パズル z はタンブラーの公開鍵（e, N）で値 ε を RSA を利用して暗号化したデータである（$z = \varepsilon^e \bmod N$）。パズルの解答は z を復号化して得られる ε で、ε を使い Puzzle-Promise Protocol のもう1つのアウトプットを使うと、キャッシュアウト ^{Tx} で必要なタンブラーの署名が入手できる。

69 受取人はブラインドファクターとしてランダムな数値 r を選択し、$z' = r^e z \bmod N$ を計算してブラインドしたパズル z′を得る。

用することで、タンブラー自身も送金元と送金先の関連を知ることができない。

但し、ユーザはペイメントチャネルのオープン・クローズで 2 トランザクションをブロードキャストする必要があり、手数料という意味では 1 トランザクションタイプのプロトコルと比べてコスト高となる。

また、以下が課題として挙げられる。

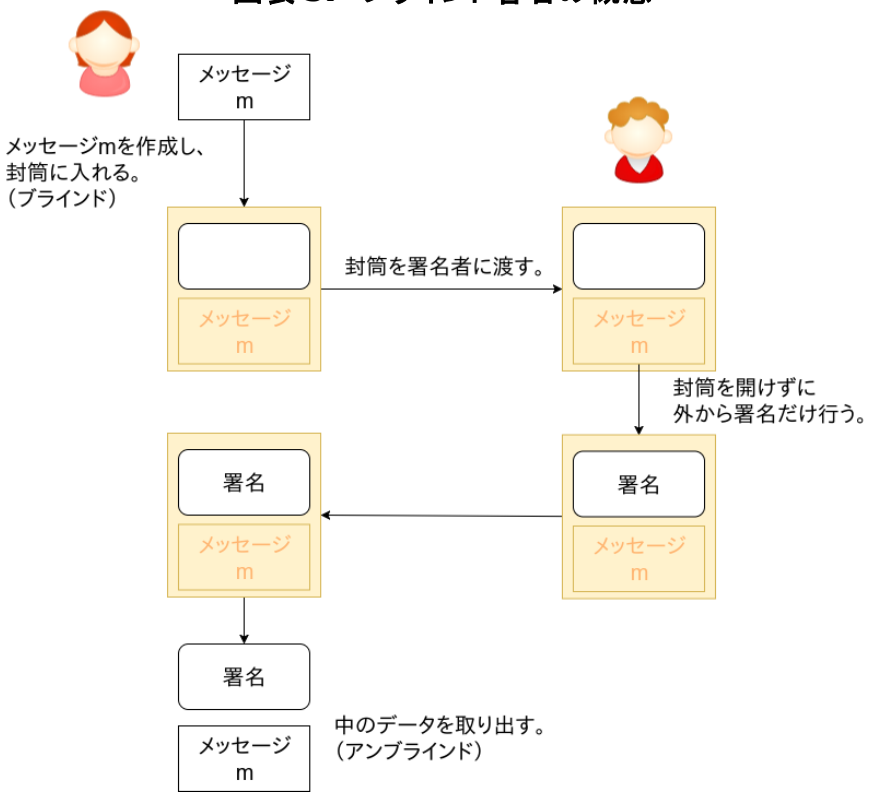
- タンブラーに対する匿名を考えた場合、CoinJoin と同様に送金するコインの量の均一化が必要である。また、利用するユーザ数（匿名セット）が十分多い必要がある（ユーザが一人ではタンブラーに送金元と送金先の関係が把握されてしまうため）。
- タンブラーは利用者全員の送金額分のコインを保持している必要がある。そのため、匿名セットを上げようとする程、タンブラーは多額の流動性を保持している必要がある。

(v) Chaumian CoinJoin

TumbleBit と同様にタンブラーが存在するモデルで CoinJoin トランザクションを構成するプロトコルが Chaumian CoinJoin になる。TumbleBit が RSA パズルを利用して送金元と送金先の関連をタンブラーに分からなくしていたのに対し、Chaumian CoinJoin では Chaum のブラインド署名を利用することで同様の特性を提供する。通常、任意のデータに対してデジタル署名をする際は、署名者は署名対象のデータについて知っているが、ブラインド署名では、署名者がメッセージのデータを知らない状態でそのメッセージに対してデジタル署名をすることができる暗号技術であり、1982 年に David Chaum によって発表された[70]（図表 37）。

70 電子投票などで、投票先は秘匿したまま、選挙管理委員会に投票の正当性を保証してもらうためにブラインド署名をしてもらうといったユースケースでの使用が考えられる。

図表 37 ブラインド署名の概念



Chaumian CoinJoin では以下の 3 つのフェーズを介して、ブラインド署名を使用することでタンブラーに送金元と送金先の関連を知られることなく、CoinJoin トランザクションを構成する（図表 38）。なお、送金人と受取人は同じ人物であってもよいが、その場合、タンブラーに同一人物であることが分からないよう、異なるアドレスを使うなど身元が把握されないよう注意する必要がある。

(1) インプット登録フェーズ

各送金人がタンブラーに対して以下の情報を提供する。

- CoinJoin トランザクションのインプットとなる未使用のコイン（UTXO）
- 未使用のコインが自分のものであることの証明[71]
- お釣りの送付先アドレス
- コインの送付先であるブラインド済みのアウトプットアドレス

タンブラーは、コインが使用済みでないか、提供された証明が正しいかを確認し、問題なければブラインドされたアウトプットに署名をし、送金人に返す。送金人はタン

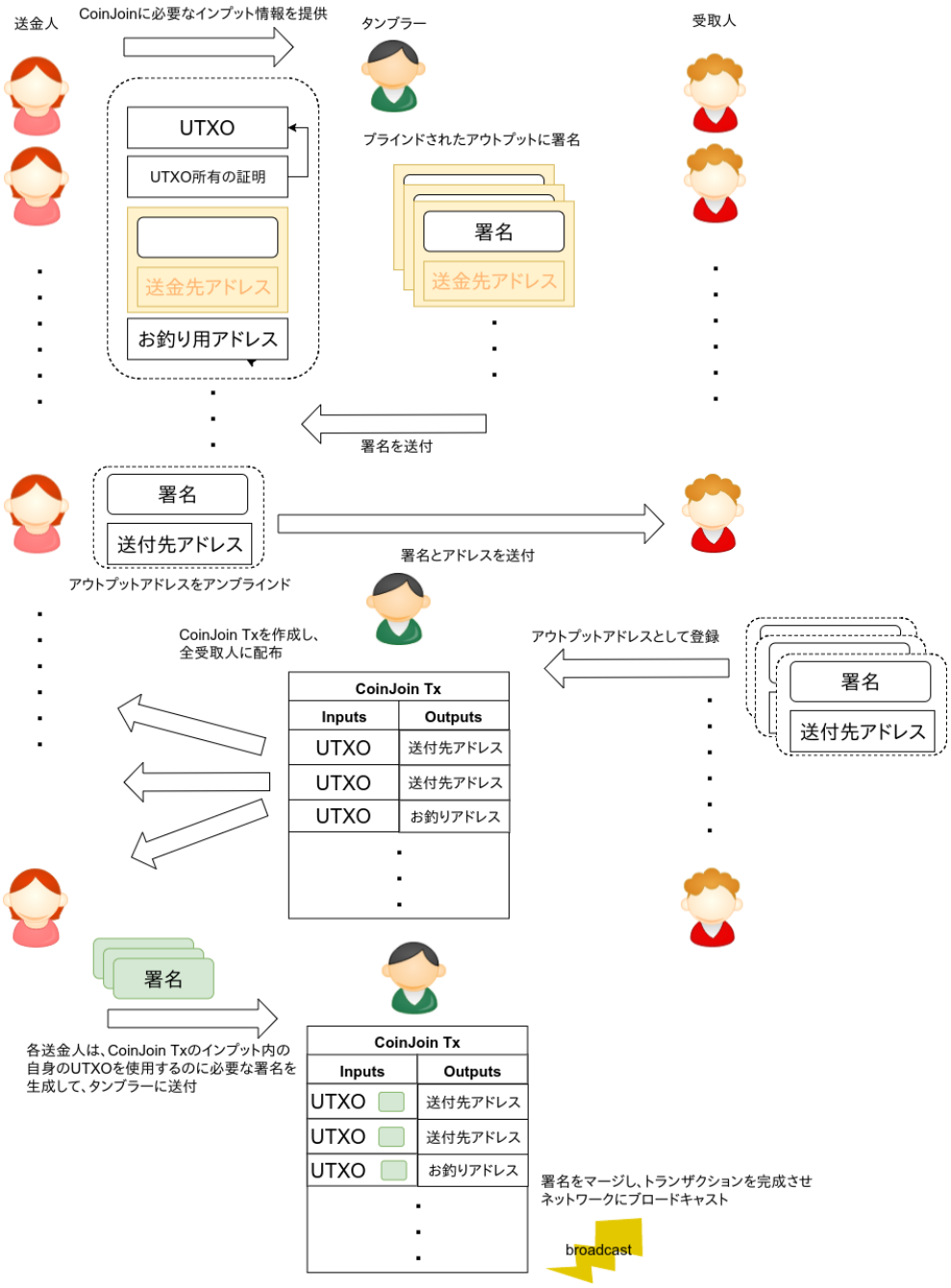
71 UTXO に紐づく秘密鍵でメッセージに署名したデータを提供することで、そのコインを使用するための秘密鍵を保持していることを証明する。

ブラーが署名したアウトプットをアンブラインドし、受取人に渡す。

(2) アウトプット登録フェーズ

受取人は署名済みのアウトプットをタンブラーに登録する。タンブラーはこの時初めて、送金先のアドレスを認識するが、このアドレスとインプット登録フェーズで提供されたブラインド済みのアウトプットアドレスとの関連を知ることはできない。

図表 38 Chaumian CoinJoin のフロー



(3) 署名フェーズ

タンブラーは未署名の CoinJoin^{Tx}を構成し、署名のため各送金人に渡す。全送金人から署名が届くと、CoinJoin^{Tx}に署名をマージし、ネットワーク上にブロードキャストする。送金人が秘密鍵を渡したり、一度タンブラーに送金する訳ではないので、タンブラーがコインを盗むことはできない。

上記のように Chaumian CoinJoin はブラインド署名を利用して送金元と送金先の関連をタンブラーに知られることなく CoinJoin のトランザクションを構成するミキシングプロトコルである。TumbleBit などの比べるとシンプルであることから、ビットコインのプライバシー保護を目的として作られたフレームワーク ZeroLink[72]で採用され、Hidden Wallet や Wasabi Wallet、Samourai Wallet などの一部のウォレットで実装されている。

但し、CoinJoin タイプのミキシングプロトコルであるため、1 トランザクションあたりの匿名セットの制限及び、送金するコインの量の均一化という制限は残る。

(vi) ValueShuffle

ValueShuffle[73]は CoinShuffle に Confidential Transaction とステルスアドレスを組み合わせたミキシングプロトコルの提案である。Confidential Transaction は 2015 年に Gregory Maxwell によって発表された、コインの量を秘匿するためのプロトコルであり、サイドチェーンの実装である Elements や Liquid、匿名通貨である Monero 等で利用されている。

通常、ビットコインのトランザクションではアウトプットに送金するコインの量が数値として明示的に記録されているが、Confidential Transaction では、この数値を秘密鍵として他のブラインドファクターと組み合わせて楕円曲線上の点（すなわち、公開鍵）にして、それをアウトプットに記録する。コインの量はその秘密鍵の一部となっていることから、このコインの量が分かるのは送金人と、それを受け取る受取人のみとなる[74]。

---

72 nopara73, GitHub, "The Bitcoin Fungibility Framework", https://github.com/nopara73/ZeroLink, 2018/12/4

73 Ruffing, T., et al., "Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin", https://eprint.iacr.org/2017/238.pdf, 2018/12/4

74 楕円曲線暗号の加法準同型性を利用しており、他のノードは全インプットの公開鍵を全て加算して出来た楕円曲線上の点から、全アウトプットの公開鍵を加算して出来た楕円曲線上の点を減算して 0 になれば、トランザクシ

CoinJoin の利便性の低さの要因の1つはアウトプットのコインの量の均一化である。これは、コインが均一化されないと、その量の違いからインプットとアウトプットの関係性が推測され、匿名性が損なわれるために必要なものであるが、Confidential Transaction のようにコインの量が秘匿できるのであれば、この制限はなくなり CoinJoin の利便性は大きく改善される。

但し、Confidential Transaction は現在のビットコインのプロトコルとは互換性がないため、ビットコインで ValueShuffle を利用することは本稿執筆時点では出来ない。

3.2.2.1.3 課題およびそれらに関連した新たな取り組み

ミキシングプロトコルは中央集権的なサービス型から、分散型のプロトコル、また集中型であっても仲介者（ミキサー、タンブラー）にコインのコントール権を渡すことなく送金元と送金先の関連を秘匿するようなプロトコルが提案され、匿名化の取り組みが進んでいる。様々なプロトコルが提案される中で、本稿執筆時点の課題としては以下の点が挙げられる。

- 匿名セットの物理的な上限

  1トランザクションでミキシングを行う CoinJoin 型のミキシングプロトコルは、匿名セットの最大数が、暗号資産のトランザクションサイズによって制限される。ビットコインであれば標準トランザクションは 100KB に制限されるため、匿名セットの最大値は 350～470 に制限される。他方で、TumbleBit のように 1 トランザクションに集約しない場合、こういった技術的な匿名セットの制限はなくなる。但し、技術的な制約がないだけで実際に十分な利用者（匿名セット）を確保できるかは別の課題となる。

- シビル攻撃への耐性

  匿名セットの上限がある場合、匿名性を破壊しようとする攻撃者によるシビル攻撃が懸念される。すなわち、攻撃者は多数の UTXO を用意し、それぞれ異なるアイデンティティとしてミキシングプロトコルに参加することで、実質的な匿名性を低下させることが可能になる。このようなシビル攻撃を防ぐには、手数料を付与する等のシビル攻撃への耐性を持つプロトコルにする必要がある。

ョン内でコインの整合性は保たれていることを検証できる。このため手数料は明示的にトランザクションに設定する必要がある。

- コインの量の均一化

  現状のミキシングプロトコルの多くは、送金するコインの量を同一に揃える必要があり、そのルールが崩れると匿名性は低下する。一方、この制約はユーザの利便性を低下させ、適切なタイミングでミキシングを行う際のハードルにもなっている。この制約を回避する手段の1つは ValueShuffle が提案するような、送金額の秘匿化と組み合わせる方法になる。匿名通貨としては Monero が送金額の秘匿化をサポートしているが、暗号資産が Confidential Transaction を導入する必要があり、ビットコインやイーサリアムなどの主要暗号資産ではこういった機能は本稿執筆時点で導入される計画はない。

- DoS 攻撃への耐性

  Chaumian CoinJoin のようなプロトコルでは、最終ステップで送金人が署名を返さないことでミキシング処理を停止させることができる。そのため、多数の UTXO を用意することで悪意あるユーザが DoS 攻撃を行いやすいといった側面がある。シビル攻撃への対策と同様、手数料の徴収など攻撃への耐性をプロトコルに組み込む必要がある。

上記の他に、ミキシングプロトコルでは、作成されたトランザクションが多数のインプットとアウトプットを持つため、ミキシングプロトコルを使用したこと自体が露呈しやすい懸念がある。そのため、トランザクション自体を隠すことができれば、より匿名性は向上すると考えられる。このコンセプトをベースとしたミキシングプロトコルを提案しているのが CoinJoinXT[75]である。CoinJoinXT ではペイメントチャネルを開くことから始まり、ペイメントチャネル外から入金したり、ペイメントチャネル外へ送金したりするトランザクションをオフチェーン上で積み重ねて一連の取引履歴を構成する。これらのトランザクションをどのようにオンチェーン上に記録するかはユーザ次第であり、また、トランザクションがオンチェーン上に現れても、それがミキシングトランザクションであることは分からないという特性を持つ。CoinJoinXT はまだ PoC レベルで[76]、実用に向けたハードルがまだ多いものの、従来とは異なるトランザクション構造を持つミキシングプロトコルが今後出てくる可能性は高いと考えられる。

75 AdamISZ, GitHub, "On-chain contracting for privacy”, https://gist.github.com/AdamISZ/a5b3fcdd8de4575dbb8e5fba8a9bd88c, 2018/12/4

76 公開済みの PoC の実証コード AdamISZ, GitHub, "Multi-transaction contracts/joins. POC code only.", https://github.com/AdamISZ/CoinJoinXT-POC, 2018/12/4

3.2.2.2 ステルスアドレス

3.2.2.2.1 背景

ビットコインの送金にあたっては、送金先となるアドレスを指定する。このアドレスは「口座番号」のようなものであり、公開鍵から生成される。対となる秘密鍵は受取人のみが保持する。ここで、同一のアドレスを複数のトランザクションで使い回すと、それらのトランザクションは同一人物（ないし、秘密鍵を共有し得る極めて親しい間柄の人物）が関与したトランザクションであると考えられるため、ビットコインでは決済の都度、新しいアドレスの生成・使用が推奨されている。この場合、決済の都度、受取人が送金人に送付先アドレスを QR コード等を用いて伝える必要がある。

送金が一度だけであれば上記のやり方でも十分だが、例えば不特定多数からの寄付を受けるために一般に広く送金先アドレスを公開する必要がある場合は、複数の送金が同一のアドレスへ送られることになり、同一人物宛の送金であることが第三者に容易に把握されてしまう。同様に、複数回支払いを受ける際に同一のアドレスを使い回す場合も、同一人物宛の送金であることが第三者に容易に把握されてしまう。

上記の問題を解決するために、代表となるアドレス（以下、代表アドレス）は公開するものの、それは送金先アドレスとしては使わず、実際の送金先アドレスはワンタイムアドレスとして都度ランダムに生成する仕組みがステルスアドレスである（図表 39）。ワンタイムアドレスを利用することで、同一人物宛の送金かどうか第三者が把握することは困難となる。このためには、送金人と受取人双方だけが送金先アドレス（すなわち、それを構成する公開鍵）を共有する一方、受取人だけが当該資金を利用可能とする（すなわち、受取人のみが対となる秘密鍵を取得可能とする）必要がある。

楕円曲線 Diffie-Hellman 鍵共有（Elliptic Curve Diffie-Hellman key exchange, 以下 ECDH）プロトコルに基づくステルスアドレスの初期の概念は 2011 年 4 月に Bitcoin Forum で”ByteCoin”というアカウント名義で発表された[77]。その後、改良したプロトコルが Peter Todd から提案されたが[78]、ビットコインでは採用されず[79]、現在は

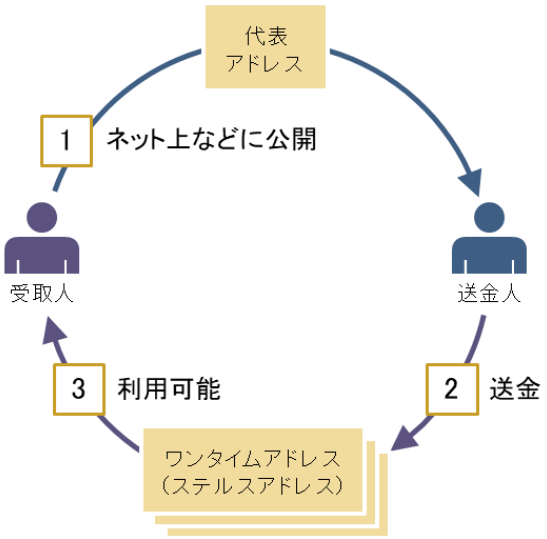
77 ByteCoin, Bitcoin Forum, "Untraceable transactions which can contain a secure message are inevitable. ", https://bitcointalk.org/index.php?topic=5965.0, 2018/11/8

78 Todd, P., Bitcoin-development, "Stealth Addresses", https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-January/004020.html, 2018/11/8

79 ステルスアドレスはブロックチェーンのコンセンサスアルゴリズム等に影響を与えずに導入可能であり、ノードやウォレットなどのアプリケーションレベルで Bitcoin にも導入可能である。同様のコンセプトが BIP-47 として定義され、Samourai Wallet や Billion app など一部のウォレットでサポートされている。

匿名通貨である Monero 等で採用されている。

図表 39 ステルスアドレスの概念図



3.2.2.2.2 仕組み

Monero の実装で用いられる CryptoNote を例に、送金人から受取人へステルスアドレスを利用してコインを送金する仕組みについて以下に記載する。

(i) ワンタイムアドレスへの送金

コインの受取人は予め自身の2つの公開鍵（A、B）を代表アドレスして公開しておく。2つの鍵のうち、片方は受取人が自身宛の着金の検知のためにブロックチェーンを走査するのに使用し、もう片方は受け取ったコインを使用する際に使用する。

以下の手順により、送金人は受取人の2つの公開鍵（A、B）と自身が生成するランダムな値（r）からコインの送付先アドレスを導出する（**エラー! 参照元が見つかりません。**）。

(1) 送金人は受取人の代表アドレスから、受取人の公開鍵 A, B を抽出する。

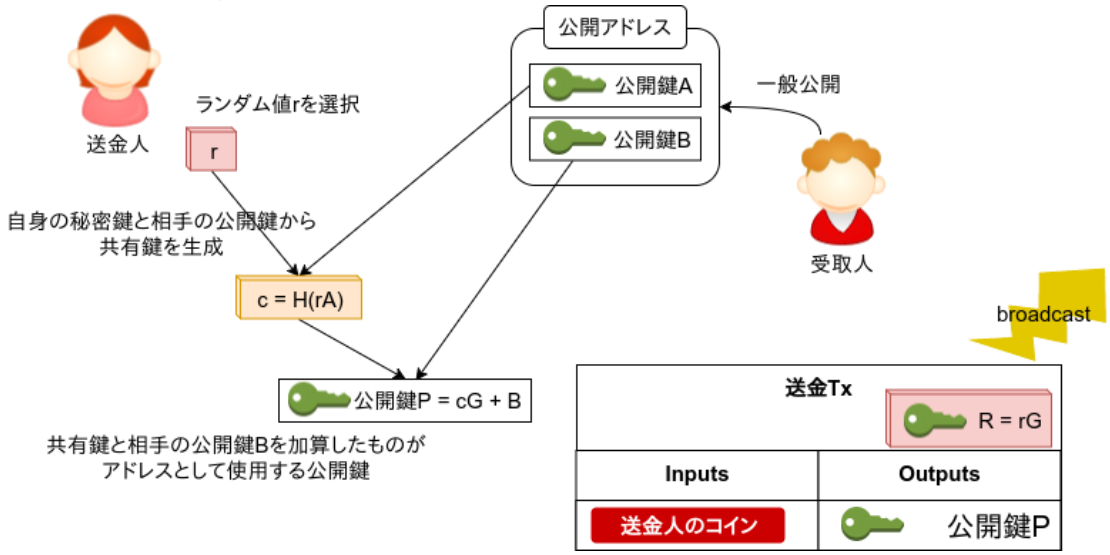
(2) 送金人はランダムな値 r、および r を秘密鍵とした場合に対となる公開鍵 R を生成する。そして送金人の秘密鍵 r と受取人の公開鍵 A から共有鍵 c を生成し、これに受取人の公開鍵 B を加えて、新たな公開鍵 P を生成する[80]。公開鍵 P から得られたアドレス $P^{address}$ が送付先アドレスとなる。

80 ハッシュ関数 H と、楕円曲線の生成点 G を使って、P = H(rA)G + B により算出される。

(3) ここで、c は、送金人の秘密鍵 r と受取人の公開鍵 A から生成できるとともに、送金人の公開鍵 R と受取人の秘密鍵 a からも生成できるため、送金人・受取人双方で共有される共有鍵となる点がポイントとなる。

(4) 送金人は送金先アドレスを P とする送金トランザクションを作成し、送金人の公開鍵 R をトランザクションに含める。送金人は作成した送金トランザクションをブロックチェーンネットワーク上にブロードキャストする。

図表 40 ステルスアドレス（ワンタイムアドレスへの送金）



(ii) 受取人による着金の検知

受取人はブロックチェーンを常時監視し、以下の手順により、受信したトランザクションが自身宛のトランザクションかどうかを確認する（図表 41）。

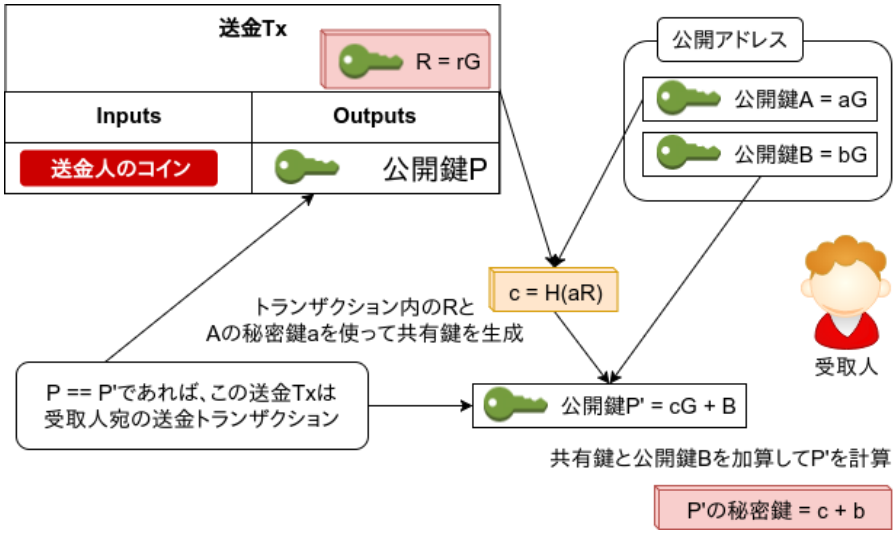
(1) 受取人はトランザクションから送金人の公開鍵 R を抽出する。

(2) 受取人は自身の公開鍵（A、B）と対応する秘密鍵（a, b）を用いて、送金人の公開鍵 R と受取人の秘密鍵 a から共有鍵 c を生成し、これに受取人の公開鍵 B を加えて、新たな公開鍵 P'を生成する[81]。

(3) もし公開鍵 P'から得られたアドレス $P'^{address}$ と、当該トランザクションの送金先アドレス $P^{address}$ が一致すれば、自身宛のトランザクションと考えることができる。

81 P' = H(aR)G + B により算出される。rA と aR は等しいため、P = P'となる。

図表 41 受取人による着金の検知



(iii) 受信コインの利用

受取人が受信したワンタイムアドレス $P^{address}$（すなわち、$P'^{address}$）宛のコインを使用するのに必要な秘密鍵 x は、受取人の秘密鍵（a, b）と送金人の公開鍵 R を使って生成可能である[82]。ここで、秘密鍵 x は送金人には生成できない点がポイントとなる。

以上のように、ステルスアドレスとは、受取人の公開鍵と送金人がランダムに選択した値を秘密鍵とした鍵ペアを利用して共有鍵を生成する仕組みであり、これは二者間で自分の秘密鍵と相手の公開鍵から共有鍵を生成する Diffie-Helman 鍵共有プロトコルを利用した仕組みとも言える。

3.2.2.2.3 課題およびそれらに関連した新たな取り組み

当初のステルスアドレスの提案では、受取人が公開する公開アドレスには1つの公開鍵しか含まれていなかったが、この場合、着金を検知するためにブロックチェーンを走査する際に必要な秘密鍵と、受け取ったコインを利用する際に使用する秘密鍵が同じものとなる。コインの利用に必要な秘密鍵を常時使用することは安全性の観点でリスクが高いと考えられる。また、受取人は着金検知のためブロックチェーンを常時監視することが必要となる。

上記の課題を克服するため、着金検知で用いる走査用の鍵と、コインの利用で用いる鍵の2つを用いる現在の方式が採用されることとなった。このように2つの鍵を用いることにより、受取人が着金検知用の秘密鍵とコインを利用する際の公開鍵を、信

82 x = H(aR) + b により算出される。

頼できる第三者に渡す形で、着金監視をアウトソースすることも可能となった。そのため、スマートフォンなどで動作する SPV（Simplified Payment Verification）クライアント（所謂、軽量クライアント）を用いる場合に、何らかの事業主体などの信頼できる第三者に着金監視をアウトソースすることができるようになった。

3.2.2.3 リング署名

3.2.2.3.1 背景

ビットコインの送金にあたっては、そのトランザクションにどのアドレスからどのアドレスへいくらのコインが送付されたという情報が含まれ、それらは全てブロックチェーン上に記録される。これらの記録からアドレス間の送金の流れを第三者が容易に把握することができる。また、トランザクションのインプットが複数存在するようなトランザクションにおいては、それらのインプットの所有者は同じ人物であるというヒューリスティックなどを用いて分析されることが多い[83]。このようなトランザクションの入出力の関連付けをできなくすることで、送金の匿名性を向上させる仕組みの1つが CryptoNote で提案されているリング署名[84]である。

3.2.2.3.2 仕組み

CryptoNote のプロトコルでは、リング署名を利用し、実際に送金するコイン以外のダミーのコインをトランザクションのインプットに混ぜ送金対象のコインを分からなくすることで、入出力の関連付けをできなくする（図表 42）。

(i) ダミーインプットの選択

送金トランザクションを作成する際に、まずインプットとなる送金対象のコインを用

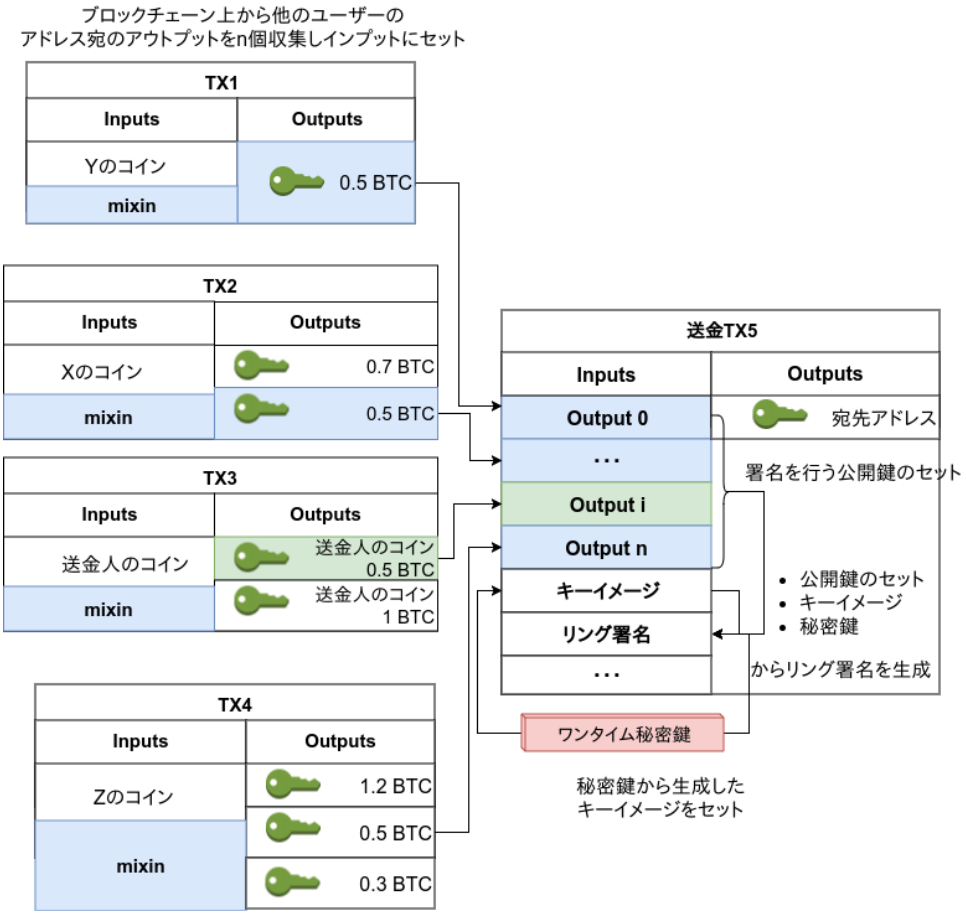
83 ミキシングのトランザクションのような特殊なトランザクションを除き、このヒューリスティックを元に分析するサービスが多いが、最近は、一般的な二者間の取引においても、このようなヒューリスティックを破壊しプライバシーを向上させるための提案が出ている。これらの提案は、通常のコインの送金時に、トランザクションにインプットに受信者のコインも混ぜて送金トランザクションを構成することで、インプットの所有者が同一人物であるというヒューリスティックを破壊する。
Blockstream, Blockstream Corp, "Improving Privacy Using 2018-08-08 (P2EP)", https://blockstream.com/2018/08/08/improving-privacy-using-pay-to-endpoint/, 2018/11/15
bitcoin, GitHub, "BIP79: a practical coinjoin protocol", https://github.com/bitcoin/bips/blob/master/bip-0079.mediawiki, 2018/11/15

84 リング署名は暗号学的には、それぞれが鍵を持つユーザグループにおいて、任意のメンバーが実行できるデジタル署名の一種で、グループ内の誰かによって署名されたことは明らかになるが、誰が署名したのかは分からないという特性を持つ。

意する。具体的には、実際に送金するアウトプットと同じ量のコインを持つ他のユーザが所有するアウトプットを n 個ブロックチェーン上から選択し、トランザクションのインプットにセットする。この時選択するアウトプットは直近 10 ブロックより古いブロックのアウトプットで、5日以内の最近のアウトプットから n 個の内 25%をランダムに選択し、残り 75%は古いアウトプットから三角分布を使って選択される[85]。このようにトランザクションに含めるものの実際には使用しないダミーのアウトプットを mixin と呼ぶ。

このトランザクションに含まれる一つインプットが実際に使用される送金人のものである確率は 1/(n+1)となる。n の数が多い程、匿名性が強化される反面、署名のデータサイズは O(n+1)で、n の数が増えるほど署名のデータサイズも線形に増加する。このため n を増やすほどトランザクションの手数料は高額になる。

図表 42 Monero のトランザクションイメージ



上記の方法で、インプットを選択したトランザクションにリング署名を使用して署名すると、インプットにある多数のコインの内、実際に送金されているものは1つのみであり、それがどれかは分からないトランザクションになる。多数のインプットを加えるこ

85 2015 年 4 月から三角分布による収集が適用され、それ以前は一様分布により収集されていた。

とで誰からの送金か分かりにくくするという点ではミキシングで使用される CoinJoin と似た方法であるとも言える。

(ii) キーイメージの生成

トランザクションの各インプットには、実際に送金に使用するアウトプットと mixin に加えキーイメージをセットする。このキーイメージは実際に使用するコインに紐づく秘密鍵から生成される値で秘密鍵毎に一意になる[86]。生成されたキーイメージから元の秘密鍵や対応する公開鍵を復元することはできない。そのためこのキーイメージがインプット内のどのアウトプットのものかを判断するのは、秘密鍵の保持者以外には不可能と言える。

このキーイメージはコインの二重使用を防ぐために用いられる。トランザクションに mixin を含めると、実際に使用されたアウトプットがどれかは送金人にしか分からないため、他のノードから二重使用の検証ができないという問題が残る。あるアウトプットが、多数のトランザクションのインプットにあり、そのうち、複数のトランザクションがダミーではなく実際にそのアウトプットを使用する場合、どちらかは二重使用にあたるため、使用不可能にする必要がある。そのため、各ノードは、トランザクションインプットにセットされているキーイメージと同一のキーイメージがこれまで使用されていないかどうか検証することで、コインの二重使用を防ぐ。

(iii) リング署名の生成

最後に送金に使用するアウトプット、mixin、キーイメージからリング署名を生成する。通常のデジタル署名であれば公開鍵・秘密鍵の鍵ペアとデジタル署名は1対1で対応し、署名はある公開鍵に対応した秘密鍵を使って作られたことが明らかになる。他方で、リング署名では、複数の鍵ペアを使って1つのデジタル署名を作成し、そのデジタル署名はどの公開鍵に対応した秘密鍵で行われたのか分からないが、指定した公開鍵のセットの内のいずれかの秘密鍵で署名されたことが保証される。

ここでは、公開鍵のセットは、トランザクションの各インプットが参照する公開鍵のセットで構成されるが、そのインプット内で実際に使用するインプットに紐づく秘密鍵を使って署名が行われる。他のノードはトランザクション内の署名を確認しても、トランザク

86 秘密鍵の値 x とした場合、その公開鍵の値は P = xG となり（G は楕円曲線の生成点）、キーイメージは I = xHp(P)で計算される（Hp は特殊なハッシュ関数で、楕円曲線上の点を入力として取り、ランダムな楕円曲線上の点を返す）値となる。つまり公開鍵からランダムな点を算出し、さらにその点を秘密鍵で乗算した点＝公開鍵がキーイメージとなる。

ション内のいずれかのインプットに紐づく秘密鍵で署名されたことは分かるが、そのインプットを特定することはできず、トランザクションで実際に使用されるインプットが何であるかは分からない。

3.2.2.3.3 課題およびそれらに関連した新たな取り組み

2017 年 4 月に Monero に関して、リング署名を利用しても、以下のヒューリスティックにより匿名性が損なわれる危険性があるという報告もなされており[87]、匿名性を維持するためには、利用者の注意が必要な部分もある。

- ダミートランザクションが存在しない場合

  ダミーインプットなしでトランザクションを構成すると、インプットには実際に送付するアウトプットのみとなり送金元が確実に特定できる。これは単に、このトランザクションの匿名性が損なわれるだけでなく、他のトランザクションの匿名性にも影響を与える。例えば、他のトランザクションのインプットに、ダミーインプットなしのトランザクションで使用されたアウトプットが使われた場合、そのアウトプットは確実に送金元が分かるため、トランザクションに含まれる取引全体の匿名性が低下する。当初の取引ではダミーインプットなしのトランザクションが多くを占めていたため、インプットの 95%以上が追跡可能であった。

  この問題は、最小リングサイズ（mixin の数）の指定が必須となったことで 2016 年 3 月に解消される。そしてその後のハードフォークで最小リングサイズは徐々に引き上げられ、2018 年 10 月のハードフォークで 11（ダミーインプット数は 10）になっている。最小 mixin が 2 に設定された直後にインプットの追跡可能性は 65%まで低下し、その後の最小リングサイズの増加と共に追跡可能性は低下し、本稿執筆時点では、このヒューリスティックを利用した再識別は非常に困難となっている。

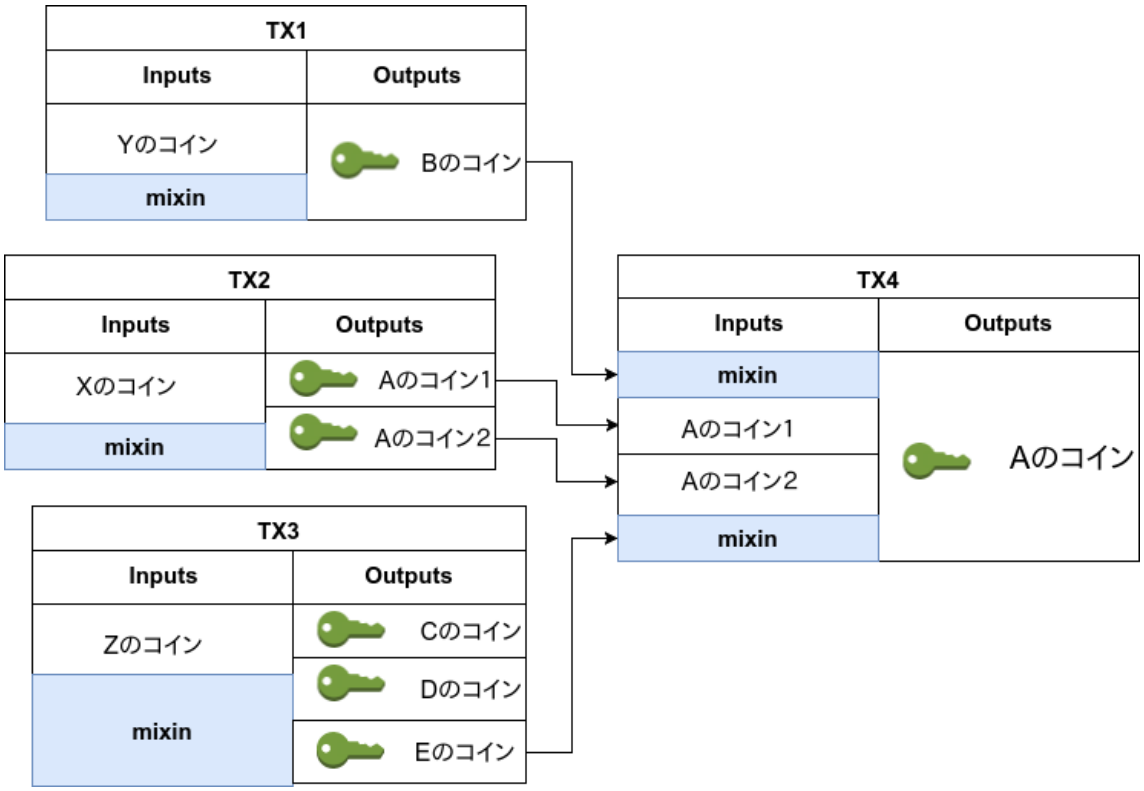
- アウトプットのマージ

  2つめのヒューリスティックは、複数のインプットを持つトランザクションを作成する場合、各インプットに mixin するアウトプットを収集する際に、複数のインプットで同一トランザクションのアウトプットを選択する可能性は低いという仮定に基づく。

87 Kumar, A., et al, Eprint, "A Traceability Analysis of Monero's Blockchain", https://eprint.iacr.org/2017/338.pdf, 2018/11/13

例えば図表 43 は、ユーザが 1 つのインプット（mixin は 1 つ）と 2 つのアウトプットを持つトランザクション TX2 を作成し、その後、2 つのインプット（A のコイン1、A のコイン2）と1つのアウトプットを持つトランザクション TX4 を作成した場合を示している。この場合、TX4 の 2 つのインプットがそれぞれ同一トランザクション TX2 を参照している。このようなケースでは上記の仮定に基づき TX4 が実際に使用するインプットは TX2 の 2 つであると識別される可能性が高い。このように単一のトランザクションのアウトプットを別のトランザクションでマージするようなトランザクションは、匿名性を維持する上では問題となる。

図表 43 アウトプットのマージ



- 時系列分析

3 つめのヒューリスティックは、古いトランザクションアウトプット（TXO）ほど、多くのトランザクションで mixin 候補として選択される確率が高いという仮定に基づいている。この仮定の下では、リング署名を作成する際に利用されるインプットのセットにおいて、その中で 1 番ブロック高が高い（すなわち、最も新しい）アウトプットが実際に使用されるものである可能性が高いと考えられる。

この問題は、mixin するアウトプットを収集する際の確率密度関数を変更することで改善可能と報告されているが、本稿執筆時点では確率密度関数は変

更されておらず三角分布を継続して使用している。

3.2.2.4 ゼロ知識証明

3.2.2.4.1 背景

ゼロ知識証明とは、相手に秘密の値は秘匿したまま、秘密の値を知っていることを検証させる証明方式であり、Goldwasser らによって定式化された[88]。ゼロ知識証明では以下に挙げる 3 つの要素を満たす必要がある[89]。

- 完全性（completeness）

  証明者が秘密の値を知っているのであれば、必ず検証者が承認することができる証明を提出できる。

- 健全性（soundness）

  証明者が秘密の値を知らないのであれば、基本的には、証明者の提出した証明は検証者による検証を通らない[90]。

- ゼロ知識性（zero-knowledge）

  証明者が秘密の値を知っているのであれば、検証者は「証明者は秘密の値を知っている」という事実以外何もわからない。つまり、検証者が秘密の値を知ることはできない。

以下では、上記の要素を満たすゼロ知識証明の簡単な例について記載する。 前提として、ある暗号化関数 E を定義する。E(x)には、E(x)の値から秘密の値 x を類推できないという性質があり、一般には離散対数問題や素因数分解問題の困難性を利用したものが E として用いられる。また、E(x)で暗号化された値を、暗号化されたままの状態で計算可能にする、準同型性[91]をもつ。つまり、E(x) + E(z) = E(x+z)が成り

88 Goldwasser, S., et al., "The knowledge complexity of interactive proof systems", SIAM Journal on Computing, Philadelphia: Society for Industrial and Applied Mathematics, 18 (1): 186-208, doi:10.1137/0218012, ISSN 1095-7111, 2018/12/13

89 Wikipedia, "Zero-knowledge proof", https://en.wikipedia.org/wiki/Zero-knowledge_proof#Definition (last edited on 2018/12/10 15:53 UTC), 2018/12/11

90 これは殆ど全ての場合において成り立つ必要があるが、（理論的には偶然に検証を通ることもあり得るため）常に成り立つ必要はない。

91 準同型暗号とは暗号化された数を暗号化されたまま計算可能であるという性質のことである。特に、zk-SNARKs では検証時間の高速のため、また検証時に掛け算を1度だけ行えば良いという特性からレベル 2 準同型暗号が用いられる。より詳しい説明は Wikipedia, "準同型暗号",

立つという性質である。上記の 2 つの性質を持つ関数は RSA 暗号で使われている関数などが該当する[92]。ゼロ知識証明では、この暗号化関数 E を用いて、証明者が秘密の値 x を秘匿したまま検証者に証明者が確かに x を持っていることを確信させるために、次のやり取りを行う[93]（図表 44）。

(1) 証明者はランダムな数 r を暗号化した値 a = E(r)と秘密の値 x を暗号化した y = E(x)を検証者に送る。

(2) 検証者は、証明者に 1 もしくは 0 である数 b を返す。

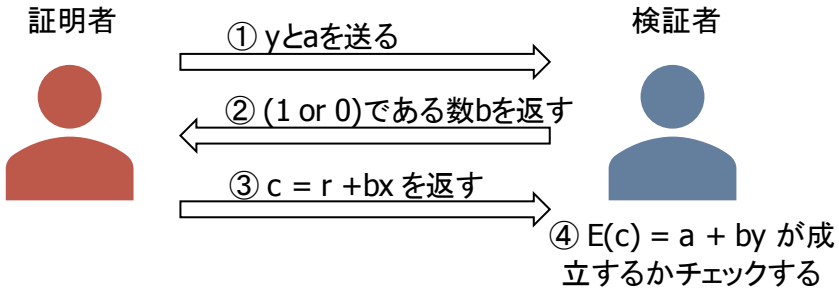
(3) 証明者は検証者から渡された b を用いて、c = r + bx を返す。検証者は r の値を知らないので、c から x を復元することはできない。

(4) 検証者は証明者から渡された値、c を用いて、E(c) = a + by つまり E(C) = E(r) + bE(x)が成立するか確認する。

上記の一連のやり取りを、証明者はランダムな数 r を、検証者は b を変えながら複数回行うことで、証明者が x を保持している確率を高める。そのため、このやり方は対話型のゼロ知識証明と分類されることがある。

図表 44 ゼロ知識証明の例

※y = E(x), a = E(r)とする



①～④までのやり取りを、rとbの値を変えながら複数回行う。

ゼロ知識証明の一種である zk-SNARK とは Zero-Knowledge Succinct Non-

---

https://ja.wikipedia.org/wiki/%E6%BA%96%E5%90%8C%E5%9E%8B%E6%9A%97%E5%8F%B7, 2018/12/14 および、Mitsunari, S., SlideShare, "ペアリングベースの効率的なレベル 2 準同型暗号（SCIS2018）", https://www.slideshare.net/herumi/2scis2018, 2018/12/14 などを参照。

92 Reitwiesner, C., GitHub, "zkSNARKs in a Nutshell", http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf, 2018/12/11

93 土井, "ゼロ知識証明入門 情報セキュリティ大学院大学公開講座『暗号入門7講』", http://lab.iisec.ac.jp/~arita/pdf/lecture3.pdf, 2018/12/12

Interactive Argument of Knowledge の略であり、検証が簡易であり（Succinct）、知識の証明が非対話（NonInteractive）で行われ、計算によって知識を証明する（Argument of Knowledge）といった性質をもつゼロ知識証明（Zero-Knowledge）を指す。zk-SNARKs は Gennaro らによって発表された Quadratic Span Programs（QSP）[94]および、Parno らによって発表された Pinocchio Protocol[95]などを発展させたものであり、Ben-Sasson らによって整理された[96]。zk-SNARKs は NP 完全問題[97]に対してもゼロ知識証明を可能にする仕組みであり、汎用性が高いと言える。

zk-SNARKs は匿名通貨である Zerocash や Zcash 等で取引を秘匿するために用いられている。また、2017 年 10 月には イーサリアム にも zk-SNARKs が導入[98]された。イーサリアムでは Zcash 等と同様に情報を秘匿する目的の他、トランザクションの検証コストの削減としての利用も検討されている[99]。ただし、 イーサリアム に実装された機能は zk-SNARKs で用いられる検証機能のみである[100]。そのため、鍵の生成ステップ（トラステッドセットアップ）や証明データの作成はオフチェーンで行う必要がある。特に、トラステッドセットアップは、秘匿する対象が変わる毎（証明に用いる関数が変わる毎）に行う必要があり、実運用では難しい場面が生じ得る。

以下では、この zk-SNARKs について記載する。

94 Gennaro, R., et al., ePrint, "Quadratic Span Programs and Succinct NIZKs without PCPs", https://eprint.iacr.org/2012/215.pdf, 2018/12/13

95 Parno, B., et al., ePrint, "Pinocchio: Nearly Practical Verifiable Computation", https://eprint.iacr.org/2013/279.pdf, 2018/12/13

96 Ben-Sasson, E., et al, Eprint, "Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture", https://eprint.iacr.org/2013/879.pdf, 2018/12/13

97 NP 完全問題とは計算の複雑性の度合いを指す用語であり、Non-deterministic Polynomial time（非決定性多項式時間）の略である。多項式時間で検算可能な問題（NP）のうち、最も難しい問題を指す。例えば、大きさと金額が指定された複数の品物を一定容量のナップザックに詰め込む際に、合計の価値が閾値より大きく成る組み合わせが存在するかどうかという部分和問題は NP 完全問題とされる。

98 Ethereum Team, Ethereum Blog, "Byzantium HF Announcement", https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/, 2018/12/12

99 vbuterin, Ethereum Research, "On-chain scaling to potentially ~500 tx/sec through mass tx validation", https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477, 2018/12/12

100 Reitwiessner, C., Ethereum Blog, "An Update on Integrating Zcash on Ethereum (ZoE)", https://blog.ethereum.org/2017/01/19/update-integrating-zcash-ethereum/, 2018/12/12

3.2.2.4.2 仕組み

(i) 処理の流れ

zk-SNARKs は大きく、鍵生成ステップ、証明データ作成ステップ、証明データ検証ステップの三つに分けられる[101]（図表 45）。

- 鍵の生成ステップ（トラステッドセットアップ）

  最初に、ある秘密の値 r と証明に用いる関数 C から証明鍵（pKey）と検証鍵（vKey）を生成する。証明鍵（pKey）と検証鍵（vKey）は一般に公開され、共通参照文字列 (common reference string、以降 CRS)と呼ばれる。

  他方で、秘密の値 r は誰にも知られてはならない。これは r を知っている人は検証に成功する、偽の証明データを作成可能となるためである。そのため、このステップは信頼の置ける第三者によって行われることが前提であり、一般にトラステッドセットアップ（Trusted Setup）と呼ばれる。

- 証明データの作成

  証明者は、トラステッドセットアップで生成された証明鍵（pKey）、広く公開される情報 X と、公開情報 X を導出するのに利用した秘密の情報 s を用いて、証明データ prf を生成する。証明者は、秘密情報 s を秘匿したまま、証明データ prf を検証者に1度だけメッセージを送信することで（つまり非対話な方法で）証明を行う。

  ここで、C(s) = X であり、情報 X は証明に用いる関数 C に入力値 s を代入することで算出される値である。一例を挙げると、証明に用いる関数 C をハッシュ値の同値性を確認する関数、秘密情報 s を任意の値（シークレット）、公開情報 X を s のハッシュ値という例が考えられる[102]。

- 証明データの検証

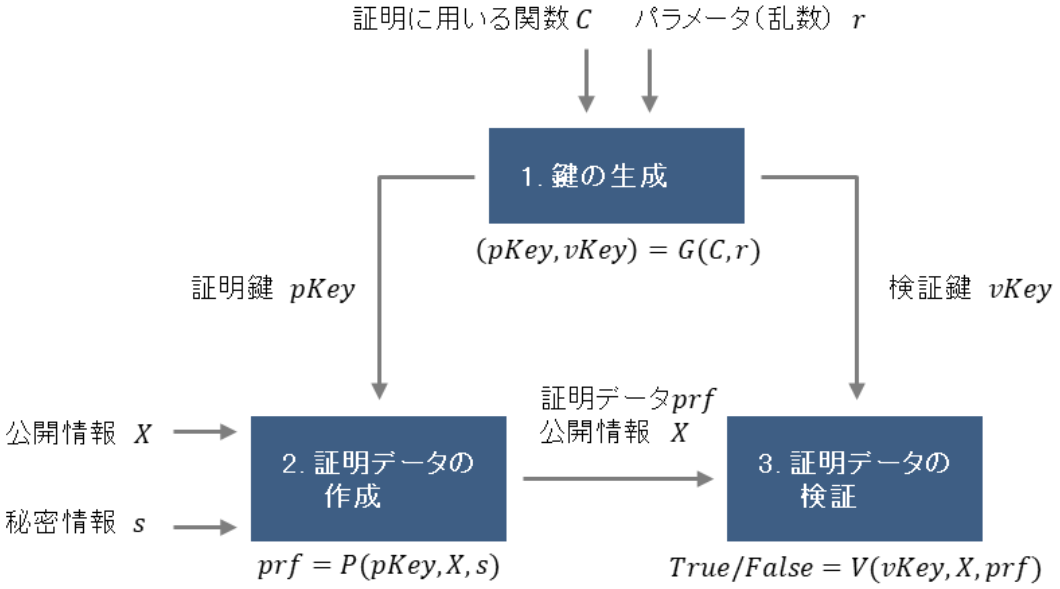
  検証者は、トラステッドセットアップで生成された検証鍵（vKey） 、証明者が生成した証明データ prf、公開情報 X を用いて、証明データ prf が「正しいか否か」を調べる。検証者は準同型暗号を用いて乗算を行うのみであるため検証に

101 ZOOM, "イーサリアムに導入されたプライバシー保護技術「zk-SNARK」とは", https://zoom-blc.com/what-is-ethereum-zk-snark, 2018/12/13

102 ただし、公開情報 X が一切存在しない（すなわち、一切公開しない）場合もあり得る。

要する計算コストは証明者が証明を生成するのに比べて非常に小さい。また、証明を行いたい問題が複雑でも、証明データサイズは非常に小さい[103]。

図表 45 zk-SNARKs の利用イメージ



(ii) 特徴

トラステッドセットアップにおいて、zk-SNARKs では以下の 3 つの手順を経て、多くの問題をゼロ知識証明の検証が可能な形式へ変換する[92]。

(1) 検証機の生成

証明に用いる関数は、証明を行いたい問題から 2 つの多項式の 2 次方程式 t(x)h(x) = w(x)v(x)の形に変換される（図表 46）。そして、検証者は、この 2 つの多項式の等価性を検証することで、証明データが証明を行いたい問題を正しく計算した結果であることを確認する。

上記の 2 つの多項式は元の問題とは全く別の関数になる。そのため、元の問題が同じであれば（秘匿する対象が同じであれば）、同じ検証機を使い回すことが可能だが、元の問題が変わる場合は新しい検証機を作り直す必要がある。

(2) ランダムサンプリングによる検証の簡易化

検証機は 2 つの多項式の等価性を調べるものであるが、多項式のまま等価性を検証するのは非常に計算コストがかかる。そのため、ある評価点 a についての

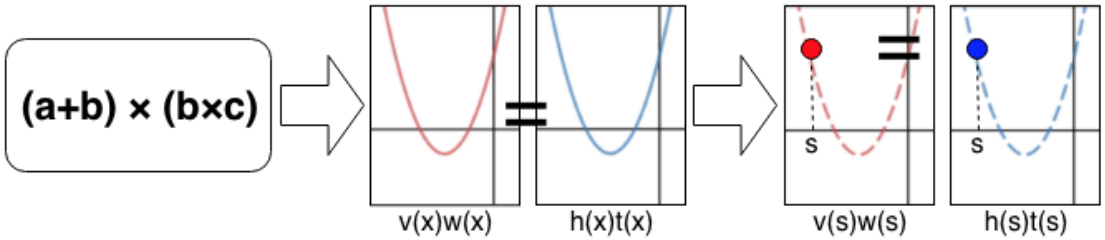
103 Zcash Company, "What are zk-SNARKs?", https://z.cash/ja/technology/zksnarks/, 2018/12/14

等価性を検証することとしている。これにより、検証者は単純な掛け算の結果の等価性を検証するだけで済むため、証明データサイズと検証時間が大幅に短縮される。なお、この場合、証明者は検証機の関数のうち、 評価点 a を送るのではなく、w(a)、v(a)、h(a) をそれぞれ個別の値として検証者に送る。検証者は、自身で t(a)を算出し証明者から送られてきた値を用いて t(a)h(a)=w(a)v(a)が成立するかを検証することになる[104]。

(3) パラメータの暗号化

トラステッドセットアップにおける秘密の値 s が分かると、検証に成功する偽の証明データを生成することが可能である。そのため、秘密の評価点 s は準同型暗号 E を用いて暗号化され、その結果が証明鍵（pKey）となる。また、この時に検証を簡易にするために、もう一つの秘密の値を用いて検証鍵(vKey)を生成する。最終的に zk-SNARKs の証明・検証はこれらの鍵を用いて行われる。

図表 46 zk-SNARKs の変換ステップのイメージ（ここでは、例として二次関数のグラフを記載している、ある評価点を用いて等価性の評価を行う）



(iii) 課題およびそれらに関連した新たな取り組み

zk-SNARKs の主な問題点として以下のような点が挙げられる。

- 信頼の置ける第三者による鍵生成の必要性

トラステッドセットアップでは、検証に成功する偽の証明データの生成を防ぐため、トラステッドセットアップで用いられる秘密の値 r は誰にも知られてはならない。Zcash では秘匿対象が支払い情報のみであるため、証明に用いる関数は 1 つのみであるが、イーサリアムのスマートコントラクトでは様々な問題があり得る。しかし、イーサリアムでは、zk-SNARKs によって秘匿された情報を検証

104トラステッドセットアップで用いる秘密の値 r の一部が、ここでの評価点 a に相当する。トラステッドセットアップとは、いわば評価点 a を暗号化するステップと考えることもできる。

する関数をサポートしているのみであり、 CRS（共通参照文字列）の安全なセットアップ方法については利用者に委ねられている。そのため、この CRS のセットアップを安全な方法でサポートすることは現在課題として挙げられている[105]。

この点は、Zcash では Multi-Party Computation という方式を用いて解決している。 Multi-Party Computation とは複数人が秘密の値を持ち寄り CRS を生成する方式である。この方式を利用する場合、参加者のうちの誰かが自身の提出した秘密の値を削除するだけで、CRS を生成する元となった秘密の値が復元できなくなる。Zcash では CRS の生成のために持ち寄った値をそれぞれの参加者が各々方法で処分することで、秘密の値は誰からも秘匿されているとしている[106]。

近年では、トラステッドセットアップを不要とする zk-STARKs（Zero-Knowledge Scalable Transparent ARguments of Knowledge）[107]や Bulletproofs[108]等が提案されているが、逆に証明データが増加するなどの問題も生じている。

- 計算量と証明データのサイズ

zk-SNARKs は、証明に用いる関数の複雑性による影響が大きく、問題が複雑な場合、特に証明データを作成する時間が長くなる。そのため、問題の複雑性にあまり影響を受けない zk-STARKs が提案されているが、さらに改善が試みられている。

図表 47 zk-SNARKs と他の手法との比較[109]

評価軸	zk-SNARKs	zk-STARKs	Bulletproofs
Algoritmic complexity: prover	O(N * log(N))	O(N * poly-log(N))	O(N * log(N))
Algoritmic complexity: verifier	~O(1)	O(poly-log(N))	O(N)

105 Zcash が公開している CRS を利用することで、暗号トークンを作成するプロジェクトなどもあるが、実用的に使うためには更なる改良が必要とされている。ConsenSys, GitHub, "Project Alchemy", https://github.com/ConsenSys/Project-Alchemy, 2018/12/12

106 Zcash Company, "Parameter Generation", https://z.cash/technology/paramgen/, 2018/12/12

107 Ben-Sasson, E., et al., ePrint, "Scalable, transparent, and post-quantum secure computational integrity", https://eprint.iacr.org/2018/046.pdf, 2018/12/12

108 Bunz, B., et al, Eprint, "Bulletproofs: Short Proofs for Confidential Transactions and More", https://eprint.iacr.org/2017/1066.pdf, 2018/12/12

109 gluk64, Github, "Awesome zero knowledge proofs (zkp)", https://github.com/gluk64/awesome-zero-knowledge-proofs, 2018/12/12 より三菱総研作成

Communication complexity (proof size)	~O(1)	O(poly-log(N))	O(log(N))
- size estimate for 1 TX	Tx: 200 bytes, Key: 50 MB	45 kB	1.5 kb
- size estimate for 10.000 TX	Tx: 200 bytes, Key: 500 GB	135 kb	2.5 kb
EVM verification gas cost	~600k (Groth16)	~2.5M (estimate, no impl.)	N/A
Trusted setup required?	YES	NO	NO
Post-quantum secure	NO	YES	NO
Crypto assumptions	Strong	Collision resistant hashes	Discrete log

- 量子耐性

  zk-SNARKs は、離散対数問題の困難性を利用した楕円曲線暗号を用いているが、これは量子コンピュータに対する耐性（量子耐性）がない。そのため、zk-STARKs では、量子耐性のある衝突困難ハッシュ関数を用いた方法が提案されている。

- 秘匿内容を変更する際の数学的素養の必要性

  zk-SNARKs では幅広い問題に対して証明・検証機を生成できるが、そのためには、証明したい問題を正しい数式を用いて表す必要がある。また、証明を行いたい問題が正しく NP 問題に含まれているかといった必要十分条件の確認も必要である。これらの要素は一般的にはプログラミングの領域ではなく、数学領域の知識が必要とされる領域である。そのため、zk-SNARKs を用いて任意の問題の検証機を作成したい場合は、数学に関する深い知識が必要とされ、一般のプログラマが zk-SNARKs を用いて任意の問題に対して秘匿プロトコルをつくり出すハードルは高いと言える。

zk-SNARKs を利用したプロジェクトとしては、送金元と送金先の関係を秘匿するミキシングに用いるもの（Miximus[110]）、トランザクションの検証コストを削減することでスケーラビリティ改善に用いるもの（RollUp[111]）、開発効率改善を目指し、証明データの作成関数と検証用スマートコントラクトの生成を自動化するフレームワークを提供するもの（Zokrates[112]）などが挙げられる。ただし、Miximus ではデポジットできる回数

110 miximus, "Miximus - Decentralized Ethereum Mixer", https://github.com/barryWhiteHat/miximus, 2018/12/12
111 roll_up, "roll_up", https://github.com/barryWhiteHat/roll_up, 2018/12/12
112 ZoKrates, "ZoKrates", https://github.com/Zokrates/ZoKrates, 2018/12/12

に制限がある、RollUp では証明データの生成に非常に時間がかかるなど、未だ克服すべき課題も残されている。

3.2.2.5 ライトニングネットワーク

3.2.2.5.1 背景

ビットコインの用いるコンセンサスアルゴリズムである Proof of Work（以下、PoW）の主な問題点として、以下の三点が挙げられる。

- 1 秒間に取引可能な件数が 4-5 件程度に留まること

  ビットコインのパフォーマンスの低さはスケーラビリティ問題として広く知られており、根本的な解決策が長年模索されてきた。

- 取引が完了したと見なされるまでに長い時間を要すること

  一般的には、当該取引を含むブロックが生成されてから、概ね 6 ブロック程度後続のブロックが生成されると取引完了と見なす。この場合、ある取引を含むトランザクションがブロックチェーンネットワーク上にブロードキャストされてから、当該取引が完了したと見なせるまで、最低でも 1 時間程度の時間がかかることになる[113]。

- 取引の都度、手数料が必要となること

  マイナーがブロックを生成する上では、手数料の高い取引から優先的にブロックに取り込むと考えられるため、全体として手数料の高騰を招く懸念がある。また、取引の都度手数料がかかることは、マイクロペイメントなどの用途にビットコインを用いることを困難とする懸念がある。

上記に挙げた問題点の解決策として、Joseph Poon と Thaddeus Dryja の共著として 2015 年に提案された手法がライトニングネットワークである[114]。ライトニングネッ

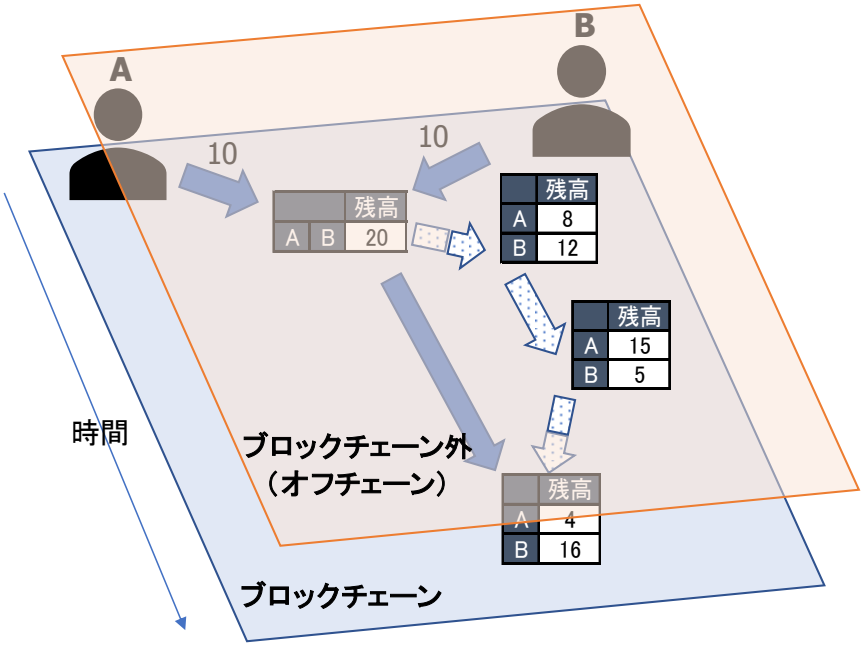
113 実際には、あるトランザクションがブロードキャストされてから、中継ノードによる複数回のブロードキャストを経て、マイナーのメモリプールに取り込まれ、次に、ブロック生成にあたりマイナーがメモリプールに格納されているトランザクション群から当該トランザクションを選び出し、当該ブロックが生成されてから 6 ブロック程度後続ブロックが生成される、という一連の処理が必要となるため、実態としては 1 時間より相当程度長くなることが予想される。クリスマスシーズンなど、多くのトランザクションがブロードキャストされる時期では、1 週間以上かかることもあると言われている。

114 Poon, J., et al., "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", http://lightning.network/lightning-network-paper.pdf, 2018/11/30

トワークにより、ビットコインのスケーラビリティ問題の解決、即時決済、手数料の低減等が見込まれている。

ライトニングネットワークの基本的なコンセプトは、ブロックチェーン上に記録する取引を最小限とし、ブロックチェーン外（以下、オフチェーン）で取引を行うというものである（図表 48）。このコンセプトから派生して、以下の特徴が挙げられる。

図表 48 ライトニングネットワークのコンセプト

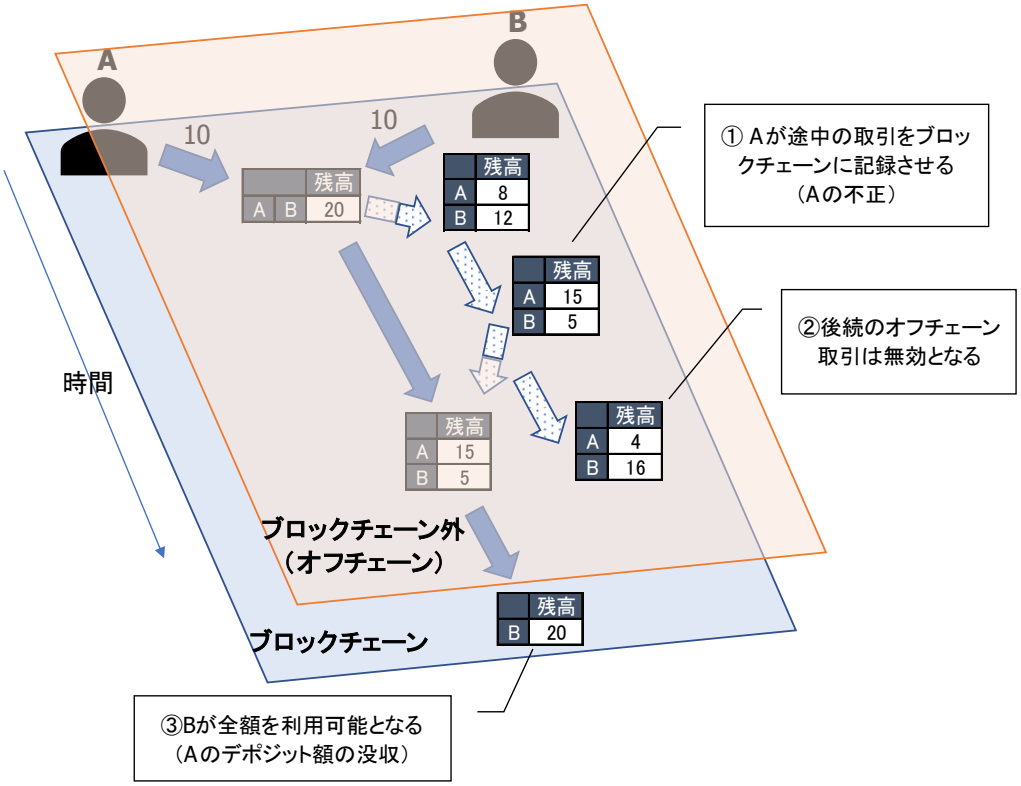


ブロックチェーン上には、当事者間の最初と最後の取引のみ記録し、途中の取引履歴は記録しない
（オフチェーンでの取引は、最初の取引でデポジットされた資金の範囲内に限られる）

- 取引当事者が互いに相手を信頼せずとも（トラストレスであっても）安全に取引を行えること

  ブロックチェーン上には記録されないオフチェーンで取引の大半を行うが、取引当事者の片方が不正を行った場合、不正を行った側がペナルティを受ける（最初にデポジットした全額を相手方に没収される）形としている（図表 49）。

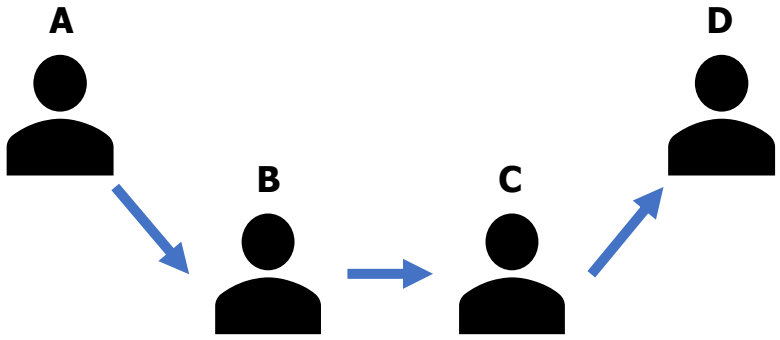
図表 49 トラストレスに安全に取引を行う仕組みのイメージ



- 二者間の取引を組合せ、任意の二者間の取引を可能とすること

二者間でのオフチェーン取引を可能とする仕組みをペイメントチャネルというが、ペイメントチャネルを開いた取引当事者以外に、直接ペイメントチャネルが開かれていない当事者間においても、他のペイメントチャネルを組合せて取引を行うことが可能である（図表 50）。

図表 50 ペイメントチャネルの組合せのイメージ

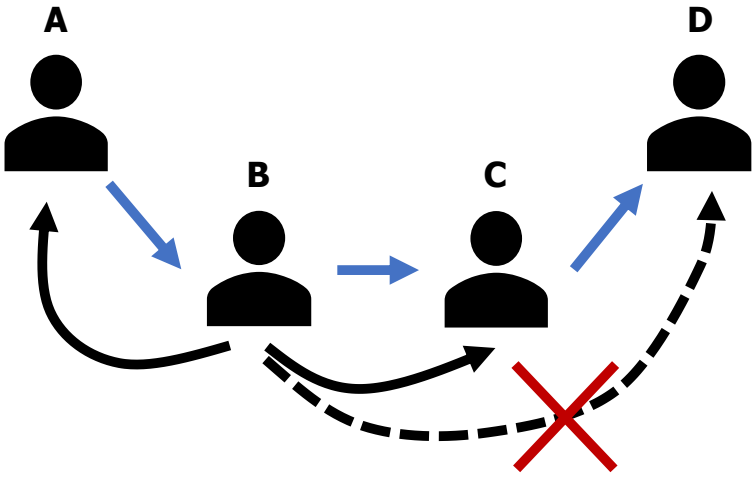


ペイメントチャネルを開いていない当事者間（A、D）であっても、他のペイメントチャネルを経由して、取引が可能

- ペイメントチャネルの組合せにあたっては、Tor と同様の Onion Routing が用いられ、匿名性が確保されること

ペイメントチャネルを経由した取引においては、起点ノードがルートを決定する。送信ノードは経路上の中継ノードおよび最終ノードの公開鍵から生成した共通鍵によって送信データを複数回暗号化するため、中継ノードは自身の直前の送信ノードと次の宛先ノードしか知ることができず、元々の送信ノードや最終的な受信ノードが分からないことになる。そのため、Tor 等の匿名通信と同様に、中継ノードの数を増やすほど、匿名性の強度が増すことになる（図表 51）。

図表 51 ペイメントチャネルの匿名性のイメージ



各中継ノードは前後1ホップは把握できるが、それ以上のノードは把握できない

ライトニングネットワークが提案された当時は、技術的な制約から、ライトニングネットワークの利用にあたってセキュリティ上の問題が存在した。具体的には Segregated Witness（以下、SegWit）が当時は導入されていなかったため、取引当事者双方がオフチェーンで保持するトランザクションはトランザクション展性問題により改変される危険性が存在した。2017 年 8 月 23 日に SegWit がビットコインに導入されたことで、ライトニングネットワークが可能となる下地が出来た。

現在、Blockstream 社、Lightning Labs 社、ACINQ 社、Nayuta 社など複数の開発グループが協力しながら、それぞれ異なるプログラミング言語でライトニングネットワークの実装を進めているが、他方で仕様の改訂[115]も続いており、実用段階に至るにはある程度時間がかかることが予想される。

115 Lightning Network に関する仕様は BOLT (Basis of Lightning Technology)という名称で公開されている。lightningnetwork, GitHub, "Lightning Network In-Progress Specifications", https://github.com/lightningnetwork/lightning-rfc, 2018/11/15

3.2.2.5.2 仕組み

Poon と Dryja によって提案されたライトニングネットワークの仕組み [114] について以下に記載する。ライトニングネットワークを用いた二者間の取引は以下の 4 つのステップから構成される。以降ではステップ毎に分けて記載する。

(i) ペイメントチャネルの構築

(ii) ペイメントチャネルの更新（オフチェーン取引）

(iii)ペイメントチャネルのクローズ

(iv)複数のペイメントチャネルを経由した送金

(i) ペイメントチャネルの構築

ライトニングネットワークを用いる取引当事者 A、B は初めにペイメントチャネルを開く必要がある。具体的には、以下の手順を行う（図表 52）。

- ファンディングトランザクションの作成

  (1) A と B は双方でデポジットする額を取り決める。ペイメントチャネル構築後のオフチェーンの取引では、デポジット額の範囲内で取引を行うことになる。

  (2) B は自身の公開鍵を A に伝える。A は B の公開鍵と自身の公開鍵を組合せて 2-of-2 のマルチシグアドレス（$AB^{address}$）を生成する。ここで、このマルチシグアドレスへ送金されたコインを利用するには、A と B 双方の秘密鍵が必要となる。

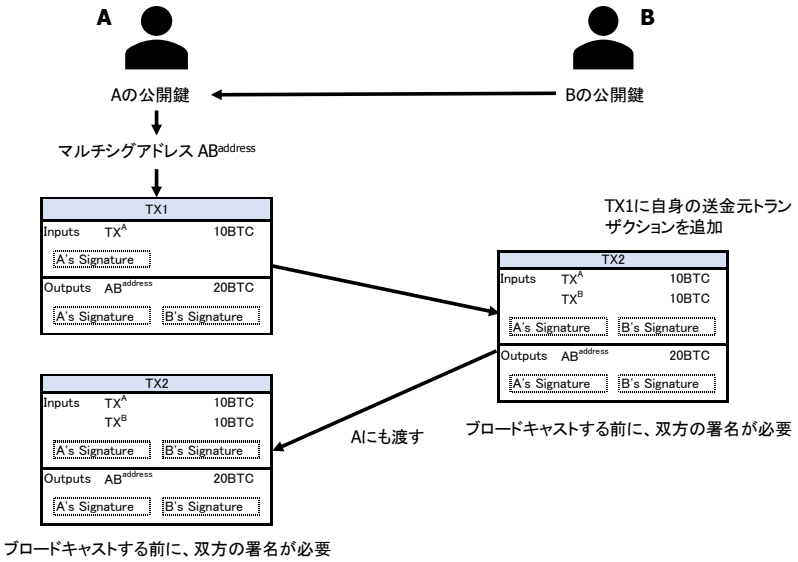
  (3) A は送金元を自身のトランザクション、送金先を $AB^{address}$ とするトランザクション TX1 を作成し、B へ渡す。ここで、$AB^{address}$ に送金するコインの総額は、予め A と B のデポジット合計額とする。

  (4) B は、TX1 の内容を確認して問題なければ、自身のトランザクションも送金元として追加したトランザクション TX2 を作成し[116]、A へ渡す。ここで、ブロックチェーン上に TX2 をブロードキャストするには、A と B 双方の署名が必

116 例えば、最初の取引において取引当事者のどちらか片方からしかデポジットできないなど、本稿執筆時点の実装では差異も見られる。

要となるため、まだ A と B のどちらもブロードキャストすることはできない。

図表 52 ファンディングトランザクションの作成



- コミットメントトランザクションの作成

以降では A が B へ 2BTC 送金する場合を考える（図表 53）。

(1) A と B はそれぞれランダムな値（以下、シークレット）$r1^A$、$r1^B$、およびそのハッシュ値 $R1^A$、$R1^B$ を生成し、お互いに $R1^A$、$R1^B$ を交換する。

(2) A は送金元をファンディングトランザクション TX2、送金先を A のアドレス（8BTC）および特殊なアドレス（12BTC）とするトランザクション $TX3^A$ を作成し、自身の秘密鍵で署名する。ここで、特殊なアドレス宛のコインは、B のシークレット $r1^B$ を A が掲示すれば[117]A が利用可能であるが、指定した時間[118]が経過すると B も利用可能となる。

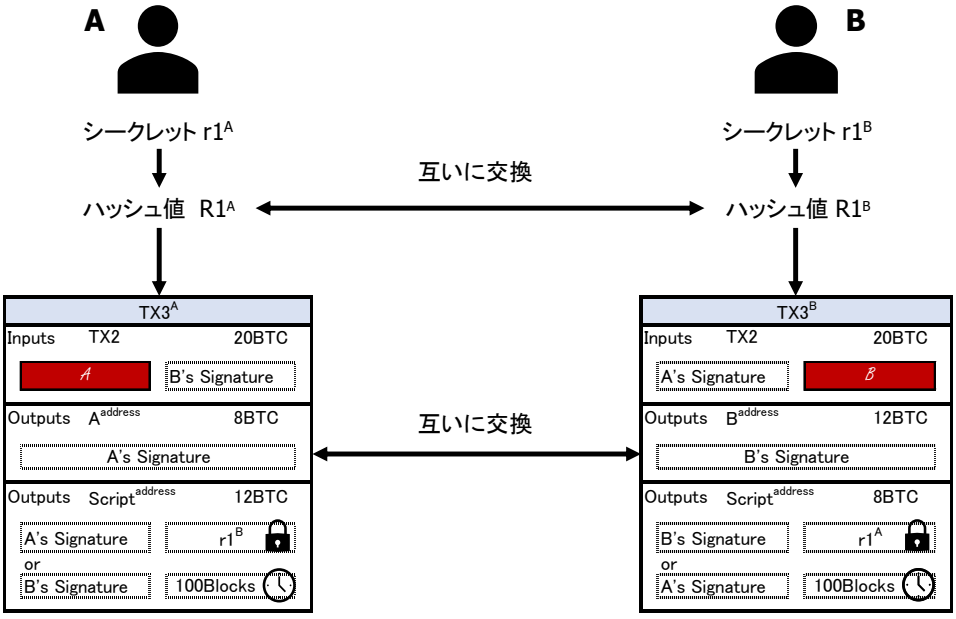
(3) 同様に、B も送金元をファンディングトランザクション TX2、送金先を B のアドレス（12BTC）および特殊なアドレス（8BTC）とするトランザクション $TX3^B$ を作成し、自身の秘密鍵で署名する。ここで、特殊なアドレス宛のコインは、A のシークレット $r1^A$ を B が掲示すれば B が利用可能であるが、指定した時間が経過すると A も利用可能となる。

117 正確には「ハッシュ値が $R1^B$ と等しい値」と指定する。そのため、この段階で、シークレット $r1^B$ を直接トランザクションに記録することはない。

118 実際には、時間ではなくブロック数で指定しており、指定したブロック数生成された後に利用可能となる。Bitcoin では BIP-112 で導入された OP_CHECKSEQUENCEVERIFY (OP_CSV)を用いる。ここで、絶対時刻でなく、相対的な時間で定義しているのは、ペイメントチャネルをクローズする時刻が事前には分からないためである。

(4) A と B は $TX3^A$、$TX3^B$ を交換する。

図表 53 コミットメントトランザクションの作成[119]



お互いに自身の署名を付せば、ブロードキャストすることが可能

➢ ファンディングトランザクションのブロードキャスト

(1) この段階に至って、A（ないし B）がファンディングトランザクション TX2 に自身の署名を付して、相手へ渡す。ここで、A が TX2 を改竄した場合、それを送金元とする $TX3^A$、$TX3^B$ は無効となる[120]。

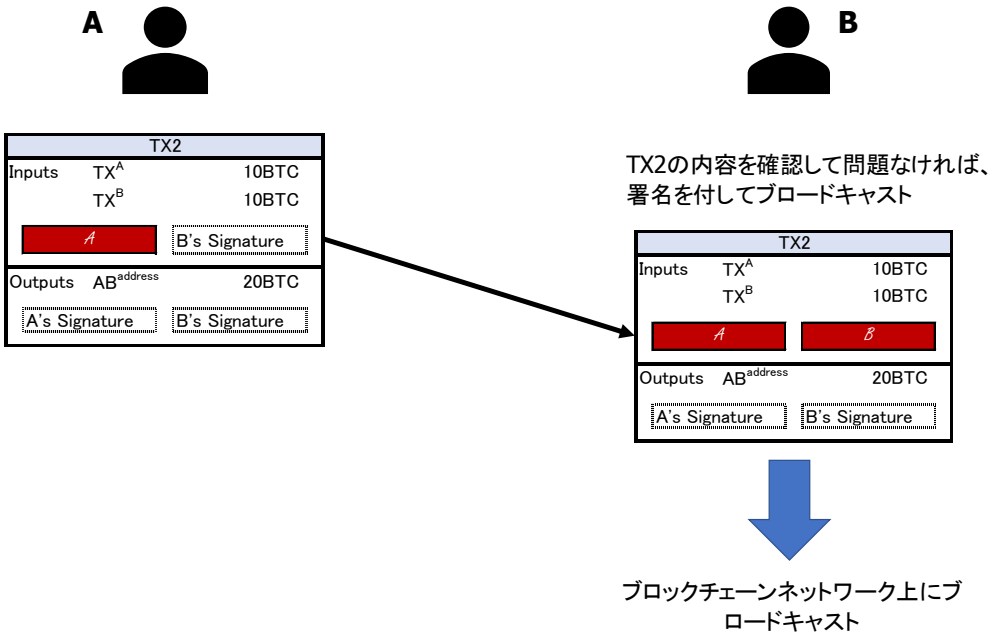
(2) B は、TX2 の内容を確認して問題なければ、自身の署名を付して、ブロックチェーンネットワーク上にブロードキャストする。TX2 がブロックに取り込まれると、ペイメントチャネルが開かれたことになる。ここで、TX2 には A の署名が付されているため、B が TX2 を改竄すると、TX2 およびそれを送金元とする $TX3^A$、$TX3^B$ は全て無効となる。

ファンディングトランザクションがブロックに格納された時点で、A と B の間のペイメントチャネルが構築されたことになる（図表 54）。

119 $TX3^A$ のアウトプットの上段では、正確にはシークレット $r1^B$ と指定はせず、「ハッシュ値が $R1^B$ と等しい値」と指定する。また下段では、一定数のブロックが生成された後に利用可能となることを、例として 100 ブロックとしている。

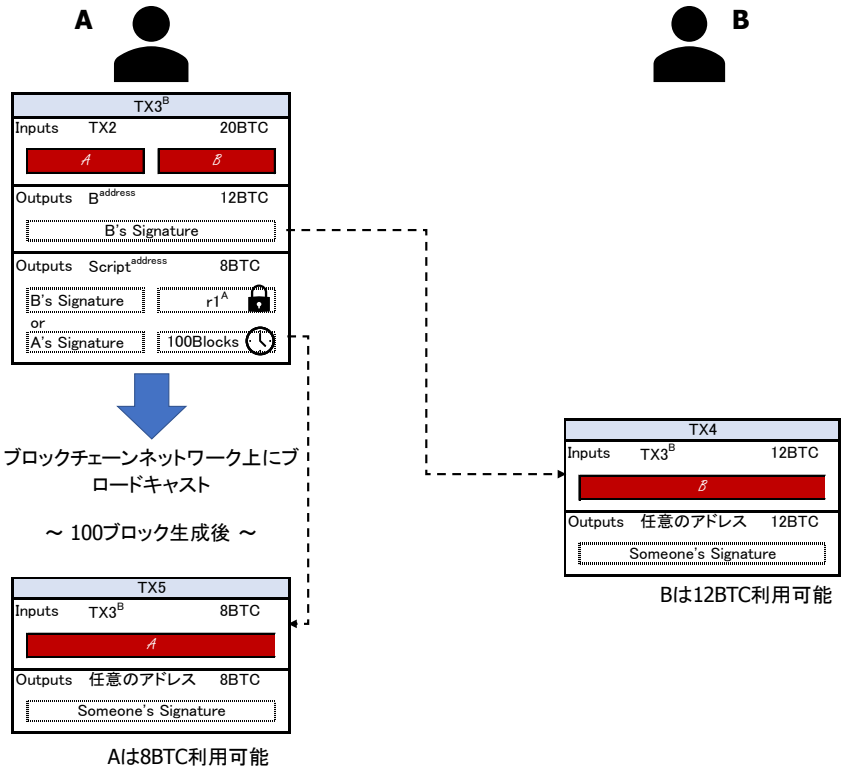
120 ブロードキャスト時の確認にて無効とされ、ブロードキャストできない。もしブロードキャスト出来た場合も、マイナーを含む他のノードで無効なトランザクションと判断され、排除される。

図表 54 ファンディングトランザクションのブロードキャスト



上記の手順を終えた後、もし A が $TX3^B$ をブロードキャストした場合、B が 12BTC を利用可能となる。ただし、B には A のシークレット $r1^A$ が分からないため、残りの 8BTC は一定時間経過後に A が利用可能となる（図表 55）。B が $TX3^A$ をブロードキャストした場合も同様である。

図表 55 コミットメントトランザクション $TX3^B$ がブロードキャストされた場合



(ii) ペイメントチャネルの更新

ペイメントチャネルを構築した取引当事者 A、B は、コミットメントトランザクションの手順を繰り返すことで、オフチェーン取引を行う。以降では B が A へ 7BTC 送金する場合を考える（図表 56）。

(1) A と B はそれぞれシークレット $r2^A$、$r2^B$、およびそのハッシュ値 $R2^A$、$R2^B$ を生成し、お互いに $R2^A$、$R2^B$ を交換する。

(2) A は送金元をファンディングトランザクション TX2、送金先を A のアドレス（15BTC）および特殊なアドレス（5BTC）とするトランザクション $TX4^A$ を作成し、自身の秘密鍵で署名する。ここで、特殊なアドレス宛のコインは、B のシークレット $r2^B$ を A が掲示すれば A が利用可能であるが、指定した時間が経過すると B も利用可能となる。

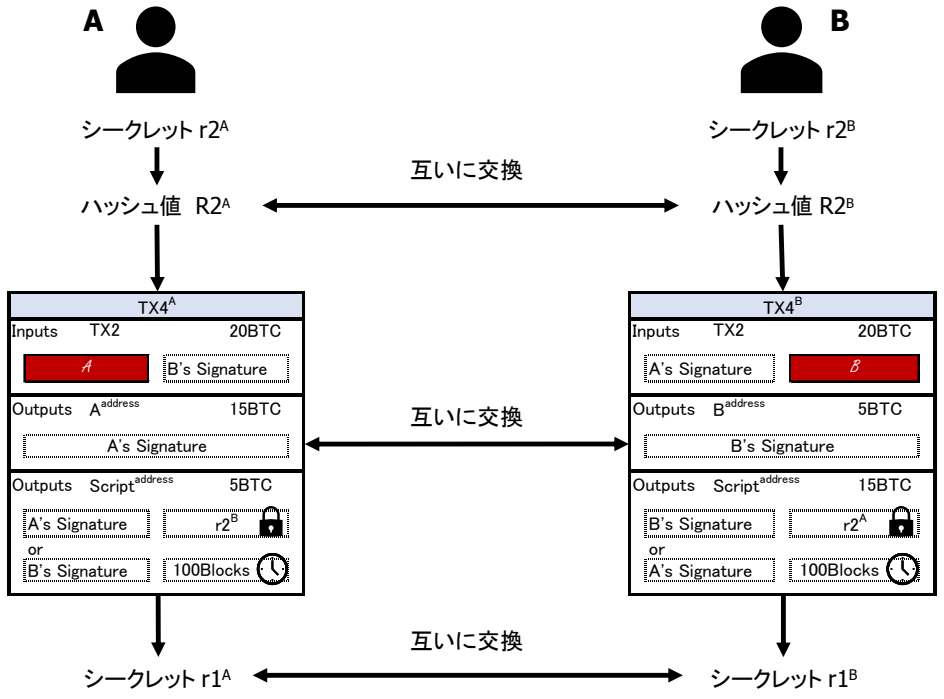
(3) 同様に、B も送金元をファンディングトランザクション TX2、送金先を B のアドレス（5BTC）および特殊なアドレス（15BTC）とするトランザクション $TX4^B$ を作成し、自身の秘密鍵で署名する。ここで、特殊なアドレス宛のコインは、A のシークレット $r2^A$ を B が掲示すれば B が利用可能であるが、指定した時間が経過すると A も利用可能となる。

(4) A と B は $TX4^A$、$TX4^B$ を交換する。また、新たなコミットメントトランザクション交換後（ないし交換時）に、前回のコミットメントトランザクションで用いた双方のシークレット $r1^A$、$r1^B$ を交換する。

このように、ペイメントチャネルの更新においては、同一のファンディングトランザクションを送金元として、最新の状態を更新する処理を繰り返す（図表 57）。

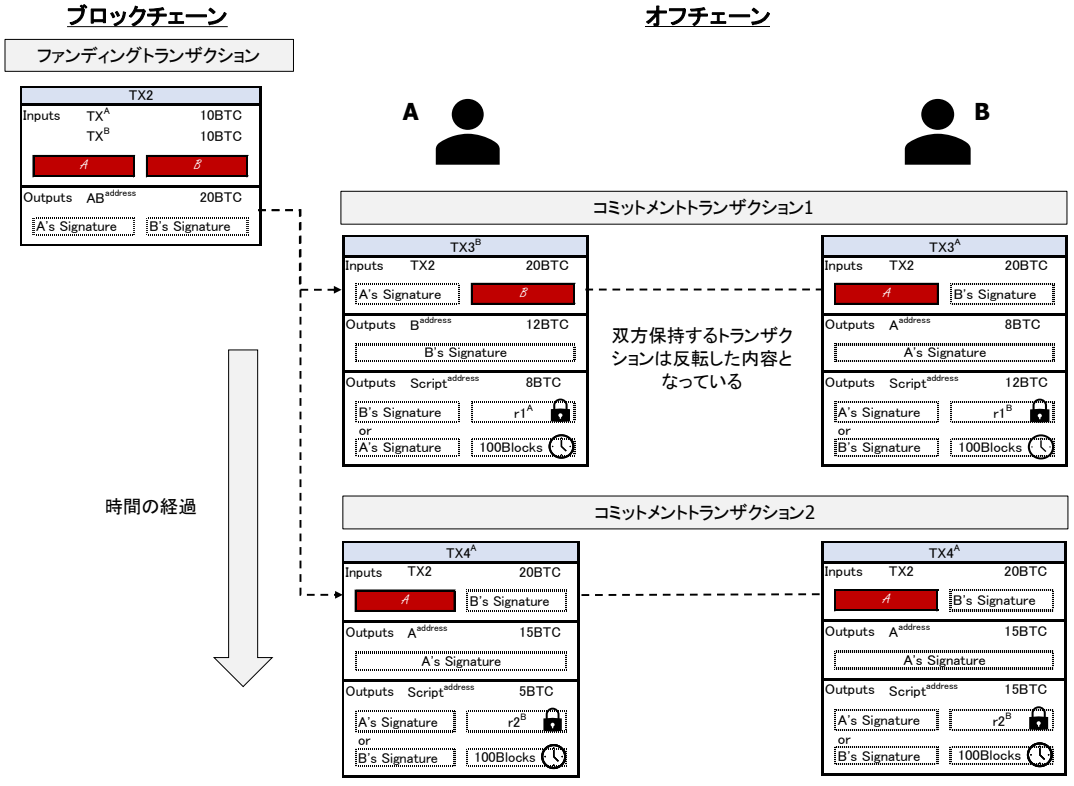
そしてペイメントチャネルをクローズする際には、A か B のどちらかが最新のコミットメントトランザクションに自身の署名を付してブロックチェーンネットワーク上にブロードキャストする。コミットメントトランザクションがブロックに格納されると、図表 55 と同様に、双方その時点の取引結果に応じたコインが利用可能となる。

図表 56 ペイメントチャネルの更新（コミットメントトランザクションの作成）



前回のコミットメントトランザクションのシークレットを交換する
（トランザクションは、お互いに自身の署名を付せば、ブロードキャストすることが可能）

図表 57 ペイメントチャネルの更新の意味



…

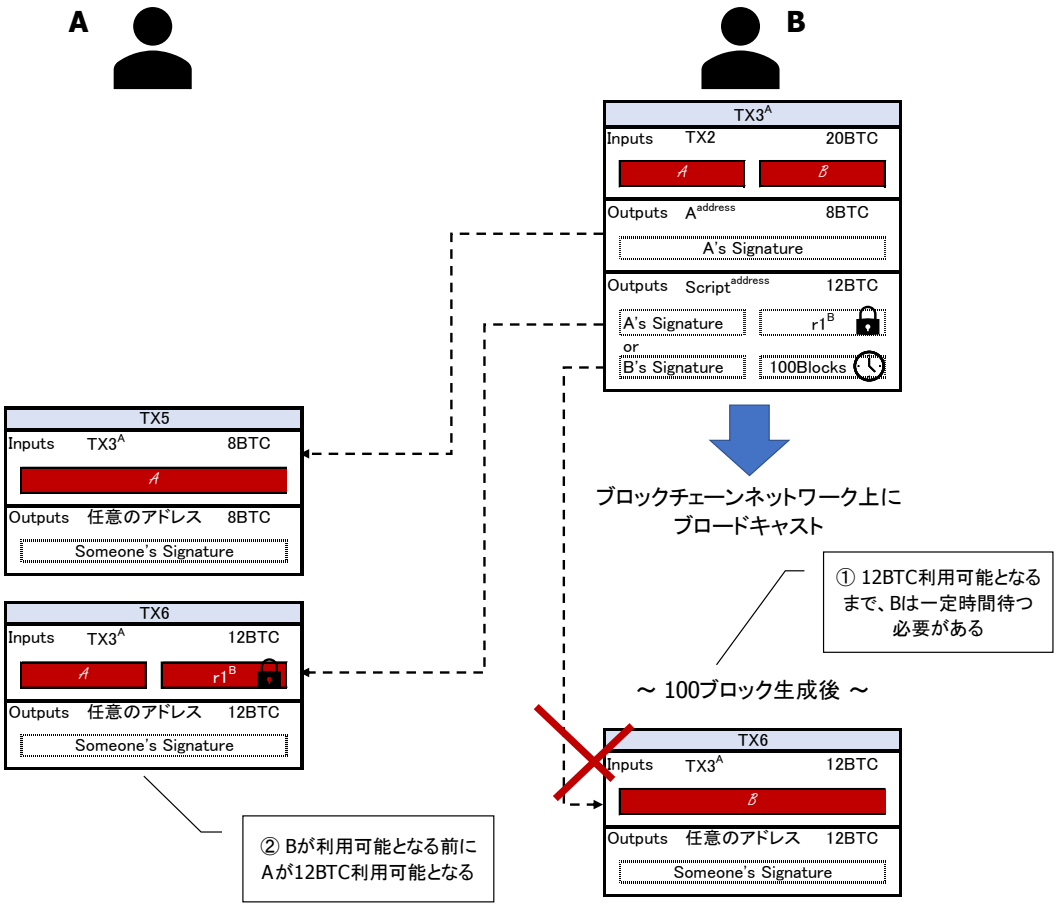
どちらかが自身の署名を付してブロードキャストすればペイメントチャネルはクローズされたことになる。
（取引の終了）

上記の例では B は初回のコミットメントトランザクション（$TX3^A$、$TX3^B$）では 12BTC が利用可能だが、二回目のコミットメントトランザクション（$TX4^A$、$TX4^B$）では 5BTC のみとなる。ここで、最新の取引結果に関わらず、B が初回のコミットメントトランザクション $TX3^A$ をブロードキャストした場合を考える（図表 58）。

この場合、$TX3^A$ がブロックに格納されると、A は 8BTC が利用可能となるが、B は 12BTC が利用可能となるまで一定時間待つ必要がある。しかし、$TX3^A$ で用いているシークレット $r1^B$ は既に A が保持しているため、A は残り 12BTC も（一定時間待つことなく）利用可能となる。

そのため、自分に有利な過去のコミットメントトランザクションをブロードキャストするという不正を行った場合、不正を行った側のデポジット全額が没収される（逆に言うと、相手側が利用可能となる）こととなる。このように、取引当事者が不正を行うインセンティブを無くすことで、互いに相手を信頼しない前提で、すなわち、トラストレスで、安全にオフチェーンで取引を行えるようにしている。

図表 58 不正を行った側への罰則の仕組み



不正を行った側がデポジット全額を没収されることとなる

(iii) ペイメントチャネルのクローズ

ペイメントチャネルをクローズする際には以下のいずれかを行う。

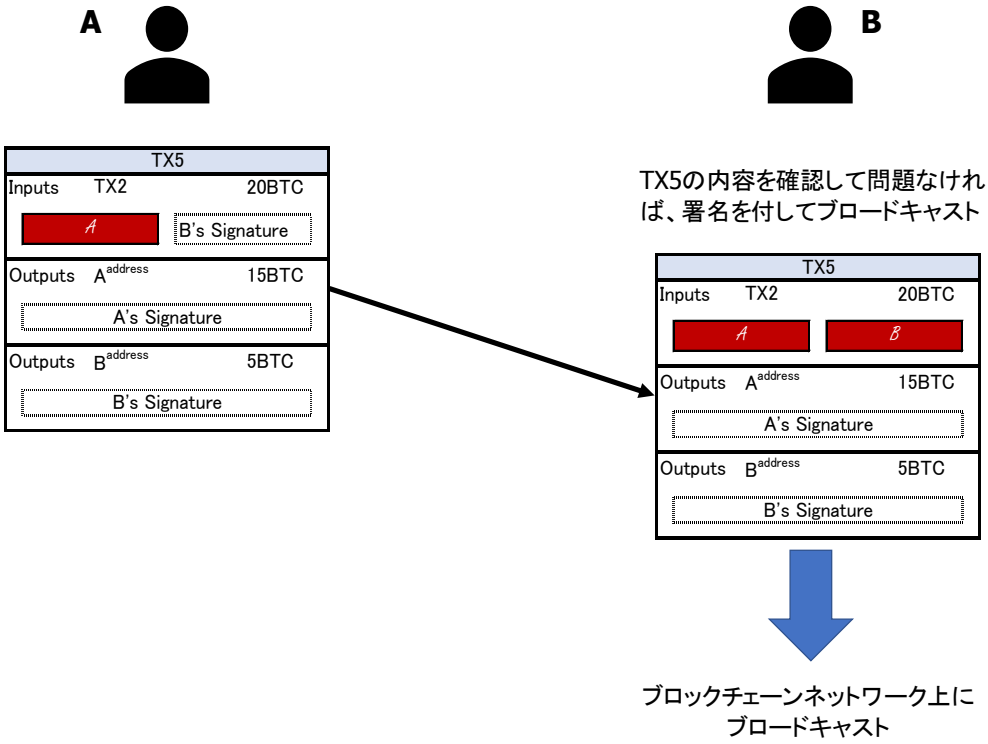
- A か B のどちらかが最新のコミットメントトランザクションに自身の署名を付してブロックチェーンネットワーク上にブロードキャストする。

  図表 55 の通り、ブロードキャストした側は、その時点のコインを利用可能になるまでに一定時間待つ必要が生じる。

- A と B で協力してクロージングトランザクションを生成し、ブロックチェーンネットワーク上にブロードキャストする（図表 59）。

  クロージングトランザクションとは、送金元をファンディングトランザクション TX2、送金先を A および B のアドレスとして、最新時点の取引結果を指定したトランザクションである。この場合、ブロードキャストした側は、コインが利用可能となるまでに一定時間待つ必要はない。

図表 59 クロージングトランザクションを用いたペイメントチャネルのクローズ

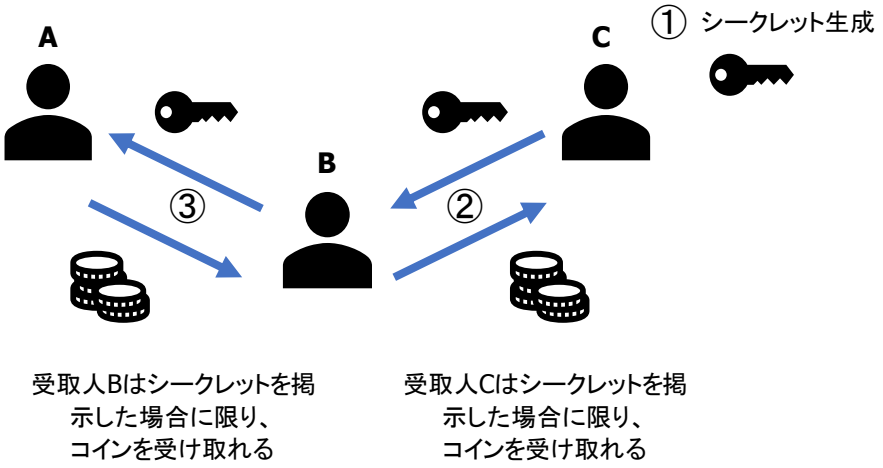


(iv) 複数のペイメントチャネルを経由した送金

以下では例として A が B を経由して C へ 2BTC 送金する場合を考える[121]（図表 60）。重要なポイントは、A から B および B から C への支払が確実に行われるように（i）B から C への送金を先に行い、A から B への送金を後に行うことと、（ii）両方の支払が確実に行われる、もしくは両方の支払が行われないという、いずれかの状態になるように条件付けること[122]の二点である。

（i）については、A から B への送金が先に行われる場合、仲介者 B は A のコインを得ながら C へ送金しないことが可能となるため、これを防ぐために必要となる。(ii)については、ペイメントチャネルで用いたシークレットの仕組みを用いて、受取人がシークレットを掲示しない限りコインを受け取れない、もしくは一定時間が経過すると送金人にコインが戻るという形で条件付けを行っている。このような条件を指定するスマートコントラクトは、特に「ハッシュ・タイムロック・コントラクト」（Hashed Timelock Contracts、以下 HTLC）と呼ばれる（HTLC の詳細は 3.2.2.6.2 節「仕組み」を参照）。

図表 60 複数のペイメントチャネルを経由した送金の概要



具体的には、以下の手順を行う。ここで、A から C へ 2BTC 送金する場合を考える（図表 61）。

(1) C はシークレット r、およびそのハッシュ値 R を生成し、ハッシュ値 R を A に渡す。

121 この場合、A と B の間のペイメントチャネル、B と C の間のペイメントチャネルという2つのペイメントチャネルを組合せて利用することになる。

122 このような、一連の処理が全て実行されるか、全く実行されないかのいずれかになる性質は、コンピュータサイエンスの用語を用いて「アトミック性」とも呼ばれる。

(2) A は C までの経路を決定する。ここでは B を経由することとするが、実際には、A は他のノードと経路情報（当該ノードがペイメントチャネルを開いている先や当該ノードが保持するコインの量、当該ノードを経由する際の手数料等）を交換しており、その情報に基づいて最適な経路を決定する。

(3) A と B はペイメントチャネルの更新と同様の作業を行うが、後述の通り、C の生成したハッシュ値 R を含める点が異なる。まず、A と B はそれぞれシークレット $r10^{A}$、$r10^{B}$、およびそのハッシュ値 $R10^{A}$、$R10^{B}$ を生成し[123]、お互いに $R10^{A}$、$R10^{B}$ および R を交換する。

(4) A は送金元をファンディングトランザクション[124]$TX2^{AB}$、送金先を A のアドレス（8BTC）、特殊なアドレス①（10BTC）、特殊なアドレス②（2BTC）とするトランザクション $TX12^{A}$ を作成し、自身の秘密鍵で署名する。

(5)　ここで、特殊なアドレス①宛のコインは、B のシークレット $r10^{B}$ を A が掲示すれば A が利用可能であるが、指定した時間が経過すると B も利用可能となる。また、特殊なアドレス②宛のコインは、（i）B のシークレット $r10^{B}$ を A が掲示すれば A が利用可能、（ii）指定した期日が到来すると A が利用可能、（iii）指定した時間が経過した後に C のシークレット r を B が掲示すると B が利用可能となる。

特殊なアドレス②宛のコインが複雑になっているのは、不正をした側のデポジットが没収されるというペイメントチャネルの仕組みに、ハッシュ値のシークレットと交換にコインが利用可能となるという HTLC を含めているからである[125]。

(6) B は送金元をファンディングトランザクション $TX2^{AB}$、送金先を B のアドレス（10BTC）、特殊なアドレス③（8BTC）、特殊なアドレス④（2BTC）とするトランザクション $TX12^{B}$ を作成し、自身の秘密鍵で署名する。

ここで、特殊なアドレス③宛のコインは、A のシークレット $r10^{A}$ を B が掲示すれば B が利用可能であるが、指定した時間が経過すると A も利用可能となる。また、特殊なアドレス④宛のコインは、（i）A のシークレット $r10^{A}$ を B が掲示すれば B が利用可能、（ii）指定した期日が到来すると A が利用可能、（iii）C

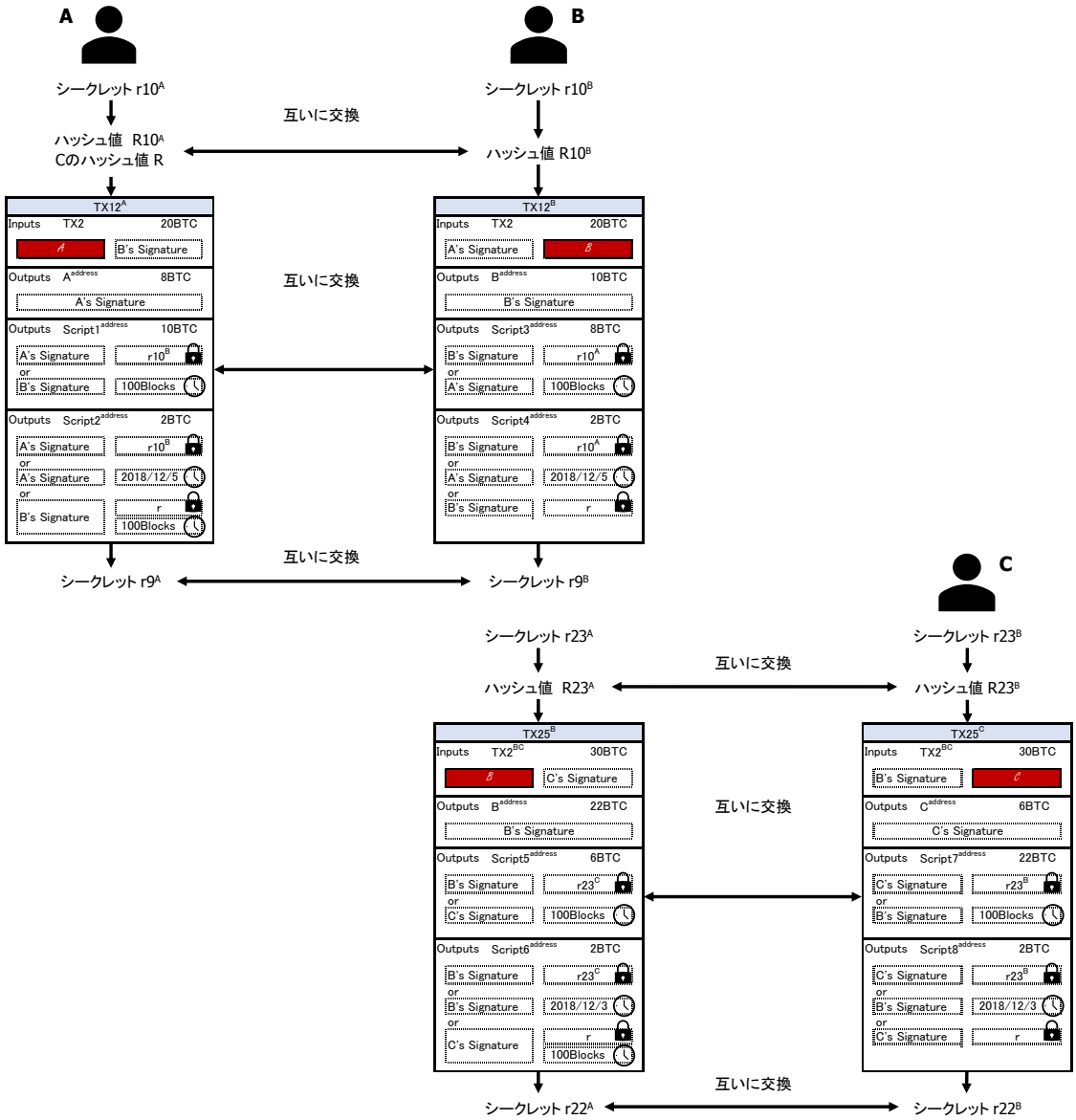
123 ここでは、これまでに取引を 9 回行ったと想定している。
124 B と C の間のファンディングトランザクションと区別するため、ここでは TX2 に AB と上付き文字で表記している。
125 特殊なアドレス②宛のコインは、B が過去のトランザクションをブロードキャストした場合に A が即時に没収できるように、C のシークレット r を B が掲示しても一定時間が経過した上で初めて利用可能となるようにしている。

のシークレット r を B が掲示すると B が利用可能となる[126]。

(7) A と B は $TX12^A$、$TX12^B$ を交換する。また、新たなコミットメントトランザクション交換後（ないし交換時）に、前回のコミットメントトランザクションで用いた双方のシークレット $r9^A$、$r9^B$ を交換する。

(8) B と C の間でもペイメントチャネルの更新と同様の作業を行うが、A と B の場合と同様、C の生成したハッシュ値 R を含める点が異なる。

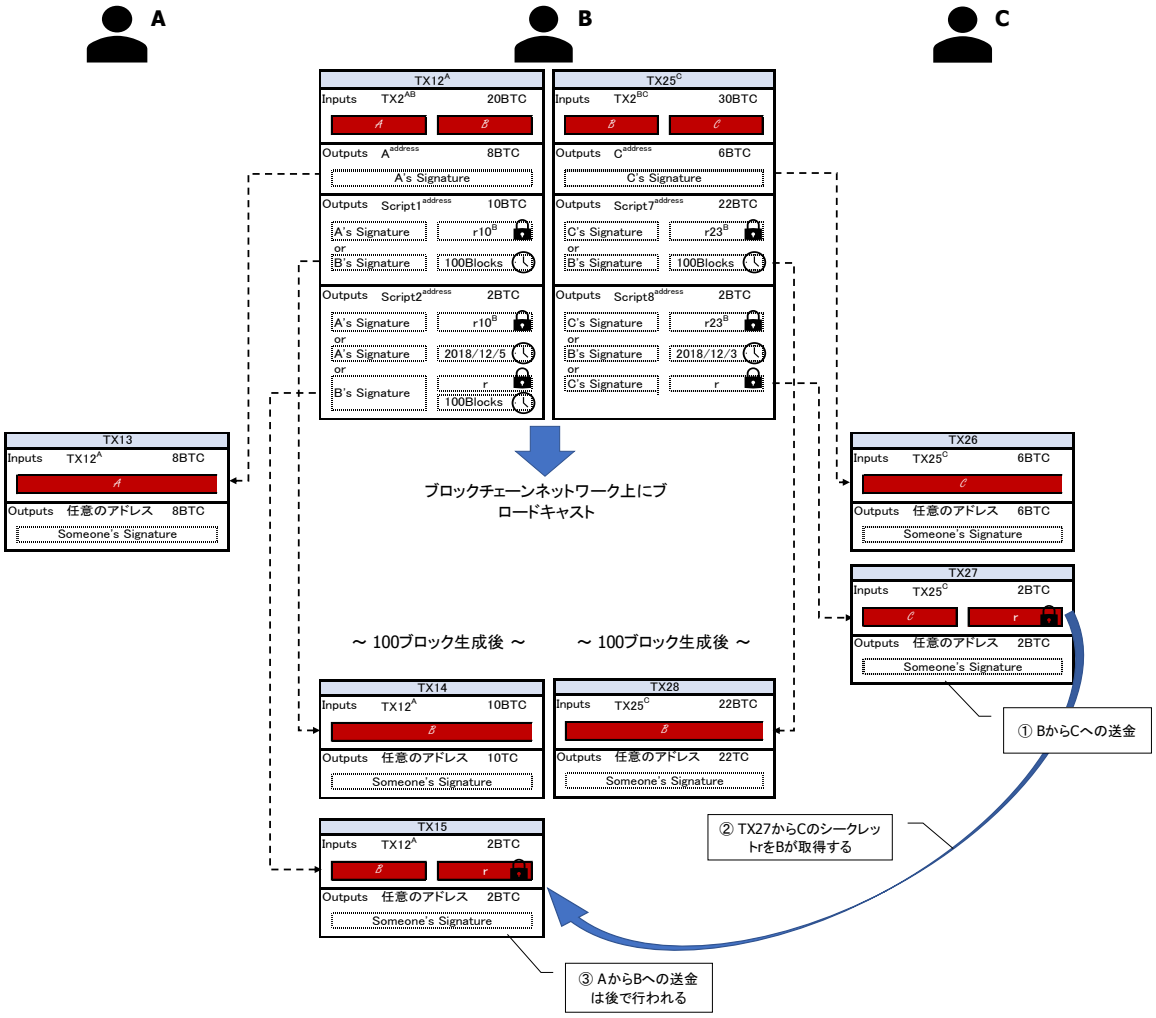
図表 61 複数のペイメントチャネルの更新



126 ②の（iii）の条件と異なり、④の場合、特殊なアドレス④宛のコインは、A が過去のトランザクションをブロードキャストした場合に B が即時に没収できるように、一定時間待つ必要がないようにしている。

ここで、B がペイメントチャネルをクローズするため、C[127]の作成した $TX25^C$ および A の作成した $TX12^A$ をブロードキャストした場合を考える（図表 62）。この場合、B と C の最新時点の取引結果の反映に加え、C は自身の生成したシークレット r を用いて 2BTC が利用可能となる（図表 62 の TX27）。ここで、C は 2BTC を受け取る代わりに、シークレット r をブロックチェーン上にブロードキャストし、ブロックチェーン上に記録することになる。そのため、ブロックチェーン上に記録された r を用いることで、B は 2BTC が利用可能となる（図表 62 の TX15）。

図表 62 複数のペイメントチャネルのクローズと A から C への送金



この段階に至っては、A から B を経由して C へ 2BTC 送金するか、全く送金しないかのいずれかの状態のみになる。ペイメントチャネルをクローズせず、さらに更新を続ける場合、A、B、C は先程の 2BTC の送金を反映した形で、次のコミットメントトランザクションを生成することになる[128]。

127 ここでは、B と C の間でも既に相当数の取引を行っていると仮定している。
128 本稿執筆時点の実装では、シークレットを都度やり取りする形となっている。

3.2.2.5.3 課題およびそれらに関連した新たな取り組み

ライトニングネットワークによるオフチェーンの決済が普及するためには、チャネルが多数存在し、多くの先と低廉な手数料で接続できることが必要となる。また、あらゆる決済に対応できるように、多額の決済にも対応可能であることが望ましい。最後に、いつでも決済できるように、ペイメントチャネルが長時間開いている状況が望ましい。これらを踏まえると、本稿執筆時点の課題としては主に以下の点が挙げられる。

- キャパシティ問題

  ペイメントチャネルの中では、最初にデポジットした金額（以下、キャパシティ）の範囲内でしか取引が行えない。また、複数のペイメントチャネルを経由した場合、経由チャネルのキャパシティの最小値の範囲内でしか取引が行えない。

- 流動性の分断問題

  デポジットしたコインは、ペイメントチャネル内の決済（オフチェーン決済）でしか利用できず、通常のブロックチェーン上の決済（オンチェーン決済）に利用することはできない。そのため、利用者の流動性はオンチェーンとオフチェーンで分断されることになる。

  また、デポジットしたコインはペイメントチャネルをクローズしない限りブロックチェーン上で利用できないため、ペイメントチャネルを長時間開くインセンティブを削ぐ結果ともなる。

- プライバシーの問題（送金経路を特定される問題）

  ライトニングネットワークで複数のペイメントチャネルを経由した送金を行う場合、経路上の各ノード間の通信において、同じハッシュ値やシークレットを用いる必要がある。そのため、ネットワークを流れるデータを確認することで第三者が、各ノード間のハッシュ値やシークレットから、経路を特定することが可能となる。この点は、取引のプライバシーの観点からは問題があると考えられる。

- 常時監視やバックアップ・リカバリーの必要性

  ライトニングネットワークで不正が行われた場合、不正を行った側がデポジットしたコインは全額没収されるが、そのためには被害を受けた側が常時ブロックチェーンを監視し、不正が行われると速やかにそれを認識し、全額没収する

必要がある。このような処理は（電波状態によりオフラインの可能性も高い）スマートフォンのウォレットアプリでは困難である。

また、障害などから復旧した際、誤って古いコミットメントトランザクションをブロードキャストすると、デポジットした額を全額没収されてしまう。そのため、障害発生等に備え、ペイメントチャネルの状態を適切にバックアップ・リカバリーする仕組みも必要となる。

- ルーティング問題

多数のペイメントチャネルが存在する中で、送金先までの最適な（最も手数料の低い）経路を選択する必要がある。ここで、ペイメントチャネル毎にキャパシティと手数料は異なり、また任意のタイミングでペイメントチャネルはクローズされるため、経路は常に不定である。さらに経路情報を管理する特定の主体も存在しない。

このような状況下で、送金元から送金先までの全手数料が最小となる経路を決めることは極めて難しい[129]。

- ハブの存在

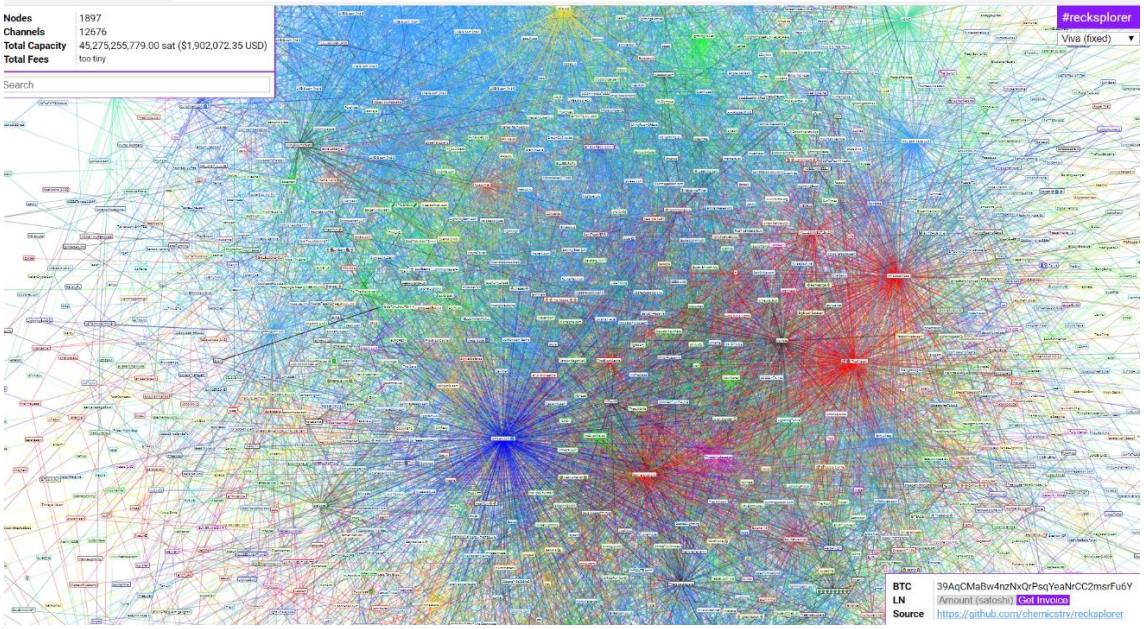
多額のコインを保持するノードは、多数のペイメントチャネルを開くことが可能であり、当該ノードへ接続した場合、多くの相手へ少ないホップ数で送金できる可能性が高い。また、当該ノードは、大きなキャパシティを許容し得るため送金額の自由度も高い。

そのため、多額のコインを保持する特定のノードへ接続が集中し、当該ノードがハブ化し、チャネルの寡占化が進むこととなる（図表 63）。この場合、ハブノードの障害やハブノードへの攻撃[130]はライトニングネットワーク全体に影響を及ぼすことになるため、ネットワーク全体の安定性が低下することとなる。

129 隣接ノードで手数料が最小となるノードを選択しても、その先のノードの手数料まで合わせた場合に、手数料が最小となる保証はない。そのため、原則としては全てのノードを確認する必要があるが、ノード数が多い場合には組合せ爆発により現実的な時間内では計算できないため。

130 意図的に送金を行わないなどの非経済合理的な行動などが挙げられる。

図表 63 実際のライトニングネットワークのイメージ（2018 年 11 月 30 日時点）[131]



上記のような課題の解決へ向け、下記に挙げるように足元様々な取組が進められている。

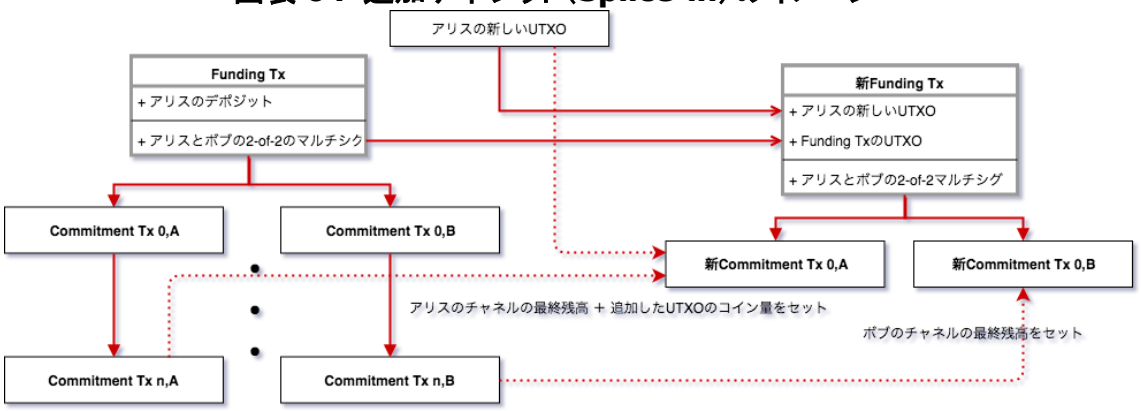
- ペイメントチャネルのキャパシティの更新（Splicing）

ペイメントチャネルのキャパシティを事後的に更新するものであり、追加のデポジットやデポジット額の一部の引出しを可能とする仕組みである[132]（図表 64）。これは前述の「キャパシティ問題」および「流動性の分断問題」の解決につながるものである。

たとえば、追加のデポジットは、送金元を古いファンディングトランザクション、送金先を新たな 2-of-2 のマルチシグアドレスとする新しいファンディングトランザクションを作成することで実現する。

131 #recksplorer, rompert.com, https://rompert.com/recksplorer/, 2018/11/30
132 Lightning-dev, Linux Foundation, "[Lightning-dev] Channel top-up", https://lists.linuxfoundation.org/pipermail/lightning-dev/2017-May/000692.html, 2018/11/30 ここで、追加のデポジットを Splice-in、デポジット額の一部引出しを Splice-out と呼ぶ。

図表 64 追加デポジット（Splice-in）のイメージ[133]



- 複数のルートを組合せた送金（Atomic Multi-Path Payments）

  送金額に満たないキャパシティのルートを組合せて、合計で送金額を満たす送金を可能とする仕組みであり[134]、前述の「キャパシティ問題」の解決につながるものである。

  複数のペイメントチャネルを経由する場合、経路上では同じハッシュ値を用いた条件付を行うが、複数のルートを用いる場合、それぞれのルートでハッシュ値を分ける必要がある。これは片方のルートのシークレットがブロックチェーン上に記録されても、第三者が同じシークレットを用いて他方のルートの送金を不正に得ることを防ぐためである。

  他方で、この仕組みにより、最適な経路の決定はさらに難しくなり、ルーティング問題を悪化させることにもなる。

- プライバシーを確保した送金

  送金経路上の各ノード間の通信において同じハッシュ値やシークレットを用いない仕組みであり、第三者が（たとえネットワークを監視していても）送金経路を特定できないようにするものである。

  具体的には、ある経路上の各ノード間で異なるハッシュ値やシークレットを用いる手法（Multi-Hop Locks）[135]や、ハッシュ値やシークレットを署名に含める手

133 techmedia-think, Hatena Blog, "ペイメントチャネルへの資金のチャージ/引き出しを行う Splicing", https://cdn-ak.f.st-hatena.com/images/fotolife/t/techmedia-think/20180623/20180623145002.png, 2018/11/30
134 Lightning-dev, Linux Foundation, "[Lightning-dev] AMP: Atomic Multi-Path Payments over Lightning", https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-February/000993.html, 2018/11/30
135 Malavolta, G., "Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability",

法（スクリプトレス・スクリプト）が提案されている。

上記の他、ブロックチェーンの常時監視および不正発生時の対処をアウトソースする仕組み（Watchtower[136]）、ペイメントチャネル状態のバックアップ・リカバリー（Data Loss Protection[137]）、不正が行われた場合に全額没収ではなく最新時点の取引結果を反映できるようにする仕組み（eltoo[138]）等が提案されている。

3.2.2.5.4 その他の論点

ライトニングネットワークでは、ハブが生成して中央集権化する点が課題と考えられているが、本調査研究で確認する限り、ハブの経済的インセンティブについてまだ深い研究はなされていないように見受けられる。

ハブの運営主体は、送金を中継する際の手数料が収入となるが、ペイメントチャネルを構築するためにはデポジットが必要となり（初期コスト）、また、デポジットしたコインを他に転用することができないというデメリット（機会コスト）も受ける。また、中継する場合は自身の直前の送信ノードと次の宛先ノードしか知ることができないため、中継した情報をマーケティング等に活用する用途も限られると考えられる。そのため、特定のハブへ集中化する度合いは、それぞれのハブにとっての手数料収入と上記のコストのバランスにも影響を受けると推測される。

3.2.2.6 アトミック・クロスチェーン・スワップ

3.2.2.6.1 背景

ビットコインやライトコインなど異なるブロックチェーン上の暗号資産は、当該ブロックチェーン上のみでやり取りされるものであり、相互にデータ形式なども異なる。そのため、異なる暗号資産の交換にあたっては、一般には仮想通貨取引所などの信頼できる第三者を介した取引（例えば、ビットコインネットワーク上でビットコインを送金する代わりに、ライトコインネットワーク上でライトコインを受け取るなど）が行われる。

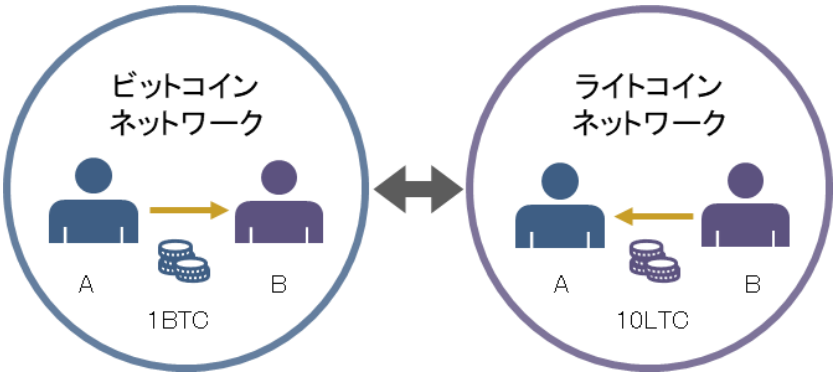
アトミック・クロスチェーン・スワップ（Atomic Crosschain Swap）とは、二つの異なる

---

https://eprint.iacr.org/2018/472.pdf, 2019/1/23
136 Lightning-dev, Linux Foundation, "[Lightning-dev] Trustless WatchTowers?", https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-April/001196.html, 2018/11/30
137 ACINQ, GitHub, "Data loss protection", https://github.com/ACINQ/eclair/pull/410, 2018/11/30
138 Blockstream, Blockstream Corp., "eltoo: A Simplified Update Mechanism for Lightning and Off-Chain Contracts", https://blockstream.com/2018/04/30/eltoo-next-lightning/, 2018/11/30

ブロックチェーン上の暗号資産を、仮想通貨取引所などの信頼できる第三者を介在させずに、相互のネットワークを接続させることもせずに、取引当事者間でのみ交換するためのものである[139]（図表 65）。例えば、ビットコインを送金したにも関わらず、ライトコインを受け取れないといった取りはぐれリスクを排除する仕組みとなっている[140]。

図表 65 アトミック・クロスチェーン・スワップのイメージ



アトミック・クロスチェーン・スワップのアイデアは Tier Nolan らによって 2013 年に初めて整理された[141]。当時は技術的な制約からセキュリティ上の問題が存在した[142]が、近年になり新たな機能がビットコイン等に導入されたこと[143]から、安全に実現できるようになった。

アトミック・クロスチェーン・スワップは、Decred というコインとライトコインの間で実施されたり[144]、ライトニングネットワーク上で行う提案がなされたり[145]、国際会議で発

139 複数のネットワーク間での異なるトークンのやり取りを概観した資料として、以下が挙げられる。STELLA - a joint research project of the European Central Bank and the Bank of Japan, "Securities settlement systems: delivery-versus-payment in a distributed ledger environment", https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf, 2019/1/9

140 アトミック性（atomicity）とは、コンピュータ・サイエンスにおいて、一連の処理の一体不可分性を指す用語であり、一連の処理が全て行われるか、全く行われないかの二者択一であることを指す。例えば、ビットコインとライトコインという二つの暗号資産の交換において、取りはぐれリスクを排除するためには、双方の引渡が両方行われるか、全く行われないかの二者択一になる（アトミック性を備える）必要がある。

141 TierNolan, Bitcoin Forum, "Alt chains and atomic transfers", https://bitcointalk.org/index.php?topic=193281, 2019/1/9

142 取引当事者は事前に返金用トランザクションに署名しておく必要があったが、トランザクション展性問題により、トランザクションが改変される危険性が存在した。

143 具体的には、2016 年にビットコインに導入された、BIP-112 で提案された OP_CHECKSEQUENCEVERIFY（OP_CSV）および BIP-65 で提案された OP_CHECKLOCKTIMEVERIFY（OP_CLTV）である。

144 Piatt, J., Decred Blog, "On-Chain Atomic Swaps", https://blog.decred.org/2017/09/20/On-Chain-Atomic-Swaps/, 2019/1/9

145 Fromknecht, C., Lightning Labs, "Connecting Blockchains: Instant Cross-Chain Transactions On Lightning", https://blog.lightning.engineering/announcement/2017/11/16/ln-swap.html, 2019/1/9

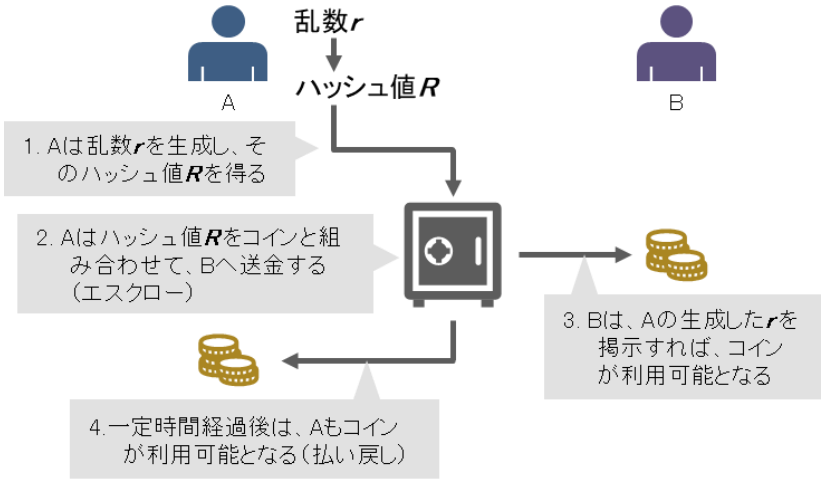
表が行われる[146]など、最近でも改善に向けた活発な取り組みが見られる。

3.2.2.6.2 仕組み

2 つの異なるネットワーク間でそれぞれの資産をアトミックに受渡するために重要となるのは、「ハッシュ・タイムロック・コントラクト」（Hashed Timelock Contracts、HTLC）と呼ばれる技術である。HTLC はライトニングネットワーク [114] で提案された用語だが、アトミック・クロスチェーン・スワップも同様の考えで整理できる[147]。

HTLC は、一方向ハッシュ関数とタイムロック機能を組合せて、条件付き支払いを可能にする技術であり、具体的には以下の手順で条件付き支払いを実現する（図表 66）。

図表 66 HTLC の動作イメージ



(1) 送金人 A は乱数 r を生成し、そのハッシュ値 R を得る。ここで、一方向ハッシュ関数を用いることにより、合理的な想定に基づけば、ハッシュ値 R から元の値 r を得ることはできない。

(2) 送金人 A は、受取人 B 宛に、暗号資産に R を組合せて送金する。ここで、受取人 B は、R の元の値である r を掲示しない限り、当該暗号資産を受け取ることができない。

(3) 受取人 B は、（何らかの方法で取得した）r を掲示すれば、当該暗号資産を受

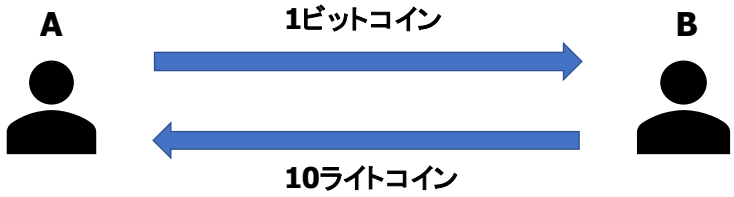
146 一例として、Scaling Bitcoin 2018 における以下の発表などが挙げられる。Diyhpluswiki, "The State of Atomic Swaps", http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/atomic-swaps/, 2019/1/9
147 その他に、Ripple Interledger Protocol（ILP）や Utility Settlement Coin も HTLC を活用していると整理できる。

け取る。

(4) 一定時間経過後は、送金人 A も当該暗号資産を受け取ることができる。これは、受取人 B が取引を中止し、送金人 A が払い戻しを行う場合にあたる。

以下では、Tier Nolan の考えを改良した手順について記載する[139]（図表 67）。ここでは、取引当事者 A と B の間で 1 ビットコインと 10 ライトコインを売買する場合を考える（図表 68）。

図表 67 アトミック・クロスチェーン・スワップの例



(1) A は乱数（以下、シークレット）r を生成し、そのハッシュ値 R を得る。A は R を B に伝える。

(2) ビットコインネットワーク上で、A は送金元を自身のトランザクション、送金先を特殊なアドレス、総金額を 1BTC とするトランザクション TX1 を作成し、自身の署名を付してブロードキャストする。

ここで、特殊なアドレス宛のコインは、シークレット r を B が掲示すれば B が利用可能であるが、指定した時間が経過すると A も利用可能となる。

(3) ビットコインネットワーク上で、B は TX1 を確認する。送金額等に問題がなければ、ライトコインネットワーク上で、B は送金元を自身のトランザクション、送金先を特殊なアドレス、総金額を 10 ライトコインとするトランザクション TX2 を作成し、自身の署名を付してブロードキャストする。

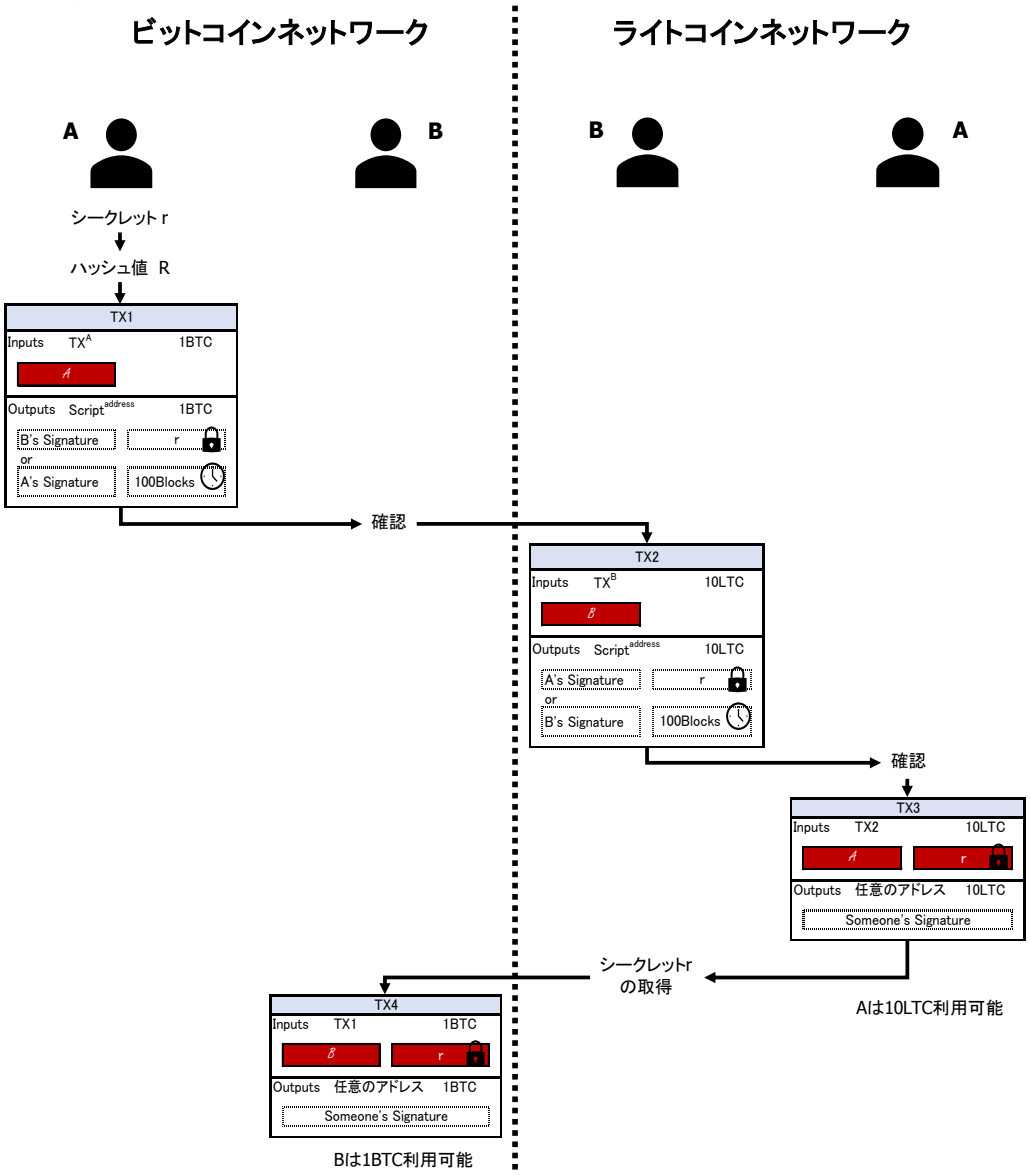
ここで、特殊なアドレス宛のコインは、シークレット r を A が掲示すれば A が利用可能であるが、指定した時間が経過すると B も利用可能となる。

(4) ライトコインネットワーク上で、A は TX2 を確認する。送金額等に問題がなければ、ライトコインネットワーク上で、A は送金元を TX2、送金先を任意のアドレス、シークレットを r とするトランザクション TX3 を作成し、自身の署名を付してブロードキャストする。

(5) ライトコインネットワーク上で、B は TX3 を確認し、シークレット r を取得する。続

いて、ビットコインネットワーク上で、B は送金元を TX1、送金先を任意のアドレス、シークレットを r とするトランザクション TX4 を作成し、自身の署名を付してブロードキャストする。

図表 68 アトミック・クロスチェーン・スワップによる、異なるコインの交換



ここで、取引当事者 A と B は任意のタイミングで取引を中止することができ、中止した場合は、原則として一定時間経過後に払い戻しされることになる。

ただし、上記のステップにおいて、B が何らかの理由で TX4 をブロードキャストしない場合においてのみアトミック性が成立しない。すなわち、B が TX4 をブロードキャストしないと、A は 10 ライトコインを受け取った後に、一定時間経過後に 1BTC も払い戻すことができることになる。そのため、A が TX3 をブロードキャストした後は、B は必

ず TX4 をブロードキャストする必要がある。

TX3 のブロードキャストと TX4 のブロードキャストを一体の処理として考えると、この一連の処理の起点である A は、取引中のビットコインとライトコインのマーケット価格を参考にして、TX3・TX4 の処理を開始するか否かのオプションを保有していると考えられる。すなわち、A はアメリカンタイプのコールオプションを購入し、B はアメリカンタイプのコールオプションを売却したことに相当すると考えられる[148]。

3.2.2.6.3 課題およびそれらに関連した新たな取り組み

アトミック・クロスチェーン・スワップの課題として、以下の点が挙げられる。

- 特定の状況においてアトミック性が担保されない問題

  前述の通り、図表 68 において、B が TX4 をブロードキャストしない場合においてのみアトミック性が成り立たないという課題がある。この課題を解決するために信頼できる第三者に TX4 のブロードキャストを委託しておくことなども考えられるが、第三者を介在させずに実現するのは技術的な難易度が高いと考えられる。

- 処理に時間がかかり、また、流動性の利用効率も低下する問題

  取引当事者 A と B は任意のタイミングで取引を中止することができる。取引が中止された場合は一定時間経過後に払い戻されるが、取引当事者はその間待つ必要があり、また、取引の間、当該取引に用いたコインを並行して他の送金に利用することなどはできないため、流動性の利用効率という観点からは問題があると考えられる。

  取引が正常に完了する場合でも、Proof of Work などのコンセンサスアルゴリズムを用いるブロックチェーンでは、片方の取引が覆らないことを確認するために、十分に長い時間を置く必要がある。

  そのため、払い戻しまでの待機時間や送金確認までの待機時間は、流動性の効率性と取引の安全性のトレードオフになっていると考えられる。

- プライバシーの問題（第三者に取引を特定される問題）

148 BitMEX Research, BitMEX, "Atomic Swaps and Distributed Exchanges: The Inadvertent Call Option", https://blog.bitmex.com/atomic-swaps-and-distributed-exchanges-the-inadvertent-call-option/, 2019/1/10

アトミック・クロスチェーン・スワップでは、ビットコインとライトコインなど異なる2つのブロックチェーン上で、同じハッシュ値 R、シークレット r を用いる必要がある。そのため、ブロックチェーンデータを確認することで第三者が双方のトランザクションを紐付けることが可能となる。この点は、取引のプライバシーの観点からは問題があると考えられる。そのため、本稿執筆時点の実装では、トランザクションを暗号化することで、ハッシュ値やシークレットを秘匿するように対応がなされている。

- 対応可能なブロックチェーンが限定される問題

双方のブロックチェーンネットワーク間には一切の接続は不要だが、双方ともに HTLC を備えている必要がある。また、図表 68 において、B が A の作成したトランザクション TX3 からシークレット r を取得するためには、TX3 が必ず B に開示される必要がある。そのため、プライバシーの点からトランザクションの開示範囲を限定する一部の許可型ブロックチェーンなどでは、アトミック・クロスチェーン・スワップを実現できない場合がある。

- 常時監視の必要性

取引当事者 A と B は相手方が所定の手順を踏んだことを把握するために、常時ブロックチェーンを監視する必要がある。

上記のような課題の解決へ向け、下記に挙げるように足元様々な取組が進められている。

- 担保による罰則の導入

片方の取引当事者（図表 68 では A）に担保を拠出させ、当該当事者が取引を中止した場合に罰則を受ける仕組み [146] であり、当該当事者が交換を行うか否かのオプションを保有している点の改善を試みるものである。

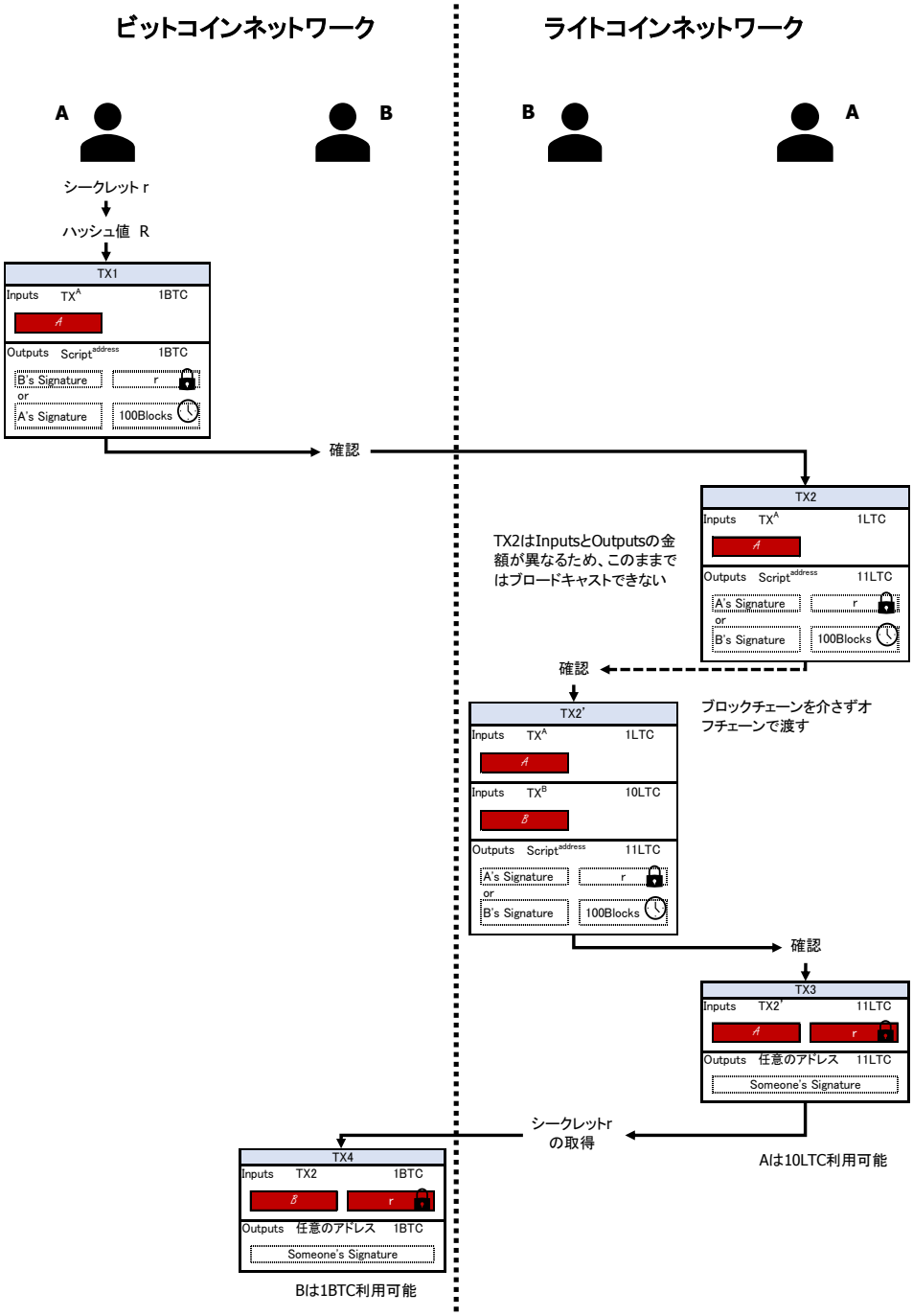
具体的には、図表 68 において B が TX2 を作成しブロードキャストする処理を以下のように変更する。

(1) A は TX1 をビットコインのブロックチェーンネットワーク上にブロードキャストした後、送金元を自身のトランザクション、送金先を自身のアドレス、送金額を罰金額（ここでは例として 1LTC とする）に本来の送金額（10LTC）を加えた値とするトランザクション TX2 を作成し、自身の署名を付して、B に渡す。

(2) B は TX2 を確認して問題がなければ、TX2 の送金元に自身のトランザクションを追加したトランザクション TX2’を作成し、自身の署名を付して、ライトコインのブロックチェーンネットワーク上にブロードキャストする。

上記に合わせて、A が TX3 を生成する際には、送信元を TX2’とし、送金額は罰金額も含めるように変更する（図表 69）。

図表 69 担保による罰則を組み入れたアトミック・クロスチェーン・スワップ



TX2’がブロードキャストされた後、A が取引を中止すると、A は罰金額（1LTC）を失

うことになる。A が取引を進めた場合は、A は当該罰金額を回収することができる。

- HTLC を備えていないブロックチェーンへの対応

  片方の取引をマルチシグで代用するやり方であり、HTLC を備えていないブロックチェーン上の資産も（マルチシグさえ備えていれば）交換を可能とするものである（詳細は 3.3.2.3 節「BarterDEX」を参照）。

- スクリプトレススクリプト

  スクリプトレススクリプト[149]とは、ハッシュ値やシークレットをスクリプト[150]のロジックとして記述する代わりに署名データにエンコードする仕組みである。これは、ハッシュ値やシークレットをもとに、異なるブロックチェーン上のトランザクションを紐付けられることがないようにする技術であり、取引のプライバシーを改善することにつながるものである。

以下では、スクリプトレススクリプトについて、Schnorr 署名[151]と ECDSA の場合に分けて記載する。

(i) Schnorr 署名を利用したスクリプトレス・アトミック・クロスチェーン・スワップ

2017 年 Andrew Poelstra は、Schnorr 署名の署名データに加えて Adaptor 署名と呼ばれる署名データを用いることで、スマートコントラクトを用いずに署名技術のみでアトミック・クロスチェーン・スワップを行う仕組み[152]を提案した。

通常 Schnorr 署名の署名データは以下の手順で計算される。ここで G は楕円曲線上のベースポイント、x は秘密鍵、x に対応する公開鍵は X = xG、H をハッシュ関数、m を署名対象のメッセージとする。

(1) 乱数 k を選び、楕円曲線上の点 K ＝ kG を計算する（k は秘密鍵、K は公開

149 2016 年に発表されたブロックチェーンのコンセプトである Mimblewimle はスクリプトの機能を持っていないため、スマートコントラクトをどう実現するかという課題が残っていた。これに対し、2017 年に Andrew Poelstra がスマートコントラクトをデジタル署名にエンコードすることでマルチシグやアトミックスワップを、スクリプトを必要とせずに実現する仕組みを提案し、この仕組が一般にスクリプトレススクリプトと呼ばれる。

150 ビットコインでは、スマートコントラクトに相当するプログラムを「スクリプト」と呼ぶ。

151 Schnorr 署名とは、Claus Schnorr により 1989 年に提案された署名技術である。2008 年まで特許で保護されていたため、ビットコインでは ECDSA が用いられている。Schnorr 署名は、ECDSA に比べ、公開鍵や署名の集約機能（複数の署名を集約して 1 つの署名で置き換える機能）がある点が大きな特徴と言える。

152 ただし、タイムロックの仕組みはスクリプトレススクリプトでは実現できないため、Adaptor 署名を利用したスクリプトレス・アトミック・クロスチェーン・スワップでは、一定期間コインの交換が行われなかった場合にコインがそれぞれの取引当事者に払い戻されるタイムロック付きの払い戻しトランザクションを用意しておく必要がある。

鍵にあたる）。

(2) s = k + H(X, K, m)x を計算し、（K, s）を Schnorr 署名データとする。

Adaptor 署名は上記の Schnorr 署名のデータにシークレットに相当する乱数 r をさらに加えたものになり、以下の手順を踏む。

(1) 乱数 k を選び、楕円曲線上の点 K ＝ kG を計算する（k は秘密鍵、K は公開鍵にあたる）。

(2) 乱数 r を選び、楕円曲線上の点 R ＝ rG を計算する（r は秘密鍵、R は公開鍵にあたる）。

(3) s’ = k + r + H(X, K, m)x を計算し、（K, R, s’）を Adaptor 署名データとする。

ここで、Schnorr 署名データ s と Adaptor 署名データ s’の 2 つがあれば、r = s’ - s でシークレット r が分かる。アトミック・クロスチェーン・スワップとの比較では、秘密鍵の r がシークレット、公開鍵の R が r のハッシュ値に相当する。アトミック・クロスチェーン・スワップと同様に、合理的な想定に基づけば、R から元の値 r を得ることはできない。

スクリプトレス・アトミック・クロスチェーン・スワップの具体的な手順は以下の通りとなる（図表 70）。ここで、前提条件は図表 68 と同じとする。

(1) ビットコインネットワークにおいて、A は秘密鍵x_A^{BTC}、公開鍵$X_A^{BTC} = x_A^{BTC}$G、乱数k_A^{BTC}、$K_A^{BTC} = k_A^{BTC}$Gおよび、乱数 r、R = rG を計算する。B はx_B^{BTC}、X_B^{BTC}、k_B^{BTC}、K_B^{BTC}を計算する。両者はX_A^{BTC}、K_A^{BTC}、R、X_B^{BTC}、K_B^{BTC}を交換する。

(2) ライトコインネットワークにおいて、A はx_A^{LTC}、X_A^{LTC}、k_A^{LTC}、K_A^{LTC}を計算する。B はx_B^{LTC}、X_B^{LTC}、k_B^{LTC}、K_B^{LTC}を計算する。両者はX_A^{LTC}、K_A^{LTC}、X_B^{LTC}、K_B^{LTC}を交換する。

(3) ビットコインネットワーク上で、A は送金元を自身のトランザクション、送金先を$X^{BTC} = X_A^{BTC} + X_B^{BTC}$から導出されるアドレス[153]、総金額を 1BTC とするトランザクション TX1 を作成し、自身の署名を付してブロードキャストする。

(4) ライトコインネットワーク上で、B は送金元を自身のトランザクション、送金先を

153 マルチシグといっても、ビットコインのようなスクリプトを利用したマルチシグではなく、Schnorr 署名には公開鍵の集約特性があるため、A と B の公開鍵を加算した新たな公開鍵を用いることになる。

$X^{LTC} = X_A^{LTC} + X_B^{LTC}$から導出されるアドレス、総金額を 10LTC とするトランザクション TX2 を作成し、自身の署名を付してブロードキャストする。

(5) 次に A は以下の二つの Adaptor 署名データ(K^{BTC}, R, s'^{BTC}_A)と(K^{LTC}, R, s'^{LTC}_A)を計算し、B へ送る。ここで、m'は、送金元を TX2、送金先を自身のアドレス、総金額を 10LTC とするトランザクション TX3、mは、送金元を TX1、送金先を自身のアドレス、総金額を 1BTC とするトランザクション TX4 を指す。

- $s'^{BTC}_A = k_A^{BTC} + r + H(X^{BTC}, K^{BTC}, m)x_A^{BTC}$、ここで、$X^{BTC} = X_A^{BTC} + X_B^{BTC}$、$K^{BTC} = K_A^{BTC} + K_B^{BTC}$、R = rG
- $s'^{LTC}_A = k_A^{LTC} + r + H(X^{LTC}, K^{LTC}, m')x_A^{LTC}$、ここで、$X^{LTC} = X_A^{LTC} + X_B^{LTC}$、$K^{LTC} = K_A^{LTC} + K_B^{LTC}$、R = rG

(6) B は A から受領した 2 つの Adaptor 署名データを用いて以下を検証する。

- R が等しいこと
- $s'^{BTC}_A G = k_A^{BTC} G + rG + H(X^{BTC}, K^{BTC}, m)x_A^{BTC} G = K_A^{BTC} + R + H(X^{BTC}, K^{BTC}, m)X_A^{BTC}$
- $s'^{LTC}_A G = k_A^{LTC} G + rG + H(X^{LTC}, K^{LTC}, m')x_A^{LTC} G = K_A^{LTC} + R + H(X^{LTC}, K^{LTC}, m')X_A^{LTC}$

(7) A の Adaptor 署名データが正しければ、B は以下の二つの Schnorr 署名データを計算し、s_B^{LTC}を A に渡す(A がライトコインを取得するのに必要なため)。

- $s_B^{BTC} = k_B^{BTC} + H(X^{BTC}, K^{BTC}, m)x_B^{BTC}$
- $s_B^{LTC} = k_B^{LTC} + H(X^{LTC}, K^{LTC}, m')x_B^{LTC}$

(8) A は送金元を TX2、送金先を自身のアドレス、総金額を 10LTC とするトランザクション TX3 を作成し、以下の Schnorr 署名データ(K^{LTC}, s^{LTC})を付して、ライトコインネットワーク上にブロードキャストし、10LTC を取得する。

$$s^{LTC} = s'^{LTC}_A G + s_B^{LTC} - r$$
$$= (k_A^{LTC} + k_B^{LTC}) + H(X^{LTC}, K^{LTC}, m')(x_A^{LTC} + x_B^{LTC})$$

(9) B はライトコインネットワーク上の TX3 からs^{LTC}を取得し、$s'^{LTC}_A G + s_B^{LTC} - s^{LTC} = r$で r を取得する。

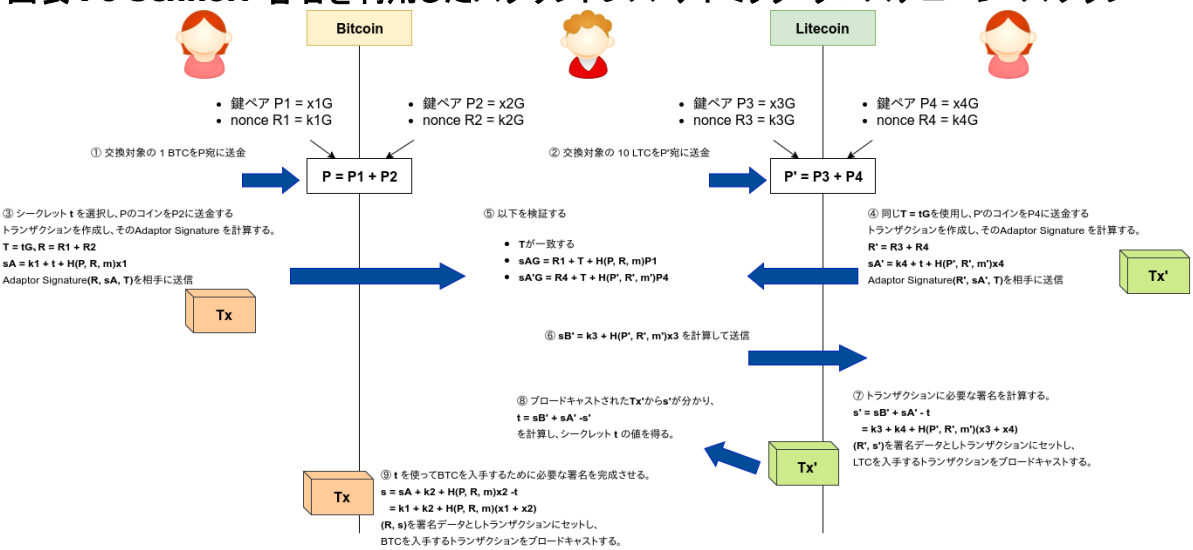
(10) B は送金元を TX1、送金先を自身のアドレス、総金額を 1BTC とするトランザ

クション TX4 を作成し、以下の Schnorr 署名データ(K^{BTC}, s^{BTC})を付して、ビットコインネットワーク上にブロードキャストし、1BTC を取得する。

$$s^{BTC} = s'^{BTC}_{A} G + s^{BTC}_{B} - r$$
$$= (k^{BTC}_{A} + k^{BTC}_{B}) + H(X^{BTC}, K^{BTC}, m)(x^{BTC}_{A} + x^{BTC}_{B})$$

シークレットの生成者である A は、B の Schnorr 署名データを受領すると、ライトコインを得ることができる。そして、A がライトコインを取得する TX3 から、B はシークレットを取得することができる。ここで、TX1～TX4 まで、ハッシュ値やシークレットを含むスクリプトは利用されておらず、それぞれのブロックチェーンデータでは通常の送金トランザクションと同じ形式で記録される。そのため、ブロックチェーンデータを解析しても、ビットコインネットワークとライトコインネットワークにおける送金に関わるトランザクションを紐付けることはできない。

図表 70 Schnorr 署名を利用したスクリプトレス・アトミック・クロスチェーン・スワップ



(ii) ECDSA を利用したスクリプトレス・アトミック・クロスチェーン・スワップ

Adaptor 署名を用いたスクリプトレス・アトミック・クロスチェーン・スワップは Schnorr 署名の公開鍵及び署名の集約特性を利用していたため、現在のビットコイン等で採用されている ECDSA では利用できなかった。

しかし、2017 年に Yehuda Lindell により加法準同型演算が可能な Paillier 暗号を利用して、自身の秘密鍵を明らかにすることなく、二者間で協力して ECDSA 署名を作

成するプロトコルが発表され[154]、その後 2018 年に Pedro Moreno-Sanchez らによって Lindell のプロトコルを組み込んだ ECDSA 用の Adaptor 署名を構成するスクリプトレス・アトミック・クロスチェーン・スワップが提案されるに至った[155]。この場合、ECDSA を用いるブロックチェーン間でスクリプトレス・アトミック・クロスチェーン・スワップが可能となる。

3.2.2.7 MimbleWimble（ミンブルウィンブル）

3.2.2.7.1 背景

Mimblewimble は匿名のユーザが、ビットコインのスケーラビリティおよびプライバシーを向上させる技術として 2016 年 8 月 1 日に IRC に投稿したダークウェブに掲示された mimblewimble.txt[156]から始まる。その後、Andrew Poelstra が改善を加えた論文が 2016 年 10 月に発表された[157]。

ビットコインのブロックチェーンのデータは線形に増加しており、2019 年 1 月時点でデータ量は 210GB を超えている[158]。今後もデータは増加していくと思われ、フルノードが必要とするストレージは増加する一方である。またストレージ量よりも課題となるのが、ノードの初期起動時に実行されるブロックチェーンの同期の時間で、この時間が増え続けることは大きな課題とされている。こうした状況を踏まえて、署名の集約と使用済み UTXO の省略を行うトランザクションカットスルー技術によってブロックチェーンのデータサイズを削減することを主な目的に Mimblewimble は提案された。また、その副次的な目的として Confidential Transaction による送金量の秘匿化や匿名性の向上がある。

---

154 Lindell, Y., ePrint, "Fast Secure Two-Party ECDSA Signing", https://eprint.iacr.org/2017/552.pdf, 2018/12/27

155 Moreno-Sanchez, P., et al., Linux Foundation, "Scriptless Scripts with ECDSA", https://lists.linuxfoundation.org/pipermail/lightning-dev/attachments/20180426/fe978423/attachment-0001.pdf, 2018/12/27

156 Tom Elvis Jedusor, "MIMBLEWIMBLE", https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt, 2019/01/28

157 Andrew Poelstra, "Mimblewimble", https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf, 2019/01/28

158 イーサリアムではアーカイブモード（全てのブロックの時点での残高等も保持するモード）で 2.3TB 超、フルノードで 200GB 弱となっている。BitMEX Research, BitMEX, "BitMEX Research Launches Ethereum Node Metrics Website - Nodestats.org", https://blog.bitmex.com/bitmex-research-launches-ethereum-node-monitoring-website-nodestats-org/, 2019/3/15

MimbleWimble を実装したものとしては Grin[159]と Beam[160]があり、双方とも既にネットワークが稼働している（図表 71）。

図表 71 Grin と Beam の比較

	Grin	Beam
言語	Rust	C++
コンセンサスアルゴリズム	Equihash + Cuckoo Cycle	Equihash
開発主体	コミュニティ主導	企業主体
Mainnet へのローンチ	2019 年 1 月 15 日	2019 年 1 月 3 日
発行量	上限なし	2 億 6300 万 BEAM コイン
ブロック報酬	60 Grin	100 BEAM (内、初年度は 20 BEAM、次の 4 年間は 10 BEAM が BEAM ファウンデーションに供給される)
半減期	なし	4 年毎に半分に

3.2.2.7.2 仕組み

(i) Pedersen Commitment による送金量の秘匿

2015 年に Gregory Maxwell が発表した Confidential Transaction を採用し、トランザクションデータ内の送金量を秘匿化している。ビットコインでは送金量が明示的に数値としてトランザクションデータに記録されているのに対し、Mimblewimble ではコインの量は以下の Pedersen Commitment として暗号化される。

Commitment = r*G + v*H[161]

159 grin, Github, "Minimal implementation of the MimbleWimble protocol" https://github.com/mimblewimble/grin, 2019/01/30

160 beam, Github, "Beam: Scalable Confidential Cryptocurrency. A Mimblewimble implementation", https://github.com/BeamMW/beam, 2019/01/30

161 Commitment が v*H のみの場合、総当りで数値を H に乗算することで、コインの量が分かってしまうため、それを防ぐために単純に v*H のみでないのは別の要素 r を使ってブラインドしている。

ここで G は楕円曲線のベースポイント、H は G から生成される別の楕円曲線上の点、r はランダムな値であるブラインド要素、v が送金するコインの量を表す。r*G および v*H はそれぞれ楕円曲線上の点であり、上記のように送金量を、点と点を加算して出来た点（Commitment）としてエンコードすることで、送金量を秘匿する。

この Commitment に隠された量を知るのはブラインド要素とコインの量を知る取引の当事者のみである。また、Confidential Transaction と同様に、オーバーフロー攻撃（例えばマイナスの金額を用いた攻撃[162]）などが引き起こせないよう、コインの量 v が[0, 264]の範囲内であることを証明する範囲証明も併せて用いられる。

この Commitment は加法準同型性を持ち、トランザクションに 2 つのアウトプットがある場合、それぞれの Commitment を加算した値は以下の関係が成立する。

(r1*G + v1*H) + (r2*G + v2*H) = (r1 + r2)*G + (v1 + v2)*H

上記の特性を利用し、トランザクションの検証にあたっては、インプットの全ての Commitment を加算した値から、アウトプットの全ての Commitment を加算した点を減算し、それが 0 になるかを確認する。この検証により、他のノードはトランザクションの実際の送金量を知ることなく、送金額が正しいか検証することができる。

(In1 + In2 + In3 + ...) - (Out1 + Out2 + Out3 + … + fee[163]*H) = 0

(ii) ブラインド要素による所有権の表現

ビットコインの場合は、任意の公開鍵宛てにロックされたコインは、対応する秘密鍵で生成したデジタル署名を提供することで、そのコインの所有権を証明するが、Mimblewimble では各 Commitment のブラインド要素を秘密鍵として扱う。

コインを受信する場合、受信者はまずブラインド要素となる秘密鍵を選択する。選択した秘密鍵を 28、送金するコインの量を 3 コインとすると、その Commitment は以下のようになる。

C1 = 28G + 3H

ブロックチェーン上では C1 は UTXO として誰もが確認できる。この 3 コインの UTXO をそのまま送金する場合、通常であればインプットのコミットメントの合計からア

162 例えば、インプットの金額を 3、アウトプットの金額を 5 と-2 にして、不当にコイン数を増やす攻撃などが挙げられる。
163 fee は手数料で明示的に設定される。

ウトプットのコミットメントの合計を差し引くと 0 になるルールのため、アウトプットの Commitment も同じブラインド要素の値を使った 28G + 3H になる。

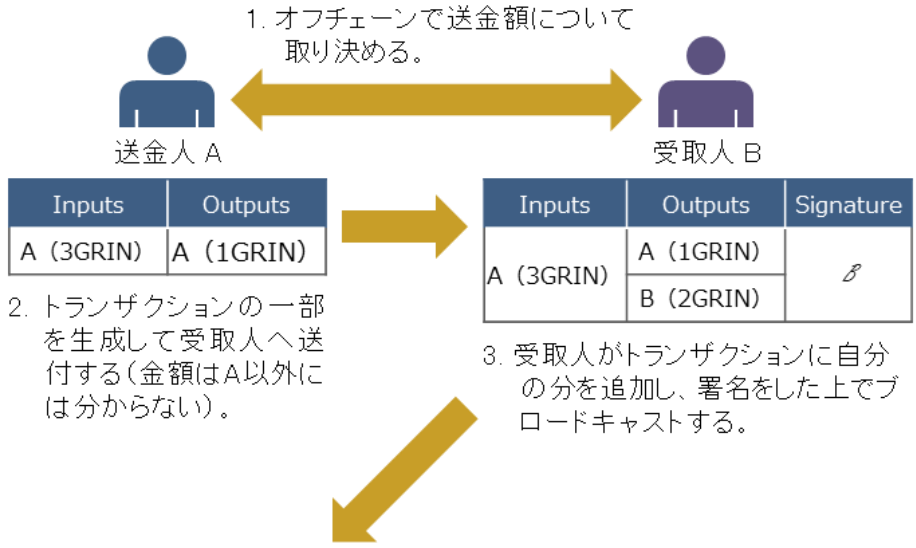
ただし、この場合、ブラインド要素を用いて所有権を証明するという意味では、C1 の所有者が送金先のコインの所有権を証明できてしまう（すなわち、送金したコインも利用できてしまう）ことになり、送金したことにはならない。この問題を解消するため、コインの受信者は必ず自分しか知らない秘密鍵を選択する。ここで C1 を受け取る際の受信者が選択した秘密鍵を 113 とすると、そのコミットメントは、以下になる。

C2 = 113G + 3H

この時、C2 - C1 = 85G + 0H となり超過値 85G が残る。85G は楕円曲線上の有効な点であるため、C2 - C1 の結果が楕円曲線上の有効な点であり、その点に対応する有効な署名が提供されれば、そのコインの所有権を証明することができる。これは、そのような署名が作成できるのはブラインド要素および、その計算によって得られた超過値の値を知る受信者のみであるためである。

上記を踏まえ、送金にあたっては、送金人と受取人の双方は協力して以下の手順でトランザクションを作成する（図表 72）。ビットコインとは異なり送金人のみでは完結しない点が大きく異なり、例えば Beam にはオフチェーンで送金人と受取人がやり取りする仕組みも含まれている。また、送金元や送金先を示すアドレスなどの識別子も不要となっている。

図表 72 Mimblewimble の送金フロー



(1) 送金人と受取人は送金するコインの量について合意する。

(2) 送金人はトランザクションの雛形を作成し、アウトプットとなる、お釣りとして受け取るコインの Commitment に使用するブラインド要素から、全てのインプットのブラインド要素の総和を引いた値を計算する。トランザクション雛形とブラインド要素の差分の値を受取人に送る。

(3) 受取人は受け取り用の Commitment で使用するランダムなブラインド要素を選択し、1 で合意したコインの量から手数料を差し引いた量を Commitment のコインの量として、作成した Commitment をトランザクションに追加する。この段階で受信者はコミットメントの総和を計算でき、超過分のブラインド要素を知ることができる。

受取人は(3)で計算した超過分の値を秘密鍵とした署名を作成し、それをトランザクションにセットしてトランザクションを完成させ、ブロードキャストする。

ビットコインであれば各インプットを使用する条件としてインプットの所有者の署名を必要とするが、Mimblewimble の場合は、上記のように受取人が署名することで、コインの受け渡しが可能になる。

(iii) トランザクションカットスルー

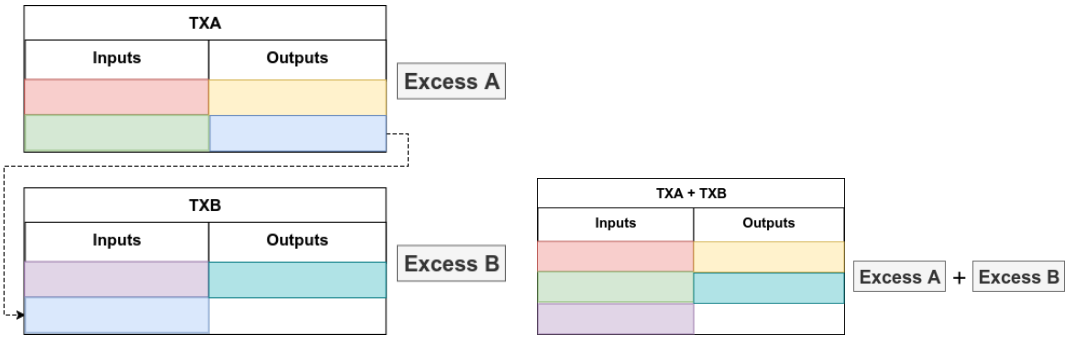
Mimblewimble のもう1つの特徴がブロックチェーンデータの削減と、それに伴うプライバシーの向上である。

2 つのトランザクション TX^A と TX^B があり、それぞれの超過分の値(Excess Value と呼ぶ)を k1G と K2G とする。これら 2 つのトランザクションはそれぞれのインプットとアウトプットのリストを組み合わせて1つのトランザクションにすることが可能で、その際、k1G と k2G も加算して k3G ＝ k1G + k2G とする。Mimblewimble では、各トランザクションを組み合わせた場合に、それぞれのトランザクションの署名を組合せたものも有効な署名となるよう集約することができる[164]。

上記の特性を活かすと、図表 73 のように、2つのトランザクション TX^A と TX^B を組み合わせて1つのトランザクションにする際、TX^A の青いアウトプットと TX^B の青いインプットを相殺して、それらを削除したトランザクションを作成することができる。

164 こうした性質を持つ署名は one-way aggregate signature と呼ばれ、Grin では Schnorr 署名が用いられている。

図表 73 トランザクションカットスルーのイメージ（左：マージ前のトランザクション群、右：マージ後のトランザクション）



こうしたUTXOの削除が可能なのは、青色のCommitmentは同値であり、差分を計算するという意味では、インプットとアウトプットの差分を計算する際に相殺され、計算結果に影響を与えないためである。この仕組みをトランザクションカットスルーと呼び、ブロックチェーン全体に適用することで、ブロックチェーンのサイズを大幅に削減することが可能になる。また、上記のように使用済みのアウトプットが相殺されることから、取引自体が削除される場合も生じ得るため、再識別が困難になるとも言える。

3.2.2.7.3 課題およびそれらに関連した新たな取り組み

MimbleWimbleの課題として以下が挙げられる。

- スクリプト機能がないこと

  MimbleWimbleには、ビットコインとはトランザクションの構造が大きく異なり、ビットコインのスクリプト機能（スマートコントラクトに相当する機能）がない。そのため、一部の機能を署名に含めるスクリプトレススクリプトなどが提案されているが、本稿執筆時点で全ての機能は代替されていない。

  例えば、ライトニングネットワークやアトミック・クロスチェーン・スワップなどで用いられるハッシュ・タイムロック・コントラクトのタイムロック機能などは、スクリプト以外で対応する方法などが提案されている。

- 金額秘匿の弊害

  特にMimbleWimbleをライトニングネットワークと組み合せる場合、第三者から金額が秘匿されているために、送金人は、受取人までの最適な経路を計算できない問題が生じ得る。

- 量子耐性

Pedersen Commitment は量子耐性がないため、量子コンピュータが実用化されると、コインを任意の量生成することが可能となり、ネットワーク全体に影響を与えることになる。そのため、量子耐性を備えた Switch Commitments[165] などが提案されている。

3.2.2.8 Schnorr 署名（シュノア署名）

3.2.2.8.1 背景

ビットコインで導入されているデジタル署名方式は楕円曲線暗号をベースとした ECDSA だが、今後の Bitcoin の拡張の1つとして Schnorr 署名のサポートが検討されている[166]。Schnorr 署名は ECDSA と異なり数学的に安全性が証明されており、ECDSA のようなトランザクションの展性問題もなく[167]、特に複数の公開鍵や署名データを1つに集約することができる線形特性が注目されている。この特性を利用することで、トランザクションのデータサイズを削減し、プライバシーを向上させることが可能になると期待されている。

3.2.2.8.2 仕組み

(i) 署名の作成

Schnorr 署名の署名データは以下の手順で計算される。ここで G は楕円曲線上のベースポイント、x は秘密鍵、x に対応する公開鍵は X = xG、H をハッシュ関数、m を署名対象のメッセージとする。

(1) 乱数 k を選び、楕円曲線上の点 K ＝ kG を計算する（k は秘密鍵、K は公開鍵にあたる）。

(2) s = k + H(X, K, m)x を計算し、公開鍵 X とメッセージ m に対して有効な Schnorr 署名データを（K, s）とする。

165 Ruffing, T., et al, Eprint, "Switch Commitments: A Safety Switch for Confidential Transactions", https://eprint.iacr.org/2017/237.pdf, 2019/2/15

166 bips, Github, "bip-schnorr.mediawiki", https://github.com/sipa/bips/blob/bip-schnorr/bip-schnorr.mediawiki, 2019/02/12

167 署名検証に影響しないように余計なバイトコードなどを追加して、トランザクションの意味する内容は変えずに、そのハッシュ値のみを変えることにより引き起こされる問題を指す。

(ii) 署名の検証

公開鍵 X とメッセージ m、署名データ（K, s）が与えられた場合、署名の有効性は以下の数式が成り立つかを確認することで検証する。

$$sG = kG + H(X, K, m)xG = K + H(X, K, m)X$$

(iii) 署名の集約

Schnorr 署名を用いることにより、以下のような署名の集約が行えると期待されている。ここでは A と B がそれぞれ秘密鍵 x1、x2 と、それに対応する公開鍵 X1 = x1G、X2 = x2G を持つとする[168]。

(1) A は乱数 k1 を選び、楕円曲線上の点 K1 ＝ k1G を計算する。

(2) B は乱数 k2 を選び、楕円曲線上の点 K2 ＝ k2G を計算する。

(3) 両者はそれぞれ K1、K2 および公開鍵 X1、X2 を交換し、X = X1 + X2、K = K1 + K2 を計算する。

(4) A は s1 = k1 + H(X, K, m)x1 を計算する。

(5) B は s2 = k2 + H(X, K, m)x2 を計算する。

(6) 両者はそれぞれ s1、s2 を交換し、以下を計算する。

$$s = s1 + s2 = k1 + k2 + H(X, K, m)(x1 + x2)$$

（K, s）が公開鍵 X（＝X1 + X2）とメッセージ m に対して有効な署名データとなる。すなわち、各自の署名を加算することで、X に対して有効な署名データを 1 つに集約することができるようになる。

168 単純に A が B から送られた公開鍵を自分の公開鍵に加算するだけでは、予め B が不正を行う場合が考えられる。具体的には、B の公開鍵から A の公開鍵を減算した公開鍵（X2 - X1 の点）を B が送ってくる可能性があり、A がこの送られた公開鍵に自分の公開鍵を加算しても B の公開鍵になり（X2 - X1 + X1 = X2）、B の秘密鍵だけでコインが利用できてしまう。そのため、Schnorr 署名をマルチシグに利用する場合、こうした攻撃に耐性のあるプロトコルを採用する必要があるが、本稿では割愛している。Maxwell, G., et al, "Simple Schnorr Multi-Signatures with Applications to Bitcoin", https://eprint.iacr.org/2018/068.pdf, 2019/02/12

3.2.2.8.3 新たな取り組み

(i) Schnorr 署名を用いたマルチシグ

マルチシグとはあるコインを利用する際に、予め決められた一定数のユーザの署名が必要となる機能である。マルチシグに Schnorr 署名を用いることにより、トランザクションサイズの縮小とプライバシーの向上が期待されている。

例えばコインの使用に 2 人の署名を必要とするマルチシグは、現状のビットコインでは以下のスクリプトが用いられる。

2 <公開鍵 X1> <公開鍵 X2> 2 OP_CHECKMULTISIG

このようなスクリプトが使われたコインを利用するには、公開鍵 X1と公開鍵 X2 に対応するそれぞれの秘密鍵による署名が 2 つ必要になる。

これを Schnorr 署名で行う場合は、2 つの公開鍵 X1、X2 を加算した X = X1 + X2 という別の公開鍵を用いて、この X 宛てにコインを送金する。このコインを使用するためにはとなる二人の署名を集約した署名 s = s1 + s2 が必要となり、二人の協力が必要という点でマルチシグと同等の機能を持つことになる。また、Schnorr 署名は、全員の署名が必要となる n-of-n 以外に[169]、m-of-n のような閾値署名を実現することもできる。

このように公開鍵および署名を集約することで、今まで個別に必要だった公開鍵および署名データが1つになり、ブロックチェーンに記録されるデータを削減する効果が見込まれる。

また、ブロックチェーン上は単一の公開鍵宛にコインを送っているように見えるが、実際はマルチシグ宛にコインを送っており、その事を当事者以外誰も知り得ないという意味でプライバシーの向上にも寄与すると考えられる。

(ii) Schnorr 署名を用いたトランザクションサイズの削減

Schnorr 署名を利用するとマルチシグのトランザクションデータを削減する以外に、複数のインプットを持つようなトランザクションのデータも削減できる。これは、現在のビットコインではインプット毎に各々署名が必要になるが、Schnorr 署名を利用する

169 マルチシグは、例えば 5 人のうち 3 人が署名を行ったら有効となるように指定することもできる。これは一般に 3-of-5 と表記される。一般化して考えると、m-of-n のマルチシグとは n 人のうち m 人が署名を行えば有効となるものを指す。n-of-n マルチシグとは、n 人のうち n 人全員が署名を行えば有効となるマルチシグである。

と、このような複数のインプットの署名を1つの署名に集約することが可能であるためである。

(iii) Schnorr 署名を用いたスクリプトレススクリプト

署名集約以外にも、Schnorr 署名と、Schnorr 署名に乱数 r をさらに加えた Adaptor 署名を用いることで、スクリプトレス・アトミック・クロスチェーン・スワップを実現することも可能になる。詳細は 3.2.2.6.3(i)節「Schnorr 署名を利用したスクリプトレス・アトミック・クロスチェーン・スワップ」を参照のこと。

(iv) ビットコインへの導入

2019 年 2 月時点で Schnorr 署名を Bitcoin へ導入するための具体的な計画は合意されていないが、Schnorr を利用した署名検証の仕組みは Segwit[170]の導入時に新たに追加されたスクリプトのバージョン機能を利用して、ソフトフォークで導入されると見られている。Segwit では、以下のような形式のロックスクリプトの雛形を導入した。

<witness version> <witness program>

最初の要素（witness version）がスクリプトのバージョンで、2 つ目の要素（witness program）がスクリプトになる。スクリプトのバージョンには 0～16 までのバージョンが定義可能で、Segiwt ではバージョン 0 のスクリプトが定義された[171]。バージョン 1～16 は未定義で、例えばバージョン 1 を Schnorr 署名を使った検証を行うスクリプトであると定義することで、バージョン 1 の場合は ECDSA ではなく Schnorr 署名を使った検証を行うようルールを追加することができる。

上記以外に実現する方法としては、未定義の OP_NOP 系の opcode を Schnorr 署名に割り当て、Segwit のバージョンに関係なく既存のスクリプトの中でも Schnorr を利用した署名検証を可能にするというアプローチもある。いずれにしてもソフトフォークで導入可能である。

---

170 2017/08/24 にビットコインでアクティベートされた機能であり、署名を個々のインプットから分離して記録することで、より多くの取引を記録できるようにする機能を指す。

171 バージョンが 0 で、その後の witness program のデータ長が 20 バイトであれば、それを公開鍵のハッシュとして認識しスクリプトは P2WPKH として扱い、データ長が 32 バイトであれば、それをスクリプトのハッシュとして認識し P2WSH として扱うというルールが定められた。

(v) Taproot と Graftroot

Schnorr 署名の導入に向けて、Schnorr を利用したさまざまな機能追加の提案もされている。代表的なのが Taproot[172]と Graftroot[173]という新しいコンセプトである。

Taproot とは、マルチパーティ間で行うスクリプトのプライバシーを向上させる仕組みである。Bitcoin のスクリプトを使ってコントラクトを構成する際によくあるのが、以下のように、アンロック条件が 2-of-2 のマルチシグか、その他の条件となるスクリプトである。

```
OP_IF
    2 <公開鍵 P1> <公開鍵 P2> 2 OP_CHECKMULTISIG
OP_ELSE
  <タイムロック> OP_CSV OP_DROP <公開鍵 P3> OP_CHECKSIG
OP_END
```

上記のロックスクリプトをアンロックするには、以下のいずれかが必要になる。

- 公開鍵 P1、公開鍵 P2 に対応した秘密鍵で作られた2つの署名
- タイムロック期間が経過した後であれば、公開鍵 P3 に対応した秘密鍵で作られた署名

ただし、上記のようなコントラクトを実行する場合は、実際にアンロックに使用する条件はどちらか1つにも関わらず、両方の条件がブロックチェーン上に記録されてしまう。これには未使用の条件が公開されるというプライバシーの問題とブロックチェーンに記録するデータ量が増えるという問題の 2 つの問題が存在する。この問題を解決する仕組みが Taproot である。

Taproot では以下の手順で上記のロックスクリプトを1つの公開鍵に変換する。

(1) 最初の OP_IF に対応する部分は、公開鍵 P1 と P2 を集約して公開鍵 P4 = P1 + P2 を作成する。

172 Gregory Maxwell, Linux Foundation, "[bitcoin-dev] Taproot: Privacy preserving switchable scripting", https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html, 2019/2/20
173 Gregory Maxwell, Linux Foundation, "[bitcoin-dev] Graftroot: Private and efficient surrogate scripts under the taproot assumption", https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-February/015700.html, 2019/2/20

(2) 次の OP_ELSE に対応する部分は

S = <タイムロック> OP_CSV OP_DROP <公開鍵 P3> OP_CHECKSIG

とする。

(3) P4 と S から、公開鍵 P5 = P4 + H(P4, S)G を計算する。

公開鍵 P5 宛てにコインを送金すると、そのコインを利用する方法は以下の2つに限られるため、元々のスクリプトに送金したのと同じ効果が得られる。

- 最初の OP_IF に対応する部分でアンロック（コインを利用）する場合

  公開鍵 P5 は、公開鍵 P1 と P2 を集約した公開鍵 P4 と、H(P4, S)を秘密鍵として生成した点 H(P4, S)G を加算した点であるため、P1 と P2 のそれぞれの秘密鍵を使って集約署名 s を計算し、その s に H(P4, S)をもう1つの秘密鍵として加算することで、P5 に対して有効な署名を作成することができる。この署名を提供することで、コインが利用可能になる。

- タイムロック期間が経過した場合の条件を使ってアンロック（コインを利用）する場合

  P5 を構成する集約鍵 P4 とスクリプト S を提供し[174]（この場合、P4 + H(P4, S) が P5 と合致する）、さらに公開鍵 P3 に対して有効な署名を提供することで、コインが利用可能になる。

OP_IF に対応する部分でアンロックする場合、ブロックチェーン上には公開鍵 P5 に対して有効な署名が提供されるだけであるため、ブロックチェーン上に記録される情報の範囲は最小限となり、アンロックされる以外のもう片方の条件は秘匿される。そのため、データサイズを削減するとともに、不要な条件を記録しないという点でプライバシーも保つこともできると考えられる。

もう一方の Graftroot は、コインをロックした後から柔軟にアンロック条件を追加できるようにする仕組みである。Graftroot も Taproot と同様に、公開鍵 P1 と公開鍵 P2 から集約公開鍵 P4 = P1 + P2 を作るところまでは変わらない。Taproot の場合、そこからさらにアンロック条件のスクリプトを加味して公開鍵を作っていたが、Graftroot の場合は単純に P4 に対してコインを送金する。P4 のコインは当然、P1 と P2 に対応する秘密鍵を持つユーザが協力して集約署名を作成することでアンロック

174 取引当事者は公開鍵 P5 を作成する過程で、公開鍵 P4 を保持している。

することができるが、それ以外のアンロック条件は後から任意に追加することができる。具体的には以下のような手順で別のアンロック条件を追加する。

(1) アンロック条件を記載したスクリプトを作成する。

S = <タイムロック> OP_CSV OP_DROP <公開鍵 P3> OP_CHECKSIG

(2) S を署名対象のメッセージとして公開鍵 P4 に対して有効な署名を作成する。

(3) S と(2)で作成した署名を提供し、その署名が P4 に対して有効な署名であれば S の条件を使ってコインをアンロックすることができるようになる(すなわち、公開鍵 P3 に対して有効な署名を提供することで、コインが利用可能になる)。

コントラクトの公開範囲を最小限に留め、データ量を削減するという意味では Taproot と同じ効果があるが、Graftroot の場合 Taproot と異なり後からいつでもどのようなアンロック条件でも追加できるというメリットがあり、より柔軟なコントラクトの作成が可能になると考えられる。

3.2.2.9 Dandelion(ダンデリオン)

3.2.2.9.1 背景

ビットコインでは、各ノードは新しく作成された情報(ブロックやトランザクション)を隣接するノードに対して送信し、各ノード間でこの情報伝達を繰り返し行い P2P ネットワーク全体にデータを配信するゴシッププロトコルを採用している。

ビットコインの主要なクライアントである Bitcoin Core では、ノードがトランザクションを中継する際、ノード毎にランダムな遅延時間を設けてトランザクションを伝播させることで、当該トランザクションの発信元 IP アドレスを匿名化する仕組みを持っている。ただし、これだけでは必ずしも十分ではなく、大量のセンサーノードを用意して P2P ネットワークを流れるデータを分析することで、トランザクションの発信元 IP アドレスを特定することができると指摘されている。

このような問題を解決するために、2017 年に、Giulia Fanti らによって P2P ネットワークに匿名性の保証を提供するプロトコル Dandelion[175]が発表された。当初発表された内容には、第三者による再識別(非匿名化)につながる複数の脆弱性が発見され

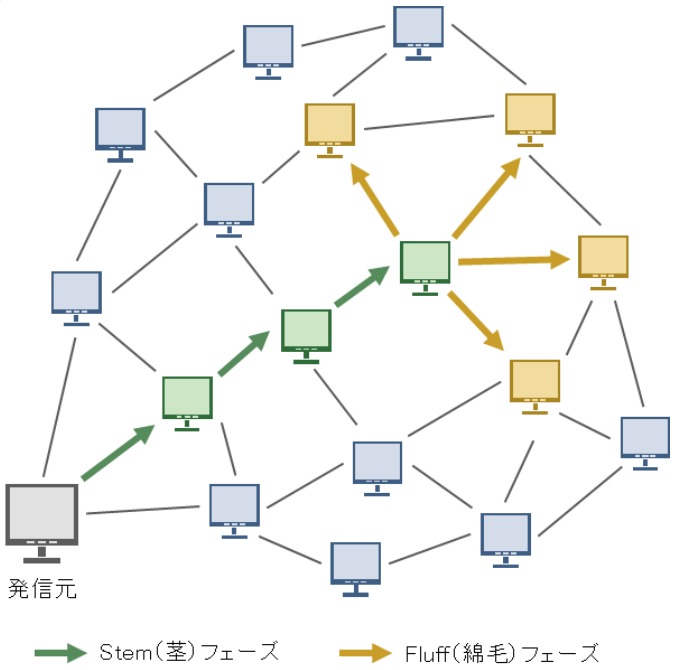
[175] Venkatakrishnan, S., et al, arXiv, Cornell University, "Dandelion: Redesigning the Bitcoin Network for Anonymity", https://arxiv.org/pdf/1701.04439.pdf, 2019/02/22

たため、2018 年 5 月に元のプロトコルを改良した Dandelion++[176]（以下省略して Dandelion と表記する）が提案された。

3.2.2.9.1 仕組み

Dandelion プロトコルでは、トランザクションを拡散する前に、ランダムに選択した経路を使ってトランザクションを一定数ホップする匿名化層を追加することで、トランザクションの発信元ノードの特定を困難にする。このトランザクション拡散までのルーティングは以下の3つのフェーズで構成される（図表 74）。

図表 74 Dandelion のトランザクション中継のイメージ



(i) 匿名グラフの構築

最初に、ビットコインの P2P ネットワークの部分グラフである匿名グラフを構築する。各ノードは接続元となるインバンドノードと接続先となるアウトバウンドノードを持つが、アウトバウンドノードのサブセットを宛先としてランダムに選択する。これが次の Stem フェーズでトランザクションを送信する対象ノードとなる。このサブセットは 10 分毎に定期的に更新されるため、攻撃者がネットワーク内の匿名グラフを分析するのは困難である。

[176] Fanti, G., et al, arXiv, Cornell University, "Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees", https://arxiv.org/pdf/1805.11060.pdf, 2019/02/22

以降では、Dandelion を用いるトランザクションを通常のトランザクションと区別するため、Dandelion トランザクションと表記する。

(ii) Stem（茎）フェーズ

Stem フェーズで発信元ノードから Dandelion トランザクションが送信される。Dandelion トランザクションを受信したノードは、当該トランザクションをランダムに選択した宛先ノードに中継し Stem フェーズを継続するか、次の Fluff フェーズに移行するかを決定する。この決定は確率的に行われ 90%の確率で Stem フェーズが継続されるようになっており、Stem フェーズのホップは約 10 ホップとなる。

なお、Stem フェーズで受信した Dandelion トランザクションは、通常のトランザクションと一緒にメモリプールに入れられることはなく、Stem プールと呼ばれる別のプールに隔離して管理され、他のノードから照会があっても Dandelion トランザクションについては応答しない。

(iii) Fluff（綿毛）フェーズ

Stem フェーズから Fluff フェーズに移行するのは、Stem フェーズで Dandelion トランザクションを受信した各ノードが Fluff フェーズへの移行を決定した場合か、各ノードに予め設定されている有効期限を過ぎた場合かのどちらかである。

Fluff フェーズに入ると、Dandelion トランザクションは通常のトランザクションと同じ扱いとなる。従来と同じく、アウトバウンドノード全てへランダムな遅延時間を設けてブロードキャストされ、Dandelion トランザクションは通常のメモリプールへ移動させられる。また、それまで Dandelion トランザクションを中継してきた Stem フェーズのノードも当該トランザクションを通常のトランザクションと同様にブロードキャストする。

有効期限はノード毎にランダムな値が設定される。これにより Stem ノード内のどのノードが最初に有効期限切れになるかは予測できなくなるため、ブロードキャストを行うノードを事前に予測することはできない。また有効期限を設定することは、Stem ノードが処理をせず、トランザクションが永遠に処理されない等の事態を防ぐ効果もある。

上記のように、Stem フェーズではトランザクションは単一のノードから単一のノードに中継され、Fluff フェーズで一気に拡散する構造がタンポポの構造と似ていることが Dandelion の由来となっている。

3.2.2.9.2 新たな取り組み

Dandelion プロトコルは軽量で複雑な計算の必要もなく、ブロックチェーンの基盤プロトコルに大きな変更を加えることなく導入でき、Stem フェーズのオーバーヘッドも 10 ホップ程度であれば数秒で済み、匿名性の強化に伴い速度を大幅に犠牲にすることもない。そのため、ゴシッププロトコルを採用する多くのブロックチェーンで広く採用される可能性がある。

2018 年 9 月 28 日には、匿名通貨の一種である Zcoin が Dandelion++の実装を発表している他[177]、Mimblewimble をサポートしている Grin も Dandelion を導入しており、現在引き続き Dandelion++の対応が進められている。

Mimblewimble のプロトコルで Dandelion をサポートする場合、オリジナルの Dandelion プロトコルに若干の変更が加えられる。Dandelion ノードが Stem フェーズでトランザクションを中継する際に、一定時間待機し、集まった複数のトランザクションに対してそれぞれ Stem フェーズに進むか Fluff フェーズに進むか決定した後、Stem フェーズに進むトランザクションについては、集約およびカットスルーを行う。そして集約されたトランザクションが次の Dandelion ノードへ中継される。こうすることでトランザクションを拡散する前に、Stem フェーズ中のトランザクションの集約により、その存在自体削除される取引が生じることになり、匿名性はさらに高まることになる。

またビットコインにおいても、BIP 156[178]としてビットコインに Dandelion を適用するための提案が提出され、2019 年 2 月時点ではまだコードはマージされていないものの、Dandelion を Bitcoin Core に実装するプルリクエスト[179]は提出されており、今後ビットコインに採用される可能性も考えられる。

---

[177] Reuben Yap, ZCoin, "Plus Plus Privacy: Zcoin Integrates Dandelion", https://zcoin.io/plus-plus-privacy-zcoin-integrates-dandelion/, 2019/02/22

[178] Denby, B., et al, Github, "Dandelion - Privacy Enhancing Routing", https://github.com/bitcoin/bips/blob/master/bip-0156.mediawiki, 2019/02/22

[179] MarcoFalke, Github, "Dandelion transaction relay (BIP 156)", https://github.com/bitcoin/bitcoin/pull/13947, 2019/02/22

3.3 分散型取引所（DEX、Decentralized EXchange）にかかる調査

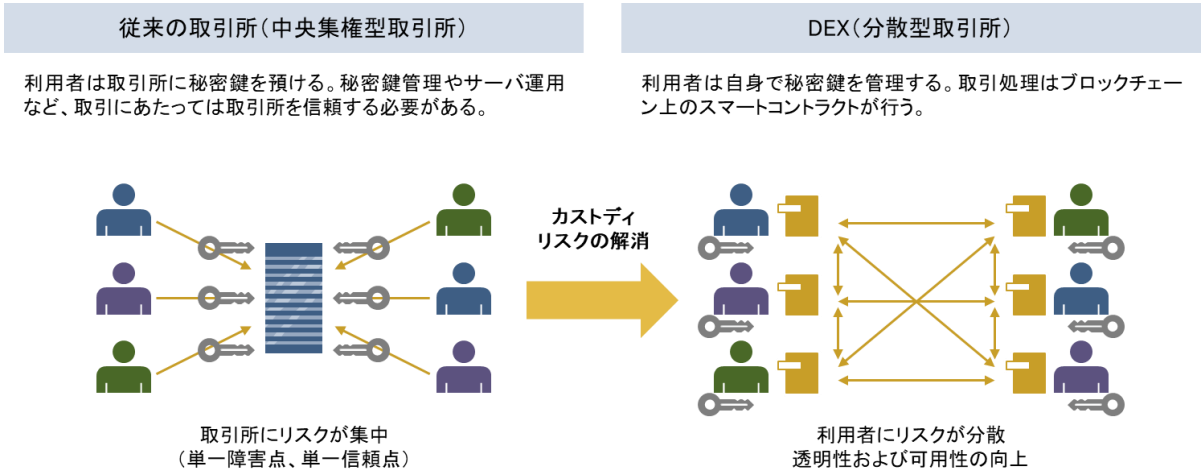
本節では、「プライバシー保護技術及び分散化技術を巡る開発状況の調査」における DEX の開発状況について記載する。

3.3.1 概要

本章では、「プライバシー保護技術及び分散化技術を巡る開発状況の調査」における DEX の開発状況について記載する。

DEX とは中央管理主体の存在しない取引所を指し、Peer to Peer 技術を用いて、売り手と買い手のマッチング、価格形成、決済など、取引所として必要な一連の機能を中央管理主体なしに提供するものである（図表 75）。

図表 75 中央集権型取引所と DEX の比較



3.3.1.1 DEX が生まれた背景

暗号資産の利用にあたっては秘密鍵が必須となる。そのため、秘密鍵を失うことは当該暗号資産を失うことを意味し、反対に、秘密鍵を取得することは当該暗号資産を得たことを意味する。

ここで、特定の事業者が運営する従来の取引所（以下、中央集権型取引所）では、利用者の秘密鍵を管理するサービス（カストディ・サービス）も提供している。これは主に利用者の利便性（利用者側で、複数のブロックチェーン毎の秘密鍵の管理やトランザクションの生成、ブロードキャスト等が不要等）や実務上の効率性（取引所側で注文時の残高確認が可能、取引所では顧客間のネッティングなどブロックチェーン外の処理を行うため利用者が勝手にブロックチェーン上にブロードキャストできないように

コントロールが必要等）が理由となっている。

他方で、これは中央集権型取引所にはカストディリスクが存在することを意味し、例えば、当該取引所がハッキング被害等に見舞われると顧客資産が不正に流出する[180]、当該取引所のシステムが障害に見舞われると取引が不可能となる、多額の顧客資産（を意味する秘密鍵）を保持するため当該取引所へのハッキングが誘発されやすいなどの問題が生じる。

上記のような中央集権型取引所のカストディリスクを解消するために、利用者が取引所に秘密鍵の管理を委ねること無しに、自分自身で秘密鍵を管理する形で取引を可能とする取引所が DEX である[181]。

図表 76 中央集権型取引所と DEX の比較例

	中央集権型取引所	DEX
障害点・信頼点	取引所運営主体	DEX 運営主体やスマートコントラクトの場合が多い
法定通貨との交換	可能	不可能の場合が多い
暗号資産との交換	可能	可能
カストディ機能	あり（取引所が顧客の秘密鍵を管理）	なし（利用者が自身で秘密鍵を管理）
流動性管理機能（オーダーブック管理機能）	あり	ありの場合が多い 他に、販売所機能のみでオーダーブックを使わないものもある
ユーザビリティ	良い（証拠金取引等が可能、ストップロスやリミットオーダー等がある、取引可能な暗号資産の種類が多い）	悪い（一般に証拠金取引等はない、一般にストップロスやリミットオーダーはない、取引可能な暗号資産の種類は少ない）
流動性	高い	低い
本人確認	必須	なしの場合が多い

DEX の大きな特徴としては、①秘密鍵を利用者が管理すること、②特定の事業者ではなくスマートコントラクトが取引処理を行うことの二点が挙げられる。①は、トランザクションの生成やブロックチェーン上へのブロードキャストを利用者が行うことで、カストディリスクの排除を図っている。②は、ブロックチェーン上にデプロイされてロジッ

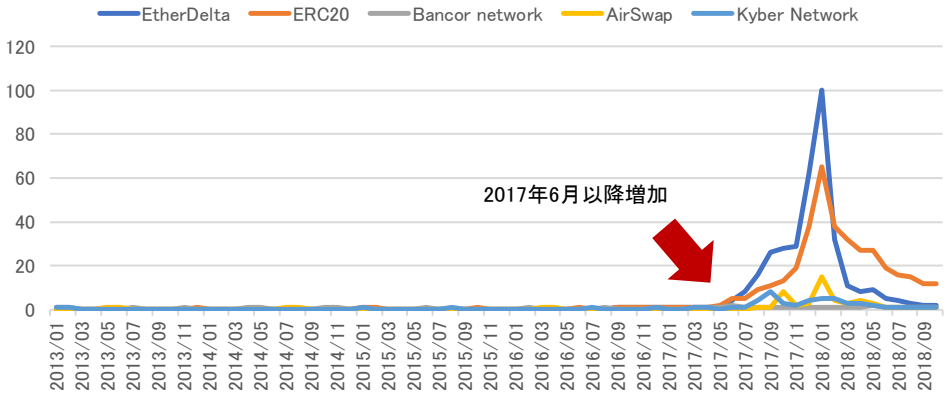
180 実際に、既に廃業・事業譲渡に至っている過去 36 の中央集権型取引所のうち 13 取引所でハッキング被害が報告されている。Parker, L., BRAVE NEW COIN., "36 bitcoin exchanges that are no longer with us", https://bravenewcoin.com/insights/36-bitcoin-exchanges-that-are-no-longer-with-us, 2018/12/27

181 これはカストディ・リスクを個人に移転することにあたるため、個人がハッキング被害のリスクを背負うことになる点には留意する必要がある。

クが公開されているスマートコントラクトが処理を行うことで、DEX が不正を行う可能性や障害等で停止する可能性を排除している（透明性および可用性の向上）。

DEX という概念は、仮想通貨取引所マウントゴックス（Mt.GOX）や ShapeShift、Bitfinex などの大手仮想通貨取引所でのハッキングによる顧客資産流出事件を教訓に古くから提案がなされていた[182]。その後、ブロックチェーン上のスマートコントラクトを活用する有望なユースケースの一つとして 2017 年前半頃から一般に認知されるようになった[183]（図表 77）。

図表 77 DEX のキーワードの検索状況[184]



DEX は、特に暗号資産基盤イーサリアムのコミュニティを中心に開発が進められている。これは、イーサリアムがチューリング完全なプログラム言語を提供することや、イーサリアムでは独自トークンを発行するための仕様（ERC20[185]）が整備されており、約 14 万弱のトークンが存在する[186]。ICO（Initial Coin Offering[187]）等で既に様々なトークンが発行されていること[188]などが要因と考えられる。

---

182 ビットコインを用いた DEX である Bisq の Alpha Version0.1.0 が 2014 年 12 月にリリースされたのが、今回調査した限りでは最古の記述であった。Bisq, "Roadmap", https://bisq.network/roadmap/, 2018/12/27

183 Warren, W., et al., "0x: An open protocol for decentralized exchange on the ethereum blockchain", https://0xproject.com/pdfs/0x_white_paper.pdf, 2018/12/27

184 Google トレンドウェブサイト, Google, https://trends.google.co.jp/trends/, 2018/12/27 より三菱総研作成

185 イーサリアムブロックチェーン基盤上でのみ動くトークンであり、ERC20 Token Standard という仕様を満たすものである。The Ethereum Wiki, "ERC20 Token Standard", https://theethereum.wiki/w/index.php/ERC20_Token_Standard, 2018/11/5
ethereum, Github, https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md, 2018/11/5

186 Etherscan, etherscan.io, "Token Tracker", https://etherscan.io/tokens, 2018/11/5

187 新規の暗号資産関連プロジェクトが、プロジェクトの資金調達のために、当該プロジェクトで用いるトークンを事前に投資家に販売すること。クラウドファンディングの一種でありつつ、当該トークンの二次流通市場がある点が主な特徴と考えられる。BlockchainHub, "Initial Coin Offerings – ICOs", https://blockchainhub.net/ico-initial-coin-offerings/, 2018/11/5

188 2016 年には主要な ICO だけで 64 件、計約 1 億ドル調達したと報告されている。Coindesk, "2016: The Year Blockchain ICOs Disrupted Venture Capital", https://www.coindesk.com/2016-ico-blockchain-replace-

3.3.1.2 取引量等の規模

3.3.1.2.1 トランザクション数

DEX は開発中のものも多く、全体の取引量を取得することが困難であるが、一般に DEX の取引量（トランザクション数）は全体の約 1%程度と見積られている[189]。トランザクション数を Etherscan で確認すると、DEX はイーサリアム全体のトランザクション数の約 2-3%を占めることが分かる（図表 78）。

図表 78 DEX の占めるトランザクション数の割合（2018 年 11 月 7 日時点、DEX は Etherscan が把握している 22 取引所を指す）[190]

対象期間		イーサリアム全体	DEX	
		トランザクション数	トランザクション数	全体に占める割合
過去 7 日間	2018/10/31～2018/11/6	3,918,720	94,931	2.4%
過去 30 日間	2018/10/8～2018/11/6	16,615,189	483,034	2.9%

3.3.1.2.2 取引高

DEX の取引高は、過去 24 時間、過去 7 日間ともに全取引所の約 0.1%程度と考えられる（図表 79、図表 80、図表 81）。取引高が小規模に留まる理由としては、DEX の多くがイーサリアムの ERC20 トークンを扱うものであり、そのイーサリアムが 2018 年初来、時価総額およびレートを大きく落としていることも考えられる。

図表 79 DEX の取引高（2018 年 11 月 13 日時点）[191]

	過去 24 時間の取引高（調整あり）	過去 7 日間の取引高（調整なし）
USD	$7,413,898	$39,736,254
円	¥843,701,592	¥4,521,985,705

traditional-vc/, 2018/11/5

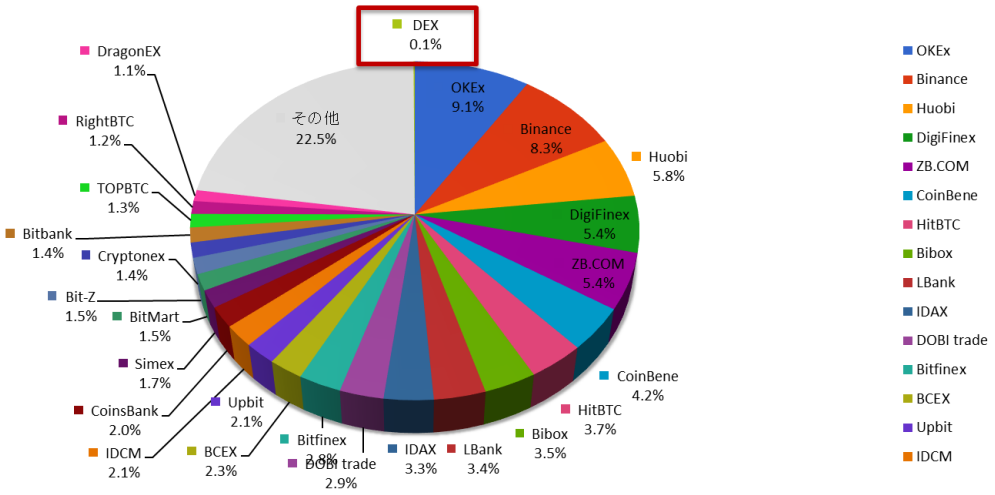
189 Sexer, N., Consensys, "State of Decentralized Exchanges, 2018", https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79, 2018/11/7

190 Etherscan, etherscan.io, "DEX Tracker Statistics", https://etherscan.io/stat/dextracker, 2018/11/7 より三菱総研作成

191 DEX は 17 存在した。調整有無とは手数料の無い取引を含むか否かを指す。CoinMarketCap, coinmarketcap.com, "Top Cryptocurrency Exchanges by Trade Volume", https://coinmarketcap.com/rankings/exchanges/, 2018/11/13 より三菱総研作成、

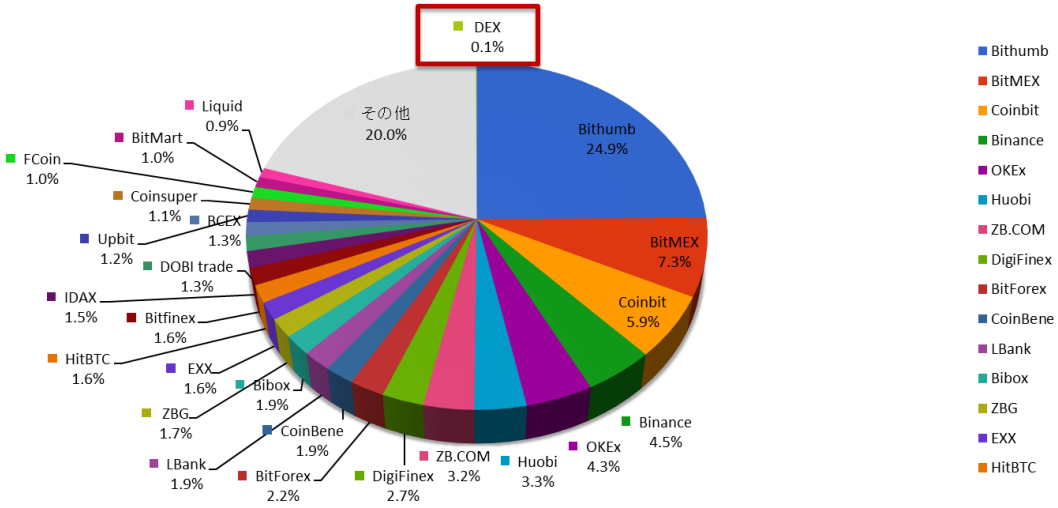
図表 80 過去 24 時間の取引高（手数料の無い取引等を除く）[192]

過去24時間の取引高割合（調整あり） 2018/11/13時点



図表 81 過去 7 日間の取引高（手数料の無い取引等を含む）

過去7日間の取引高割合（調整なし） 2018/11/13時点



3.3.1.2.3 アクティブユーザ数

ユーザ数については、ケンブリッジ大学の推定では全世界の 2017 年の暗号資産のアクティブユーザ数は 290 万～580 万と推定している[193]。最大のシェアを持つとされる IDEX（シェアについては図表 88 参照）においても、アクティブユーザ数は 2 千人程度（ユーザ数は約 25 万人以上）と公表されている。図表 82 をみると、DEX のア

192 脚注 191 の資料より三菱総研作成、ここで全取引所は 228、DEX は 17 存在した。調整有無とは手数料の無い取引を含むか否かを指す。

193 Cambridge Centre for Alternative Finance, "Global Cryptocurrency Benchmarking Study", https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf, 2018/11/13

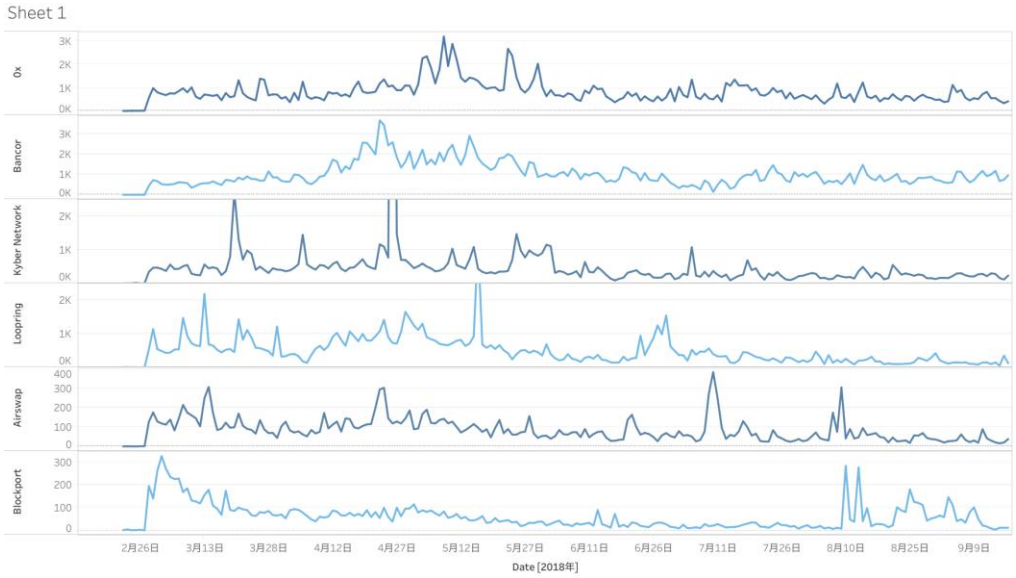
クティブユーザ数（約 6 千人）は全世界の暗号資産のアクティブユーザ数（290 万～580 万）対比で約 0.1%～0.2%程度に相当する。

図表 82 IDEX のアクティブユーザ数[194]

DEX	Daily Active Users
IDEX	2,056
ForkDelta	1,149
CryptoKitties	552
Etheremon	485
Bancor	422
FairDapp	411
Dai Stability System	371
PoWH 3D	295
DailyDivs	286
CryptoGirl	258
合計	6,285

他では、ERC20 トークンに絞った場合の暗号資産取引量を確認した結果では、DEX の 0x では平均 334 アクティブユーザ、一日あたり 818 トランザクション数程度と指摘されている[195]（図表 83）。

図表 83 DEX の ERC20 トークンの取引件数の推移（2018 年 2 月 24 日～2018 年 9 月 16 日）[196]



194 Whaling, F., Medium, "IDEX Q3 Recap: Product Updates, Integrations, Media & More", https://medium.com/aurora-dao/idex-q3-recap-product-updates-integrations-media-more-87bda4a5cadf, 2018/11/13 より三菱総研作成

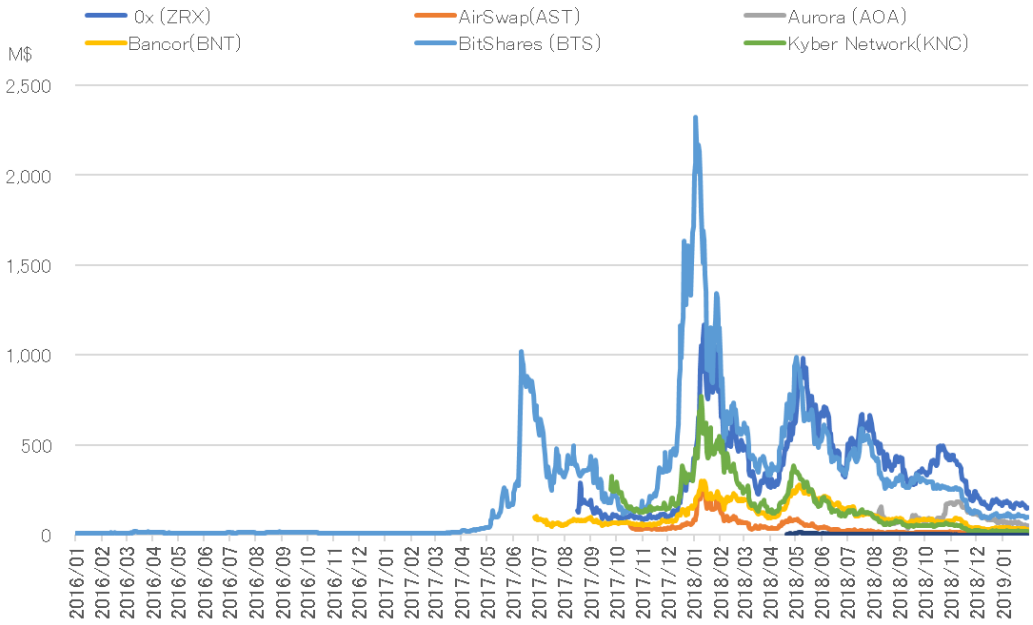
195 Wood, J., Medium, "Thoughts on Decentralized Exchanges and Real World Usage of their own Tokens ", https://medium.com/trivial-co/thoughts-on-decentralized-exchanges-and-real-world-usage-of-their-own-tokens-d0a6a16f5d3d, 2018/12/27

196 Jon, Tableau Public, https://public.tableau.com/profile/jon4285#!/vizhome/DEXTokenTransactions/Sheet1, 2018/11/13

3.3.1.2.4 時価総額

ICO を行っている DEX で主要な 0x について確認すると、約 2.9 億ドル（2018 年 9 月 17 日時点、当日の終値ベースで約 324 億円）程度であり、ビットコインの時価総額約 12 兆円やイーサリアムの時価総額約 2 兆円などと比較すると、規模は数%程度と限定的である（図表 84、図表 85）。

図表 84 主要な DEX の時価総額の推移[197]



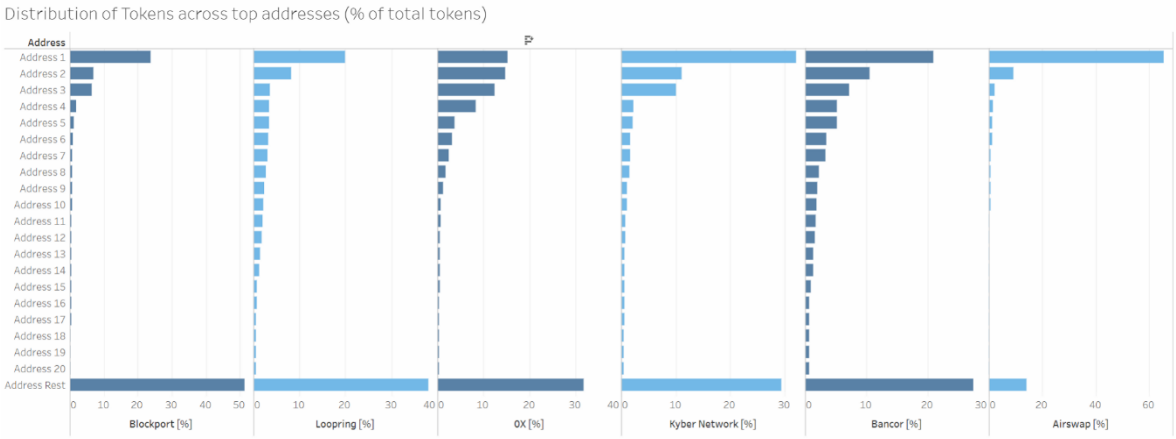
図表 85 時価総額の比較（2018 年 9 月 17 日時点）[198]

	米ドル	日本円	ビットコイン時価総額に対する割合	イーサリアム時価総額に対する割合
ビットコイン	108,497,127,334	¥12,133,233,749,761.20	100.00%	-
イーサリアム	20,188,412,622	¥2,257,670,183,518.26	18.61%	100.00%
0x	289,316,656	¥32,354,281,642.72	0.27%	1.43%
IDEX(Aurora)	10,125,938	¥1,132,383,646.54	0.01%	0.05%

なお、ICO で調達した資金は極少数のアドレスで保持されていることが指摘されている。これらのアドレスの所有者は開発グループと推定されている（図表 86）。

197 CoinMarketCap, coinmarketcap.com, "Historical data", https://coinmarketcap.com/ 2019/1/31 より三菱総研作成。
198 CoinMarketCap, coinmarketcap.com, "Historical data" https://coinmarketcap.com/currencies/ethereum/historical-data/, 2018/11/13 より三菱総研作成。

図表 86 ICO で調達した資金の分布状況（極少数のアドレスに集中）[199]



以上より、仮想通貨取引所に占める DEX の占める割合は本稿執筆時点では限定的であり、ユーザ数やトランザクション数でみて凡そ数%以内の範囲と考えられる。

3.3.2 事例調査

開発者から見た場合、DEX の設計にあたっては、どの部分をオフチェーンで処理するかという点が重要なポイントとなる。処理を特定のノードや主体に集中させるほど、効率的な処理が可能となる一方、障害対応やセキュリティリスクを高めることになるからである。ここで、オフチェーン処理が存在することは、それを管理する主体が存在することを意味する。また、同一ブロックチェーン基盤上のトークン（以下、同種トークン）のみを扱うか、異なるブロックチェーン基盤上のトークン（以下、異種トークン）や法定通貨も扱うかという点も、互換性や技術的な難易度の点から重要なポイントとなる。ここで、取扱資産の充実度は、ユーザの利便性の観点から見ても、極めて重要なポイントになる。

これら二点は当局にとっても重要なポイントであり、オフチェーン処理の存在、すなわち管理主体が存在することは規制対象先が存在することを意味し、異種トークンの取扱、すなわち匿名通貨や法定通貨と交換が可能であるということは AML/CFT における DEX の重要性が大きいことを意味するからである。

そのため、本調査研究では、図表 87 に示すとおり、特定の管理主体の有無および取扱トークンの種類の二軸で DEX を分類し、それぞれのカテゴリにおいて代表的

199 Wood, J., Medium, "Thoughts on Decentralized Exchanges and Real World Usage of their own Tokens ", https://cdn-images-1.medium.com/max/2600/1*rtrn2x4dJ9adOUvXKUna9w.png, 2019/2/22

なプロジェクトについて調査を行った[200]。

図表 87 DEX の分類表（*は法定通貨との交換が可能な DEX）

特定の管理主体	あり（括弧の中は管理主体の名称）		なし	
取扱トークン	同種トークン	異種トークン（法定通貨含む）	同種トークン	異種トークン
分類	（1）	（2）	（3）	（4）
オフチェーン処理（障害点・信頼点）	マッチング・価格形成（オーダーブックや残高情報等）	決済（異種トークンや法定通貨の管理）	ー	ー
プロジェクト例	IDEX（IDEX Server）	OpenLedger*（OpenLedger ApS）	EtherDelta	BarterDEX
	EtherDelta（Orderbook）	CryptoBridge*（Crypto Bridge）	Bancor	BitSquare*
	0x（Relayer）	Waves DEX*（Waves Platform）	Kyber Network	Altcoin.io
	AirSwap（Indexer）			

図表 87 の（1）～（4）までの分類の意味は以下の通り。

(1) 特定の管理主体がオーダーブックや残高情報等をオフチェーンで管理し、決済はオンチェーンで行われる。取扱通貨は同種トークン（大半は ERC20 トークン）に限られる。

(2) 特定の管理主体が、法定通貨を含む異種トークンとの決済を管理する[201]。一般的には、当該管理主体が、異種トークンや法定通貨等とペッグするトークンを特定のブロックチェーン上で発行し、利用者は当該ブロックチェーン上でそれらを取引する形をとる。最終的に異種トークンや法定通貨と交換するのはアセット発行主体でもある当該管理主体である[202]。

200 異なるブロックチェーン間の相互互換性（インターオペラビリティ）の確保を目指す COSMOS、Wanchain、AION などのプロジェクトも、異なるブロックチェーン上のトークンの交換を行うという点で DEX に含まれるが、提案段階のものが多いため、本稿では割愛した。

201 （1）「管理主体あり、同種トークン」の場合と同様に、当該管理主体がオーダーブックや残高情報等もオフチェーンで管理する場合も考えられる。

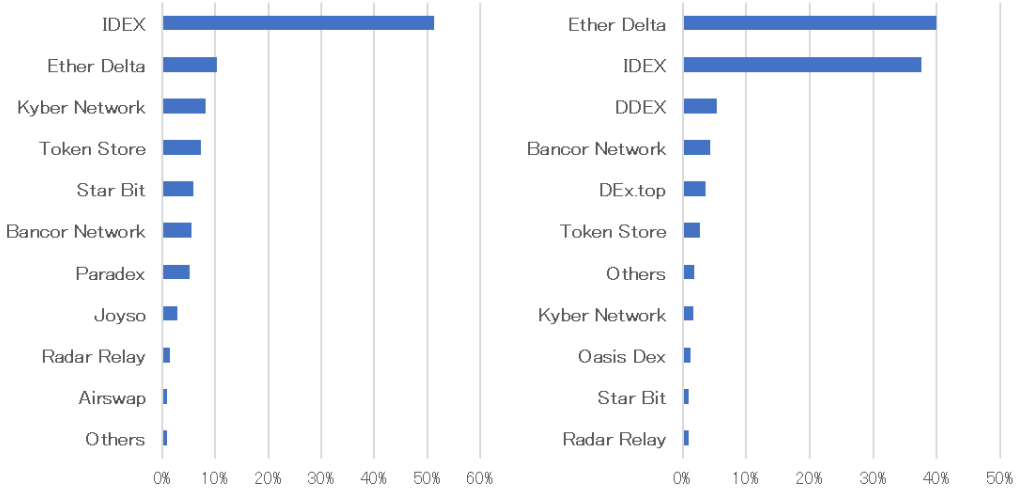
202 IOU(預かり証）取引とも呼ばれる。本稿執筆時点では、（2）「管理主体あり、異種トークン」の全ての DEX で、法定通貨（正確には法定通貨とペッグしたトークン）と暗号資産の交換が可能であった。

(3) 特定の管理主体は存在せず、全ての処理はオンチェーンで行われる。取扱通貨は同種トークン（大半は ERC20 トークン）に限られる[203]。

(4) 特定の管理主体は存在せず、異種トークンとの決済も含めた全ての処理はオンチェーンで行われる。特定の管理主体なしに、異なるブロックチェーンを跨いで決済するために、利用者は複雑な手順を踏む必要がある。

取引所業務には強いネットワーク効果が働くと考えられるが、DEX においても取引高が一部に偏っていることが認められる（図表 88）。本稿執筆時点では分類（1）の DEX である IDEX が過半のシェアを占めている。

図表 88 DEX のシェア（2019 年 2 月 1 日時点、左図：過去 30 日間、右図：全期間）[204]



3.3.2.1 各分類の概要

DEX 毎に、売り手（以下、メイカー）と買い手（以下、テイカー）の「マッチング」、「価格形成」、「決済」という三つの主要機能について様々な特徴が見られるため、以下では図表 87 の分類毎に代表的なプロジェクトについて記載する。

203 （3）「管理主体なし、同種トークン」の場合では、Bancor のみ EOS との交換が可能となっている。Bancor, "BancorX is Live: Automated Conversions Between Ethereum & EOS Tokens", https://blog.bancor.network/bancorx-is-live-automated-conversions-between-ethereum-eos-tokens-3e05da4873e4, 2018/11/20

204 Etherscan, etherscan.io, "Top DEX Pie Chart", https://etherscan.io/stat/dextracker, 2019/2/1 より三菱総研作成。

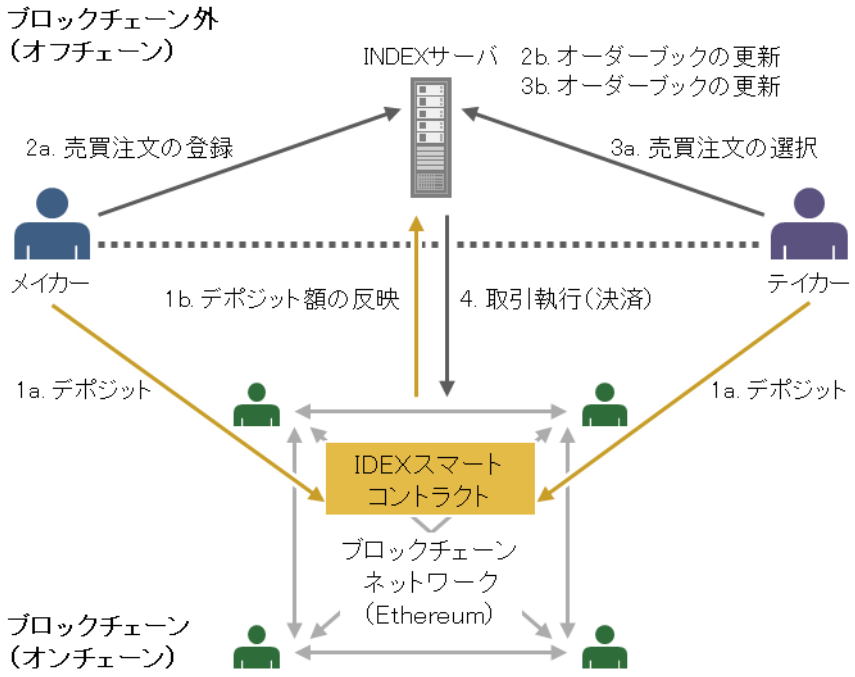
3.3.2.1.1 管理主体あり・同種トークンのみ

(i) IDEX

IDEX はイーサリアム上の DEX であり、メイカーとテイカーの「マッチング」および「価格形成」はオフチェーン（イーサリアム外）で管理されるオーダーブックを通して行われ、「決済」はオンチェーン（イーサリアム上）で行われる。オーダーブックおよび残高情報等をオフチェーンで管理することにより、取引の高速化を実現するとともに、訂正／取消注文等にも手数料のかからない仕組みとなっている。

具体的には、メイカーは自身の保有するトークンをスマートコントラクトにデポジットし、その範囲内で交換したいトークンの種類および量をオーダーブックに登録する。同様に、テイカーも、デポジットしたトークンの範囲内で、オーダーブックから注文を選択する。テイカーが注文を選択すると、当該取引はブロックチェーン上にブロードキャストされ、決済が処理される（図表 89）。ここで、メイカーとテイカーはオフチェーンの残高データベースが更新された時点で新たな取引が可能となるため、ブロックチェーン上の決済を待つことなく高速な取引が可能となっている[205]。

図表 89 IDEX のイメージ図



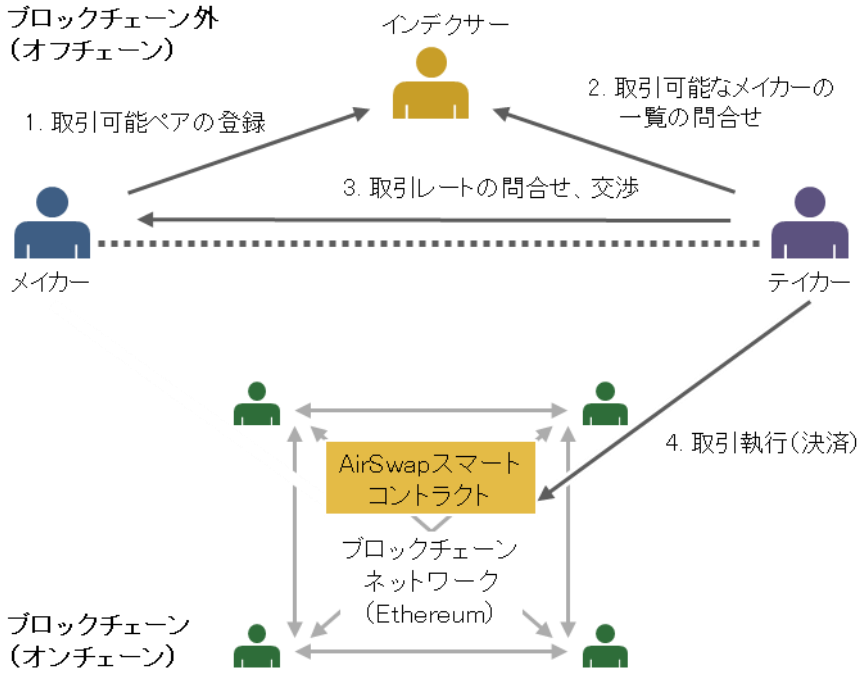
205 IDEX、EtherDelta、0x は基本的なスマートコントラクトは同じであるが、それぞれセキュリティ等の面で違いが見られる。

(ii) AirSwap

AirSwap はイーサリアム上の DEX であり、メイカーとテイカーの「マッチング」および「価格形成」はオフチェーン（イーサリアム外）で行われ、「決済」はオンチェーン（イーサリアム上）で行われる。ここで、「マッチング」は仲介者（インデクサー[206]）を介して行われ、「価格形成」はメイカー・テイカーの相対で行われる。

具体的には、メイカーは取引を希望するトークンのペアをインデクサーに登録しておく。テイカーは、取引を希望するトークンのペアを持つメイカーの一覧をインデクサーから取得し、各メイカーに取引レートを問合せる。その上で、一番有利なレートを提示したメイカーを選び、当該注文をブロックチェーン上にブロードキャストする（図表 90）。なお、レートについて、メイカーおよびテイカーは、他の取引所のレート情報を提供するオラクルへ問い合せを行うこともできる[207]。

図表 90 AirSwap のイメージ図



206 インデクサーに関する詳細やソースコードは開示されておらず、メイカーがインデクサーへ登録依頼する際は 'wss://connect.airswap-api.com/websocket'へ送信する形となっていた。以上より、インデクサーは AirSwap 開発グループないし関係者のみに限定して運用されていると考えられる。

207 オラクルが提供する価格は強制されるものではなく、あくまで参考値として利用される。

3.3.2.1.2 管理主体あり・異種トークンも取扱

(i) OpenLedger、CryptoBridge

OpenLedger、CryptoBridge ともに、BitShares というブロックチェーン基盤上の DEX であり、メイカー・テイカーの「マッチング」・「価格形成」はオンチェーン（BitShares 上）で行われ、「決済」はオンチェーン（BitShares 上）とオフチェーン（BitShares 外）の両方で行われる。特定の運営主体（以下、ゲートウェイプロバイダ）[208]が異種トークンや法定通貨等とペッグするトークンを BitShares 上で発行し[209]、利用者は BitShares 上でそれらを取引する。決済に特定の主体（ゲートウェイプロバイダ）が深く関与するため、決済リスク（信用リスクや流動性リスク）が存在すると考えられる。

具体的には、メイカーは売り注文を BitShares 上にブロードキャストする[210]。テイカーは希望する売り注文を選択し、売り応答注文（Fill Order）[211]をブロードキャストする。メイカーは売り応答注文を見ると、買い応答注文をブロードキャストする。メイカー・テイカー双方の応答注文が揃った時点で BitShares 上での決済が行われる。ただし、ここでの決済はあくまで BitShares 上のトークンの交換に過ぎず、異種トークンや法定通貨との実際の交換は、ゲートウェイプロバイダが利用者から受領した BitShares 上のトークンを交換する形で行われる（図表 91）。

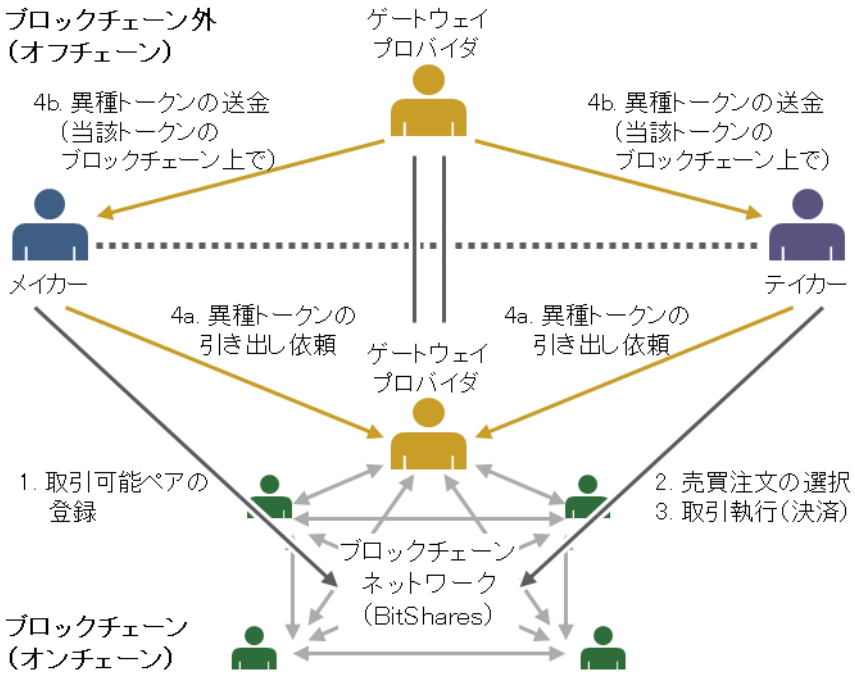
208 ゲートウェイプロバイダになるためには OpenLedger ないし CryptoBridge 管理主体から承認を得る必要がある。

209 BitShares は既存の金融システムを置き換えることを目標にしており、BitShares 上のトークンは、他の暗号資産だけでなく金や石油なども含むことが構想されている。

210 BitShares ではブロックチェーンのデータがオーダーブックとして機能する。すなわち、希望する取引ペア情報を持つトランザクションをブロックチェーンのデータから集めることでオーダーブックが生成されることになる。また、指値注文や成行注文などをトランザクションとして表現できる。これらは BitShares Open Explorer（http://open-explorer.io/#/dashboard）からも確認できる。

211 テイカーの売り応答注文の内容は、メイカーの売り注文を売買反転させたものとなる。

図表 91 OpenLedger、CryptoBridge のイメージ図



3.3.2.1.3 管理主体なし・同種トークンのみ

(i) Bancor

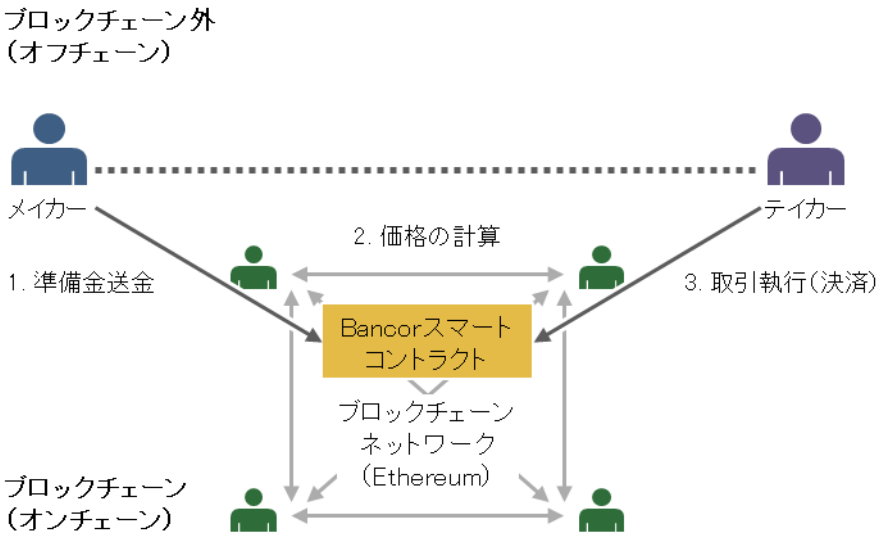
Bancor はイーサリアム上の DEX であり、メイカーとテイカーの「マッチング」・「価格形成」・「決済」は全てオンチェーン(イーサリアム上)で行われ、特定の管理主体は介在せずにスマートコントラクトによる販売所取引のみが行われる。これは、人を排除することによる不正行為[212]の撲滅や取引が活発でない暗号資産の流動性リスクの解決を目指しているためである。

具体的には、あるトークンの発行主体がメイカーとなり、メイカーは他のトークンを準備金として Bancor へ予め送金しておく。Bancor は当該トークンの総量と準備金等から当該トークンの理論価格を計算し[213]、テイカーは当該価格で当該トークンを購入ないし売却する。テイカーによる購入・売却の都度、理論価格は修正されていくことになる(図表 92)。理論価格の算出は複雑な処理となっており、トランザクションの手数

212 同一人物ないし関係者が共謀して買い注文と売り注文を出して取引高を偽装することなど。
213 価格は、準備金残高／(トークン総量 x 準備率)として定義される。ここで、準備率(Connector Weight)はトークン発行時に指定される値であり、事後に変更されることはない。売買の度に準備金残高は変動するが、常に準備率が一定となるように、トークン総量と価格が調整される。

料が高くなることが開発者からも指摘されている[214]。

図表 92 Bancor のイメージ図



(ii) Kyber Network

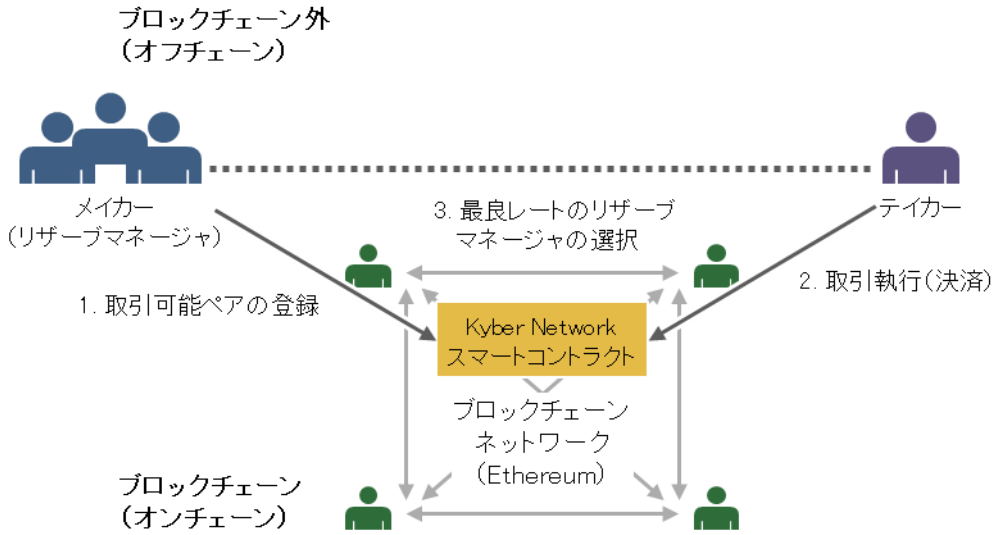
Kyber Network はイーサリアム上の DEX であり、メイカーとテイカーの「マッチング」・「価格形成」・「決済」は全てオンチェーン（イーサリアム上）で行われ、特定の管理主体は介在しない。ただし、「価格形成」において、理論価格を計算する Bancor と異なり、Kyber Network のスマートコントラクトは、最もレートの良いメイカーの選択のみを行う。

具体的には、メイカー（リザーブマネージャと呼ばれる）は、自身の希望する取引ペアについて、独自のスプレッドを設定した取引レートを Kyber Network に登録する。テイカーは自身の希望する取引ペアを Kyber Network へ送信すると、Kyber Network が自動的に複数のメイカーの中から、最もレートの良いメイカーを選択して決済を行う（図表 93）。Bancor、Kyber Network のどちらもオーダーブックを廃すことで管理主体の排除や処理の高速化を目指すが、1つのトークンに対して、Bancor ではメイカー（トークン発行主体）が 1 人のみであるのに対し、Kyber Network ではメイカーが複数存在する点が異なる。そのため、Kyber Network では各メイカーの戦略により価格が決定されることになる。

214 コインテレグラフ日本版ウェブサイト, "「ほとんどの仮想通貨取引所で不正」分散型取引所バンコールはどう差別化するか", https://jp.cointelegraph.com/news/bancors-cofounder-almost-all-of-crypto-exchanges-are-abusive, 2018/12/4

ただし、メイカーになるには、Kyber Network オペレータ[215]を通して登録することが必要であり、本稿執筆時点ではメイカーの数は僅かである。他にも HP で身分証明書をアップロードすると取引額の上限が増加する[216]など、取引所機能以外の部分（KYC 等）は特定の管理主体が介在していると考えられる。

図表 93 Kyber Network のイメージ図



3.3.2.1.4 管理主体なし・異種トークンも取扱

(i) BarterDEX

BarterDEX は、Komodo というブロックチェーン基盤上の DEX であり、メイカー・テイカーの「マッチング」・「価格形成」はオンチェーン（Komodo 上）で行われ、「決済」もオンチェーン（Komodo 上と取引ペアとなる異なるブロックチェーン上）で行われる。BaterDEX ではオーダーブックは分散して保持されており、また、マーケットメイカーになるための仕組み（流動性プロバイダと呼ばれる）なども存在する。

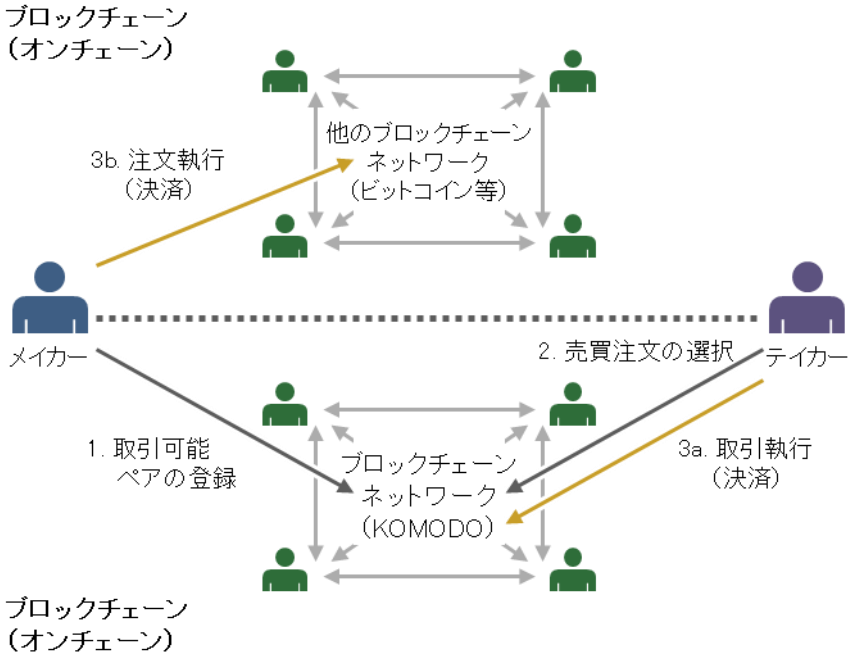
具体的には、分散保持されるオーダーブックにメイカーが売買注文を登録し、テイカーが自身の希望する注文を選択すると、取引ペアとなる異なるブロックチェーン上でのメイカー・テイカー各々の残高確認を経て、問題なければマッチングが成立する。その後は、メイカー・テイカーはアトミック・クロスチェーン・スワッププロトコル[217]に従っ

215 開発者グループ等が運営していると推察される。
216 身分証明書をアップロードしなくとも取引は可能である。
217 ビットコイン等で用いられるアトミック・クロスチェーン・スワッププロトコルではなく、BarterDEX 独自のプロトコルとなっている。

て取引ペアとした二つのブロックチェーン間でのコインの交換を行う（図表 94）。

取引ペアとなるブロックチェーンのファイナリティが確率的である場合、メイカー・テイカーは十分な時間待つ必要がある。また、利用者は取引ペアとなる異なるブロックチェーン上の秘密鍵を管理した上で、複雑な手順を踏む必要があるなど、他の DEX に比べ、利用者側の負担が大きい。執筆時点で Komodo Coin（KMD）[218]との取引のみ提供されている。

図表 94 BarterDEX のイメージ図



(ii) Bisq

Bisq は独自の P2P ネットワーク上の DEX であり、メイカー・テイカーの「マッチング」・「価格形成」は独自ネットワーク（Bisq ネットワーク）上で行われ、「決済」はオンチェーン（ビットコイン上）で行われる。古くから開発が行われており[219]、「決済」にランダムに選ばれた仲裁人を置く点などが特徴である[220]。

---

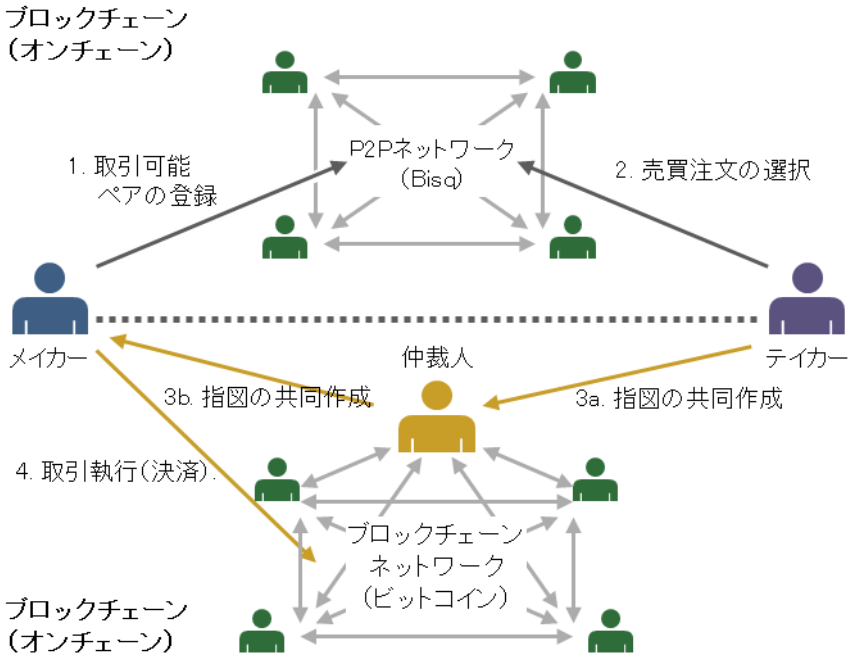
218 Komodo プラットフォームのネイティブトークンであり、Zcash をハードフォークして作成された。Komodo Platform, "Komodo - An Advanced Blockchain Technology, Focused on Freedom", https://komodoplatform.com/wp-content/uploads/2018/05/2018-05-09-Komodo-White-Paper-Full.pdf, 2018/12/7

219 Github 上では 2014 年 3 月から開始されている。bisq-network, Github, https://github.com/bisq-network/bisq, 2018/12/4

220 その他、取引ペアの片方は必ずビットコインを指定する必要があること（取引ペアには法定通貨も含まれる）、Tor を経由することなど、他の DEX とは異なる特徴が見られる。

具体的には、オーダーブックは Bisq ネットワーク上で分散して保持されており、メイカーが売買注文を登録し、テイカーがオーダーブックから自身の希望する注文を選択すると、テイカーはメイカーへ法定通貨ないし暗号資産を支払う。メイカーはテイカーの支払を待ってから、テイカーへ法定通貨ないし暗号資産を支払う。 ここで、取引の都度、メイカー・テイカー双方の証拠金（0.01BTC 程度）およびランダムに選ばれた仲裁人を立てることとしている[221]。仲裁人はビットコイン上の取引については、2-of-3 のマルチシグに加わるとともに、取引に問題が生じた際は取引の仲裁を行う[222]（図表 95）。Bisq では個人の信用力が重要となるため、取引日数等に応じて取引可能な額が制限されている[223]。

図表 95 BitSquare のイメージ図



以降、特定の主体が介在し同種トークンに限られる IDEX と、特定の主体が介在することなく異種トークンの交換が可能である BarterDEX のそれぞれについて、その詳細を記載する。

221 仲裁人は十分な金額の Bisq 専用トークンをデポジットすることで立候補できる。また、メイカー・テイカー双方の証拠金は取引が正常に終了すると返却される。
222 仲裁人が被害者へ現金を支払い、代わりに加害者の証拠金を受け取る。この際、被害者は加害者へ支払いを済ませたことを仲裁人に証明する必要がある。他に、Bisq で定められた日数を超えても相手から支払いがない場合に、仲裁人へ仲裁を申し出ることが可能となる。
223 Bisq, "What are the trade limits?", https://bisq.network/faq/#3, 2018/11/29

3.3.2.2 IDEX

IDEX[224]は、イーサリアムブロックチェーン基盤上で動作し[225]、メイカーとテイカー間で異なる ERC20 トークンを交換することを念頭に設計された DEX である。イーサリアム上の DEX としては世界最大の取引量であり、凡そ半分強のシェアを持つとされる[226]。IDEX の特徴として、オーダーブックや残高情報等がオフチェーンで管理される点が挙げられる。一部の処理はオフチェーンで行われるものの、IDEX ではメイカーとテイカーが通貨の交換を行う際に、その売買注文を IDEX では改竄できない仕組み[227]を備えている。また、成立した取引のみをブロックチェーン上にブロードキャストすることにより、注文のキャンセルや変更による手数料を抑えている。他方で、オフチェーンで処理される部分が存在するために、その部分が単一障害点になるとともに、最初に行うデポジットやフロントランニング問題[228]等については IDEX のスマートコントラクトやオーダーブックの管理主体を信頼する必要がある。

IDEX は 2017 年 10 月に稼働を開始し、その後、API の改善[229]が図られている。将来的にはシャーディング技術の活用により、複数の IDEX を連携させることで、流動性を束ね、処理を高速化させるロードマップが公開されている[230]。

3.3.2.2.1 取引の流れ

IDEX での取引は、大きく①デポジット、②マッチングおよび価格形成、③決済の三ステップからなる（図表 96）。各ステップの詳細は次節以降に記載する。

(1) デポジット

メイカーおよびテイカーは自身の保有するトークンを IDEX にデポジットすることで、その範囲内で取引を行うことができる。

(2) マッチングおよび価格形成

---

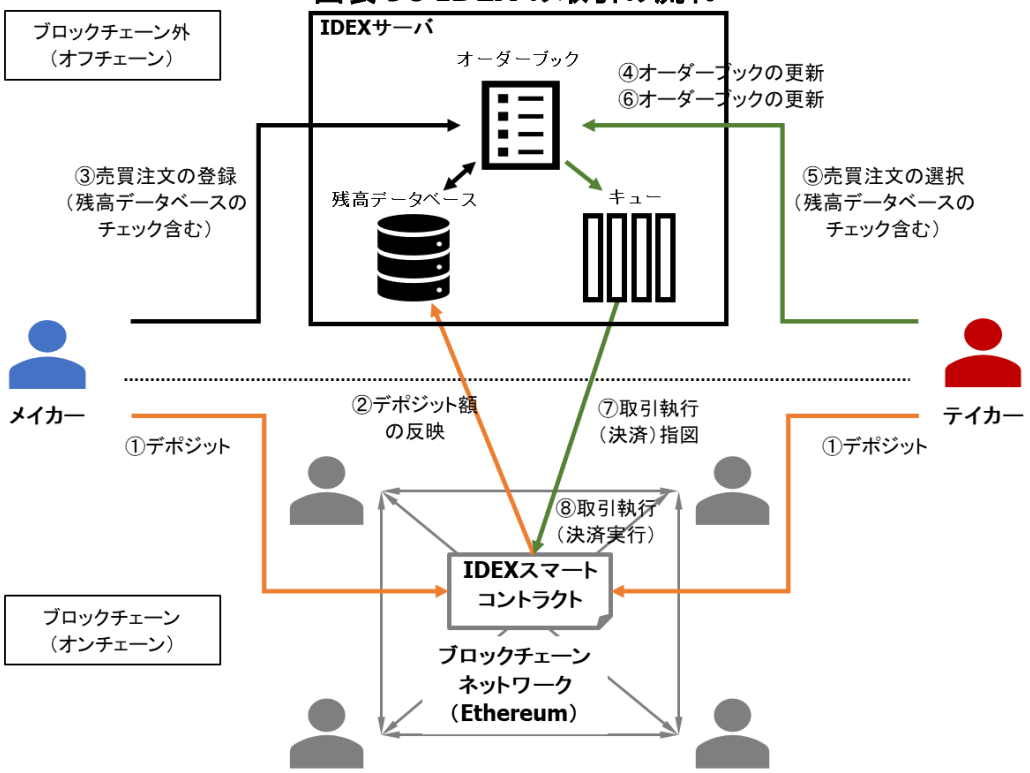
224 Aurora Labs, "IDEX", https://idex.market/, 2018/10/28
225 イーサリアムブロックチェーン上にデプロイされた IDEX のスマートコントラクトは以下の場所から確認できる。Etherscan, etherscan.io, https://etherscan.io/address/0x2a0c0dbecc7e4d658f48e01e3fa353f44050c208#code, 2018/10/28
226 DEXWatch, "24h Highest Volume DEXs", https://dex.watch/, 2019/1/9
227 メイカーとテイカーの売買注文には署名が付されているため、IDEX のスマートコントラクトが売買注文を改竄した場合は、署名検証により当該取引は失敗することとなる。
228 ここでは、顧客からの注文を受けた仲介者が顧客の注文の前に自分の注文に先に出す行為。
229 トレーディングボットの開発、流動性の向上、市場効率の改善等が可能となった。
230 Aurora Labs, "IDEX: A Real-Time and High-Throughput Ethereum Smart Contract Exchange", https://idex.market/static/IDEX-Whitepaper-V0.7.5.pdf, 2019/1/9

オフチェーンで管理されるオーダーブックがメイカーとテイカーのマッチングおよび価格形成の役割を担う。具体的には、メイカーが売買注文をオーダーブックに登録し、テイカーが当該注文を選択することで行われる。

(3) 決済

成立した売買注文について、オーダーブックから当該注文が削除されるとともに、当該取引がイーサリアムブロックチェーン上にブロードキャストされる。ブロードキャストされたトランザクションがマイニングによりブロックに記録されると取引が完了したことになる。

図表 96 IDEX の取引の流れ



3.3.2.2.2 デポジット

メイカーおよびテイカーは自身の保有するトークンを IDEX のスマートコントラクト宛にデポジットするトランザクションをイーサリアムブロックチェーン上にブロードキャストする。IDEX のスマートコントラクトは、ブロックチェーン上で当該トークンをメイカー・テイカー別に管理するとともに、オフチェーンで別途管理されている残高データベース上のメイカーおよびテイカーの残高に当該デポジット額を反映する。なお、追加のデポジットは任意のタイミングで行うことが可能である。

デポジットされたトークンは IDEX のスマートコントラクトが自由にコントロールできるため、この点においては当該スマートコントラクトが不正な処理を行わない[231]ことを信頼する必要がある。

3.3.2.2.3 マッチングおよび価格形成

メイカーは売買注文を IDEX のオフチェーンサーバへ送信する。注文情報には、売却する ERC20 トークンの種類と数量、購入する ERC20 トークンの種類とその数量、およびメイカーの署名が含まれる。IDEX はオフチェーンの残高データベースを参照して、当該メイカーが売却する ERC20 トークンの種類と数量を保持していることおよび署名がメイカーのものであることを確認する。問題なければ、IDEX はオフチェーンで管理されているオーダーブックに当該注文を登録する。

テイカーはオフチェーンのオーダーブックを見て、希望する売買注文があれば、対応する売買注文を IDEX のオフチェーンサーバへ送信する。テイカーの売買注文は、メイカーの売買注文の内容を売り買い反転させたものであるが、売却量に関してはメイカーの希望する購入量以下でも構わない[232]。IDEX は残高確認および署名検証を行い、問題なければ当該注文をオフチェーンのオーダーブックから削除する。

3.3.2.2.4 決済

IDEX はオフチェーンの残高データベースの更新を行うとともに、メイカーとテイカーの売買注文を 1 セットとしたトランザクションを作成し、キューに格納する。これは適宜ブロックチェーン上にブロードキャストされる[233]。この時点ではブロックチェーン上では当該注文はまだ処理されていないが、（ブロックチェーン上の処理結果の反映を待たずに）メイカーとテイカーは更新された残高情報に基づき、続けて取引を行うことが可能となっている。

トランザクションがブロードキャストされると、それを受信した IDEX の決済処理用スマートコントラクトは、ブロックチェーン上で管理するメイカー・テイカー別の残高を更新

231 不正な処理の例としては、特定ユーザへ特権アクセスを認める場合やバグが含まれる場合などが挙げられる。

232 テイカーがメイカーの希望する購入量以下を売却する場合、メイカーのテイカーへの売却量も比例して減額される仕組みとなっている。Etherscan, etherscan.io, https://etherscan.io/address/0x2a0c0dbecc7e4d658f48e01e3fa353f44050c208#code, 2019/1/9

233 マイナーによってトランザクションが処理される順番は事前には想定できないため、同一のメイカーないしテイカーが関わるトランザクション群は、間隔を置いてブロードキャストするなどの調整が行われる。なお、トランザクションの手数料は IDEX が肩代わりする。

する。当該トランザクションがマイニングによりブロックに記録された段階で、ブロックチェーン上に売買注文の結果が反映されることになる[234]。

IDEX は、メイカー・テイカーの残高情報をオフチェーンとオンチェーンの二重で管理しているが、両者は非同期に同期されることになる[235]。なお、たとえオンチェーンで決済が完了した場合であっても、IDEX がオンチェーンで管理するメイカー・テイカーの残高が更新されるだけであり、実際にオンチェーン上のメイカー・テイカーの残高が変更される訳ではない点には留意が必要である。 当該残高は、メイカーないしテイカーが IDEX のスマートコントラクト宛にトークンの引出しを行うトランザクションをブロードキャストし、当該トランザクションがブロックに記録された段階で、変更されることになる。

また、IDEX はオフチェーン・オンチェーンの残高情報を更新する際に、自身への報酬も含める。処理を実行するための手数料は IDEX が負担するが、最終的にオンチェーンで取引が成立しない限り、IDEX はメイカー・テイカーから報酬を受け取ることができない。このような形をとることで、IDEX による改竄やトランザクションの廃棄など不正な処理を行うインセンティブがないことを利用者に示している。

3.3.2.3 BarterDEX

BarterDEX は、Komodo というブロックチェーン基盤上で動作する DEX であり、独自のアトミック・クロスチェーン・スワッププロトコルを用いて、第三者を介さずに、異なるブロックチェーン上で決済を行う点が特徴である[236]。オーダーブックは分散して保持される。また、流動性プロバイダ（Liquidity Provider、LP)と呼ばれるマーケットメイカーになるための仕組みも提供されており、外部の取引所の価格と BarterDEX のオーダーブックに価格差が生じると自動的に売買注文を出すことで、Barter DEX の流動性を向上させる役割を果たす。これらアトミック・クロスチェーン・スワップ、分散オーダーブック、流動性プロバイダという 3 つが BarterDEX の主要コンポーネントとなる。

BarterDEX は 2018 年 1 月に稼働を開始し、ERC20 トークンを含む取扱通貨の拡

234 イーサリアム上で決済が処理されるタイミングはマイニングに依存するため、IDEX ではコントロールすることができない。

235 本稿ではオフチェーンの情報をオンチェーンに同期させる仕組みを中心に記載しているが、実際にはオンチェーン側でのチェーン分岐による再編成により、数段階遡ってオフチェーンの情報をオンチェーンに同期させる場合の考慮も必要となる。

236 Komodo Platform, "Komodo - An Advanced Blockchain Technology, Focused on Freedom", https://komodoplatform.com/wp-content/uploads/2018/05/2018-05-09-Komodo-White-Paper-Full.pdf, 2018/12/7

充や API の改善などが進められている。

3.3.2.3.1 取引の流れ

BarterDEX での取引は、大きく①マッチングおよび価格形成、②決済のニステップからなる（図表 97）。各ステップの詳細は次節以降に記載する。

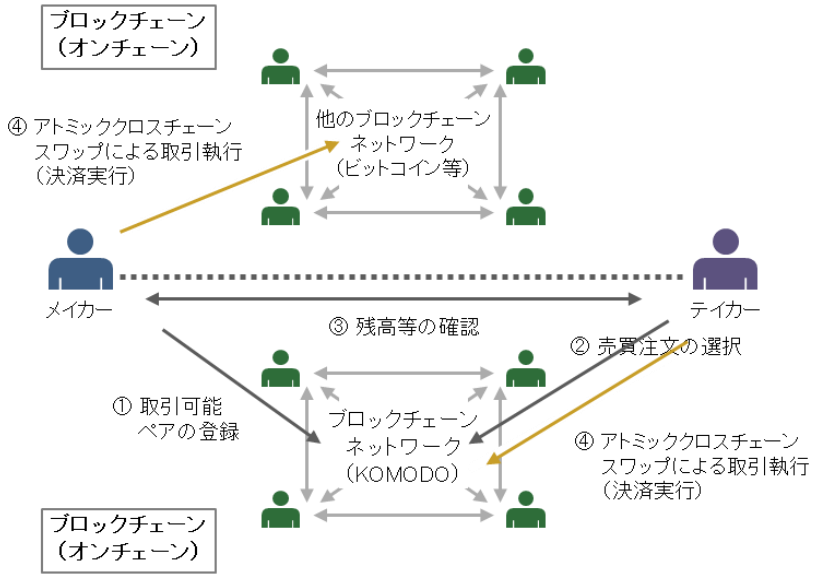
(1) マッチングおよび価格形成

Komodo ブロックチェーンネットワーク上で分散して保持されるオーダーブックがメイカーとテイカーのマッチングおよび価格形成の役割を担う。具体的には、メイカーが売買注文を登録し、テイカーがオーダーブックから自身の希望する注文を選択する形で行われる。取引ペアとなる異なるブロックチェーン上でのメイカー・テイカー各々の残高確認を経て、問題なければマッチング成立となる。

(2) 決済

成立した売買注文について、メイカー・テイカー間でアトミック・クロスチェーン・スワッププロコトルにしたがって、異なるブロックチェーンを跨いだ決済が行われる。第三者は介在せず、メイカー・テイカー間でのみ決済が行われるが、双方ともに任意のタイミングで決済を中止することができる。すなわち、たとえマッチングが成立しても取引がキャンセルされる場合がある。また、決済にあたっては複雑な手順を踏む必要があるため、利用者は BarterDEX やブロックチェーンについて、良く理解している必要がある。

図表 97 BarterDEX の取引の流れ



3.3.2.3.2 マッチングおよび価格形成

BarterDEX ネットワークは中継ノード（Full-Relay node）と非中継ノード（Non-Relay node）から構成され[237]、オーダーブックは各ノードで保持される。中継ノード同士ではオーダーブックの送受信が行われるが、非中継ノードはオーダーブックを他のノードへ送信することはなく、少数の中継ノードからオーダーブックの受信のみを行う。中継ノードには十分な帯域幅が必要とされるが、多くの接続先があることから、非中継ノードよりも最新のオーダーブックを迅速に取得して高速に取引できる可能性が高い[238]。

なお、各ノードは、中継ノード・非中継ノードを問わず、外部の取引所（Bittrex, Cryptopia, Coinmarketcap 等）[239]の価格情報と BarterDEX ネットワーク上のオーダーブックとの間に価格差が発生すると、自動的に価格差を埋めるような発注を行うマーケットメイカーになることもできる。これにより BarterDEX ネットワークにとっては、外部の取引所との価格差が是正され、また流動性も確保される。マーケットメイカーにとっては、BarterDEX と外部の取引所との価格差により利益を得ることができ、また取引手数料も免除される[240]。

メイカーは売買注文の登録にあたり、DEX 利用手数料（DEX Fee と呼称される）として取引額の 1/777 を中継ノードへ送金し、代わりに中継ノードは当該注文を含めたオーダーブックを他のノードへ送信する。DEX 利用手数料を徴収するのは、実行する意図のない発注を大量に行う DoS 攻撃を防ぐためであるとされる。そして、テイカーがオーダーブックから自身の希望する注文を選択すると、取引ペアとなる異なるブロックチェーン上でのメイカー・テイカー各々の残高確認が行われる。ここで、利用可能な残高が売買注文で指定された額に満たない場合は、利用可能な残高分のみの取引に調整される[241]。

---

237 BarterDEX ネットワーク上ではノードは IP アドレスではなく公開鍵ベースのアドレスで特定される。ただし、中継ノードは公開鍵ベースのアドレスと IP アドレスを紐付けることが可能であるため、プライバシーを確保するためには、匿名通信の一つである JUMBLR の併用が推薦されている。

238 その他、取引通貨ペア毎にネットワークを分けて、各々のネットワークそれぞれでオーダーブックを管理することも可能とされている。また中継ノードは、送受信対象となるオーダーブックを特定の通貨ペアのみに絞ることで、帯域幅を削減することも可能とされている。

239 Komodo Platform, GitHub, https://github.com/KomodoPlatform/KomodoPlatform/wiki/barterDEX-API-Summary-by-Category#autoprice, 2019/1/9

240 マーケットメイカーは誰でもなることができるが、自動取引の設定は自身で詳細に行う必要がある。

241 具体的には、売買注文で指定された額以下の最大の UTXO（Unspent Transaction Outputs）が取引に用いられる。

3.3.2.3.3 決済

BarterDEX では以下のニステップで決済行われる。

- 事前準備（鍵生成）

メイカーとテイカー双方が公開鍵を交換するにあたり、出鱈目な鍵ではなく、確かに対応する秘密鍵が存在する公開鍵であることを担保するために、下記の手順を踏む（図表 98）。

(1) メイカーとテイカーともに、秘密鍵と公開鍵のペアを 1,000 個生成する。

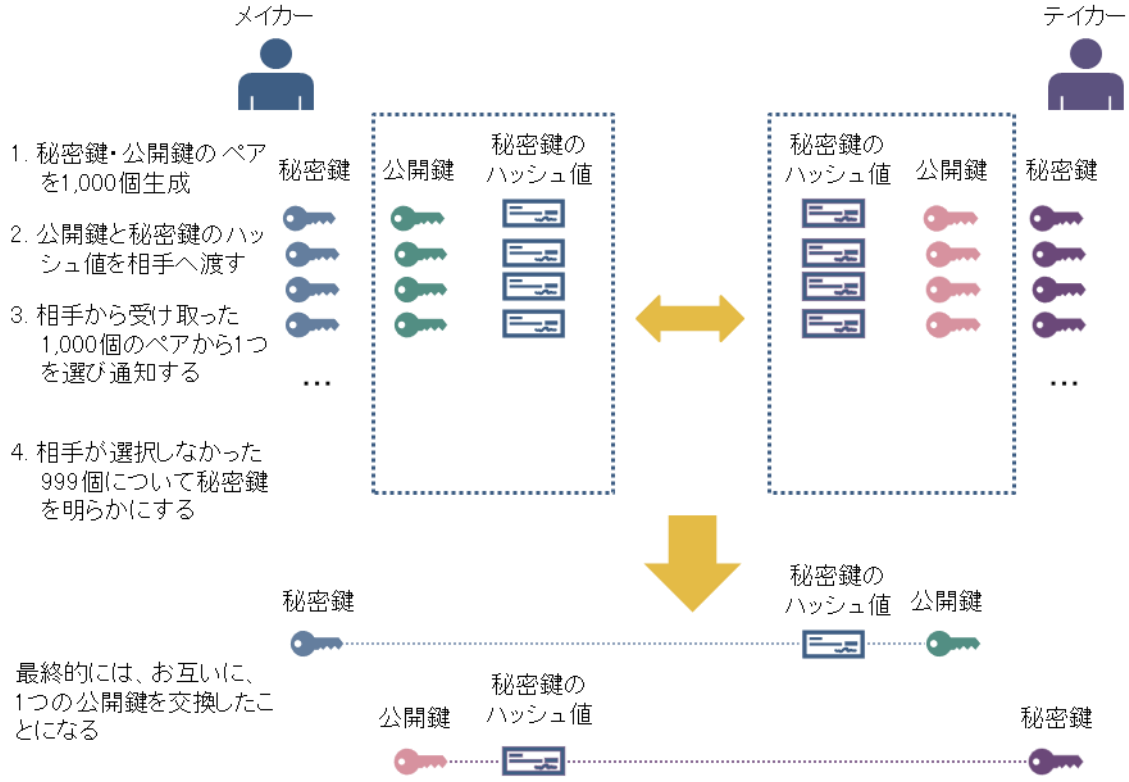
(2) メイカーは、（1）で生成した秘密鍵のハッシュ値と公開鍵のペア 1,000 個をテイカーに渡す。テイカーも同様に自身のペア 1,000 個をメイカーへ渡す。

(3) メイカーは、テイカーの生成した 1,000 個のペアの中からランダムに 1 つのペアを選択して、それをテイカーに通知する。テイカーも同様に、メイカーの 1,000 個の中から 1 つを選び、それをマイカーに通知する。

(4) メイカーは、テイカーに選ばれなかった 999 個の秘密鍵をテイカーに明らかにする。テイカーは、999 個の秘密鍵から、そのハッシュ値と公開鍵を算出し、（2）で受領した 1,000 個のペアのうち、自分が選択したペア以外のものについて受領したものと算出したものが一致することを確認する。テイカー側でも一連の処理を行う。

最終的に、メイカーとテイカーともに、（2）で選択したペアを用いて決済を行う。すなわち、テイカーは、メイカーの保持する秘密鍵 $r^{メイカー}$ に対応した公開鍵 $R^{メイカー}$ を保持しており、逆にメイカーは、テイカーの保持する秘密鍵 $r^{テイカー}$ に対応した公開鍵 $R^{テイカー}$ を保持しており、これら二種類の秘密鍵・公開鍵ペアを決済に用いることになる。

図表 98 BarterDEX における事前準備の流れ



➢ 決済

以下では、メイカー（M と表記する）が 10KMD（Komodo Coin）を、テイカー（T と表記する）が 1 ビットコインを交換する場合を考える（図表 99）。

(1) テイカーT は保証金として取引額の 112.5%にあたる額を含むトランザクション TX1を、ビットコインネットワーク上でブロードキャストする[242]。当該ビットコインは、テイカーT が自身の秘密鍵 $r^{テイカー}$を掲示すれば任意のタイミングで払い戻せるが、一定時間が経過するとメイカーM も利用可能となる。そのため、テイカーT は当該時間内に取引を終わらせる必要がある。

(2) メイカーM は、ビットコインネットワーク上で TX1 の内容を確認する。問題なければ、Komodo ネットワーク上で、メイカーM からテイカーT へ KMD を送金するトランザクション TX2 をブロードキャストする[243]。これは、実際には、秘密鍵 r

242 ビットコインのスクリプトでは以下のように表現される。
OP_IF <現在時刻＋ロック時間x2> OP_CLTV OP_DROP <メイカーの公開鍵> OP_CHECKSIG
OP_ELSE OP_HASH160 <$r^{テイカー}$のハッシュ値> OP_EQUALVERIFY <テイカーの公開鍵> OP_CHECKSIG
OP_ENDIF
243 ビットコインのスクリプトでは以下のように表現される。
OP_2 <$R^{メイカー}$> <$R^{テイカー}$> OP_2 OP_CHECKMULTISIG

メイカーrとテイカーrの両方を掲示すれば当該 KMD が利用可能になるというマルチシグの形で指定される。

(3) テイカーT は、Komodo ネットワーク上で TX2 の内容を確認する。問題なければ、ビットコインネットワーク上で、テイカーT からメイカーM へビットコインを送金するトランザクション TX3をブロードキャストする[244]。当該ビットコインは、メイカーM が自身の秘密鍵メイカーrを掲示すれば任意のタイミングで利用可能だが、一定時間が経過するとテイカーT も利用可能となる（払い戻される）。

(4) メイカーM はビットコインネットワーク上で TX3 を確認する。次に、ビットコインネットワーク上で、自身の秘密鍵メイカーrを掲示するトランザクション TX4 をブロードキャストして、テイカーT のビットコインを取得する。

(5) テイカーT はビットコインネットワーク上の TX4 からメイカーrを取得する。次に、Komodo ネットワーク上で、自身の秘密鍵テイカーrと、取得したメイカーrを掲示するトランザクション TX5 をブロードキャストして、メイカーM の KMD を取得する。

(6) (5)と同時に、テイカーT は、ビットコインネットワーク上で、自身の秘密鍵テイカーrを掲示するトランザクション TX6 をブロードキャストして、（1）の保証金の払い戻しを行う。

メイカーからの送金とテイカーからの送金は、ともに秘密鍵を掲示しない限り利用可能とならず、また、上記の手順を踏む中で、メイカー・テイカーともに、自身の秘密鍵メイカーrとテイカーrを必ず掲示する必要があるという点がポイントである。たとえば、（4）において、メイカーがテイカーのビットコインを受け取るためには、メイカーrを掲示しなくてはならないが、このことにより、（5）で、テイカーはメイカーの KMD を受け取ることが可能となる。

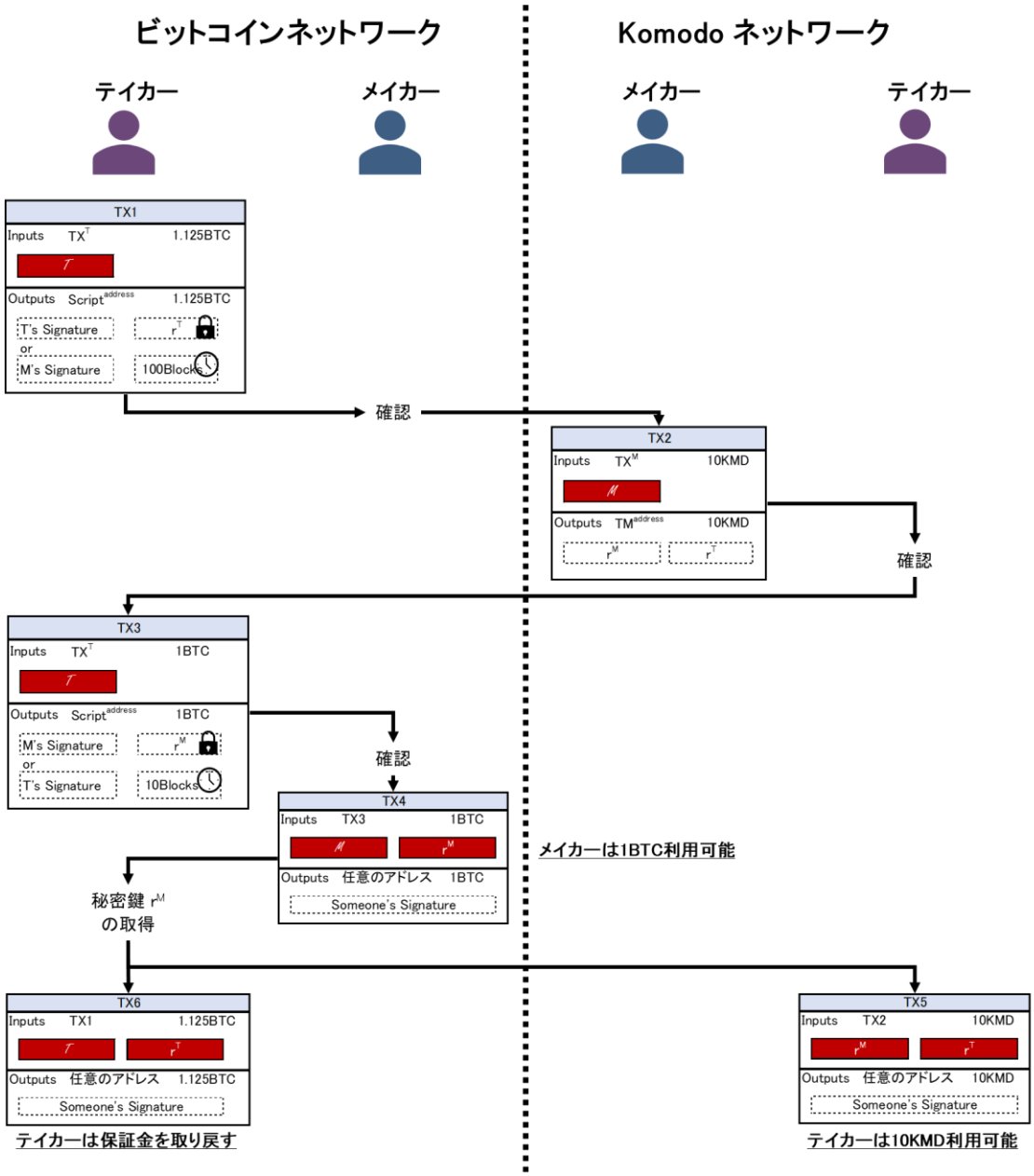
また、（1）の TX1 と（3）の TX3 は、秘密鍵の掲示ないし一定時間経過後に当該コイン（ここではビットコイン）が利用可能になるという機能[245]が当該ブロックチェーン基盤（ここではビットコイン）に必要だが、（2）の TX2 はマルチシグのみを用いている。そ

244 ビットコインのスクリプトでは以下のように表現される。
OP_IF <現在時刻＋ロック時間> OP_CLTV OP_DROP <テイカーの公開鍵> OP_CHECKSIG
OP_ELSE OP_HASH160 <メイカーrのハッシュ値> OP_EQUALVERIFY <メイカーの公開鍵> OP_CHECKSIG
OP_ENDIF

245 こうした機能は、ハッシュ・タイムロック・コントラクト（Hashed Timelock Contract、HTLC）と呼ばれており、ビットコインでは OP_CSV（BIP-112 で導入）や OP_CLTV（BIP-65 で導入）という専用のコマンドが導入されたことにより利用することが可能となった。

のため、取引ペアとなる暗号資産の片方（ここでは KMD）のブロックチェーン基盤（Komodo ブロックチェーン）は、マルチシグ機能のみ備えていれば良いことになる。BarterDEX で取り扱える暗号資産の種類を増やすために、このような仕組みが取られている。

図表 99 BarterDEX における決済の流れ



メイカー・テイカーともに任意のタイミングで決済を中止することができるが、上記の各手順において、取引が中止された場合は以下のようなペナルティが課されることになる。このようなインセンティブづけを通して、取引が中止される確率を下げるようにしている。

- テイカーが TX1 を送信しない場合

  メイカーは売買注文の登録にあたって送金した DEX 利用手数料を無為に失うことになる。そのため、メイカーはテイカーの BarterDEX 上のアカウントに低評価をつけることでペナルティを与える。

- テイカーが TX1 を送信した後にメイカーが TX2 を送信しない場合

  テイカーは $r^{テイカー}$を掲示することで、TX1 の保証金を払い戻すことができる。そのため、メイカーは DEX 利用手数料を無為に失うことに加え、BarterDEX 上のアカウントにテイカーから低評価をつけられることになる。

- メイカーが TX2 を送信後にテイカーが TX3 を送信しない場合

  テイカーが TX1 の保証金を払い戻す場合、テイカーは $r^{テイカー}$を掲示しなくてはならないため、その $r^{テイカー}$を用いてメイカーは TX2 の KMD を払い戻すことができる。テイカーが TX1 の保証金を払い戻さない場合、メイカーは TX2 の KMD を失うことになるが、一定時間経過後にテイカーの TX1 のビットコイン建ての保証金（取引額の 112.5%）を受け取ることが可能となる。また、「テイカーが TX1 を送信しない場合」と同様に、メイカーは DEX 利用手数料を無為に失うため、テイカーはメイカーから低評価をつけられることになる。

- テイカーが TX3 を送信後にメイカーが TX4 を送信しない場合

  TX3 のビットコインは一定時間経過後にテイカーに戻る。テイカーは TX1 の保証金を払い戻すことができ、その際に掲示した $r^{テイカー}$を用いてメイカーは TX2 の KMD を払い戻すことができる[246]。また、「テイカーが TX1 を送信した後にメイカーが TX2 を送信しない場合」と同様に、メイカーは DEX 利用手数料を無為に失い、さらに、メイカーはテイカーから低評価をつけられることになる。

- メイカーが TX4 を送信後にテイカーが TX5 を送信しない場合

  テイカーは TX2 の KMD を受け取ることができない。テイカーが TX1 の保証金を払い戻す場合は、その際に掲示した $r^{テイカー}$を用いてメイカーは TX2 の KMD を払い戻すことができる（すなわち、メイカーはテイカーのビットコインを受け取り、さらに自身の KMD を払い戻せることになる）[246]。

246 もしテイカーが TX1 の保証金を払い戻さない場合、メイカーは TX2 の KMD を失うが、一定時間経過後にテイカーの TX1 の保証金（取引額の 112.5%）を受け取ることができる。

- テイカーが TX5 を送信後にテイカーが TX6 を送信しない場合

  メイカーは一定時間経過後に TX1 の保証金（取引額の 112.5%）を受け取ることができる。

3.3.3 課題と今後の見通し

DEX は、中央集権型取引所のカストディリスクを解消するために、取引所という信頼できる第三者を介在させずに、スマートコントラクトを用いて取引当事者間で取引を行う機能を提供するものである。

ここで、取引所業務は強いネットワーク効果が働くものであり、流動性は更なる流動性を生む。そのため、DEX の課題および今後の見通しを考えるにあたっては、利用者視点でのメリット・デメリットを念頭に置くことが重要と考えられる。ここでは技術面とユーザビリティ面の2つに分けて記載する。

3.3.3.1 技術面

技術的にみると、DEX は、既存の中央集権型取引所と同様に、売り手と買い手のマッチング、価格形成、決済という三つの主要機能を提供する。DEX は、本来カストディリスクの解消を目指すものであるため、その意味で全ての機能を分散化させることが望ましい。しかし、技術的には、情報システムの効率性（例えば、処理量や応答速度など）と安全性（例えば、処理の分散化による可用性の度合い）との間にはトレードオフの関係が存在する。効率性は、利用するユーザ数、すなわち流動性の厚みに大きな影響を与えるため、近年は、安全性よりも効率性を重視した取組が活発化している（図表 100）。

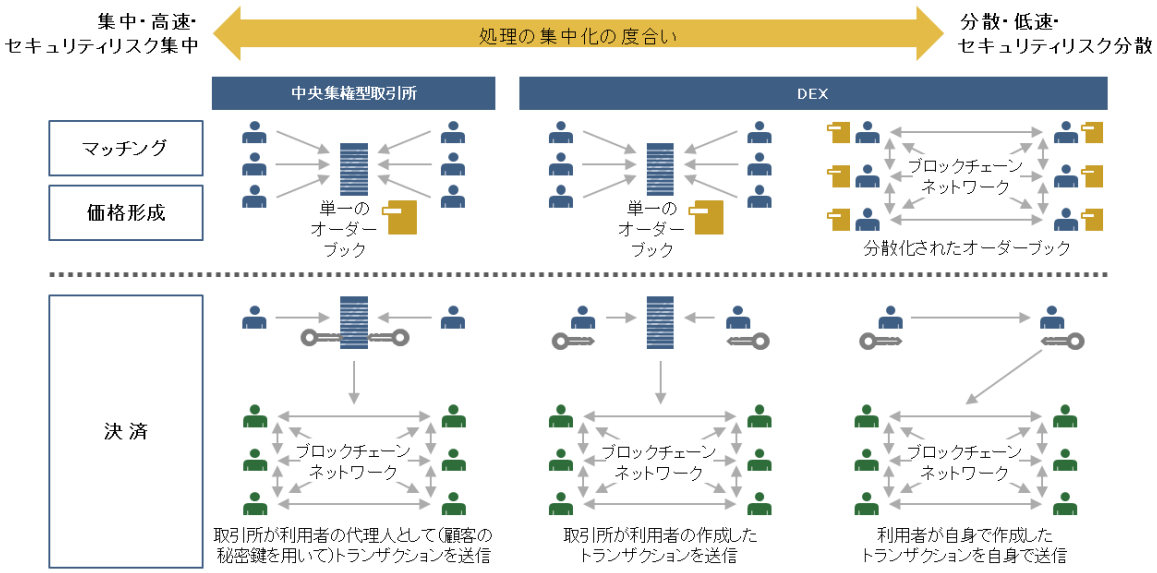
たとえば、安全性を重視して全ての処理をブロックチェーン上で行う場合、ブロックチェーン基盤の処理能力の低さ[247]に起因する処理の遅延、発注/訂正/取消などの都度手数料がかかること等がユーザビリティの観点からは大きな問題となる。

そのため、効率性を重視して、決済はブロックチェーン上（オンチェーン）で分散化して行うものの、決済以外（マッチングおよび価格形成）の処理はブロックチェーンネットワーク外（オフチェーン）のプライベートサーバ等で集中化して行うという方式が 2017 年前半以降多く見られるようになった。ここでは、オーダーブックをオフチェーンで管理

247 一般に、イーサリアムの処理能力は 15 件/秒とされる。Smith, K., BRAVE NEW COIN., "Vitalik - Ethereum en route to a million transactions per second", https://bravenewcoin.com/insights/vitalik-ethereum-en-route-to-a-million-transactions-per-second, 2018/11/5

することにより、処理の高速化、（流動性の増加とともに増えていく）訂正／取消処理への手数料負担の軽減などの効果が見込まれる。他方で、処理を集中化させることは、当該処理が単一障害点、単一信頼点となることにつながり得るため、この点を更に改善しようとする取組も見られる。

図表 100 DEX における技術的なトレードオフ



その他、DEX に内在する問題として、マイナーや他の利用者からの、フロントランニング攻撃（既に成立した取引より先に自身の取引を処理させる攻撃）や嫌がらせ攻撃（残高不足等で取引を失敗させ続けることで手数料を無駄に消費させる攻撃）などを防ぐように設計される必要がある[248]。しかし、マイナーによる攻撃は防ぐことが非常に難しい。

- フロントランニング攻撃について

  マイナーはどのトランザクションをブロックに含めるのかの大きな裁量権を持っているため、成立した取引のオファーを自分が出したオファーに上書きすることがマイナーの場合は可能となる[249]。

248 Will Warren, 0x Blog, "Front-running, Griefing and the Perils of Virtual Settlement (Part 1)", https://blog.0xproject.com/front-running-griefing-and-the-perils-of-virtual-settlement-part-1-8554ab283e97, 2018/11/5
Will Warren, 0x Blog, "Front-running, Griefing and the Perils of Virtual Settlement (Part 2)", https://blog.0xproject.com/front-running-griefing-and-the-perils-of-virtual-settlement-part-2-921b00109e21, 2018/11/5

249 マイナーができるのは基本的にオファーを出したテイカーのオーダーを自分が出し直すことのみである。メイカーのオーダーの数字を書き換えるといったことはできない。

具体的には、メイカーがオーダーとなるトランザクションをブロードキャストし、テイカーがそのオファーとなるトランザクションをブロードキャストした後で、マイナーはテイカーのオファートランザクションをブロックに格納する代わりに、自身のオファートランザクションをブロックに格納することで攻撃が行われる[250]。他の利用者がトランザクションを伝播する際に、自身のオファートランザクションで差し替えることでも攻撃は可能となる。

- 嫌がらせ攻撃について

メイカーがオーダーを出した後に、売却予定のトークンをオーダートランザクションに設定したアドレスから他のアドレスへ移動することで、テイカーがオファートランザクションを出した際に必ず取引が失敗し、テイカーの手数料を無駄に消費させることで攻撃が行われる。ただし、この攻撃を行うためにはメイカーもある程度の手数料を無駄にする必要があるため、それほど頻繁に起こるものではないと考えられる。

回避策としては、IDEX のように事前にデポジットした金額の範囲に取引を限定することや、オファーを出す直前にオーダーが有効かをチェックする仕組みを用意するなどが考えられる。

技術的な効率性と安全性のトレードオフを踏まえた、DEX の最適な着地点については未だ模索中の段階であり、今後も検討が続けられると考えられる。

3.3.3.2 ユーザビリティ面

DEX を用いる場合の利用者にとってのメリットとしては以下が挙げられる。

- 中央集権型取引所に関連した被害（ハッキング被害や価格操作・仮装売買による被害、サーバ障害による被害等）を受けないこと
- 常時取引可能であること（高い可用性）
- KYC を経ずに取引可能であること（取引の手軽さ、高い匿名性）
- 中央集権型取引所が扱っていない暗号資産の取引が可能であること

250 Ethereum では約 15 秒ごとにブロックが生成されるが、マイナーは瞬時にオファートランザクションを差し替える必要はない。これは、近年のトランザクション量急増により、マイナーのメモリプールに待機される時間が長くなっているからである。ただし、他のマイナーよりも先んじて、最初にブロックを生成して、他のノードへブロードキャストする必要がある。

他方で、デメリットとしては、以下が挙げられる。

- 利用者の自己責任の範囲が広い

利用者は最低限、取引ペアとなるブロックチェーンの秘密鍵を自身で適切に管理する必要がある。さらに、BarterDEX など一部の DEX では複雑な決済手順も適切に行うことが必要となる。

それ以外にも、利用者は、決済以外の部分のリスクを負う必要がある。例えば、ブロックチェーン基盤やスマートコントラクトの品質については、自身で確認するか、開発グループ等を信頼する必要がある。また、万一、トラブルが発生した際には自ら主体的に対処する必要がある。決済以外の処理をオフチェーンで集中化して行う DEX では、トラブル発生時も含めて、オフチェーン処理を行う管理主体が正しく処理を行うことを信頼する必要がある。さらに、OpenLedger、CryptoBridge など一部の DEX では、トークン発行主体が適切にトークンを交換してくれることを信頼する必要がある。

- 中央集権型取引所に比べて使い勝手が悪い

DEX では、一部の処理をオフチェーンで行うなどして処理の高速化を図っているが、基本的に中央集権型取引所よりも処理速度は遅い。これは、中央集権型取引所では、取引所外との入金・出金以外は、取引所内でブロックチェーンを用いずに処理できるからである。

DEX で取引できる暗号資産の種類には制約があり、法定通貨と交換できる DEX は OpenLedger や CriptoBridge 以外は僅かである。他に、ストップロスやリミットオーダーなどの指定はできない DEX が一般的である[251]。取引手数料も、中央集権型取引所に比べ低廉になる訳ではないと考えられる[252]（特に、トランザクションを処理するための手数料は、高くするほど取引が成立する可能性が高まるため、手数料が上昇しやすいと考えられる）。

さらに、DEX では現物取引が中心であり、信用取引や証拠金取引が行える

251 例えば、IDEX、OpenLedger・CryptoBridge ではストップロスは利用できない（それぞれ、2017 年 5 月時点および 2017 年 9 月時点）。

252 例えば、IDEX では、決済用の手数料以外に、メイカーは 0.1%、テイカーは 0.2%を IDEX 運営主体へ手数料として支払う必要がある。他方で、国内の中央集権型取引所の手数料は概ね 0%～0.2%である（対象となる暗号資産による）。

ものは少ないと考えられる[253]。例えば、ビットコインの場合、レバレッジ取引のように、自身の保持しているUTXO以上のコインを送金することは本稿執筆時点ではできない。さらに、保証金の扱い（担保管理）やロスカットなど、信頼できる第三者を介さずにレバレッジ取引を行うには技術的なハードルが相当高いことが予想される。

他に、マイナーや他の利用者からのフロントランニング攻撃や嫌がらせ攻撃を防ぐために、事前に流動性がロックされるなどの対策が行われていた場合、当該流動性を自由に利用できないなど、利用時の不便を生じさせる。

特定の管理主体を介在させずに異種トークンを交換する場合は、価格変動により取引が途中で中止されるリスクも存在する（これは取引当事者間でのコールオプション取引に相当するという指摘もなされている[148]）。また、異種トークンの交換は技術的な難易度が高いとともに、利用者の負担が大きい。たとえば、取引ペアとなるブロックチェーンのファイナリティが確率的である場合、メイカー・テイカーは十分な時間待つ必要がある。さらに、異なるブロックチェーン上の秘密鍵を管理した上で、それらのブロックチェーンを跨いで決済するために複雑な手順を踏む必要があり、それらを行ったとしても、決済が（取引相手の都合等により）途中で中止される可能性もある。他に、取引相手が不正を行う場合や、取引が途中で中止される場合に備えて、常に両方のブロックチェーン上を監視しておく必要もある。また、事前に取り決めた時間内は取引に用いる暗号資産（BarterDEXのテイカーの場合は、保証金を含めて取引額の212.5%）は他の取引に用いることができないため、流動性の利用効率が悪化することにもなる。

本稿執筆時点ではDEXの法規制上の扱いが明確でないため、特定の管理主体が介在するDEXの場合、（顧客資産には影響を与えないものの）取引所が突如閉鎖されるリスクも考えられる。

- 流動性が低い

「利用者の自己責任の範囲が広いこと」や「中央集権型取引所に比べて使い勝手が悪い」ことの帰結として、2017年前半よりDEXのプロジェクトが本格化

253 2019年に入り、証拠金取引（margin trading）を拡充するDEXの動きが出てきている。Daily Hodl Staff, The Daily Hodl, "Leading Crypto Exchange Increases Margin Trading Leverage for Bitcoin, Ethereum, Bitcoin Cash, Litecoin and EOS", https://dailyhodl.com/2019/02/26/leading-crypto-exchange-increases-margin-trading-leverage-for-bitcoin-ethereum-bitcoin-cash-litecoin-and-eos/, 2019/3/15

しているにも関わらず、本稿執筆時点では未だユーザ数は限定的であり、図表 80 および図表 81 から分かる通り、取引高は全取引所の約 0.1%程度に留まる。DEX の流動性が低いことは、DEX を利用するインセンティブを減少させ、さらに流動性を低くさせる懸念がある。

暗号資産市場は、株式や債権など他の市場に比べ、個人投資家の割合が大きいと言われる[254]。ここで、FX 取引のアセットの一種として暗号資産取引を捉える、一般の個人投資家にとっては、取引所の手数料や流動性、ユーザビリティ、取り扱う暗号資産の種類等が最大の関心事と考えられる。そのため、そのような投資家は、取引所機能を利用したいのであれば DEX よりも既存の中央集権型取引所を好む可能性が高く、販売所機能を利用したいのであれば DEX よりも既存の販売所（CoinPayments や ShapeShift 等）や中央集権型取引所を好む可能性が高いと考えられる。

3.3.3.3 まとめ

今後も DEX の技術開発は進展し、少なくとも一部の利用者を中心に取引が行われ、DEX は中央集権型取引所と併存していくシナリオが考えられる。しかし、パフォーマンス（応答速度等）や各種機能（ストップロス・リミットオーダーなどの機能、信用取引や証拠金取引等）、取扱通貨の種類（法定通貨を含む）などは技術的・制度的なハードルが高く、また、たとえそれらを実現しても中央集権型取引所と同じことができるに過ぎない。

DEX が広く普及していくためには、中央集権型取引所ではできず DEX でしか行えない機能が何よりも必要になると考えられる。当初 DEX のメリットとして考えられていたカストディリスクの削減や取引の匿名性、取引所の可用性などは、DEX のプロジェクトが本格化してから一年超を経た本稿執筆時点では、幅広い層にアピールできているものとは言い難いと考える。

以上より、技術的な効率性と安全性のトレードオフを踏まえた最適な着地点に加え、DEX でしか実現できない機能について、今後さらに模索されていくものと考えられる。例えば、現状、ICO などで多くの種類の暗号資産が氾濫しているため、サービス毎に異なる暗号資産を用意する必要があり、ユーザビリティの観点から大きな問題が

254 木内, 野村総合研究所ウェブサイト, "ビットコイン投資に乗り出すヘッジファンドと市場の変調 2017/12/25", http://fis.nri.co.jp/ja-JP/knowledge/commentary/2017/20171225.html, 2019/1/4

あると指摘されている[255]。その意味で、例えば、アプリケーションが DEX と連携して、手持ちの暗号資産を、あるサービスの利用やある処理に必要な暗号資産に交換して支払いを行う、という一連の処理を自動化して行うユースケースなど、投資手段よりも決済手段としての DEX を念頭にした開発が進む可能性もある[256]。

当局の視点で考えた場合、DEX の取引高は本稿執筆時点で中央集権型取引所に比べ極僅か（1%未満）であり、大半の DEX は特定の管理主体が存在していることから、AML/CFT 上の DEX の重要性は限定的であり、規制を行う際の対象先も存在すると言える。依然として、DEX よりも、KYC 等を徹底しない中央集権型取引所の方が脅威と考えられるが、何らかのブレークスルーにより、特に特定の管理主体を介さない DEX が普及した場合は、AML/CFT 上、中央集権型取引所以上の脅威となる可能性が考えられる。そのため、DEX の開発状況については今後も注意して見ていくことが重要であると考えられる。

255 Abela, L., Medium, "Kyber Network - It Is More Than Just A DEX", https://medium.com/@lewisabela1/the-path-to-a-decentralised-world-2c035e16cecf, 2019/1/9

256 大手取引所の Binance が独自の DEX を開始するなど、今後も注意すべき動きが見られる。Yogita Khatri, coindesk, "Binance(s Decentralized Exchange Is About to Launch for Public Testing", https://www.coindesk.com/binances-decentralized-exchange-is-about-to-launch-for-public-testing, 2019/2/11

3.4 匿名通信技術にかかる調査

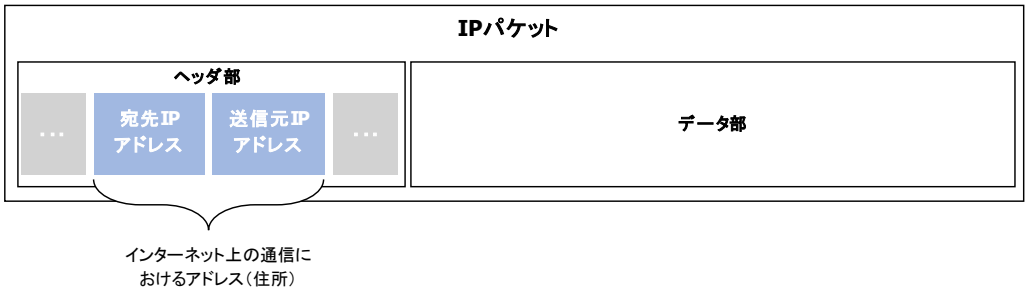
本節では、「プライバシー保護技術及び分散化技術を巡る開発状況の調査」における匿名通信技術の開発状況について記載する。

3.4.1 概要

3.4.1.1 インターネット上の通信の特徴

インターネット上で行われる通信は、「IP パケット」というデータの塊でやり取りが行われており、IP パケットは大きくヘッダ部とデータ部によって構成されている。ヘッダ部には通信を行うための必要な情報が格納されており、そのうち受信者や送信者のアドレス（住所）として「宛先 IP アドレス（受信者 IP アドレス）」と「送信元 IP アドレス（送信者 IP アドレス））」が格納されている。

図表 101 IP パケットと IP アドレス



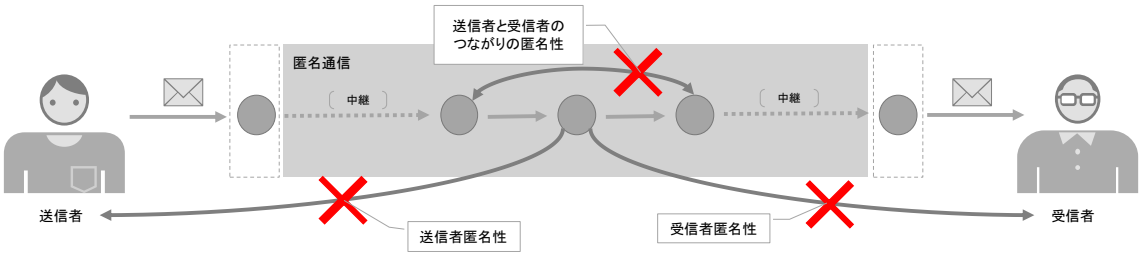
IP パケットを送信元から宛先まで届けるためにネットワーク上の伝送経路を決めることを「ルーティング」と呼び、ネットワーク上にあるルータは、IP パケットにある宛先や送信元の IP アドレスを基にルーティングを行う。

3.4.1.2 匿名性の分類

インターネットにおける通信は、IP パケットが送信者から受信者にルーティングで決まった伝送経路に沿って送信される。ここで伝送経路に関する匿名性として、「送信者匿名性」、「受信者匿名性」、「送信者と受信者のつながりの匿名性」の 3 つの匿名性が挙げられる[257]（図表 102）。また、伝送経路以外に、通信内容の匿名性も考える必要がある。

257 送信者匿名性とは、第三者に加え、通信の端点である受信者からみて、もう片方の端点である送信者の匿名性が担保される場合も指す。受信者匿名性も同様。

図表 102 通信の匿名性



3.4.1.3 匿名通信技術の概要

インターネット上の通信において通信途中の IP パケットを送信者および受信者以外の第三者が取得した場合、ヘッダ部を解析すると受信者の IP アドレスや送信者の IP アドレスを入手することができる。通常は IP アドレスから実際の個人（送信者または受信者）まで特定することは困難であるが、警察の開示請求がある場合など[258]、インターネットサービスプロバイダの通信履歴等を調べることによって当該 IP アドレスを使用していた個人を特定することが可能な場合もある。他に、IPv4[259]に代わって今後普及が予想される IPv6 では事実上無限のアドレス（約 3.4×10^{38} 個）を生成可能であり、設定にも依るが[260]、個々の端末単位で固有のアドレスが割り当てられるため、アドレスを基に通信端末が特定・把握される可能性もある[261]。

他にも、伝送系路上のネットワークを監視し、IP パケットのデータ部を解析することで、通信内容を把握することもできる。

以上のように、通常のインターネット通信では IP パケットから受信者／送信者の IP アドレスや通信内容を第三者に把握される懸念があり、3.4.1.2 節「匿名性の分類」で挙げた匿名性が担保されない懸念がある。これらを解決する技術の一つとして、暗号技術等を活用して受信者や送信者の IP アドレスの特定や通信内容の特定を困難にする、匿名通信技術が存在する。

匿名通信技術は、プライバシー保護、検閲・言論統制下での自由な情報発信や情

258 木村, 総務省ウェブサイト, "ISP における個人情報の取扱いの現状等", http://www.soumu.go.jp/main_content/000340244.pdf, 2019/1/7

259 現在普及している IPv4 では、IP アドレスは全世界で約 43 億個しかないため、NAT や NAPT といった技術で IP アドレスを置き換えて通信を行っている。そのため、IP アドレスから、それを使用していた個人を特定することが難しい場合が存在する。

260 ハッシュ関数を利用した「一時アドレス（匿名アドレス）」により定期的にアドレスを変更することも可能。

261 日本ネットワークインフォメーションセンターウェブサイト, "IPv6 セキュリティ ～問題点と対策～", https://www.nic.ad.jp/ja/newsletter/No54/0800.html, 2019/1/7

報共有を目的として開発された一方で、違法な物品の売買や犯罪に使用されるケースも発生しており、我が国においてもそれら匿名通信技術を悪用した事件が発生している（図表 103）。

図表 103 我が国における匿名通信技術を悪用した事件の例

事件名称	内容
パソコン遠隔操作事件[262]	2012 年 10 月、マルウェアに感染した PC が犯行予告や脅迫の書き込みに利用され、警察が IP アドレスを頼りに操作した結果、PC の持ち主が誤認逮捕された。 真犯人は、マルウェアのアップロードや感染後の PC の遠隔操作に Tor を利用したとされている。
年金情報の流出事件[263]	2015 年 5 月に日本年金機構がサイバー攻撃を受け、約 125 万件の個人情報が流出した。 通信に Tor が使われたとされており、犯人の特定や捜査を困難となった結果、容疑者不詳のまま書類送検された。
学校の爆破予告事件[264]	2017 年 1 月、専門学校に対する爆破予告のメールが 19 回にわたり送信され、同校の生徒が逮捕された。 同生徒は Tor を使ってメールを送信していたが、メールの内容などから学校関係者とみて逮捕に至った。
不正送金を行うマルウェア事件[265]	「DreamBot」は金融機関におけるインターネットバンキング用の認証情報の窃取や、遠隔操作によって不正送金を行うマルウェアであり、マルウェアをダウンロードさせるためのリンクを記載した日本国内向けのメールが 2017 年 10 月以降に急増した。 DreamBot は命令の送受信に Tor を利用しているとされる。
児童ポルノ公開事件[266]	2018 年 6 月、Tor を利用したダークウェブ内の会員制サイトに児童ポルノを公開していた容疑者が逮捕された。 Tor を利用したダークウェブ内のサイト開設者を摘発するのは全国初であり、世界的にも逮捕事例は少ないとされる。

3.4.1.4 匿名通信技術の分類

本調査研究では、匿名通信技術を分類する観点として、ルーティングという軸で整

262 日本ネットワークセキュリティ協会ウェブサイト, "（1）遠隔操作マルウェア事件から学ぶべきこと", https://www.jnsa.org/secshindan/secshindan_1.html, 2019/1/7
263 毎日新聞ウェブサイト, "年金情報流出 125万件時効 匿名ソフトが捜査の壁", https://mainichi.jp/articles/20180520/k00/00m/040/152000c, 2019/1/7
264 産経ニュースウェブサイト, "「2週間以内に爆破」と専門学校に予告 容疑で19歳の元生徒を送検", https://www.sankei.com/affairs/news/170801/afr1708010019-n1.html, 2019/1/7
265 Allied Telesis Blog ウェブサイト, "不正送金を行うウイルス「DreamBot」、国内で猛威をふるう(1)", https://www.allied-telesis.co.jp/blog/curation149.html, 2019/1/7
266 ITmedia NEWS ウェブサイト, "匿名化ソフト「Tor」使い児童ポルノ公開疑い 京都府警が初摘発", http://www.itmedia.co.jp/news/articles/1806/06/news063.html, 2019/1/7

理を行った。

3.4.1.4.1 ルーティング

インターネット上の通信では、IP パケットに記録された送信元・送信先 IP アドレスにしたがって当該 IP パケットが各中継ノードで伝送される。そのため、匿名化にあたっては、伝送系路上の全てのノードに対して「全体の伝送経路」を如何に隠蔽するかがポイントになる。

全体の伝送経路を隠蔽する手段として、暗号技術を活用した匿名ルーティング（Anonymous Routing）がある。匿名ルーティングは、通信における送信者や受信者のアイデンティティやロケーションに関する情報を秘匿化（匿名化）する技術である。匿名ルーティングにおいて受信者／送信者アドレス間の中継経路を選択する主な方法としては、ソースルーティング方式とホップバイホップ方式が存在する（図表 104）。

図表 104 匿名通信技術のルーティング方式

種類	内容
ソースルーティング方式	受信者との通信を中継するノードやその順序を送信者が決定する。送信者は、各中継ノードが最終的な受信者や元の送信者を知ることなくデータを転送可能となるよう、暗号化等を活用してデータを送信する。
ホップバイホップ方式	事前にデータの伝送経路は決定されず、各中継ノードにデータが到達した時点で自身が最終的な宛先であるか判断し、最終的な宛先でなかった場合は各中継ノードが次の宛先を決定してデータを送信する。

上記のソースルーティング方式およびホップバイホップ方式は、いずれも送信者から受信者の間に複数の中継ノードを経由させ、各中継ノードは自身の直前・直後の送信者・受信者のみを把握可能とする方式であり、元の送信者や最終的な受信者を知ることなくデータの受信・送信（転送）を可能とする。匿名ルーティングにおいて、中継ノードの個数は匿名性の強度と性能に影響を及ぼす[267]ため、ユースケースに応じて性能要件の比重を変える必要がある。

なお、ソースルーティング方式では、送信者が全体の伝送経路を決定するため、事前に全ての中継ノードを把握している必要がある。一般には、特定のノードが全ノード情報を集中的に管理する方式（ディレクトリ型とも呼ばれる）が用いられ、送信者は事前に当該ノードにノード情報を問合せてから、伝送経路の決定を行い、送信を行う。

267 中継ノードの個数が増えるほど匿名性は増すが、性能（通信速度等）は低下する。

3.4.2 事例調査

匿名通信技術は、前述のとおり通信の匿名性を高めるものであり、送信者と受信者の匿名化に加え、送信者と受信者間のつながりを匿名化する技術である。本節では、専門家等の意見を踏まえ、匿名化通信技術のうち、著名な Tor、I2P および Freenet という 3 つのプロトコルについて記載する（図表 105）。

図表 105 事例調査の対象（Tor、I2P および Freenet）

ルーティング	ソースルーティング方式		ホップバイホップ方式
代表的なプロジェクト名	Tor （The Onion Router）	I2P （Invisible Internet Project）	Freenet
ノード情報の管理方法	特定ノードによる集中管理	特定ノードによる分散管理	各ノードが近傍のノード情報のみ管理
主な用途	通常の Web サイトとの間の匿名通信	独自のネットワーク内で閉じた匿名通信	独自のネットワーク内で閉じた匿名情報共有
	Web ブラウジング等を目的としているため、通信遅延を抑えることを重視している。	I2P ネットワーク内の通信遅延を抑えることを重視するが、通常の Web サイトに対する通信遅延は大きい。	ファイルが分散管理されるため、元の保有者がオフラインでも参照可能。
匿名性の程度	全体の伝送経路は中継ノード含めて第三者から隠蔽される（ただし、通信内容は、HTTPS 通信を用いていない場合、出口ノードが把握可能）。	全体の伝送経路は中継ノード含めて第三者から隠蔽される。	全体の伝送経路は中継ノード含めて第三者から隠蔽される。

3.4.2.1 Tor

3.4.2.1.1 目的

Tor（The onion router）は、インターネット通信における匿名性を担保することを目的としており、トラフィック解析などで IP パケットのヘッダから送信者や受信者が特定されることを防ぐものである。

Tor は、1995 年に ONR（Office of Narval Research：アメリカ海軍研究局）の出資

により技術的基盤である Onion Routing の研究を開始し、その後 1997 年から 2004 年までは ONR に加えて DARPA（国防高等研究計画局：Defense Advanced Research Projects Agency）の支援により研究開発が行われた。Tor は 2003 年にオープンソースコードとしてリリースされ、その後研究開発の主体が非営利組織である Tor Project に引き継がれたものの、研究開発資金の大半は米国政府（国務省、国防総省）とされている[268]。

Tor は一般的なインターネット通信（Web ブラウジング等）における匿名性の担保を念頭に置いており、「送信者匿名性」および「送信者と受信者のつながりの匿名性」を実現するとともに、Web ブラウジング等の用途として耐えうる用に通信のレイテンシを抑えることを重視している。

Tor は上記の技術に加え、受信者側を秘匿する仕組みである Tor 秘匿サービス（Tor Hidden Service）[269]も提供しており、この場合は「送信者匿名性」および「送信者と受信者のつながりの匿名性」に加え、「受信者匿名性」や「通信内容の匿名性」も実現される。さらに、検閲体制下で Tor を利用していることを秘匿するため、Tor ネットワークとの間の通信を他の通信に偽装するブリッジモードという仕組みも提供されている。

Tor は匿名通信技術のなかでは最も人気があると指摘されており[270]、2018 年 11 月時点で 200 万人ほどのユーザがいるとされている[271]。

3.4.2.1.2 匿名化の実現方法

(i) ソースルーティング方式

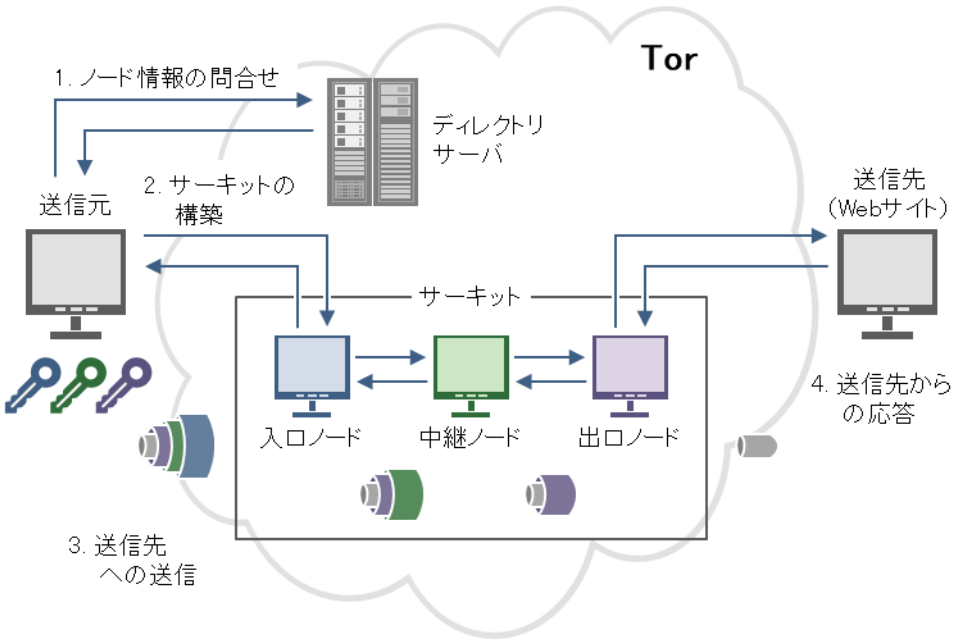
Tor は、ソースルーティングによって通信経路を決定する。Tor を利用する際にはクライアント上で Onion Proxy（OP）と呼ばれるソフトウェアを実行し、通信を行う際に OP によって Circuit と呼ばれる通信経路が構築される。Circuit は仮想的な双方向通

268 isBuzz news, "The Secret History of Tor", https://www.informationsecuritybuzz.com/news/secret-history-tor/, 2019/1/7 によると、2007 年から 2014 年における米国政府の出資比率は間接的なものも含めて 70%～90%とされている。
269 受信者側のサイトアドレスには「.onion」が含まれ、原則として、Tor ネットワーク内からでしか接続できない。
270 Akamai ウェブサイト, "ダークウェブの現状 2016", https://www.akamai.com/jp/ja/about/our-thinking/threat-advisories/akamai-2016-state-of-the-dark-web.jsp, 2019/1/7
271 Tor Project, Users, https://metrics.torproject.org/userstats-relay-country.html, 2019/1/7

信のネットワークで、OP と複数の Onion Router（OR）[272]によって構成される。

OR は Circuit を構築するために必要なネットワークの構成要素で、OR は Circuit において 3 つの役割（Entry Guard Router、Intermediate Router、Exit Router）[273]に分類される（図表 106）。Tor における Directory Server（DS）は全 OR に関するリストを保持しており、Circuit 構築において、Entry Guard Router は OP がリストとして保有している 3 つの OR[274]からランダムに選択され、Intermediate Router と Exit Router は DS が保持する帯域情報等を踏まえて確率的に選択される。

図表 106 Tor を介した通信のイメージ[275]



一旦構築された Circuit 上では複数の TCP ストリームが伝送されるが、攻撃者（敵対者）にそれらの TCP ストリームを統合して解析されることを防ぐため、Circuit のデフォルトの持続時間（タイムアウト）は 10 分に設定されており、その時間が経過すると Circuit は廃棄され、新たな Circuit が構築される。

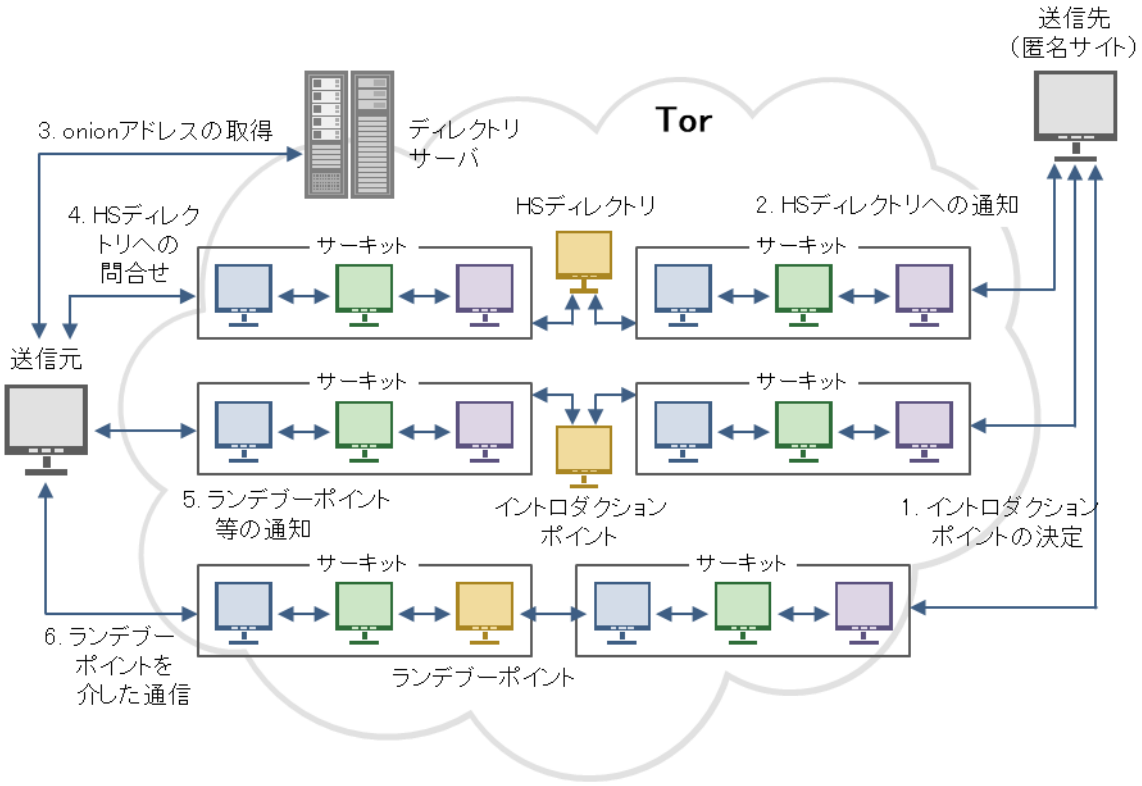
タイムアウトが発生すると新たな Circuit が必要となるが、予めバックグラウンドで次の Circuit を構築し、さらに Circuit 構築後の通信経路は固定化されるため、匿名性を担保しつつ、比較的レイテンシが小さい通信を実現している。

---

272 Austin, D., "TOR Node List", https://www.dan.me.uk/tornodes, 2018/11/1 によると、OR は全世界で 7394 存在する（2018/11/1 時点）とされている。
273 「router」は、「node」や「relay」と呼ばれる場合もある。
274 通常は 30 日周期で Entry Guard Router のリストは再作成される。
275 Elgzil, A., et al., Department of Computer Science University of Colorado, "Cyber Anonymity Based on Software-Defined Networking and Onion Routing", Table2 より三菱総研作成

なお、Tor ネットワーク経由でしか接続できない Tor 秘匿サービスは、クライアント（送信者）とサーバ（受信者）の双方の匿名性を担保するため、さらに複雑な仕組みとなっている（図表 107）。秘匿サービスでは、クライアント（送信者）とサーバ（受信者）それぞれがサーキットを構築し、それぞれのサーキットはランデブーポイント（Rendezvous Point、RP）にて合流する。クライアントは、RP まで暗号化されたサーキットを構築し、サーバも RP まで暗号化されたサーキットを構築する。中継ノードは、クライアントからサーバまで、RP も含めて通常は 6 ノードを経由し[276]、クライアント側で RP も含めて 3 つ、サーバ側で 3 つ指定する。RP はクライアント側で指定し、RP に関する情報は、サーバが指定したイントロダクションポイント（Introduction Point、IP）を通じてサーバに伝えられる。クライアントは、IP に対して RP の情報を送り、IP はサーバにクライアントが指定した RP の情報を転送する。IP に関する情報は、後述のとおりディレクトリサーバに登録され、RP 及び IP によりクライアントとサーバの匿名性を担保したまま、データの送受信が可能となる。

図表 107 Tor 秘匿サービスのイメージ



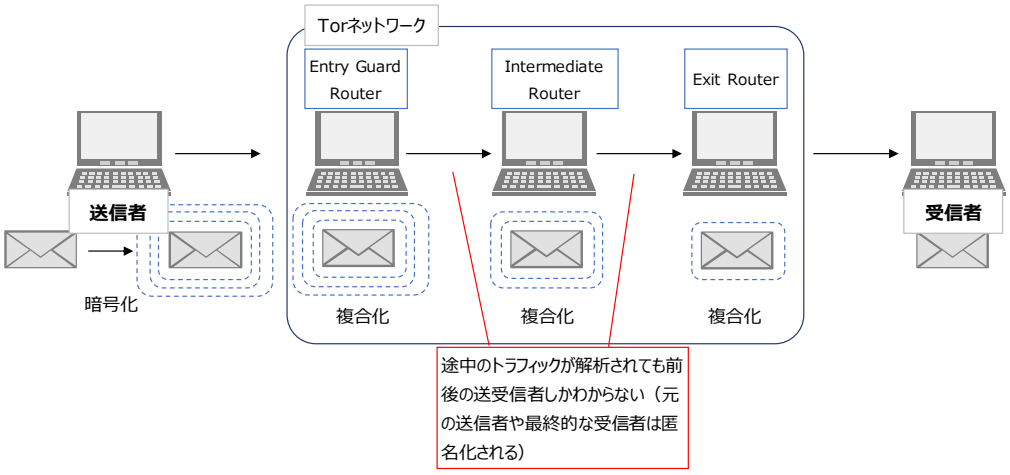
276 Biryukov, A., et al., "Bitcoin over Tor isn't a good idea", https://arxiv.org/pdf/1410.6079.pdf, 2019/1/7

(ii) 送信者／受信者の秘匿化

Tor では Circuit でデータを伝送するにあたり、Onion Encryption によって送信者と受信者を匿名化している。Circuit の構築後、OP は Circuit 上にある各 OR の公開鍵から生成した共通鍵によって送信データを複数回暗号化する[277]。暗号化は Exit Router から順番に行い、最終的には Entry Guard Router の鍵によりデータを暗号化する。データは多層に暗号化された状態で Circuit に送信され、Circuit 上の OR を移動するたびにそれぞれの OP 上で復号化される（図表 108）。各 OR は自身の直前の送信者と次の宛先となる受信者しか知ることができず、元々の送信者や最終的な受信者を匿名化した通信を実現する。

ただし、Exit Router と受信者の間の通信は平文となっているため、この部分を監視されると、第三者に通信内容が把握されてしまうことになる。そのため、SSL などを用いて、Exit Router と受信者の間の通信も暗号化することが推奨されている。

図表 108 Onion Encryption のイメージ



(iii) P2P 環境下における名前解決

Tor における名前解決は、DS によって行われる。クライアントにインストールされた OP はデフォルトで DS のリストを保有しており、OP は Circuit 構築時に自動的に DS に接続し、必要な OR の情報を取得する。DS は利用可能な全ての OR のリストを提供し、DoS 攻撃等に対応するため、DS は複数台用意されている。

なお、Tor 秘匿サービスでは、接続するために必要な情報（HS descriptor）を 6 つ

277 Tor では Diffie-Hellman 鍵共有により各 OP 間の共通鍵を生成し、生成された共通鍵は Circuit を逆にたどって送信者に届けられる。

のノード（HS ディレクトリ）に通知する。Tor 秘匿サービスの onion アドレスは SNS やブログ等を介して送信元に伝えられ、送信元はディレクトリサーバから HS ディレクトリの一覧を得て、onion アドレスに対応する HS ディレクトリから HS descriptor を取得する[278]。

3.4.2.2 I2P

3.4.2.2.1 目的

I2P（Invisible Internet Project）は、ネットワーク上の通信における端点（送信者や受信者）を匿名化するものであり、基本的なルーティングの考え方などは Tor と類似している。しかしながら、Tor は一般的なインターネット通信における匿名化を目的としているのに対し、I2P は独自の完結したネットワークを構築し、当該ネットワーク内で匿名通信を実現することを目的としている。I2P は、「送信者匿名性」、「受診者匿名性」、「送信者と受信者のつながりの匿名性」、「通信内容の匿名性」を実現するとともに、通信のレイテンシを抑えることも重視している。

なお、Tor と同様に I2P のネットワークから一般的な Web サイト等に接続することも可能ではあるが、ネットワークの出口（Outbound Proxy）が限られていることもあり、アクセスには非常に時間を要する。

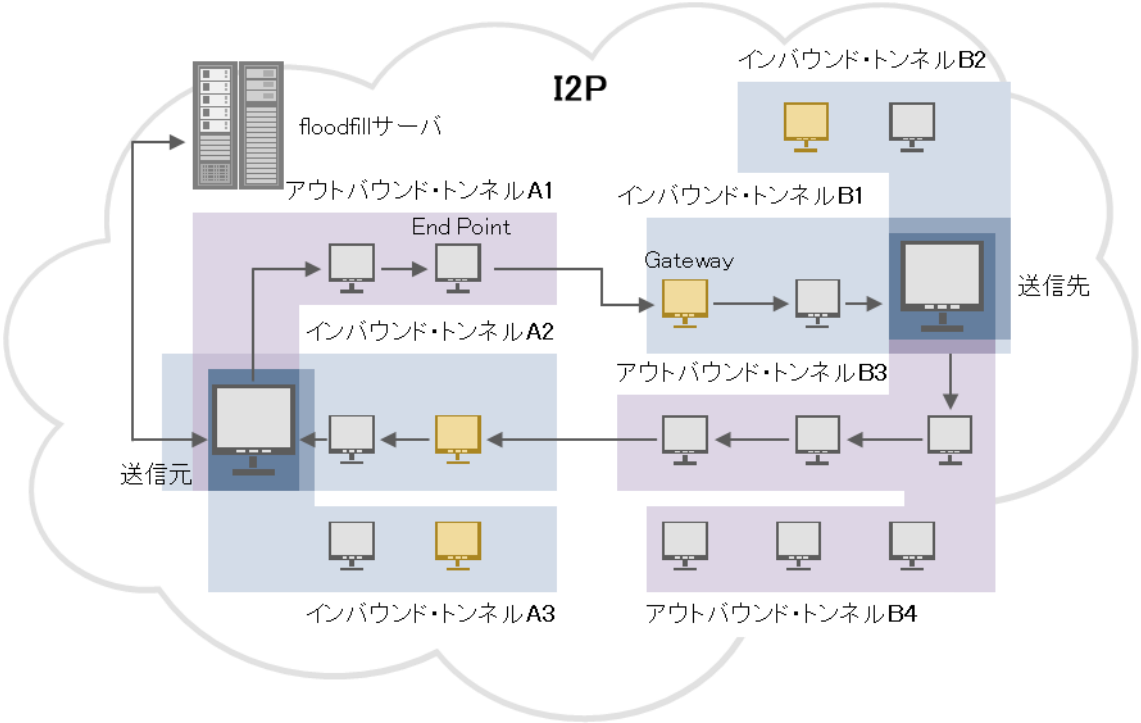
3.4.2.2.2 匿名化の実現方法

(i) ソースルーティング方式

I2P ネットワークの通信は Tunnel という通信経路を通じて行われ、Tunnel は複数の I2P Router により構成される。Tunnel は Tor の Circuit のように双方向通信ではなく、一方向通信となっている。そのため、受信用の Inbound Tunnel と送信用の Outbound Tunnel があり、送信者と受信者の I2P Router は送受信用の Tunnel を複数保持している（図表 109）。I2P もソースルーティングの一種であるが、送信者となる I2P が予め受信者までのすべてのルートを決定するのではなく、自身の Outbound Tunnel の出口（Endpoint）から受信者の Inbound Tunnel の入口（Gateway）となる I2P Router までのルートを決定する。

278 EXPOSING THE INVISIBLE, "Leak and Onion Soup", https://exposingtheinvisible.org/guides/leak-and-onion-soup/, 2019/1/7

図表 109 I2P を介した通信のイメージ



I2P Router のリストや各受信者[279]の Gateway に関する情報は netDB（networkDB）と呼ばれるデータベースに格納されており、netDB はfloodfill サーバという特権的な I2P Router が管理する。ただし、Tor における DS と異なり、floodfill は I2P ネットワークの部分的な情報が分散して格納されており[280]、送信者が問い合わせた近傍の floodfill サーバに必要な情報が保持されていない場合は、別の floodfill サーバに問い合わせを行う。また、floodfill サーバは予め設定された特権的な I2P Router ではなく、帯域などの分類（Fast、High-capacity、Well-integrated、Not-failing）で Fast に分類された I2P ルータが floodfill サーバになることができる。

なお、Tunnel のデフォルトの持続時間（タイムアウト）は 10 分であり、その時間が経過すると Tunnel は廃棄され、新たな Tunnel が構築される。I2P ではトラフィック解析に対抗するため、継続的に Tunnel の構築と廃棄を繰り返している。

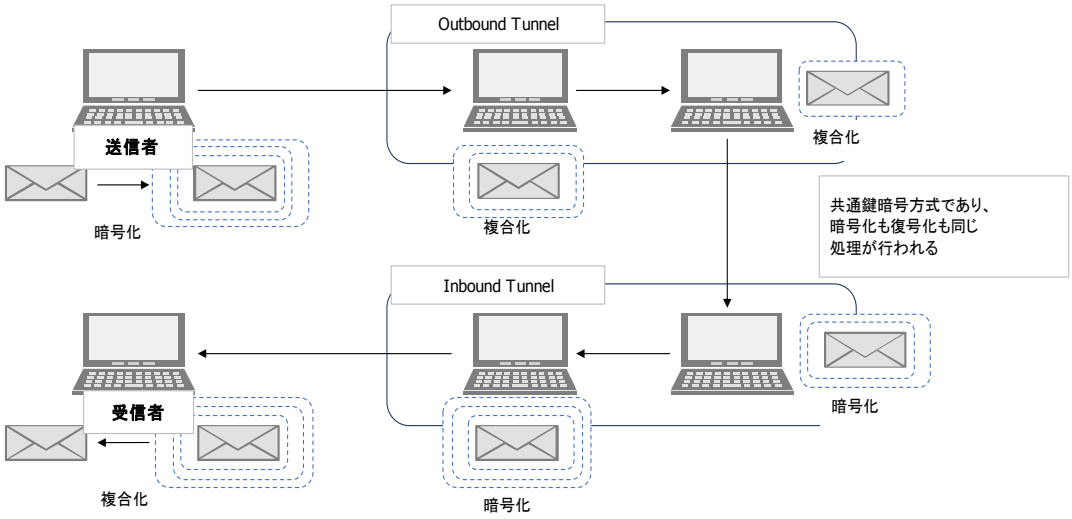
(ii) 送信者／受信者の秘匿化

I2P は、Tor と同様に、中継する I2P Router の暗号鍵でデータを多層的な暗号化を実施する（図表 110）。送信者は受信者の暗号鍵と、自身の Outbound Tunnel の各 I2P Router の暗号鍵で暗号化する。Tor と同様に、データは多層的に暗号化さ

279 またはアクセスしようとする I2P 内部のサービス。
280 DHT（分散ハッシュテーブル, Distributed Hash Table）によりデータが格納されている。

れ、Outbound Tunnel の各 I2P Router を通過するたびにデータは復号化される。一方、受信者の Inbound Tunnel 内の各 I2P Router は受け取ったデータを各自の暗号鍵で暗号化し、Inbound Tunnel の Endpoint（最終的な受信者）となる I2P Router は、自身の Inbound Tunnel 内の I2P Router の鍵で受信したデータを繰り返し復号化する[281]。

図表 110 Tunnel における暗号化[282]



I2P は End to End で暗号化され、Tor のように中継ノードの区別（Entry Guard Router や Exit Router）もないため、各中継ノードは、自身の送信元や送信先が元の送信者や最終的な受信者であることを知ることなく通信を行う。

なお、I2P では、複数のメッセージをひとつのデータとして送る Garlic Routing を用いている。この場合、複数の宛先に向けたデータが一つのデータに格納されるため、トラフィック内容の分析に加えてトラフィックパターンの分析にも耐性を有し、匿名性が強化されていると考えられる。

(iii) P2P 環境下における名前解決

I2P における名前解決は、netDB に格納された leaseset や routInfo といったデータにより実現される。leaseset は、受信者（または I2P のサービス）に接続するための情報がまとめられたものであり、各サービスの入口（lease）となる I2P Router（Inbound Tunnel の入口）に関する情報が蓄積されている。routerInfo は、I2P

281 Tunnel における暗号化は共通鍵暗号方式であり、暗号化も復号化も同じ鍵（処理）で行われるため、各 I2P Router は自身の処理が暗号化か復号化か判断することなく同じ処理を行う。
282 The Invisible Internet Project, Tunnel overview, https://geti2p.net/en/docs/tunnels/implementation, 2019/1/7 を元に三菱総研作成

Router に関する情報（IP アドレス、port、peer ID、公開鍵等）である。netDB は前述の通り floodfill サーバという特権的な I2P Router が管理するが、Tor と異なり、各floodfill サーバに全てのデータが格納されるのではなく、分散管理されている。

3.4.2.3 Freenet

3.4.2.3.1 目的

Freenet は、検閲に対する表現の自由や情報共有を目的とした完全分散型のファイル共有システムであり、「送信者匿名性」、「受診者匿名性」、「送信者と受信者のつながりの匿名性」や「通信内容の匿名性」の実現を目指している。Freenet への参加にあたって自身のハードディスクの容量およびネットワークの帯域を一部提供する必要があり、Freenet 上で発信したデータはネットワークに参加しているノードに分散されて格納される。そのため、元の発信者が Freenet からオフラインとなった場合でも、当該データはネットワーク上に残り続け[283]、検閲などに対し、発信者の匿名性確保やデータの完全性および可用性を担保することが可能となる。一方、Freenet は Tor や I2P と異なり完全な分散型ネットワークであるため、ノードを一元的に管理する主体などは存在しないものの、通信のレイテンシが大きい。

3.4.2.3.2 匿名化の実現方法

(i) ホップバイホップ方式

Freenet は、中央管理サーバや特権的なノードへの攻撃を避けるため、そのような中央管理が不要なホップバイホップによるルーティングを実装している。

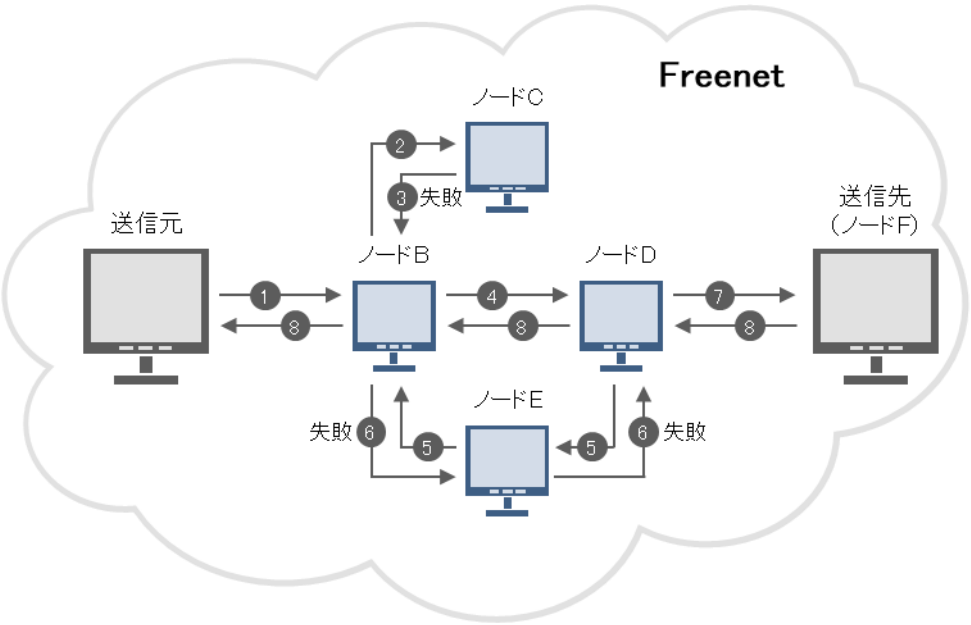
Freenet 上でデータを取得する場合、取得するデータの GUID（Globaly Unique Identifier） key を含むリクエストメッセージを自身の近傍にあるノードに送信し、リクエストを受信したノードは送られてきたリクエストの key に対して自身がデータを持っているか確認し、自身がデータを保有していない場合は次のノードにリクエストを転送する。各ノードは、近傍のノードが保有していると考える GUID key のテーブルを保有しており、各ノードにおいて転送先を決定する際は、それらのテーブルを基にリクエストの key に近い GUID を持っていると想定されるノードにリクエストを転送する。最終的にデータを持っているノードは、リクエストメッセージの経路を辿ってデータを返送す

283 ただし、十分なアクセスがないファイルは削除・上書きされる可能性がある。

る。返送経路の途中にあるノードは、送られてきたデータを自身にキャッシュし、GUID key のテーブルも更新する（図表 111）。

なお、ホップバイホップは中央的な管理を不要とする一方で、ルーティング自体は非効率であるため、レイテンシが大きく、さらにノード数の拡張に伴い性能も低下する。

図表 111 Freenet を介した通信のイメージ



1. 送信元は、取得したいデータのGUID（Globally Unique Identifier）keyを含むリクエストメッセージを近傍のノードBへ送信する。
2. ノードBは自身のGUID keyテーブル上で、リクエストされたkeyと近いノードCに確認を行う。
3. ノードCはリクエスト失敗という応答を返す。
4. ノードBは自身のGUID keyテーブルで、次に近いノードDに確認する。
5. ノードDはノードEを経てノードBに確認する。
6. ノードBはノードEを経てノードBにリクエスト失敗という応答を返す。
7. ノードDは自身のGUID keyテーブルで、次に近いノードFに確認する。
8. ノードFは当該データを保持しているため、ノードDへデータを転送する。ノードD、ノードBの順に送信元へデータを転送するとともに、それぞれデータをキャッシュし、自身のGUID keyテーブルを更新する。

(ii) 送信者／受信者の秘匿化

Freenet における通信の暗号化は、Tor や I2P のような多層的な暗号化は行われず、直接通信を行うノード間でのみ暗号化がなされる。送信者や受信者は各中継ノードで転送する際に上書きされ、元々の送信者や受信者を秘匿化して通信が行われる。

Freenet におけるデータの取得（要求）時は、データを要求する人（送信者）が近傍のノードにリクエストメッセージを送信し、データを所有する人（受信者）が見つかるまでリクエストメッセージが転送される。また、データの作成（発信）時は、データの作成者（送信者）がデータの GUID key を生成し[284]、データのリクエスト時と同様に近傍のノードに当該 key に衝突があるか確認を依頼し、設定した TTL（生存時間, Time to Live）内に衝突が発生しなければ各中継ノードにデータが格納され、テーブルも更新される。

(iii) P2P 環境下における名前解決

Freenet は名前解決のための中央管理サーバ等は存在せず、最終的な宛先の名前解決は行わずに通信を行う。ただし、Freenet の宛先の識別子である GUID key は事前に把握しておく必要があり、送信者は宛先となる key を知らなければデータの要求等を行うことはできない。Freenet ではそれらの key についてもリスト化等の集中管理はなされておらず、key の伝達方法として電子メールやポータルサイトでの情報交換が想定されている[285]。

3.4.3 課題と今後の見通し

匿名通信技術に関する攻撃は様々な研究がなされているが、運用や実装上の脆弱性をつく場合を除き、本稿執筆時点までにプロトコルレベルで致命的な脆弱性は発見されていない。他方で、Tor、I2P および Freenet の匿名通信技術の特徴のうち、課題として考えられる点について以降に記載する。

3.4.3.1 主な課題

- 匿名セットのサイズと質のトレードオフ

  一般的にネットワークにおいて自身の匿名性を担保するには、自身に近しい質を持った参加者が複数必要であり[286]、Tor、I2P および Freenet においても十分なノード数を確保できることが望ましい。他方で、ノード数が十分だとしても、参加者（クライアント側、サーバ側）の知見や技術的なレベルが十分でない

284 GUID key はハッシュ関数（SHA-1）により計算される。
285 Freenet, "Help, If I publish something in Freenet, how will people find it? Don't they have to know the key I used?", https://freenetproject.org/pages/help.html, 2019/1/7
286 例えば同じ内容の発言をしそうな人が複数いること。

場合は、脆弱な設定や不用意な使用により、十分な匿名性が得られない可能性も増大する。それ以外にも Tor や Freenet などは参加者が増え過ぎると通信の性能が低下する可能性があり[287]、匿名性は担保されつつも利便性に問題が生じる可能性がある。

- トラストポイントの存在

Tor や I2P は、名前解決のために中央管理するサーバやデータベースが用意されており、一種のトラストポイント（信頼点）として機能しているため、攻撃者にとってのターゲットとなり得る。特に Tor の DS の数は全世界で 10とされており[288]、その DS に全 OR の情報がリストされているため、（他のノードもキャッシュを保持しているとはいえ）攻撃の対象になりやすいと考えられる。なお、I2P の floodfill も特権的な I2P Router であるが、データが分散管理されているため、トラストポイントの影響度は Tor よりも低いと考えられる。

また、Tor、I2P および Freenet は全て中継ノードを経由した通信を行うが、各ネットワークにおける中継ノードは必ずしも善意の第三者とは限らず、警察や司法当局が監視のため設けたノードの可能性もある[289]。基本的には各中継ノードにおいて元々の送信者や最終的な受信者を特定することは困難であるが、Tor における Entry Guard Router や Exit Router は、自身の送信元や送信先が元々の送信者や最終的な受信者であることを推定できる場合がある。特に、Tor の Exit Router から先の通信は暗号化がなされておらず、送信者が十分な対策を施していない場合などは Exit Router 上でデータの改竄、または送信者を特定されてしまう可能性もあるため、同様に攻撃の対象になり得る。

これらのトラストポイントは、Tor や I2P が通信を行うにあたって前提として使用される情報であり、これらに誤った情報が登録されたりこれらが使用不能になったりした場合は通信に問題が生じる。こうした問題に対処するため、例えば Freenet では全てのノードと接続する Open Freenet 以外に、中継ノードの不正対策のために、自身が信頼した限られたノードのみと接続する Dark

287 Tor は中継するノードに対してクライアントが多すぎる場合は通信速度が低下し、Freenet はリクエストで宛先が見つかるまでのノード数が増えると通信速度が低下する可能性がある。
288 Tor Project, Relay Search, https://metrics.torproject.org/rs.html#search/flag:authority, 2019/1/7
289 上野 宣, "Tor の仕組みと各国取締り機関による Tor の追い詰め方", http://sd494dce02698adec.jimcontent.com/download/version/1440636206/module/10990797390/name/Tor_Ueno.pdf, 2019/1/9 によると、NSA と GCHQ は Tor ノードを自ら設置している様子

Freenet が構築されている[290]。

- その他のプロトコル自体の脆弱性

Tor などの匿名通信技術を利用したアプリケーションで見つかった脆弱性は、他の一般的なアプリケーションと同様に継続的に公表がされており[291]、Tor の通信の再識別（非匿名化）に焦点を当てた攻撃手法等についても様々な研究が行われている[292]。

たとえば、匿名通信技術によって構築されたネットワーク上のトラフィックを統計的に解析することにより、データが伝送される経路や送信者と受信者のつながりを特定する方法などが提案されている。Tor におけるトラフィックを解析するために、Entry Guard Router と Exit Router の両方のトラフィックを観測し、Entry Guard Router と Exit Router のアクセス日時とデータのサイズを突き合わせることでアクセスログから統計的にマッチングさせ特定する方法（Collusion Attack）や、応答のトラフィックに識別情報を付与して送信者を絞り込む方法（Tagging Attack）、逆に受信者の応答を固有の指紋（Fingerprint）情報として蓄積し、受信者を推定する方法（Fingerprint Attack）などが研究されている。

- 他アプリケーションと組み合わせることによる脆弱性

特に Tor はプロキシサーバとして機能し他のアプリケーションと併用することが容易なため、一般的なインターネット通信における匿名性の確保等、他のアプリケーション（例えばビットコインなどの暗号資産ネットワークや、Telegram や Signal などのセキュアチャットツール、OpenBazaar などの P2P 通信ネットワーク）と組合せて利用されることが益々増えると予想される。ただし、組み合わせて使用すると単体としては無かった新たな脆弱性や技術的課題が生じる可能性もある。

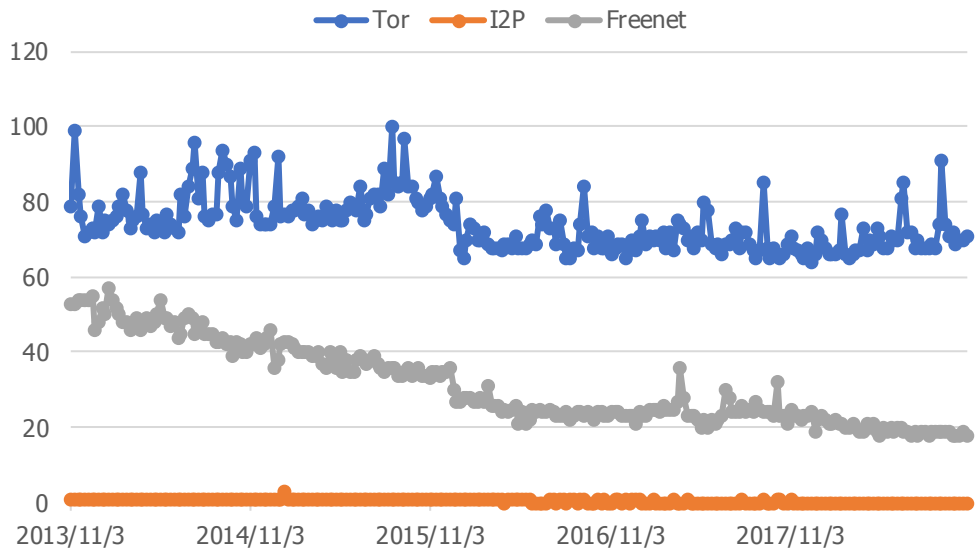
たとえば、ビットコインの取引で Tor を使う場合において、ビットコインの DoS

290 ただし、Dark Freenet が機能するためのノード数には条件があり、実際は殆ど使用されていないと言われている。
291 例えば Tor Browser の脆弱性は MITRE Corporation, "CVE Details", https://www.cvedetails.com/vulnerability-list/vendor_id-12287/product_id-23219/Torproject-TOR.html, 2019/1/7 で公表されている。
292 青木太一 他, "匿名通信システムの攻撃手法に関する調査" コンピュータセキュリティシンポジウム 2015 論文集 2015.3 (2015): 1207-1212.
図表 123 ・・・・・ p.5 Fig 1 より三菱総研作成

対策を逆に利用し[293]、Tor 経由でのビットコイン取引を悪用する方法なども提案されている[294]。

今後については、事例調査で取り上げた Tor、I2P 及び Freenet のうち、匿名での情報共有ツールとしての利便性やユーザベースの充実性という観点で、引き続き Tor を中心に利用されていくと考えられる（図表 112）。

図表 112 Tor, I2P, Freenet のキーワードの検索状況 [184]



技術面では、Tor や I2P はプロジェクトとして持続的に機能拡張や開発が行われており、例えば Tor のロードマップにおいては[295]、発見された脆弱性への対処のほか、前述の Fingerprint Attack のようなセキュリティ課題への対処や、UI 改善によるユーザビリティの向上などが検討されており、I2P のロードマップでは[296]、新しい netDB の研究や Tor と同様に UI の改善が予定されている。

3.4.3.2 当局としての関わり方

Tor や I2P は中継ノードを通じて通信を行うため、前述のとおり当局（警察や司法当局等）が秘密裏に中継ノードを設置し、それらを経由する通信を監視することが考

293 Bitcoin の peer はアクセス元の IP アドレスを採点しており、悪意あるメッセージを受けるとスコアが上昇し、一定の基準を超えると当該 IP アドレスからのアクセスが禁止される。
294 Biryukov, A., et al., "Bitcoin over Tor isn't a good idea", https://arxiv.org/pdf/1410.6079.pdf, 2019/1/7
295 Tor Project, TorBrowser, https://trac.torproject.org/projects/tor/wiki/org/roadmaps/TorBrowser, 2019/1/7
296 The Invisible Internet Project, ROADMAP, https://geti2p.net/ar/get-involved/roadmap, 2019/1/7

えられる。しかしながら、設置した中継ノードを経由するかは確率的であり、さらに中継ノードによる監視がユーザに明らかになった場合は、当該ノードがネットワークから排除されて新たに別のノードを設置する必要があるなど、いたちごっこの対応になってしまう可能性がある。

このような問題に対し、送受信者間でデータを暗号化しつつ、キーエスクローのように[297]、必要に応じて当局がデータを復号化できる環境を整えるといった、当局とユーザが協調的に取り組む仕組みも考えられている。ただし、これはユーザ、IT 企業や開発者からの強い反発を受ける恐れもある。IT 企業や開発者にとっては、製品やアプリケーションに意図的にバックドアを設置することになり、セキュリティ上の弱点を抱えることになるためである。米国では当該事件を受け、2016 年にデータの暗号化解除を企業へ義務付ける暗号化解除法案が作成されたが[298]、最終的に法案として提出されず、逆に 2018 年に捜査当局や監視機関が企業に暗号化のバックドアを設けるよう強制することを禁じる法案が提出されている[299]。

また、当局として匿名通信の再識別を試みるのではなく、例えば Tor の出口ノードとなる Exit Router がリストとして公開されていることから、掲示板などのサイト管理者に対して Tor を用いた通信の遮断（ブロック）を要請することも検討されている[300]。一方で、Tor による通信が直接的に犯罪行為につながるわけではない場合、通信の秘密を侵害する恐れもあるため、慎重な検討が必要と考えられる。

297 暗号化されたデータを復号するためのキーをエスクロー（信頼のおける第三者）に預け、その第三者が特定の状況下で当該データを復号化できるようにする仕組み。
298 2016 年の裁判所命令遵守法（Compliance With Court Orders Act of 2016）を指す。
299 2018 年のセキュアデータ法案(Secure Data Act of 2018)を指す。
300 例えば、中国では建国 60 周年を迎える 2009 年の 9 月末に Tor に接続できなくなる事象が発生し、これは中国政府により Tor へのアクセスが遮断されたことによるものとみられている。

3.5 その他の匿名技術にかかる調査

本節では、「プライバシー保護技術及び分散化技術を巡る開発状況の調査」におけるその他の技術の開発状況について記載する。

3.5.1 セキュアチャットツール

暗号資産の情報収集や情報発信にはチャットツールが頻繁に用いられる。チャットツールの中には通信内容の秘匿化に重きを置いたサービスを提供するものがあり、匿名通信ツールである Tor 等と組み合わせて犯罪に関係する通信に用いられる危険性が指摘されている。本節では、代表的なセキュアチャットツールである Telegram と Signal について、その特徴や仕組みについて記載する。

3.5.1.1 Telegram

3.5.1.1.1 概要

Telegram は、Telegram Messenger LLP が開発している、メッセージの暗号化によるプライバシー保護が可能なオープンソース[301]のチャットツールである[302]。クラウドベースのメッセージングサービス、VoIP サービスが利用でき、ユーザはメッセージやステッカーの送信、音声や写真、動画などすべてのファイルフォーマットの送受信が可能である。2018 年 3 月時点で月間アクティブユーザ数が 2 億人に到達した[303]。

Telegram は、ロシア出身の Pavel Durov 氏が中心となり 2012 年初頭から開発され、2013 年より運用されている。反テロリスト捜査の一環でロシア当局から、通信記録へのアクセス権を要求されたが Telegram 側はユーザプライバシー保護の観点からこれを拒否した経緯があり、現在ではロシア国内で使用禁止となっている。一方でこのことが非中央集権的な思想を好むコミュニティに受け入れられ、暗号資産を含むブロックチェーン関連のプロジェクトの情報の多くが Telegram 上でやりとりされていると言われる。

なお、Telegram はその通信形態として、通常チャットとシークレットチャットを用意し

301 クライント側のソースコードは公式 HP（Telegram, "Source Code", https://telegram.org/apps#source-code, 2019/1/7）でオープンソースとして公開されており、サーバ側も含めた全ソースコードは将来的にオープンソースとして公開するとしている。（Telegram, "Why not open source everything?", https://telegram.org/faq#q-why-not-open-source-everything, 2019/1/7）

302 Telegram, "Telegram", https://telegram.org/, 2018/11/7

303 Telegram, "200,000,000 Monthly Active Users", https://telegram.org/blog/200-million, 2018/11/7

ており、特に秘匿性の高い通信を行う場合はシークレットチャットが用いられる。通常チャットでは多人数間でのチャット（グループチャット）が可能だが、シークレットチャットでは 1 対 1 のやり取りに限定されている。

Telegram のシークレットチャットは米電子フロンティア財団の調査において、7 つの評価項目中すべての項目で基準を達成していると評価されている[304]。

3.5.1.1.2 通信内容の秘匿化

Telegram では通信内容の秘匿化にあたって、エンドツーエンド暗号が用いられており、MTProto という独自の暗号化プロトコルを採用している。

エンドツーエンド暗号（End to end Encryption、以下 E2EE[305]）とは、発信者、受信者のデバイス以外では通信内容を解読できないように暗号化する方式の総称である。E2EE では中継するサーバ上もデータが暗号化された状態で保持されるため、第三者がその内容を解読することはできないようになっている。

Telegram は、MTProto2.0 という独自の暗号化プロトコルを採用している（図表 113）。このプロトコルは、Diffie-Hellman 鍵共有を基本としており、前身の MTProto1.0 で脆弱性を指摘されていたSHA-1 関数の使用部分を SHA-256 関数に置き換える等の改良が図られた[306]。さらに、シークレットチャットでは前方秘匿性が確保されており、仮に 1 つのメッセージから暗号鍵が流出しても他のメッセージに影響が及ぶ事はない[307]。

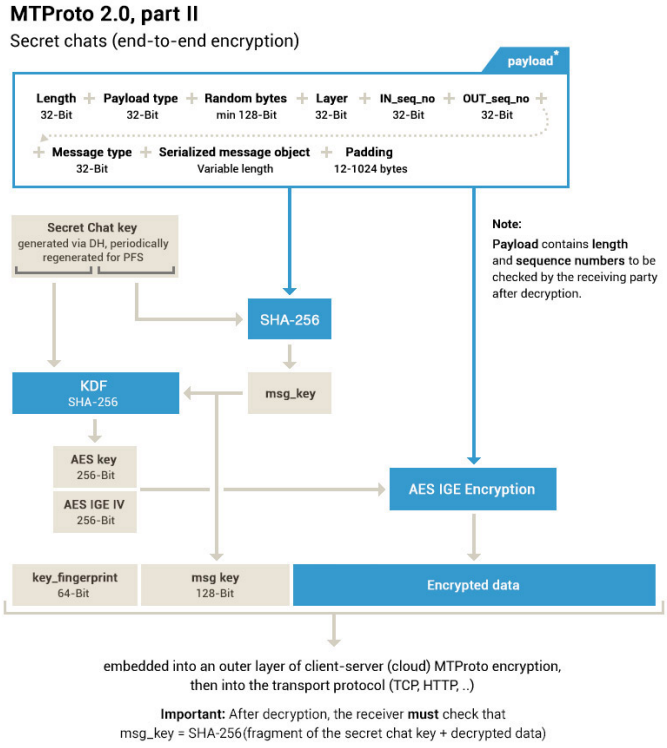
304 Electronic Frontier Foundation, "Which apps and tools actually keep your messages safe?", https://www.eff.org/node/82654, 2019/1/7 ※評価項目として「通信が秘匿化されているか」、「サービスプロバイダが解読できないような秘匿化がされているか」、「通信相手の同一性が検証できるか」、「暗号鍵が盗まれた場合に過去の通信内容の解読が防げるか」、「ソースコードがオープンにされ第三者検証がされるか」、「セキュリティ内容が適切にドキュメント化されているか」、「ソースコードのリスク検証チェックがなされているか」の 7 項目が挙げられている。

305 E2EE に相対する概念は、サーバクライアント暗号化である。この方式では、サーバ上に共有鍵が保持される。多数のユーザが参加するグループチャットを行う場合などは本方式のほうが処理や通信速度の面から使い勝手が良い。通信デバイスとサーバ以外の第三者が通信を傍受しても解読することはできないが、サーバ上に共有鍵が保持されるため、サーバ上のデータ流出の際に解読されるリスクが有る。

306 Cripto Fails, "Telegram's Cryptanalysis Contest, http://www.cryptofails.com/post/70546720222/telegrams-cryptanalysis-contest, 2019/1/7

307 Telegram, "Perfect Forward Secrecy", https://core.telegram.org/api/end-to-end/pfs, 2019/1/7

図表 113 Telegram の暗号化プロトコル MTProto[308]



3.5.1.1.3 その他の秘匿性にかかる工夫

Telegram のシークレットチャットサービスは、上記に述べた暗号化方式に加え、匿名性確保のための様々な工夫をおこなっている。メッセージそのものがサーバやクラウドに保持されることはなく、データは送信者・受信者の端末にのみ保持される[309]。さらに送信したメッセージやファイルは受信者がそれを読んだ後設定した時間で自動的に消去できるようになっており、一定度時間が経過すれば送信形跡がどのデバイスにも残らないような通信が可能となっている。

Telegram ではプロキシと組み合せることが可能であり、Tor ネットワークにつながった端末で Tor 所定のポート番号を指定して通信すれば、Telegram による通信内容の秘匿化に加えて Tor 等による伝送経路の秘匿化をおこなったメッセージ送受信が可能となっている。

308 Telegram, "MTProto 2.0, part II Secret chats (end-to-end encryption)", https://core.telegram.org/file/811140633/4/hHw6Zy2DPyQ.109500/cabc10049a7190694f, 2019/1/11
309 Telegram, telegram.org, "Telegram Privacy Policy（4.2. End-to-End Encrypted Data）", https://telegram.org/privacy#4-1-storing-data, 2019/2/8

3.5.1.2 Signal

3.5.1.2.1 概要

Signal は匿名性の高いオープンソースのチャットツールであり[310]、Open Whisper Systems というプロジェクトで開発が進められ、2014 年から Signal という名称に移行した。Signal Protocol と呼ばれるプロトコルを用いており、極めて高いセキュリティレベルから、WhatsApp など他のチャットツールでも利用されている。また Telegram にはない機能として、E2EE が適用されたグループチャットをサポートしている。

Signal の通信内容はすべて E2EE が適用されており、米電子フロンティア財団における 7 つの評価項目でもすべての項目で基準を達成していると評価された。また、アメリカ合衆国上院において議員間で連絡をとりあうためのツールとして認められており[311]、Telegram と比べてもセキュリティ上の評価が高いことが伺える。

また、Open Whisper Systems はサーバ上にユーザ情報を極力残さないような設計方針をとっており、実際 2016 年に米政府が犯罪への関与が疑われた通信データの提出を求めた際、そのデータを精査してもユーザアカウント作成日と最終使用日の情報しか得られなかったとされる[312]。

3.5.1.2.2 通信内容の秘匿化

Signal は、一方の通信相手がオフラインの場合でもサーバを中継した Diffie-Hellman 鍵共有を有効とする、Extended Triple Diffie-Hellman (X3DH) key agreement protocol などを用いた暗号化方式をとっている[313]。また、Telegram のシークレットチャットと同様に前方秘匿性が確保されている[314]。

---

310 Signal はすべてのソースコードがオープンソースとして GitHub 上で公開(Signal, GitHub, https://github.com/signalapp, 2019/1/7)されている。

311 Moon, M., Engadget, "US Senate approves encrypted chat app Signal for staff use", https://www.engadget.com/2017/05/17/us-senate-approves-signal-for-staff-use/, 2019/1/7

312 Thomson, I., The Resister, "Feds get sweet FA from Whisper Ssysmtes Signal subpoena", https://www.theregister.co.uk/2016/10/04/whisper_systems_signal_subpoena/, 2019/1/7

313 Mora, J., Medium, "Demystifyng the Signal Protocol for End-to-End Encryption（E2EE）", https://medium.com/@justinomora/demystifying-the-signal-protocol-for-end-to-end-encryption-e2ee-ad6a567e6cb4, 2019/1/7

Cohn-Gordon, K., et.al., "A Formal Security Analysis of the Signal Messagin Protocol", https://eprint.iacr.org/2016/1013.pdf, 2019/1/7

314 moxie, Signal, "Forward Secrecy for Asynchronus Messages", https://signal.org/blog/asynchronous-security/, 2019/1/7

3.5.1.2.3 その他の秘匿性にかかる工夫

Telegram と同様に自動メッセージ消去の機能を有している。その上でさらに Signal は「送信者秘匿（sealed sender）」という機能を開発中であり、この機能により、仮に通信を傍受されても送信者情報は取得できないとしている[315]。

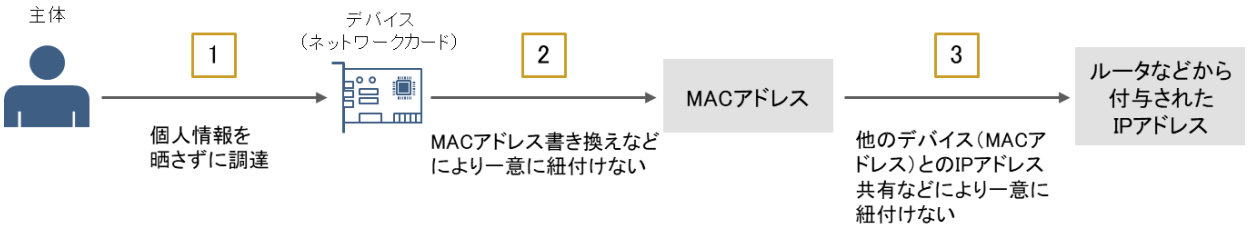
それ以外に、Telegram と同様、プロキシの設定を行うことで、Tor 等による伝送経路の秘匿化が可能である。

3.5.2 実世界レイヤーにおける匿名化技術

ある主体がインターネットに接続する際には、（1）主体、（2）当該主体が用いるデバイス（ネットワークカード等のネットワーク機器）、（3）当該デバイスに紐づく MAC アドレス[316]、（4）当該 MAC アドレスに紐づく IP アドレスという4種類の識別子が存在する。そのため、ある主体がインターネット通信を行う際の匿名化対象としては、主体とデバイス間の関係、デバイスと MAC アドレス間の関係、MAC アドレスと IP アドレス間の関係の三つが挙げられる（図表 114）。

- 主体とデバイスの関係では、如何に個人情報を晒さずにデバイスを調達するかがポイントとなる。
- デバイスと MAC アドレスの関係では、デバイスと MAC アドレスを一意に紐付けさせないことがポイントとなる。
- MAC アドレスと IP アドレスの関係では、MAC アドレスと IP アドレスを一意に紐付けさせないことがポイントとなる。

図表 114 実世界レイヤーにおける匿名化のポイント



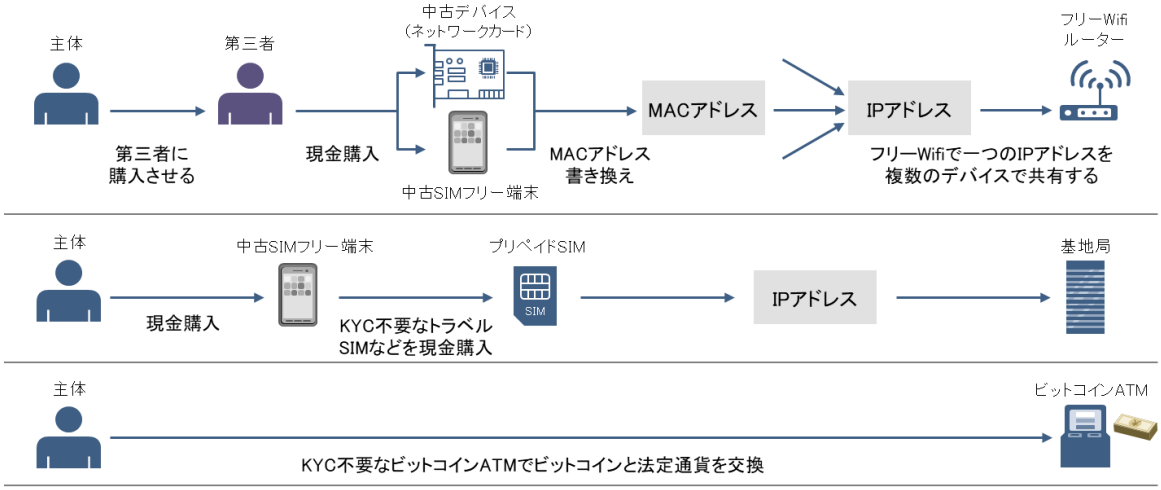
315 jlund, Signal, "Technology preview: Sealed sender for Signal", https://signal.org/blog/sealed-sender/, 2019/1/7

316 MAC アドレスとは、製造時にネットワーク機器に付与される 6 バイトの識別番号であり、原則として世界中で一意となる。70 兆個以上表現できるため、IPv4 などと異なり、本稿執筆時点では枯渇の恐れはない。ただし、ルータで区切られた範囲内で重複しなければ問題ないため、MAC アドレスを変更できるネットワーク機器も存在する。

そのため、主体を匿名化してインターネット接続を行う方法としては以下の方法が考えられる（図表 115）。

- 主体とデバイスの関係を匿名化するには、中古端末を現金で購入し、さらに（監視カメラ等を念頭に）デバイス受取は第三者に依頼する方法や窃盗などで調達する方法などが考えられる。
- デバイスと MAC アドレスの関係を匿名化するには、MAC アドレスを書き換える方法が考えられる（ただし、同一ネットワーク内で MAC アドレスが重複しないように注意する）。
- MAC アドレスと IP アドレスの関係を匿名化するには、フリーWifi で接続して他のデバイス（MAC アドレス）と IP アドレスを共有する方法や、プリペイド SIM のうち、KYC 情報なしに利用可能なものを用いる方法などが考えられる。

図表 115 実世界レイヤーの匿名化の例

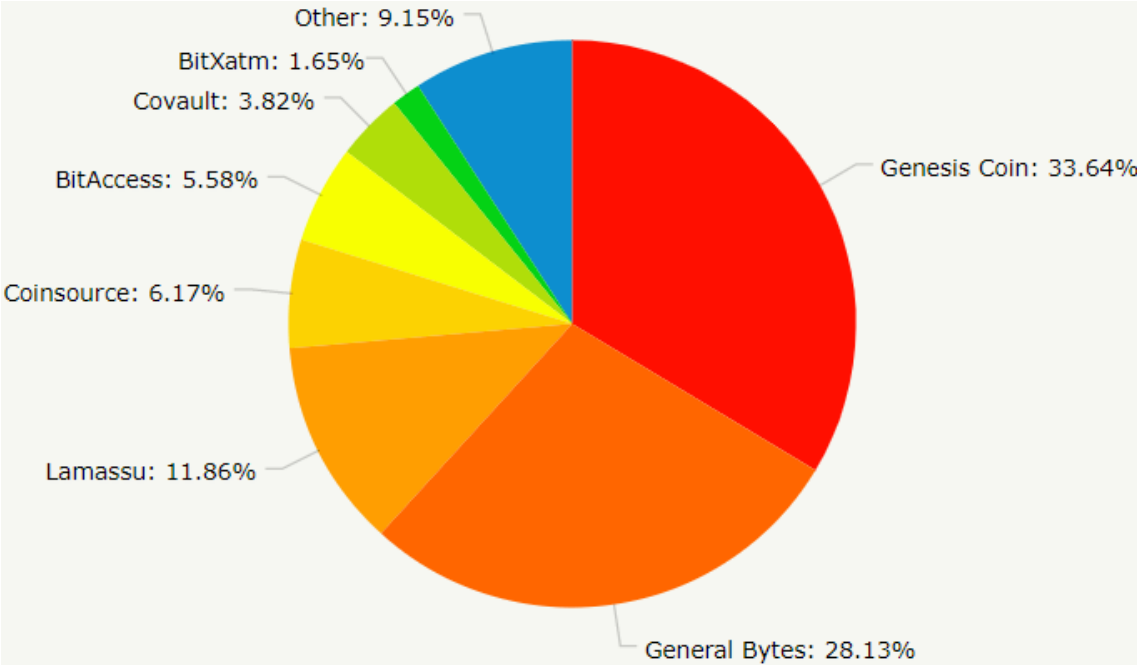


上記以外に、直接暗号資産を法定通貨に変換するには、本人確認を行わないビットコイン ATM を利用する方法なども考えられる。

ビットコイン ATM の製造販売元としては、米国では Genesis Coin 社、General Bytes 社、Lamassu 社などが大手だが（図表 116）、これらの製品は現在ではパスポートや ID カードによる本人確認が必要とされる。しかし本人確認を必要としない旧機種も存在し、また、Instacoin 社（加）や Bitrocket 社（豪）などは本人確認を行わない機種を販売していると指摘されることから、本人確認を経ずにビットコイン ATM で法

定通貨と暗号資産（ビットコイン）を交換することは可能と推測される[317]。

図表 116 米国市場におけるビットコイン ATM 製造販売元のシェア[318]



317 Peter Ivancic, CryptoSlate, "The Bitcoin ATM Black Market: Regulatory Blind Spot Allows Crypto Traders To Subvert KYC Requirements", https://cryptoslate.com/the-bitcoin-atm-black-market-regulatory-blind-spot-allows-crypto-traders-to-subvert-kyc-requirements/, 2019/2/8

318 Peter Ivancic, CryptoSlate, "The Bitcoin ATM Black Market: Regulatory Blind Spot Allows Crypto Traders To Subvert KYC Requirements", https://cryptoslate.com/wp-content/uploads/2018/04/ATM-share-by-manufactureer.png, 2019/2/8

3.6 再識別技術にかかる調査

本節では、「プライバシー保護技術及び分散化技術を巡る開発状況の調査」における再識別（追跡）技術やツールの開発状況について記載する。

3.6.1 概要

再識別化（追跡）にあたっては、大きく（1）レイヤー毎のプロトコルに基づく再識別、もしくは（2）外部のデータベースに基づく再識別という二通りのアプローチが挙げられる[319]。次節以降ではそれぞれについて記載する。

3.6.2 プロトコルに基づく再識別

3.6.2.1 アプリケーションレイヤー（ブロックチェーン）

本節ではアプリケーションレイヤーのブロックチェーンにおける再識別技術について記載する。

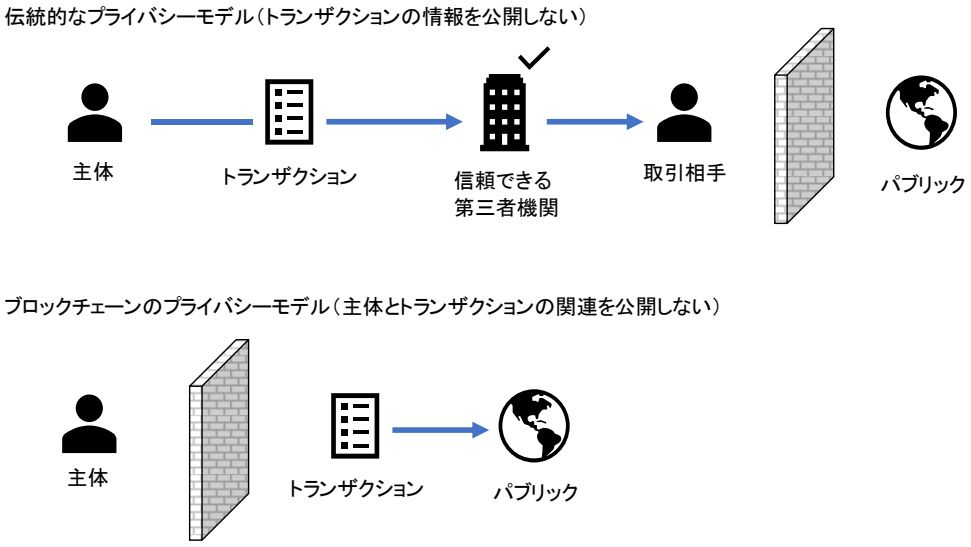
3.6.2.1.1 ブロックチェーン上の取引記録の特徴

プライバシーの観点からみると、ブロックチェーンでは仮名性を担保するようなプライバシーモデルが採用されている（図表 117）。仮名性とは、仮の識別子（ブロックチェーンの場合はアドレス）は公開されるものの、その識別子と本来の主体の関係は公開されず得ることができないという状況を指す。伝統的なプライバシーモデルでは取引内容（誰が誰にいくら送金したという情報）自体を公開しないのに対し、ブロックチェーンのプライバシーモデルでは取引内容はすべて公開されているものの、アドレスと主体の関係は公開されない点が大きく異なる[320]。

319 本調査研究では、立命館大学や筑波大学等、有識者へのヒアリングも行ったが、再識別技術については、2015 年～2016 年頃以降は学術的な論文が減ったとの意見が多く見られた。この一つの理由として、再識別技術をビジネスにするベンチャーが増えたために、企業秘密にあたる情報を公開するインセンティブが減ったのではないかとの見解も示された。

320 Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 2019/1/7

図表 117 ブロックチェーンのプライバシーモデル



3.6.2.1.2 ブロックチェーン上の取引における匿名性

通信における匿名性は、送信者匿名性、受信者匿名性、つながりの匿名性の三点が挙げられるが、一般的なパブリック型ブロックチェーンにおいては送金元アドレスや送金元アドレスは公開されている。そのため、ブロックチェーン上の取引の再識別にあたっては、特に以下の点について再識別を行う必要がある[321]。

- 非連結性（unlinkability）：主体とアドレスの紐付けができないこと（同一主体に紐付くアドレス群を名寄せできないこと）
- つながりの匿名性（untraceability）：送金元アドレスと送金先アドレスの関係を特定できないこと

3.6.2.1.3 ブロックチェーン上の取引に関する再識別技術

(i) 概要

ブロックチェーン上での追跡は、一般的には、以下の流れで行われる（図表 118）。

(1) アドレス間の関係をグラフ化した上で、一定の仮説に基づいて、それらを名寄せして複数のグループに分ける。

(2) 外部情報（KYC 情報、ウェブやダークウェブをクローリングして収集した情報、当局等から得た情報など）を別途収集して、主体とアドレスの紐付け表を作成

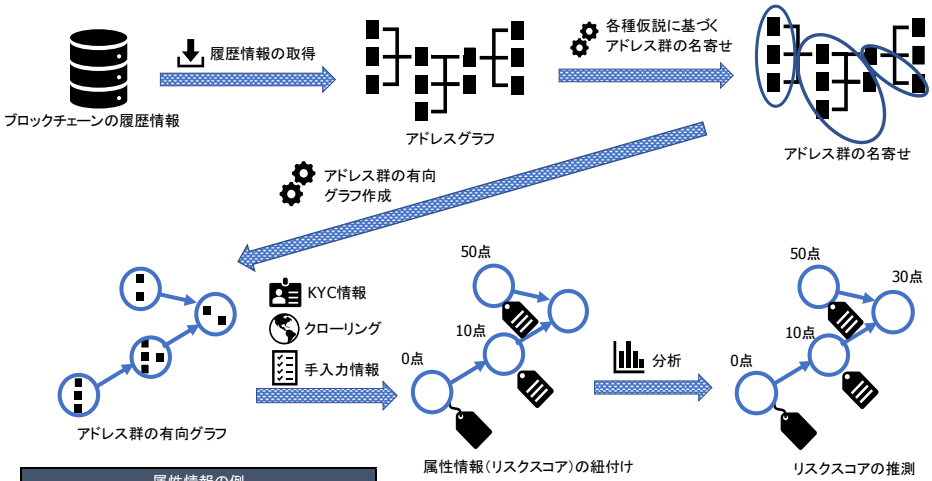
321 Kumar, A., et al, Eprint, "A Traceability Analysis of Monero's Blockchain", https://eprint.iacr.org/2017/338.pdf, 2019/1/7

し、主体ごとにリスクスコアを設定する。ここで、主体は、取引所、マイニング事業者やギャンブルサイトなどのカテゴリで分類されており、カテゴリ毎にリスクスコアが設定されているものとする。この紐付け表を（1）で得られた各アドレスグループにあてて、アドレスが一致したグループにリスクスコアを付与する。

(3) （2）の紐付け表に合致しなかったアドレスグループについては、既にリスクスコアが振られたアドレスグループとの取引関係から、リスクスコアを推定する。

ここで、主体と紐付けずに、アドレスから直接リスクレベルを推定する方法も行われることがある。上記の手順が行われる理由として、リスクはあくまで主体に紐づくものだから、という考えが紹介されている[322]。アドレス群の名寄せおよび属性情報の付与を行うことにより、著名なダークマーケットである Silk Road に紐づくアドレスの検出やランサムウェアに紐付くアドレスを特定するという研究が行われている[323]。

図表 118 ブロックチェーン上での追跡技術（アドレス群の名寄せ、属性情報の紐付け、リスクスコアの推測）



属性情報の例
仮想通貨交換所
マイニング事業者
FBI
ギャンブルサイト
Silk Road
詐欺師（売買サイトや掲示板などで指摘のあるもの）

アドレス群の名寄せに用いられる仮説で、代表的なものとしては、以下が挙げられる[324]。

322 DMG Blockchain Solutions Inc., "Walletscore; ALM Risk Scoring", https://dmgblockchain.com/walletscore/, 2019/1/7
323 Spagnuolo, M., et al., "BitIodine: Extracting Intelligence from the Bitcoin Network", https://www.ifca.ai/fc14/papers/fc14_submission_11.pdf, 2019/1/7
324 Conti, M., et al., "A Survey on Security and Privacy Issues of Bitcoin", https://arxiv.org/pdf/1706.00916.pdf, 2019/1/7

- 1 つのトランザクションに含まれる送金元アドレスの主体は同一である。

  これは複数の主体が協調してトランザクションを作成することは現実的には極めて少ないという想定に基づく。

- あるトランザクションの送金先アドレスのうち、新規のアドレス（ブロックチェーン上で初めて使われるアドレス）の主体は、当該トランザクションの送金元アドレスの主体と同一である。

  これは当該アドレスがおつりアドレスである、という想定に基づく。

しかし、上記の仮説はいかなるケースにも有効というわけではない。2つ目の仮説について、現在は Mining pool からの支払いやギャンブルサイトでの賭け金に対する支払いといった複数人宛てのトランザクションが生成される場合も存在し得るため、この仮説に基づいた名寄せ結果は誤りが多いという報告もある[325]。

アドレスグラフの構造分析に関する研究も行われている。2011 年 6 月に暗号資産の情報が集まる掲示板である Bitcoin Forum 上で allinvain というユーザが報告している 25,000BTC 流出事件について[326]、アドレスグラフの構造分析を行い、ビットコインの流出元と流出先のアドレスは同一主体に紐付く可能性（すなわち、allinvain というユーザの虚言ないし自作自演の可能性）があると報告している研究もある[327]。また、50,000BTC 以上の金額の送金元アドレスと送金先アドレスを対象として、アドレスグラフの構造分析やアドレス群の名寄せを行い、特徴的なグラフの構造を抽出するといった研究も行われている[328]。

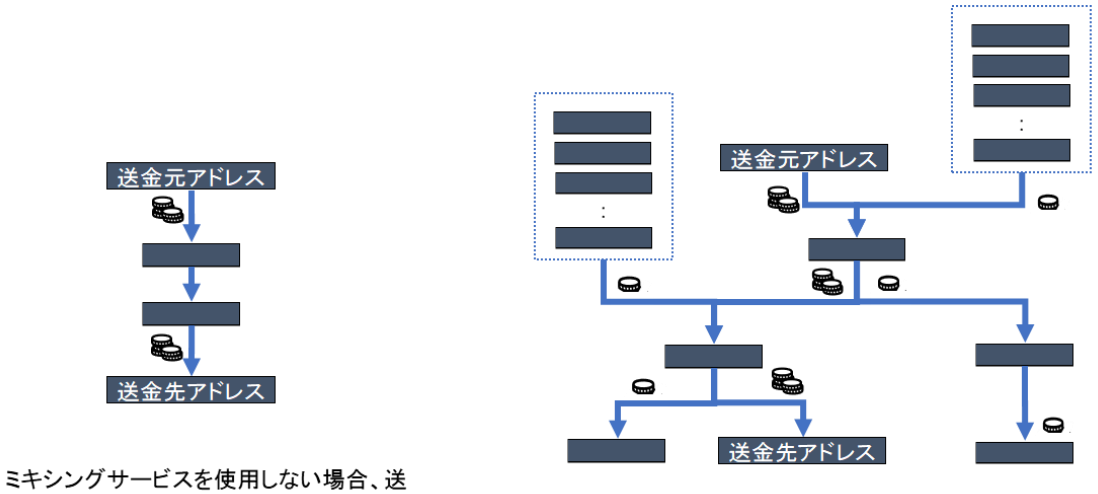
リスクスコアの推測に関する動向としては、教師なし学習としてアドレス群の名寄せを行った上で、属性情報の紐付けを行い、属性情報が紐付かないアドレスに対してはアドレスグラフにおけるリスク伝播（risk propagation）によってリスクスコアを推測する方法が提案されている [322]。

325 Meiklejohn, S., et al., "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names", https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf, 2019/1/7
326 allinvain, Bitcoin Forum, "Topic: I just got hacked - any help is welcome! (25,000 BTC stolen)", https://bitcointalk.org/index.php?topic=16457.0, 2018/12/21
327 Reid, F., et al., "An Analysis of Anonymity in the Bitcoin System", https://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf, 2018/12/21
328 Ron, D., et al., "Quantitative Analysis of the Full Bitcoin Transaction Graph", https://eprint.iacr.org/2012/584.pdf, 2018/12/21

(ii) ミキシングなど高度な匿名化手法に対する研究事例

ミキシングサービスでは送金元アドレスと送金先アドレスを指定して、送金額から手数料を除いた金額が送金先アドレスへ送金される。ミキシングサービスが利用されている場合、送金先アドレスと送金元アドレスを紐付けようとしても候補となり得る送金元アドレスの数が膨大になる。従って第三者からみて送金先アドレスと送金元アドレスの関係を特定すること、すなわち、「つながりの匿名性」を解消することは極めて困難となる（図表 119）。

図表 119 ミキシングと匿名性の関係



ミキシングサービスを使用しない場合、送金先アドレスから送金元アドレスを特定することは容易。

ミキシングサービスを使用した場合、送金先アドレスに対する送金元アドレスの候補は膨大となるため、送金元アドレスを特定することは極めて困難。

しかし、ミキシングサービスについてはいくつかの実装上の特徴が指摘されており、Helix というミキシングサービスやダークマーケットの Alphabay が提供していたミキシングサービスについて、生成されるトランザクションに関する以下のような傾向を検知したという報告がある[329]。

- 代表アドレス（Central address）の存在

  毎回特定のアドレス（Central address）へ送金される傾向がある。

- 経由するアドレスの同一性

  送金元／送金先アドレスが異なるにも関わらず、送金元アドレスから送金先

329 Balthasar, T., et al., "An Analysis of Bitcoin Laundry Services", https://www.researchgate.net/profile/Julio_Hernandez-Castro2/publication/319944399_An_Analysis_of_Bitcoin_Laundry_Services/links/5a045d410f7e9beb177883af/An-Analysis-of-Bitcoin-Laundry-Services.pdf, 2018/12/21

アドレスまでの一部の経路について、同一のアドレスを経由する傾向がある。

- 特徴的なコイン分割パターン（Peeling chain）の存在

  少しずつ皮がむかれていくように、相対的に大きな金額（実）と小さな金額（皮）の 2 つに分離（peeling）することを繰り返す。相対的に大きな金額は peeling を繰り返し、小さな金額はそれらを大量に束ねて大きな金額にして peeling を繰り返す、というパターンが存在する傾向がある。

- 特徴的なトランザクションパターン（回数や時間間隔、送金先の件数）の存在

  送金元アドレスから送金先アドレスまでに経由するアドレス数（送金回数）が一定、ないしはトランザクションが生成される時間間隔が一定、という傾向がある。また、1つの送金元アドレスに対して 2～5 の送金先アドレスというトランザクションが存在する傾向がある。これは同時に複数の利用者への送金に対応するためと考えられる。

こうした特徴を活用することで、ミキシングサービスが使用された場合でもつながりの匿名性を解消できる可能性がある。ミキシングサービスや仮想通貨取引所はそれぞれの実装に応じて特徴のあるトランザクションを生成することがあるという点に着目して、アドレスグラフの構造に対して教師あり学習を行うことによりアドレス群の名寄せを行う方法が提案されている[322]。具体的には、アドレスグラフの構造のうち以下のような情報を使用する。

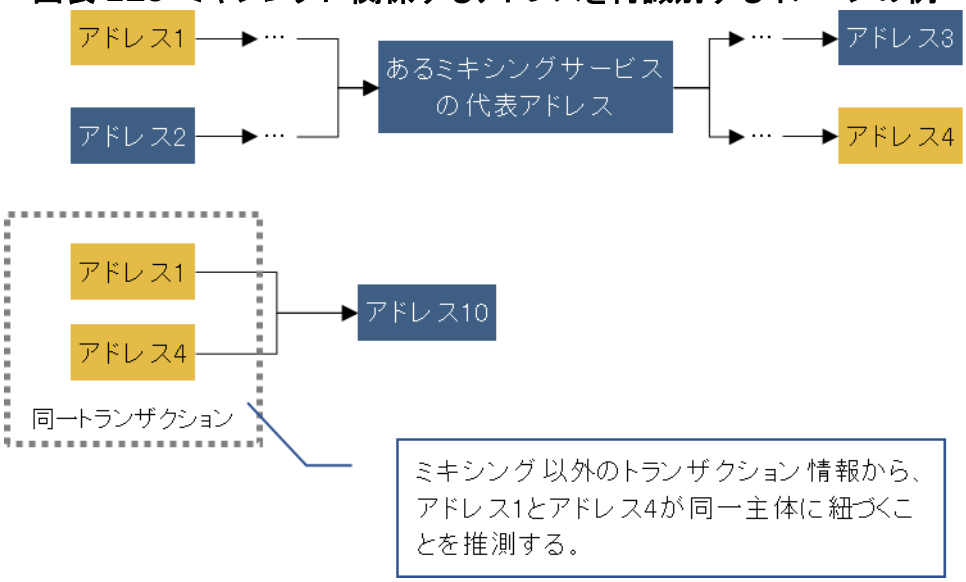
- 送金元アドレスと送金先アドレスの数と比率
- 金額の小数点以下の桁数
- 「おつりアドレス」の発生頻度
- 手数料の金額と送金額に占める手数料の割合
- 入力の金額と出力の金額のばらつき具合

その他にも、送金額と出金額の一致などを手掛かりに、アドレス群の名寄せを行う手法も提案されている[330]。また、ミキシングサービスで使い回される代表アドレスを特定した上、当該アドレスに対する送金元アドレスと送金先アドレスが、全く別のトラン

330 CoinJoin Sudoku では、縦・横・3×3 のマスに1から9の数字が一度だけ入るという条件のもとですべてのマスに数字を埋めるというパズルの考え方を用いて、金額の小数点以下の値の合算値の一致を手掛かりに送金元アドレスと送金先アドレスの名寄せを行う方法が提案されている。
Atlas, K., "CoinJoin Sudoku", https://www.coinjoinsudoku.com/advisory/, 2018/12/12

ザクションの送金元アドレスとなっている場合は、その 2 つのアドレスを同一主体のもとのみなすという方法も考えられる（図表 120）。

図表 120 ミキシングに関係するアドレスを再識別するイメージの例



しかしながら、ミキシングサービスが利用された場合の追跡は極めて困難であることに変わりはない。そのため、送金元アドレスと送金先アドレスの紐付けを行うのではなく、ミキシングサービスを利用しているという事実が認められた場合は、関連するアドレス群のリスクスコアを一律高くする（高リスクとみなす）といった方法などが取られる場合もある。ただし、適切に実装されたミキシングサービスの場合、ミキシングサービスが利用されたと特定すること自体も難しいと考えられる。

全く異なるアプローチとして、ミキシングサービスに入金されたコインと出金されたコインを、先入れ先出し方式（First In First Out、FIFO）で対応付ける考え方も提案されている[331]。これは入金と出金の本来の対応付けを推測するものではなく、入金と出金の対応付けを一定のルールで「みなす」ものであり、紛争時の法的解釈などの用途が考えられている[332]。

(iii) ベンダヒアリングの結果

ブロックチェーン分析／解析ツールを提供しているベンダ 7 社へヒアリングを行っ

331 Anderson, R., et al, Department of Computer Science and Technology, University of Cambridge, "The Taint Chain", https://www.cl.cam.ac.uk/~is410/taintchain/, 2019/2/1
332 Andy Greenberg, Wired.jp, "盗まれたビットコインを追跡するヒントは、200 年前の「事件」に隠されていた", https://wired.jp/2018/07/12/a-new-way-to-trace-stolen-bitcoins/, 2019/2/1

た結果を以下に記載する[333]。

AML/CFT 対策の取組に関して、総じて、本人確認（Know Your Customer、以下 KYC）だけでは不十分であり、ある会社によればトランザクションレベルでの確認（Know Your Transaction、以下 KYT）が必要との見解が示された。また追跡ツールは組み合せる手段の一つに過ぎず、実際の追跡においては様々な他のツールや情報源と組み合せることの重要性が力説された。ある会社によれば最も重要なのは取引所が行っている KYC であり、追跡ツールは補完的な位置づけにあたるとの見解が示された。当該企業は、アドレスグラフにおけるアドレス間の距離と属性情報に基づいてグラフ理論等を用いてリスクスコアの推測を行っているが、属性情報の紐付けやリスクスコアの推測の前提となる、仮説を前提としたアドレス群の名寄せにはやや限界があるとのことであった。

属性情報（リスクスコア）の紐付けにあたっての必要な情報の収集手段については、第三者機関からの提供を受ける、ダークウェブを含むウェブクローリングを行う、情報収集をアウトソーシングする、といった回答がみられた。また、反社データが極めて重要であることから、今回ヒアリングを行った多くの企業が海外当局と密に連携していると回答した。ある会社からは国際的な反社データベース構築に向けた取組の重要性が力説された。

なお、ある会社の仮想通貨のリスクスコアリングツールを用いて、、仮想通貨取引所「Zaif」から流出したビットコインの一時流出先アドレス等を確認したところ（詳細は 3.7.3.2 節「第一段階（暗号資産流出）」を参照）、いずれもニュートラル（不正の恐れ無し）の評価であった。当該ベンダへ本事件について情報提供を行ったところ、一時流出先アドレスはスコアが反映され、極めてリスクが高いと評価されるようになったものの、それ以外のアドレスについては依然としてニュートラルの評価のままであった。このことからも、現在利用可能な再識別技術の限界を推察することができる。

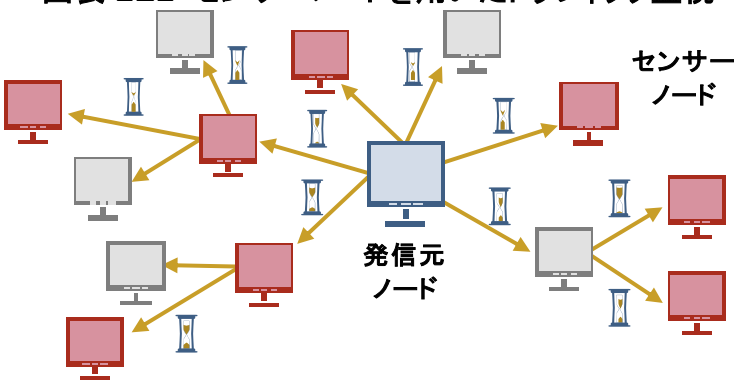
3.6.2.1.4 ブロックチェーン上の発信元に関する再識別技術

ブロックチェーンネットワークでは各ノードが P2P で相互に接続しており、トランザクション情報を受信したノードは送信元ノードの IP アドレスを把握することができる。そのためネットワーク上のトラフィックを監視するセンサーノードを多数用意して、トラン

333 ブロックチェーン分析／解析ツールを開発している Chainanalysis 社は中国の取引所 Binance との連携を公表するなど、今後多くの仮想通貨取引所がこれらのベンダのツールを活用することが予想される。Insights, "Chainalysis Partners with Binance to Tackle Global Cryptocurrency Money Laundering", https://blog.chainalysis.com/reports/chainalysis-binance, 2018/11/19

ザクションの伝播経路を推測することで、トランザクション発信元ノードの IP アドレスを推測することができる[324]（図表 121）。

図表 121 センサーノードを用いたトラフィック監視



センサーノードを用いたトラフィック監視の方針は以下の通りとなる[334]。

- トランザクション発信元ノードからのブロードキャストを直接（1ホップで）受信できるよう、地理的に分散させたセンサーノードを大量に用意する。ここで、センサーノードは、多くのノードからの接続を受けるように設定し、その分処理能力も持たせる。また、トランザクションを受信した時刻が重要となるため、センサーノード間でマシン時刻を十分同期しておく。

- それぞれのセンサーノードで受信したトランザクションの時刻を時系列解析し、対象となるトランザクションを最初に受信したセンサーノードを特定し、その接続元ノードを特定する。ここで、トランザクションはランダムな時間を経て発信されるため、発信元の特定には待機時間を考慮したデータ分析が必要となる。

2012 年 6 月から 11 月までの 5 カ月間、平均して約 2,500 のビットコインノードを監視し、アドレスに対する IP アドレスの紐付けを行っている研究もある[335]。紐付けにあたり以下の条件付き確率を計算することで、候補となりうる IP アドレスの絞り込みを行っている（図表 122）。

(1) 各トランザクションに対して、経由した中継ノードの IP アドレスのうち一番始めの IP アドレスをみつけ、トランザクションの送金元／送金先アドレスと当該 IP アドレスのペア（アドレスに紐付く IP アドレスの候補）を作成する。

---

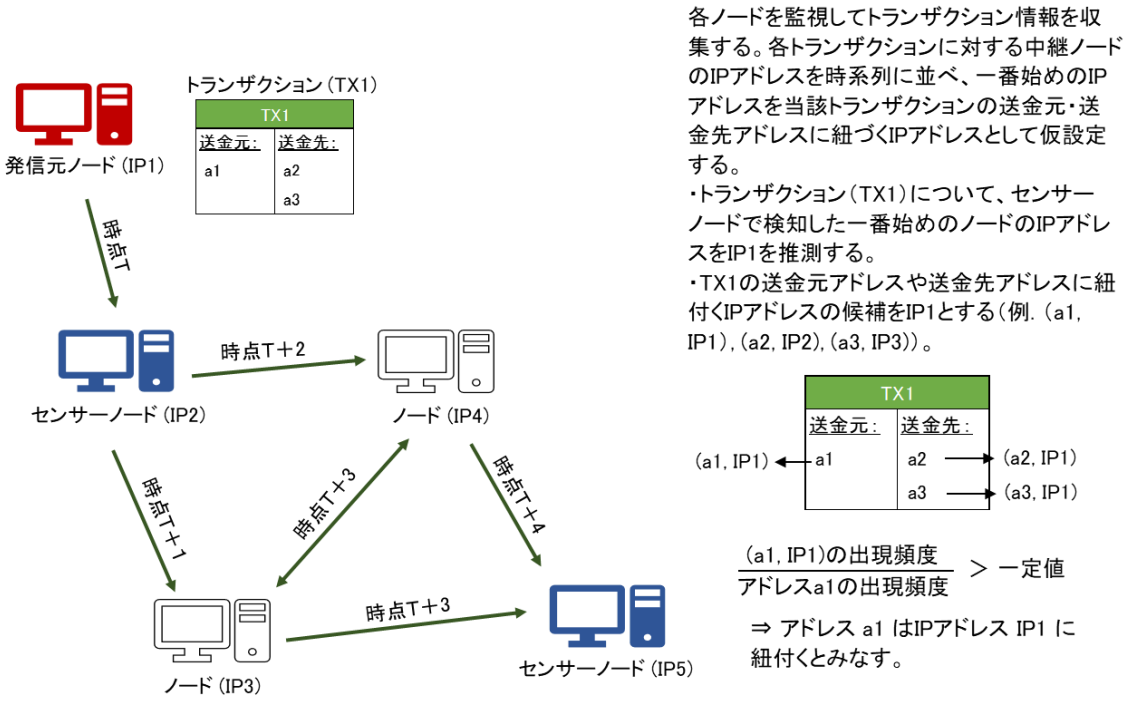
334 実際の事例は以下を参照のこと。ASCII.jp ウェブサイト, "Zaif 不正出金事件の犯人追跡につながる証拠、JDD やエルプラスが特定", http://ascii.jp/elem/000/001/767/1767194/index-2.html, 2018/12/7

335 Koshy, P., et al., "An analysis of anonymity in bitcoin using p2p network traffic", https://pdfs.semanticscholar.org/c277/62257f068fdbb2ad34e8f787d8af13fac7d1.pdf, 2018/12/21

(2) トラフィック監視中におけるアドレスの出現頻度を分母、アドレスと IP アドレスのペアの出現頻度を分子として、アドレスに対して当該 IP アドレスが紐付く条件付き確率を計算する。

(3) 条件付き確率の値が一定以上であれば、当該アドレスには当該 IP アドレスが紐付くとみなす。

図表 122 アドレスに対する IP アドレスの紐付け方法



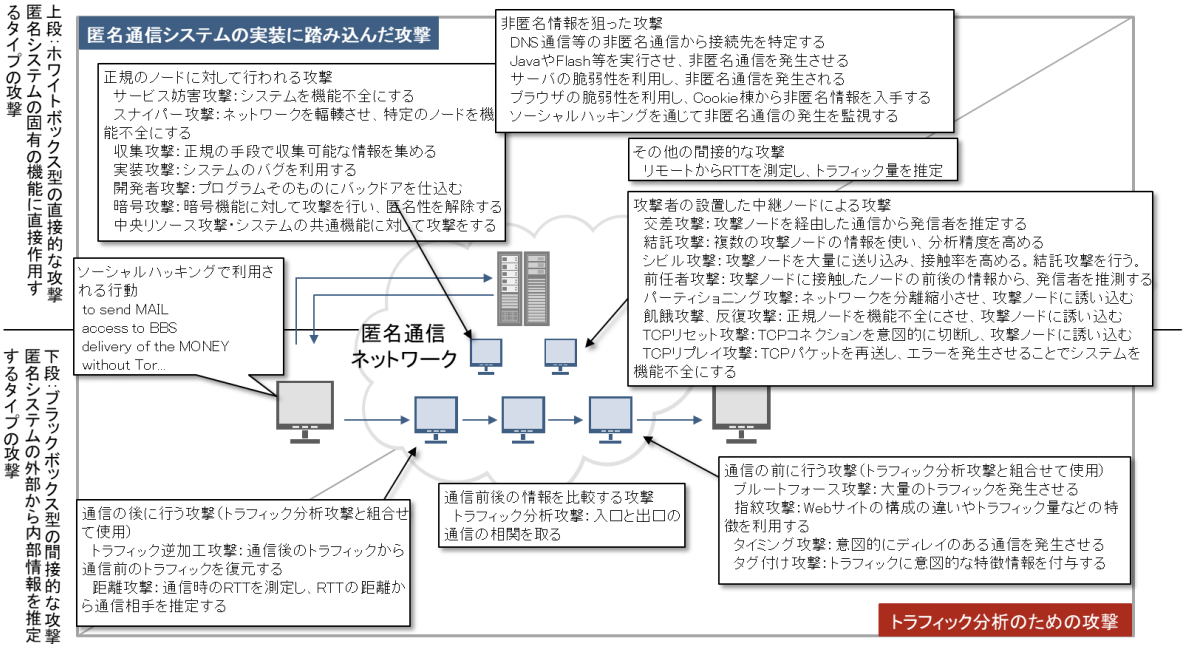
3.6.2.2 P2P レイヤー/インターネットレイヤー

本節では P2P レイヤー/インターネットレイヤーにおける再識別技術について記載する。

Tor などの匿名通信技術の再識別（非匿名化）に焦点を当てた攻撃手法等については様々な研究が行われている[292]。たとえば、匿名通信技術によって構築されたネットワーク上のトラフィックを統計的に解析することにより、データが伝送される経路や送信者と受信者のつながりを特定する方法などが提案されている。Tor におけるトラフィックを解析するために、Entry Guard Router と Exit Router の両方のトラフィックを観測し、Entry Guard Router と Exit Router のアクセス日時とデータのサイズを突き合わせることでアクセスログから統計的にマッチングさせ特定する方法（Collusion Attack）や、応答のトラフィックに識別情報を付与して送信者を絞り込む方法（Tagging Attack）、逆に受信者の応答を固有の指紋（Fingerprint）情報として蓄積

し、受信者を推定する方法（Fingerprint　Attack）などが研究されている。主な攻撃手法（再識別手法）は図表 123 の通りである。

図表 123 匿名通信手法に対する攻撃手法（再識別手法）の目的別分類 [292]



3.6.2.3 実世界レイヤー

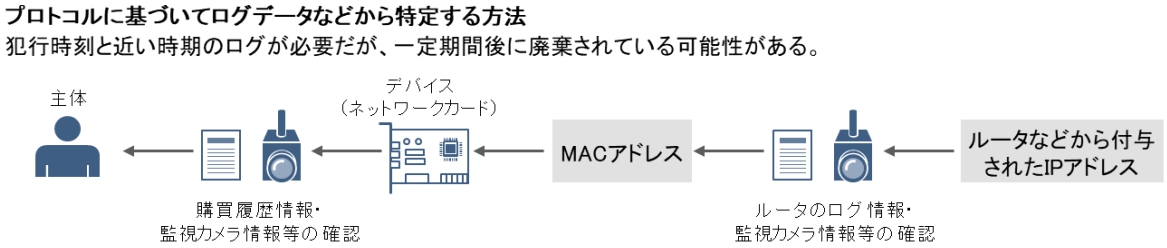
本節では実世界レイヤーにおける再識別技術について記載する。

追跡対象の IP アドレスが配分されている組織体が特定できており、かつ当該組織体が内部ネットワークを構築しているのであれば、まず①プライベート IP アドレスの特定が必要となる[336]。次に、②プライベート IP アドレスから ARP（Address Resolution Protocol）ログ等を参照して MAC アドレス（物理アドレス）を特定し、③当該 MAC アドレスからデバイスを特定し、④最終的にデバイスを所有する主体を特定する流れとなる（図表 124）。

ここで、②の IP アドレスから MAC アドレスを特定する際には、（IP アドレスと MAC アドレスの紐付けは任意に変更可能であるため）追跡対象の通信が行われた時刻の ARP ログが当該組織体によって保存されていることが必要である。

336 組織体の内部ネットワークで使用可能（内部ネットワーク内でのみ一意）な IP アドレスのことである。組織体の外部ネットワークに接続する際にはプロキシサーバや NAT（Network Address Translation）等を使用してプライベート IP アドレスを IP アドレス（グローバル IP アドレス）に変換した上で通信を行う。

図表 124 実世界レイヤーにおける再識別のイメージ



3.6.3 外部 DB に基づく再識別

本節では、外部のデータベースに基づく追跡技術について記載する。用いる情報の出所ごとに、アプリケーションレイヤーの情報を用いた追跡と、P2P レイヤー/インターネットレイヤーの情報を用いた追跡に分けて記載する。

3.6.3.1 アプリケーションレイヤーの情報を用いた追跡

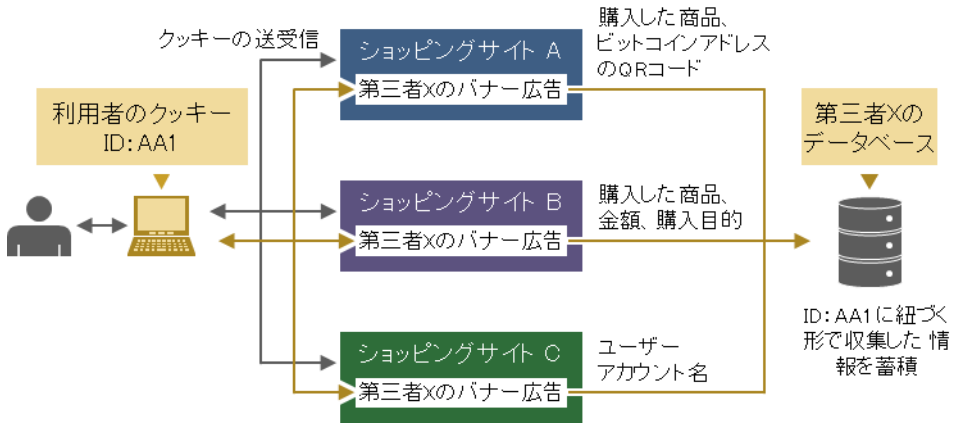
3.6.3.1.1 クッキー情報の活用

ビットコイン決済の可能なショッピングサイトの、バナー広告等から収集したクッキーを用いたアドレスの名寄せに関する研究がある[337]。

クッキーを用いた情報収集の流れを記載する（図表 125）。ショッピングサイト A にバナー広告等を掲載している第三者 X は、ID により識別可能なクッキーをショッピングサイト A の閲覧者に送信し、同時に当該サイトでの商品購入に関する情報を自身のサーバに蓄積する。同じ閲覧者が別のショッピングサイト B に訪れた際に、そのサイトにも第三者 X のバナー広告等が掲載されていれば、第三者 X はクッキーの ID により閲覧者が同一であることを識別し、ショッピングサイト A で収集した情報とショッピングサイト B で収集した情報は同一閲覧者のものと紐付けて蓄積することができる。このように複数のショッピングサイトにバナー広告等を掲載することで、それぞれのサイトにおける閲覧者の商品購入に関する情報を紐付けることができる。

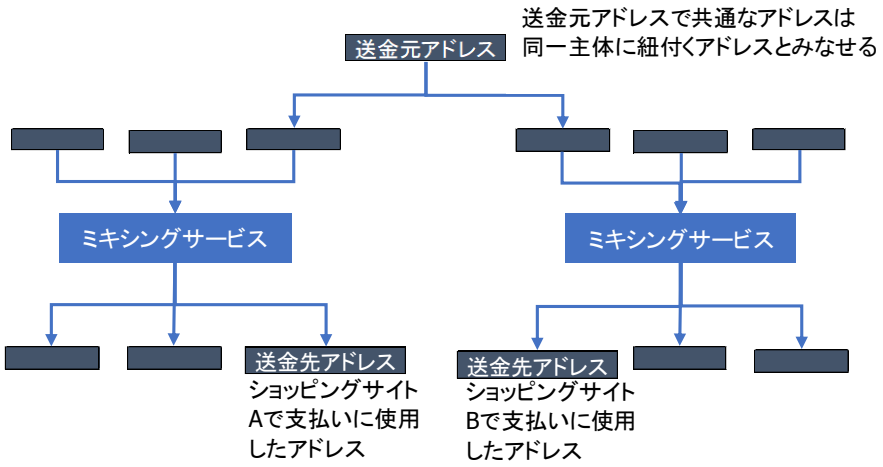
337 Goldfeder, S., et al., "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies", https://arxiv.org/pdf/1708.04748.pdf, 2019/1/7

図表 125 クッキーを用いた情報収集



こうしたクッキーなどの外部情報は、アドレスの名寄せにあたって重要な情報となる。例えば、たとえミキシングサービスが使用された後のアドレスであっても、クッキーなどの情報を使うことで、共通の送金元アドレスを検出できる可能性がある（図表126）。ただし、共通な送金元アドレスの検索対象は、送金の度に、指数関数的に増大する点には留意が必要である。

図表 126 クッキーを活用したアドレスの名寄せのイメージ



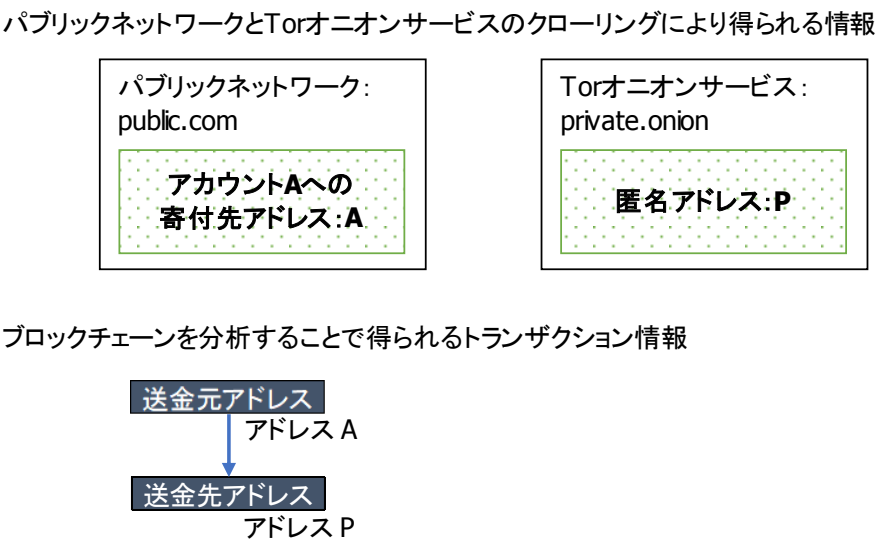
3.6.3.1.2 SNS 情報の活用

SNS 上のアカウント情報を再識別に活用する研究もなされている[338]。これはアドレスと主体を直接的に紐付けるものではないが、少なくともその紐付けにあたって役立つ可能性がある。基本的な考え方を図表 127 に示す。まず、パブリックネットワークと Tor オニオンサービスをクローリングして、アドレス A はアカウント A に紐付くことと、

338 Jawaheri, H., et al., "When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis", https://arxiv.org/pdf/1801.07501.pdf, 2019/1/7

アドレス P は private.onion に紐付くことがわかる。次に、ブロックチェーンを分析することで、アドレス A からアドレス P へ送金がされていることがわかる。以上を組み合わせると、private.onion とアカウント A を、何らかの関連があるものとして紐付けることができる。

図表 127 SNS 情報を活用した非匿名化のイメージ



当該論文では、Tor オニオンサービス上の 1,500 サイト、暗号資産の情報が集まる掲示板である Bitcoin Forum 上の 100 万ページ、ツイッター上の 50 億ツイートをクローリングしてそれぞれ 88 個、41,000 個、4,200 個のユニークなビットコインアドレスを収集し、ブロックチェーンデータを分析することで 125 ユーザを Tor オニオンサービス上の 20 サイトに紐付けることができたと報告している。

3.6.3.2 P2P レイヤー/インターネットレイヤーの情報を用いた追跡

3.6.3.2.1 レジストリデータを用いた追跡

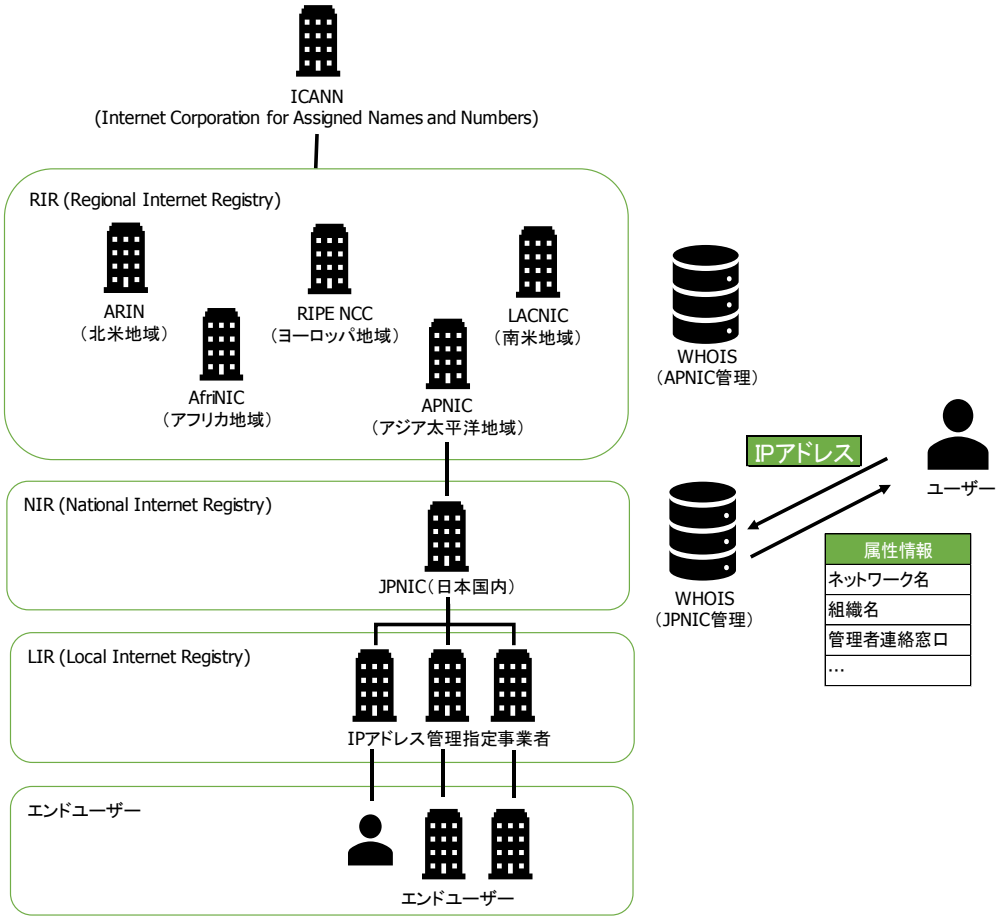
IP アドレスは Internet Corporation for Assigned Names and Numbers（以下 ICANN）によって全世界的に管理されており、地域インターネットレジストリ（Regional Internet Registry、以下 RIR）や国別インターネットレジストリ（National Internet Registry、以下 NIR）が地域ごとに IP アドレスの割り当てを行っている[339]。日本国内においては、アジア太平洋地域の RIR である Asia Pacific Network Information Centre（以下 APNIC）または、日本の NIR である日本ネットワークインフォメーション

339 RIR は北米地域（ARIN）、ヨーロッパ地域（RIPE NCC）、アジア太平洋地域（APNIC）、南米地域（LACNIC）、アフリカ地域（AfriNIC）で構成されている。

センター（Japan Network Information Center、以下 JPNIC）が IP アドレス管理指定事業者に対して IP アドレスの割り当てを行っている（図表 128）。

RIR や NIR は自身が管理する IP アドレスやドメインの情報を提供するサービスである WHOIS[35] を運営しており、各 IP アドレスがどの組織体に割り当てられているかを確認することができる（図表 129）。しかしながら、RIR や NIR への情報登録に関する正式なルールはなく、情報の抜け漏れがある、最新の情報が反映されていないといった問題は発生し得る。

図表 128 IP アドレス管理体制と WHOIS のイメージ



図表 129 実世界レイヤーにおける再識別のイメージ

3.6.3.2.2 ジオロケーションを用いた追跡

インターネットに接続している端末の地理的な位置情報の推定を行うジオロケーションについては、以下の 2 つの方法に分類できる。

- 端末依存型

  端末の GPS 情報や Wi-Fi 接続時の三点測量により位置情報を推定する（特定の精度は数 10 メートルと言われている）。

- 端末非依存型

  端末や接続方式に依存せずに位置情報を推定する（都市レベルでの精度でも低いと言われている）。

追跡を行う場合は、そもそも追跡対象の端末は分からないため、上記の中では端末非依存型のジオロケーションを行うことに該当する。ジオロケーションには RIR や NIR の提供する WHOIS データベースの使用や、ドメイン名からの位置情報の類推、ユーザからのフィードバックされる情報の利用といった方法がとられるが[340]、レジストリデータの場合と同様、データの精度や更新度といった点で課題が存在している

3.6.4 課題と今後の見通し

追跡技術やツールを俯瞰してみると、ブロックチェーンを用いた暗号資産取引の再識別にあたっては、利用可能なデータや効率性、精度の観点からは、アプリケーションレイヤー（ブロックチェーン）における再識別を中心に考えることが有効と考えられる。これは、①取引所の KYC 情報や各種 SNS 情報などを用いて、ブロックチェーン上のアドレスを主体に直接紐付ける方法が最も確度が高いこと（それ以外は基本的には「推測」に留まる）、②過去のサイバー事件のその後の経緯を見る限り、IP アドレスが得られたとしても、そこから主体を特定するのが困難と考えられること（推測の難しさやデータの不備等により、P2P レイヤー/インターネットレイヤーや実世界レイヤーでの再識別が困難であること）、③暗号資産取引はインターネット以外の方法でも可能であり、その場合アプリケーションレイヤーの情報を活用した再識別が益々重要になること、などからである。たとえば、ビットコイン取引は衛星通信[341]や短波ラジオ[342]

340 Komosny, D., et al., "Location Accuracy of Commercial IP Address Geolocation Databases", http://itc.ktu.lt/index.php/ITC/article/viewFile/14451/9010, 2019/1/7
341 Blockstream, "Blockstream Satellite", https://blockstream.com/satellite/, 2019/3/18
342 Szabo, N., et al, Scaling Bitcoin, "Weak-Signal Radio Communications for Bitcoin Network Resilience",

などを用いることでも可能であり、この場合、発信元の特定はインターネットの場合よりも、さらに困難になる可能性がある。

ブロックチェーン上における再識別技術やツールについては、総じて学術的な有効性評価は本稿執筆時点ではなされておらず、各種ベンダによるブロックチェーン分析／解析ツールの開発・提供が先行しているというのが現状である。すなわち、アドレス群の名寄せにかかる各種仮説についてコンセンサスは得られておらず、また属性情報の付与やリスクスコアの推測はあくまでも確率的な推測であるため、推測結果は用いるアルゴリズムやデータの質や量に大きく依存する。アルゴリズムの開発は今後も進展していくと思われるが、より重要なことは各社個別に進めている反社データの共有といったデータの質や量の向上であると考える。

しかしながら、プライバシー保護に関する意識の高まりとともに、企業側は IP アドレスやクッキーの収集や長期間の保持を避ける傾向にある。仮想通貨取引所「Coincheck」の事件において犯行に用いられたと思われる海外の複数のサーバで通信記録が既に廃棄されていたという事象[343]も発生している。プライバシー保護は再識別とトレードオフの関係にあるため、再識別にあたっての障害となる可能性がある。

このような状況下においても、米国国土安全保障省における匿名通貨の追跡技術確立に向けた取り組み[344]や EU における暗号資産追跡ツールの研究に対する資金提供[345]といった取り組みが各国で行われている。また、Zcash といったプライバシー保護の強化を目的とした暗号資産では、監査人などの利用を想定している「閲覧キー」という仕組みも提供されており、当局にとっても開発コミュニティにとっても、プライバシー保護と再識別のバランス感が今後益々重要になると考えられる。

---

https://stanford2017.scalingbitcoin.org/files/Day2/Weak-Signal-Radio-Communications-for-Bitcoin-Network-Resilience.pdf, 2019/3/6

343 産経新聞ウェブサイト, "【衝撃事件の核心】流出NEM事件、発生から半年 海外サーバー経由で不正通信指示 通信記録欠損で犯人特定は高いハードル",
https://www.sankei.com/premium/news/180801/prm1808010002-n3.html, 2018/12/12

344 coindesk, "US Government Interested in Tracking Privacy Coins, New Document Shows",
https://www.coindesk.com/us-homeland-security-is-interested-in-tracking-privacy-coins, 2018/12/11

345 coindesk, "EU Commits €5 Million to Fund Blockchain Surveillance Research",
https://www.coindesk.com/eu-commits-e5-million-fund-blockchain-surveillance-research, 2018/12/19

3.7 実際に発生した暗号資産追跡事例の調査

3.7.1 概要

本節では、3.2 節「ブロックチェーン要素技術にかかる調査」から 3.5 節「その他の匿名技術にかかる調査」までで調査対象とした技術を組合せた具体的なユースケースとして、実際に発生した暗号資産追跡事例について情報収集を行い、技術面・制度面から評価を行う。

ここで、専門家等の意見を踏まえ、仮想通貨取引所「Coincheck」（事業主体はコインチェック株式会社）及び「Zaif」（事業主体はテックビューロ株式会社）における暗号資産追跡事件を調査対象事例とした。

図表 130 に示すように、各調査対象事例を段階別に分けて全体像を整理した上で、各段階に関する情報収集を実施した。ここで、本調査研究の趣旨および一次情報の取得可否等を鑑み、第二段階・第三段階に特に比重を置いた。

図表 130 各調査対象事例の全体像と調査内容

段階	具体的な内容	調査内容
第一段階（暗号資産流出）	犯行者が被害者（仮想通貨取引所等）から不正に秘密鍵を取得し、直接ないし一つ以上の仮想通貨取引所等を経由して、被害者のアドレスから犯行者のアドレスへ送金する。	秘密鍵流出の経緯、等 （一次情報は取得できないため、二次情報の整理に留まる）
第二段階（暗号資産転売）	犯行者が買い手（一次バイヤー）と何らかの手段で売買交渉を行い、直接ないし一つ以上の仮想通貨取引所等を経由して、自身のアドレスから一次バイヤーのアドレスへ当該通貨を送金する。 ※一次バイヤーは犯行者へ異なる暗号資産を送金する。	バイヤーとの交渉手段／交渉方法、異なる暗号資産ネットワークを跨いだ交換方法、等
第三段階（暗号資産拡散）	一次バイヤーが、直接ないし一つ以上の仮想通貨取引所等を経由して、二次バイヤーへと送金し、こうした取引が繰り返される。	仮想通貨取引所等を用いた資金洗浄方法、等

3.7.2 仮想通貨取引所「Coincheck」における暗号資産追跡事例

3.7.2.1 経緯概要

コインチェック株式会社が運営する仮想通貨取引所「Coincheck」に対して、2018 年 1 月 26 日に、同社が管理する顧客資産である 526,300,010 XEM（当時のレート

で約 580 億円）が不正に外部へ流出する事件が発生した[346]。不正流出額は XEM 総発行量（8,999,999,999XEM）の約 5.8%に相当し、被害者は約 26 万人にも及び[347]、社会的に大きな注目を集めた。

当該事例は大きく、①犯行者がコインチェック社の管理するアドレスから自身のアドレスへ XEM を送金、②犯行者がダークウェブ上の簡易サイト等で第三者（以下、バイヤー）と売買交渉を行い、自身のアドレスからバイヤーのアドレスへ XEM を送金、③バイヤーが複数の仮想通貨取引所を経由して XEM を拡散、という三フェーズに分けられる（図表 131）。

この間、②から③にかけて、犯行者が不正に取得した XEM を他の暗号資産へ換金することを防ぐために、NEM 財団[348]関係者および有志により、不正流出された XEM を持つアドレスへ独自のモザイクを送付して、不正な資金と識別できるようにして当該 XEM を追跡する試みが行われた。

図表 131 主な時系列の推移[349]

No	発生日時		事象
1	2018/1/26	00:02 頃	コインチェック社のアドレスからの不正流出開始
2	2018/1/26	08:26 頃	コインチェック社のアドレスからの不正流出終了
3	2018/1/26	11:25 頃	コインチェック社が異常を検知
4	2018/1/26	12:07 頃	コインチェック社が NEM の入金一時停止について告知、以降、売買及び出金を順次一時停止
5	2018/1/26		コインチェック社が NEM 財団や他の仮想通貨取引所に対して追跡および売買停止要請
6	2018/1/26	17:23 頃	コインチェック社がビットコイン以外の売買の一時停止について告知
7	2018/1/26	17:40 頃	有志によりモザイク送付が開始

346 暗号資産基盤 NEM の基軸通貨。NEM では任意のアセットを発行できる機能があり、各アセットは、「ネームスペース」（インターネットのドメイン名相当）毎の「モザイク」として定義される。XEM はネームスペース NEM のモザイクとして定義されている。nemproject, GitHub, "NEM NIS API Documentation", https://nemproject.github.io/, 2019/1/7

347 コインチェック株式会社, "仮想通貨 NEM の不正送金に関するご報告と対応について", https://corporate.coincheck.com/2018/03/08/46.html, 2018/11/12

348 NEM 財団（NEM.io Foundation）は、NEM ブロックチェーン技術の振興、産官学への普及促進を目的として、非営利団体である保証有限会社（companies limited by guarantee）としてシンガポールで 2016 年に設立された。crunchbase, "NEM.io Foundation Ltd.", https://www.crunchbase.com/organization/nem-io-foundation-ltd, 2019/1/7

349 ダークウェブ上の交換サイトによる通貨交換量は以下のサイトによる。
読売新聞ウェブサイト, "コインチェック流出NEM、ダークウェブで4割販売済み", https://www.yomiuri.co.jp/science/goshinjyutsu/20180308-OYT8T50016.html, 2019/1/7
日本経済新聞ウェブサイト, "流出 NEM、財団が追跡停止 6 割超が他通貨に", https://www.nikkei.com/article/DGXMZO28377570Q8A320C1EA2000/, 2019/1/7

8	2018/1/26　23:30 頃	コインチェック社により記者会見が行われる
9	2018/1/27　03:57 頃	NEM 財団関係者がツイッターにて 24-48 時間内に追跡システムを構築すると発言
10	2018/1/28	コインチェック社が不正送金された仮想通貨 NEM 保有者に対する補償方針について告知
11	2018/2/1	NEM 財団がリアルタイムで追跡中であることを発表
12	2018/2/6	犯行者がダークウェブ上に通貨交換サイトを構築
13	2018/2/7　00:12 頃	犯行者がダークウェブ上の交換サイトの URL をメッセージに伏して告知
14	～	ダークウェブ上の交換サイトを通した通貨交換が活発化（2018/3/6 で約 38%との報道）
15	2018/3/20	NEM 財団が追跡を停止したことを発表
16	～	未換金であった残り約 40%の通貨交換が急速に進む
17	2018/3/22	犯行者がダークウェブ上の販売サイトで全ての資金の交換が完了したことを告知

3.7.2.2 第一段階（暗号資産流出）

コインチェック社の管理するアドレス（以下、流出元アドレス NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ）から犯行者の管理するアドレス（以下、一次流出先アドレス NC4C6PSUW5CLTDT5SXAGJD QJGZNESKFK5MCN77OG）への不正送金について、NEM ブロックチェーン上では計 11 回のトランザクションにより不正送金が行われたことが把握できる[350]（図表 132）。

図表 132 NEM ブロックチェーン上の不正流出の記録[351]

No	時刻	送金額（XEM）	手数料（XEM）	送信元アドレス	送信先アドレス
1	2018/1/26 0:02	10	0.05	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
2	2018/1/26 0:04	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
3	2018/1/26 0:06	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
4	2018/1/26 0:07	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
5	2018/1/26 0:08	100,000,000	1.25	NC3BI3DNM 流出元アドレス KVA5CSZ	NC4C6 一次流出先アドレス 7OG
6	2018/1/26 0:09	100,000,000	1.25	NC3BI3DNM KVA5CSZ	NC4C6 7OG
7	2018/1/26 0:10	20,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
8	2018/1/26 0:21	3,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
9	2018/1/26 3:35	1,500,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
10	2018/1/26 4:33	1,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
11	2018/1/26 8:26	800,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG

不正送金の理由として、以下の見解がコインチェック社より公表されている[347]。

350 piyolog, HatenaBlog, "Coincheck で発生した暗号通貨 XEM の不正送金事案についてまとめてみた", http://d.hatena.ne.jp/Kango/20180126/1517012654, 2019/1/7

351 以降、断りの無い限り、以下のサイトのデータを用いた。nemchina, "NEM - BlockChain Explorer", http://explorer.nemchina.com/, 2019/1/7

- 攻撃者が、コインチェック社従業員の端末にマルウェアを感染させ、当該従業員の端末経由で外部ネットワークから社内ネットワークに不正にアクセス。
- 遠隔操作ツールを用いて、社内の NEM サーバの通信を傍受することにより秘密鍵を窃取。ここで、秘密鍵はホットウォレットで管理されており、マルチシグは使われていなかった。
- 窃取した NEM の秘密鍵を使用して外部に NEM を不正に送金。

3.7.2.2.1 第一段階（暗号資産流出）にかかる考察

暗号資産不正流出を招いた主な要因としては以下の四点が挙げられる（図表 133）。

図表 133 不正流出を招いた主な要因

No	要因
1	外部からの不正アクセスを招き、それが検知されていなかったこと
2	秘密鍵が暗号化されない状態で、社内ネットワーク上で送受信されていたこと
3	マルチシグやコールドウォレットが運用されていなかったこと
4	アドレスが取引毎に分けられていなかったこと

- No1「外部からの不正アクセス」については、XEM 流出前に、コインチェック社外から複数回不審な接続があったこと[352]や、コインチェック社内から社外へ通信が発生していたこと[353]などが報道されている。
- No2「通信内容の秘匿化」については、上記コインチェック社の見解（通信傍受により秘密鍵が窃取されたこと）による。
- No3「マルチシグ[354]やコールドウォレット[355]の未使用」については、内外の多くの報道が指摘するところである[356]。他方で、NEM のマルチシグではビットコイ

352 日本経済新聞ウェブサイト, "流出前に複数回の不審接続 コインチェック", https://www.nikkei.com/article/DGXMZO26621390X00C18A2CC1000/, 2019/1/7
353 日本経済新聞ウェブサイト, "NEM 流出以前に社内から欧米へ不審な通信 コインチェック", https://www.nikkei.com/article/DGXMZO27433360X20C18A2CC0000/, 2019/1/7
354 送金する際に必要な秘密鍵を複数に指定すること。仮に秘密鍵が一つ犯行者へ窃取されても（全ての秘密鍵が犯行者へ窃取されない限り）、資金は移動されない。
355 インターネットから切り離されたオフライン環境下で秘密鍵を管理すること。一般的には秘密鍵を印刷物として運用するペーパーウォレットや、専用ハードウェア端末で運用するハードウェアウォレットが用いられる。
356 楠正憲, Yahoo! Japan ニュース, "コインチェックからの NEM 流出、なぜ安全対策が遅れたのか", https://news.yahoo.co.jp/byline/kusunokimasanori/20180128-00080965/, 2019/1/7
Youtube, "Coincheck 500M Hack Interview with Jeff McDonald, NEM VP",

ンなどの他の暗号資産と異なる電子署名方式を用いていることや[357]、NEM でのコールドウォレットの運用が技術的に難度が高いことなども指摘されている[358]。

- No4「少数アドレスによる運用」について、秘密鍵が窃取された流出元アドレスは、2017 年 6 月より半年以上に渡り使い続けられており、不正流出開始時点においては、累計で約 5.3 万回のトランザクションに用いられ、約 460 億円の残高を保持していた[359,360,361]（図表 134）。

図表 134 流出元アドレスの利用状況（不正流出直前）

不正流出直前までの利用状況	累積入金額	累積出金額	総利用回数/残高
利用回数（トランザクション数）	10,201	43,035	53,236
XEM	916,227,982	389,879,123	526,348,858
円（88.549 円/XEM）	¥81,131,071,534	¥34,523,406,497	¥46,607,665,038

以上より、コインチェック社の取引所運営体制は、不正流出防止の観点からは極めて脆弱であったと考えられる。

なお、不正流出事件を受けてコインチェック社は 2018 年 1 月 26 日深夜に記者会見を行ったが、コインチェック社および犯行者が秘密鍵を有する流出元アドレスは、記者会見の翌日以降も、計 100 回弱のトランザクションに利用されていた（図表 135）。

図表 135 流出元アドレスの利用状況（2018 年 1 月 27 日以降）

記者会見後の利用状況	累積入金額	累積出金額	総利用回数/残高
利用回数（トランザクション数）	90	7	97
XEM	45,682	40,884	4,798
円（88.549 円/XEM）	¥4,045,117	¥3,620,238	¥424,879

https://www.youtube.com/watch?v=kAN0C3__5qU&feature=youtu.be, 2019/1/7

357 nem developer center, "Multisig Account", https://nemtech.github.io/concepts/multisig-account.html, 2019/1/7

358 杉井 靖典, facebook, https://www.facebook.com/yasunori.sugii/posts/1826225380785828, 2019/1/7

359 当該アドレスを含むトランザクションデータの出典元は kengos/incoming.csv、outgoing.csv。 kengos, GitHub, https://gist.github.com/kengos/763db655d49d4329fafcd115a1e02204#file-outgoing-csv, 2019/1/7

360 以降、XEM のレートはコインチェック社の補填額 88.549 円/XEM を用いた。コインチェック社ウェブサイト, "不正に送金された仮想通貨 NEM の保有者に対する補償方針について", https://corporate.coincheck.com/2018/01/28/30.html, 2019/1/7

361 NEM ではコンセンサスアルゴリズム Proof of Importance を用いている関係上、手数料収入が期待できるため、特定のアドレスに多くの資金を集めるインセンティブが存在したことも理由として挙げられる。

3.7.2.3 第二段階（暗号資産転売）

犯行者は流出元アドレスから一次流出先アドレスへの不正送金を行っている間に、不正に得た XEM の約 99.4%（523,000,000XEM）を計 8 個の他のアドレス（以降、二次流出先アドレス）へ移動させた（図表 136）。

図表 136 一次流出先アドレスからの資産移動の動き

No	時刻	送金額（XEM）	手数料（XEM）	送信元アドレス	送信先アドレス
1	2018/1/26 2:57	30000000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NCTWFIOOVITRZYSYIGQ3PEI3IMVB25KMED53EWFQ
2	2018/1/26 2:58	50,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NA7SZ75KF6ZKK267TRKCJDJBWP5JKIC2HA5PXCKW
3	2018/1/26 3:00	50,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	[illegible]
4	2018/1/26 3:02	750,000	1.25	NC4C6	7OG
5	2018/1/26 3:14	100,000,000	1.25	NC4C6	7OG
6	2018/1/26 3:18	100,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NB4QJJCLTZWVFWRFBKEMFOONOZFDH3V5IDK3G524
7	2018/1/26 3:28	100000000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NDDZVF32WB3LWRNG3IVGHCOCAZWENCNRGEZJVCJI
8	2018/1/26 3:29	92,250,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NA6JSWNF24Y7DVIUVPKRNAY7TPOFJJ7G2URL7KU5

一次流出先アドレス

主要な二次流出先アドレス

3.7.2.3.1 NEM の取引レート

2018 年 1 月 26 日以降、NEM のレートは右肩下がりの動きを続け、不正流出事件が発生した後 2018 年 3 月末までに時価総額（ドル建）で約 76.6%下落した（図表 137、2018 年 1 月 26 日朝 9 時時点の時価総額約 85 億ドルに対し、2018 年 3 月 31 日朝 9 時時点の時価総額約 19 億ドル）。

図表 137 NEM の時価総額、ドルレート、ビットコインレートの推移[362]

362 CoinMarketCap, coinmarketcap.com, "NEM Chart", https://coinmarketcap.com/ja/currencies/nem/, 2019/1/7

3.7.2.3.2 アドレスへのマーキングによる追跡

2018 年 1 月 26 日 17:23 頃から、有志により一次流出先アドレスへモザイクを送付し、不正な資金と識別できるようにして当該 XEM を追跡する試みが開始された。これは当該 XEM の受信先に対して他通貨への換金を防ぐよう働きかけることを狙いとする。

図表 138 一次流出先アドレスへ送付されたモザイクの例[363]

項目	値
時刻	2018/1/26 17:23
送金額(XEM)	0
手数料(XEM)	0.2
送信元アドレス	NCVGXTCV7YYGCUTOWRSEALEVHVTDFRJ54BQYDKTI
送信先アドレス	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
モザイク	mizunashi.coincheck_stolen_funds_do_not_accept_trades.owner_of_this_account_is_hacker
送金額(モザイク)	1
手数料に用いるモザイク	mizunashi.coincheck_stolen_funds_do_not_accept_trades.levy_to_lock_assets
手数料(モザイク)	1
メッセージ	return the stolen funds to coincheck!

モザイクを作成する際には任意のモザイクを手数料として指定することができる。図表 138 に示す通り、追跡に用いたモザイク(以下、追跡モザイク、"mizunashi.coincheck_stolen_funds_do_not_accept_trades.owner_of_this_account_is_hacker")の手数料として、別なモザイク(以下、追跡手数料モザイク、"mizunashi.coincheck_stolen_funds_do_ not_accept_trades. levy_to_lock_assets")が指定されており、かつ、この追跡手数料モザイクを発行者(mizunashi)が全て保持し外部へ送付しないことにより、追跡モザイクが他へ送付されないようにしていた。

この取組は、他の有志も含めて行われ、最終的に NEM 財団によって行われた[364]と推察される。

3.7.2.3.3 犯行者とバイヤーのやり取り

NEM ではトランザクションに任意のメッセージを含めることができる。そのため、暗

363 NemProject, "Nembex V.3.2", http://chain.nem.ninja/#/transfer/090ab3288381bbb8f5b6da160fddbd58313ffae010e82361dc080abf569971ab, 2019/1/7

364 NEM 財団のものと思われるモザイク「ts:warning_dont_accept_stolen_funds」は 2018/2/5 02:14 頃から 2018/3/20 6:56 頃にかけて計 4,324 回送付された。

号資産流出が一般に認知されるにつれ、メッセージが付された多くのトランザクションが一次流出先アドレスへ送付された（図表 139）。

図表 139 一次流出先アドレスへ送付されたメッセージ[365]

時刻	送金額（XEM）	手数料（XEM）	送信者	受信者	メッセージ
2018/1/27 2:23	1	0.2	NCVGXTCV7YYGCUTOWRSEALEVHVTDFRJ54BQYDKTI	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Return the stolen funds to Coincheck!
2018/1/27 3:06	1	0.1	NCMKWNFWUILEVCKBSON2MS65BXU4NJ2GBJTIJBTK	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	What's happened?
2018/1/27 3:46	0	2	NBXA6FYUETSRB5FXTXGLULQOEVFNOEPE7N4HATAR	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	What makes you so that.
2018/1/27 5:27	0	0.2	NAZASOSA2DPAR5SRA3SNHUKBUZZGCDWYYWB6IFAY	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	(暗号化されています)
2018/1/27 12:41	0	0.7	NAUFIPHWAAFJWLE5C33WW36SI5BVDV32ODLFDFBK	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	(暗号化されています)
2018/1/28 2:24	1	0.25	NCJQZIGJLMVPCOZAUUSI7V7BJ6MOGO2TTZCQFPHC	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Instead of sending the trendy coin named...
2018/1/28 7:04	0	0.25	NAUFIPHWAAFJWLE5C33WW36SI5BVDV32ODLFDFBK	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	(暗号化されています)
2018/1/28 9:21	1	0.3	NBKCVZ2BU3D5XLUZD4BAI2EVIXE3MRYKEVINPWYQ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	You are the best guy that do the gamblin...
2018/1/28 10:27	1	0.7	NBY32IX3KZOPTVVAOVIP5TLWJZDQNTZ5HZ3L3NU3	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	:-) cemana kau rasa, lek...?
2018/1/29 21:25	1	0.4	NCGLWE2SVA5DP2X4TO7JBOM65PRIFZZPSPSHDGU4	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	do you know serendipity
2018/1/31 8:57	0	0.1	NBRVXOPYI2HZLBJ5I5ZTGH5M5UE42HBYZWPXGBDY	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Hello it's
2018/1/31 9:43	0	0.1	NCK7YZRXXX3ZCTFO4P4VDMHZMIR6TCLYG2S5YFYS	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	☺
2018/1/31 9:51	0	0.1	NBMCIU2LZPJA43OI6IRCD6HBYA46V32RV7JCPCMR	N	hero, give me 777777 xem plz :)
2018/1/31 9:57	0	0.15	NCK7YZRXXX3ZCTFO4P4VDMHZMIR6TCLYG2S5YFYS	N	I can help you. Please give me 100000XEM
2018/1/31 10:03	0	0.15	NC2LYYGHZQS54JEOGHH7PDMOWYVFLI3EBRMV4B52	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	wasu wasu wasu wasu bitconeeeeect!!!!
2018/1/31 10:06	1	0.1	NB4EHRVZ7JTZMYRYLMLZ47ABYZHKIBN5E4OLQHSR	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Hey, give me 250,000 XEM
2018/1/31 10:11	1	0.1	NDRVDLKWPK2M43AA6KFGCG6FSAJRZAE2GQZJSLFK	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Hi!
2018/1/31 10:14	1	0.1	NAL7Z3525F5GOSSUF7OB6EVEBBLDFG4M3C2F47TS	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	buy visio now!!!
2018/1/31 10:19	0	0.15	NBKHVCJVHNEJ6OZ2B22XV6MRTOSWXWW42EKC72LR	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Return my 100,000 xem Please :'-(
2018/1/31 10:22	0	0.15	NB3J2AGW3YCTE2F66HDC6WGGRFCOBFQQCQS63EX6	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Hello, Please kindly give me 1,000,000 X...
2018/1/31 10:23	0	0.1	NADZ7IEHY3PXFEXNIS7EH62GT5PILTW2CGHX34UZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Please return my NEM. Help me.
2018/1/31 10:24	0	0.15	NAAOWOJB7AKB47PI7UPB5VYC7OSIQMQVVEJLEOQN	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	KANE KAESE YO! if you give me your XEM, ...
2018/1/31 10:25	0	0.1	NDP6D4NPSE62RZBGAYLVQ7FXAPELNZ5ZKFHNNF6N	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	日本語読めますか？
2018/1/31 10:26	0	0.15	ND5SVCAJDRNZK37N3LGWRMTYVSSSQ4RIPAMDVQN4	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Give me a little bit of your XEM. Thank...
2018/1/31 10:29	9	0.15	NADRWU6XUJB6HO33B4N4KASQMWGLGXYJB2ANPCZP	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Please give me 10000XEM (^_-)-☆
2018/1/31 10:33	0	0.15	NCGKSSO3GKVMLN3LX4HLIPE2BPYX26UWEI7LZPNN	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	send me 1 million XEM or else I will be ...
2018/1/31 10:38	0	0.1	NAXEYMPVUO5BKGBK5NG7SIC3Y5AMBLSQ34E4J5MN	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	gj!
2018/1/31 10:41	1	2	Cryptopia NBQ73BYLVGMO7L2WFG2VVO1HOBWWJKW7D3V7UE4E	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	114514
2018/2/1 10:47	1	0.1	NCZRLPFCBEBR4WX6PY363G4WB44CRUY264KH6BEN	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	give me many xem!!!
2018/2/1 10:50	1	0.1	NBDZ6HUOSWAWW3G6T2SS2RTEYBH4FSMGLC64JDVN	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	Can I separate your xem??
2018/2/1 10:53	1	0.1	ND6QOYBLEWJN66AIDJEKUBPFTYJCS7HDZ2YSQTY7	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	please give me xem!!!
2018/2/1 10:54	0	0.1	NAOUTRRHE52MSRRXTRYDDDJ7QMXBACTDVUDAGUF6	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	please!!!
2018/2/1 10:54	1	0.1	NATRWR7ECC4IXQ2XLMWIRHEUHQCKGIUUSTZKTMOD	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	please borrow your xem
2018/2/1 10:55	1	0.1	NAW7OCQUXQM5SDKS7QCJV7BLCIGGKSSP7TFPWRO5	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	can I share your many xem?
2018/2/1 10:59	1	0.1	NDR6P7B2CLFVCLV6LYEYQOMVH56T7RQDNYD5ZMGH	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	give me!!please help!!!!
2018/2/1 11:00	0	0.15	NCPJLCHBFERHICPECSFE23LEKA3QRNWLWOS24LE2	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	I' m very hunger .please give me a money
2018/2/1 11:29	15	0.15	Huobi NDABPHWFPH7KL5FADCW66V4GYLVXHKYQIPWL4G2B	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG

一次流出先アドレス

メッセージは不正流出後、当初は犯行を称えるものや XEM を送付して欲しいと懇願するものが多かったが、徐々に暗号化したものや[366]、Dash などのアドレス等、他の暗号資産との交換を示唆するものが増えてくる。多くの報道にある通り、図表 140 に示すメッセージが交換を示唆するメッセージとして代表的なものと考えられる。

---

365 以下の cheena 氏と思われるサイトよりメッセージのあるトランザクションを抜粋したもの。"CoincheckMate Blockchain Explorer", https://coincheckmate.com/explorer/#NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG, 2019/1/7

366 NEM では、送信者と受信者で共通鍵暗号方式を用いてメッセージを暗号化することが可能である。暗号化・復号化にあたっては、送信者の秘密鍵＋受信者の公開鍵、送信者の公開鍵＋受信者の秘密鍵が用いられる。nem.io, "NEM Technical Reference Version1.2.1", https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf, 2019/1/7

図表 140 バイヤーから犯行者へのメッセージ[367]

項目	値
時刻	2018/2/2 19:04
送金額(XEM)	0
手数料(XEM)	1.15
送信元アドレス	NDUO6J6H253GULLVXJU66CIEYQYBOWU5DOYUZMZF
送信先アドレス	NC4C6PSUW5CL 一次流出先アドレス MCN77OG
メッセージ	こんにちは。すみませんお詫びがあります。。匿名ネットワークで取引所を経由している最中に、メッセージを暗号化して送ってしまい、着金に送れが発生してしまいました。少し時間がかかるかもしれません。。ただ洗浄のルートは確立できましたので、次回からはスムーズに行えるかと思います。取り急ぎ、DASH の送金確認をするために、こちらのアドレス(Xr6maJSptxgD6NRBRqnv4YwsqoJvhLc7iB)へ、0.01DASH をお送りしました。着金が出来ているかのご確認をお願いします。 txid:e6e8d429afa99b6708e187a3899460a05074ed2090e5d6516cd5a2695160b8df

他方、犯行者は 2018 年 1 月 26 日以降、100XEM などの少額の送金を断続的に繰り返していたが、2018 年 2 月 6 日までに不正に得た XEM を他の通貨と交換するサイトを Tor でアクセス可能なダークウェブ上に開設し、2018 年 2 月 7 日早朝から他のアドレスへ当該サイト(http://rfselcyqemtp3wgu.onion)の告知を始めた(図表 141)。

図表 141 ダークウェブ上の交換サイトを告知するメッセージの記録[368]

項目	値
時刻	2018/2/7 0:12
送金額(XEM)	0.1
手数料(XEM)	1.15
送信元アドレス	NDZZJBH6JZPY 二次流出先アドレス HOYTQGXR53HAW
送信先アドレス	NADZ7IEHY3PXFEXNIS7EH62GT5PILTW2CGHX34UZ
メッセージ	http://rfselcyqemtp3wgu.onion XEM -15% OFF

ダークウェブ上の交換サイトは、XEM をビットコインもしくはライトコインと交換することを意図しており、ページ下段に示されたレートは適宜更新される[369](図表 142)。ランディングページにて、入金先となる自身の NEM アドレスを入力すると、次のペー

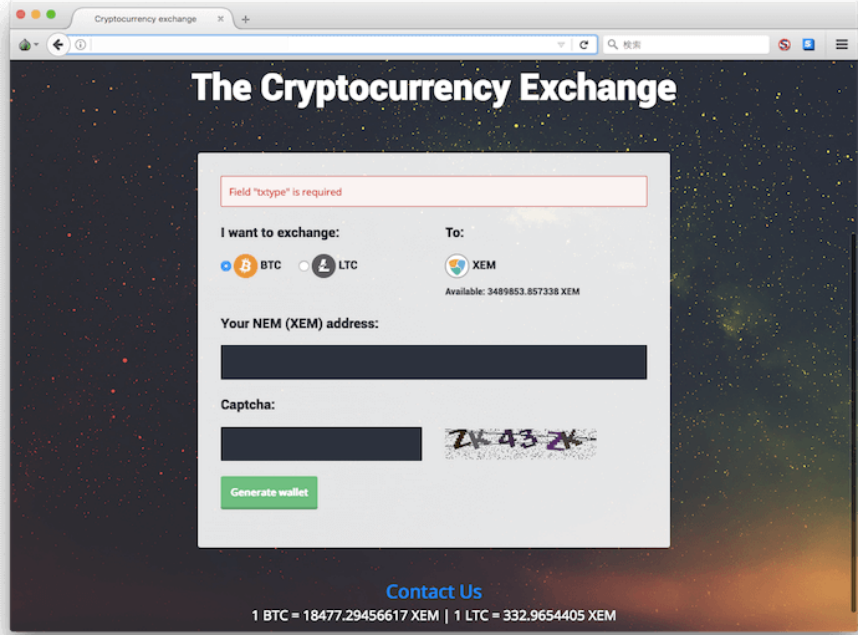
367 犯行者が日本語話者との報道がなされる要因ともなったが、一切暗号化されていない点が不自然とも指摘される。nemchina, "NEM - BlockChain Explorer", http://explorer.nemchina.com/#/s_tx?hash=dd50841ba593359383475b056ffa0c6547799a8b21bc4e0d869caec5697332ad, 2019/1/7

368 nemchina, "NEM - BlockChain Explorer", http://explorer.nemchina.com/#/s_tx?hash=e572825c74905f255f864696e82e666d18d185c994534d77f694b5c53befb248, 2019/1/7

369 一般の仮想通貨取引所でのレートよりも 15-16%前後割安となっていた。

ジにて、犯行者が管理するビットコインもしくはライトコインの入金先アドレスが表示される。そして、バイヤーが犯行者のビットコイン／ライトコインのアドレスへ入金すると、1 ブロックが生成された後に、犯行者からバイヤーのアドレスへ、レートに則った NEM が送金されたと報道されている。

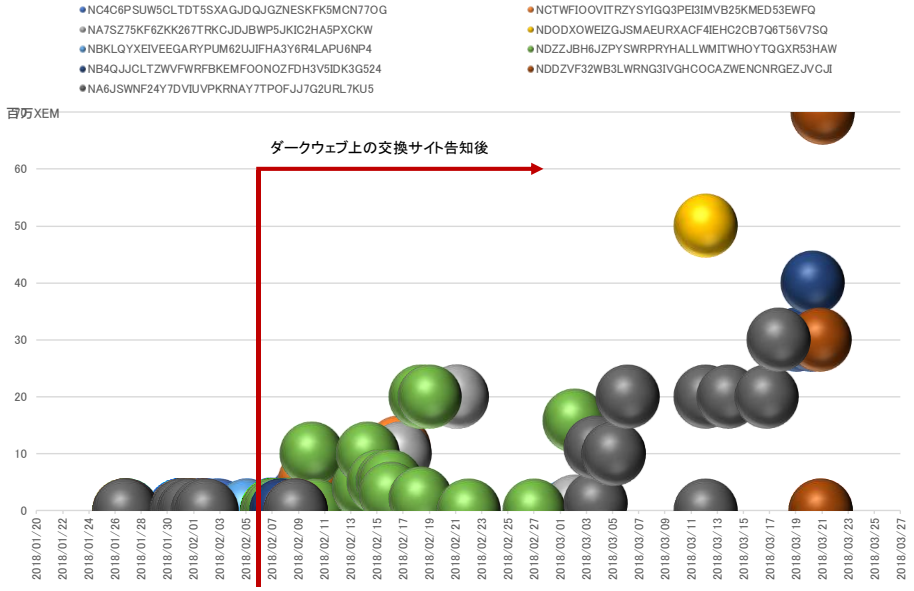
図表 142 ダークウェブ上の交換サイトの画面イメージ[370]



ダークウェブ上の交換サイト開設に合わせて、犯行者の管理する一次流出先アドレスおよび主要な二次流出先アドレスからの他のアドレスへの送金も活発化したことが NEM ブロックチェーン上のデータからも分かる（図表 143）。

370 ビットコイン新聞編集部, ビットコイン新聞, "【悲報】ハッキングされた仮想通貨 NEM が今でもダークウェブで購入できる状態に！？", https://bitcoin-shinbun.com/wp-content/uploads/2018/02/hacking-nem-darkweb-washing01.1.png, 2018/12/14

図表 143 一次流出先アドレスおよび主要な二次流出先アドレスからの出金状況[371]



3.7.2.3.4 第二段階(暗号資産転売)にかかる考察

暗号資産の転売が行われた主な要因として、犯行者とバイヤーとの間でのマッチング、価格形成、決済、資金洗浄、追跡の在り方の五点について考察する(図表144)。

図表 144 暗号資産の転売が行われた主な要因

No	要因	要因
1	マッチング	・ブロックチェーン上の情報により、**犯行者の連絡先が一般に広く周知されていたこと**
2	価格形成	**・バイヤーにとって有利な条件であったこと**(また、有利であることが他の取引所のレート等から確認可能であったこと)
3	決済	**・犯行者が信頼のある行動をとったこと** ・犯行者が換金の必要に迫られていたことが周知されていたこと ・犯行者が 1 コンファメーションでの確認というリスクを取ったこと
4	資金洗浄	**・規制の緩い取引所を経由することでマーキングを避ける資金洗浄ルートがバイヤーに把握されたこと** ・コインチェック社への制裁が中心となる一方で、資金洗浄行為に対する当局からの目立った介入がなかったこと
5	追跡の在り方	・追跡がボランティアベースで行われるものであり、追跡する側のメリットがなかったこと ・ネームスペースを借りる際および都度モザイクを送付する度に、追跡を行う側にコストがかかったこと

- 「マッチング」においては、不正流出後暫くは NEM のトランザクションに付されたメッセージ(オンチェーン)がその役割を担ったが、やがてダークウェブ上の

371 nemchina, "NEM - BlockChain Explorer", http://explorer.nemchina.com/より三菱総研作成。

販売サイト（オフチェーン）へ移ったと考えられる（図表 145）。

ここで、ブロックチェーン上の情報が一般に広く公開されていることが、犯行者の連絡先を多くのバイヤーへ周知するのに役立ったと考えられる。すなわち、犯行者が管理する一次流出先アドレスや二次流出先アドレス、ダークウェブ上の交換サイトともに、各種のブロックチェーンエクスプローラーで簡単に確認することが可能であり、犯行者への連絡先が一般に広く周知されていた状態にあったと考えられる。

図表 145 犯行者とバイヤーのマッチング・価格形成手段

利用時期	種別	媒体	マッチング	価格形成
2018/1/27～ 2018/2/7 前後	オンチェーン	NEM トランザクションに付されたメッセージ	犯行者の NEM アドレスはバイヤーにとって既知	相対でのやり取り
2018/2/7 前後～	オフチェーン	ダークウェブ上の交換サイト等	犯行者の交換サイトの URL はバイヤーにとって既知	基本的には、犯行者側からの掲示のみ

- 「価格形成」においては、ダークウェブ上の交換サイトの表示などから、バイヤーにとって有利な条件（市場レートから 15%前後割安）で XEM の交換が行われたことが推察される。

公開サイトで掲示されるレートは、他の取引所と比較して割安であったことが各種報道で確認されており、割安であることが実際に確認可能であったこともバイヤーが取引を行うインセンティブを促したと考えられる。

- 「決済」においては、双方が暗号資産を送金しあうという極めてプリミティブな手法が用いられたが、本事件においては上手く機能したと考えられる。

暗号資産の交換は「まずバイヤーが先に送金し、それを受けて、犯行者が送金する」というステップがとられた。ここでは、犯行者が持ち逃げせずに正しく送金するか否かが取引成立にあたってのポイントとなる。また、バイヤーにとっては、何ブロック生成後に犯行者が送金するかも利便性の点でポイントとなる。

ここで、犯行者は換金の必要性に迫られていることが広く周知されていた。そのため、犯行者が持ち逃げをした場合、バイヤーからの信頼を失い、他の取引が行えなくなるデメリットが容易に推察されていた。また、犯行者が（フォークのリスクを負って）1 ブロックの生成をもって取引成立とみなすとダークウェブ上で

告知したことも周知されていた[372]。

そのため、実際に交換サイトを通して取引に成功したとのバイヤーからの報告が増え、バイヤーにとって安全であり有利な取引であることが広まるにつれ、犯行者への信頼が増し[373]、更に多くのバイヤーが取引を行うインセンティブを生じさせたと考えられる。

- 「資金洗浄」においては、不正流出が発生してからダークウェブ上の交換サイトが開設されるまでの間に、有志によって、資金洗浄のルート、すなわち仮想通貨取引所へ XEM を移動することによりモザイクによるマーキングがなされないことが把握されていたと推察される（詳細は後述）。

  他方、この間、一名に事情聴取を行った以外は、当局の目立った介入が大々的に報道されず[374]、このこともバイヤーにとって安心感を深める要因となったと考えられる。

- 「追跡の在り方」においては、モザイクによる追跡が持続可能なものではなかったことが挙げられる。

  追跡する側はボランティアベースで、何らの経済的メリットもなく追跡を行うのみで、さらにマーキングに用いるモザイクを作成する際およびモザイクを送付する度にコストがかかっていた。

3.7.2.4 第三段階（暗号資産流出）

ダークウェブ上の交換サイトが開設されるまでに、バイヤーは仮想通貨取引所へ入金することで、モザイクによるマーキングがなされないことを把握していたと推察される。図表 146 は、ダークウェブで実際に取引が成立したとツイッター等で報告されたアドレスの動きを示している[375]。犯行者が管理すると考えられる一次流出先アドレ

372 ブロックチェーンは長い（ビットコインの場合、正確には累積の難易度が最大の）チェーンが正として選択される。正とされるチェーンが変わり得る（すなわち取引の事実が事後的に変わり得る）ため、ある取引を含むブロックが生成されて以降、一般的には、6 ブロック程度チェーンが変わらないことをもって、当該取引がなされたとみなす。
373 バイヤーが取引所へ送金せず、誤って犯行者へ送り返してしまい、犯行者が律儀に再度送金する事例なども指摘されている。piyolog, HatenaBlog, "Coincheck 不正送金に関連する一部のウォレットを調べてみた", http://d.hatena.ne.jp/Kango/20180209, 2019/1/7
374 毎日新聞ウェブサイト, "暗号資産流出 ネム交換の日本人男性聴取 闇ウェブ介し", https://mainichi.jp/articles/20180211/k00/00m/040/150000c, 2019/1/7
375 単眼愛（モノアイ）@mono_i_love, Twitter, https://twitter.com/mono_i_love/status/961783799234289664, 2019/1/7

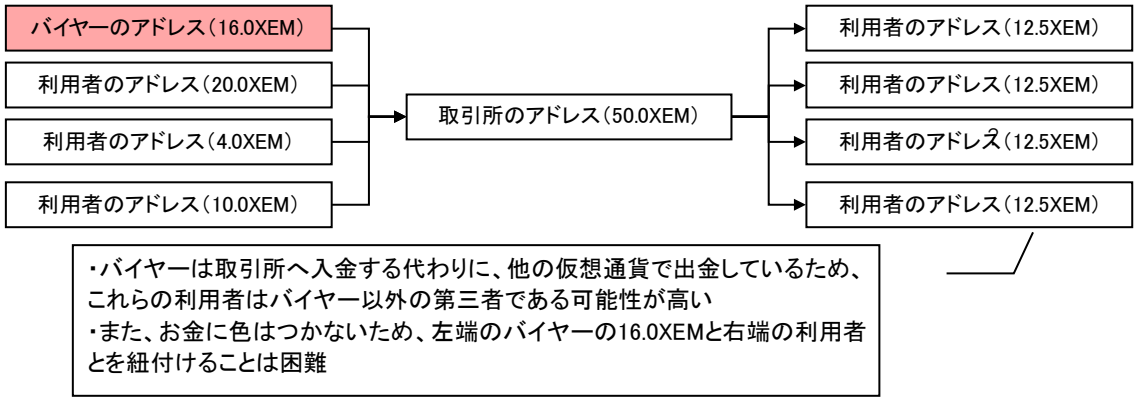
スおよび二次流出先アドレス、またバイヤーが管理すると考えられる三次流出先アドレスまではモザイクによるマーキングがなされているが、取引所（Livecoin と指摘される[376]）が管理すると考えられる四次流出先アドレスへはマーキングがなされていないことが分かる。

図表 146 取引所への送金の動き（括弧の中は推察される所有者）

No	時刻	送金額（XEM）	手数料（XEM）	送信元アドレス	送信先アドレス	モザイク送付時刻	モザイク
1	2018/2/6 22:20	5000	0.05	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG 一次流出先アドレス（犯行者）	NA6OMO3K2NXTVXUWH7UIM4KRXSVHNKA4DEYCSV4H 二次流出先アドレス（犯行者）	2018/2/7 17:32	ts:warning_dont_accept_stolen_funds
2	2018/2/6 22:38	50,000	0.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG 一次流出先アドレス（犯行者）	NA6OMO3K2NXTVXUWH7UIM4KRXSVHNKA4DEYCSV4H 二次流出先アドレス（犯行者）	2018/2/7 17:32	ts:warning_dont_accept_stolen_funds
3	2018/2/7 13:22	16.9	0.05	NA6OMO3K2NXTVXUWH7UIM4KRXSVHNKA4DEYCSV4H 二次流出先アドレス（犯行者）	ND5HFPODSWCQKLGNEEFTY6RWASME5O3YRHVF7TSR 三次流出先アドレス（バイヤー）	2018/2/7 20:14	ts:warning_dont_accept_stolen_funds
4	2018/2/7 20:09	16.0	0.1	ND 三次流出先アドレス（バイヤー）	四次流出先アドレス（取引所）		

コインチェックと同じく、一つのアドレスを複数の入金や出金に用いる取引所は、実質的にミキシングの役割を果たしており、また入金者と出金者は一般には無関係であると考えられる（図表 147）。NEM 財団等は、他の無関係な NEM ユーザが嫌疑を被らないように、取引所に入った XEM の追跡は止めたことが推察される。

図表 147 取引所の管理するアドレスを経た入出金のイメージ



実際に、Livecoin 管理下と指摘されている当該四次流出先アドレスは、2017 年 9 月 27 日より使い続けられており、2018 年 2 月 7 日 20:09 頃の取引の前までに累計 4,203 回のトランザクションに利用されていた[377]（図表 148、当該取引後も、2018 年 10 月 28 日 06:27 頃までに、計 6,788 回のトランザクションに用いられている）。そのため、当該四次流出先アドレスには、バイヤー以外にも、多くの利用者が関わっ

376 Nemermind, "NEM public agents stats", http://nemermind.be/nempublic.html, 2019/1/7
377 nemchina, "NEM - BlockChain Explorer", http://explorer.nemchina.com/#/s_account?account=NDKIDQOVCGN463JUSAUJ3YKGLVVLSZV3ZKA46JQC, 2019/1/7

ていたことが伺える。

図表 148 Livecoin とされるアドレスの利用状況（三次流出先アドレスからの資産移動直前の状況）[378]

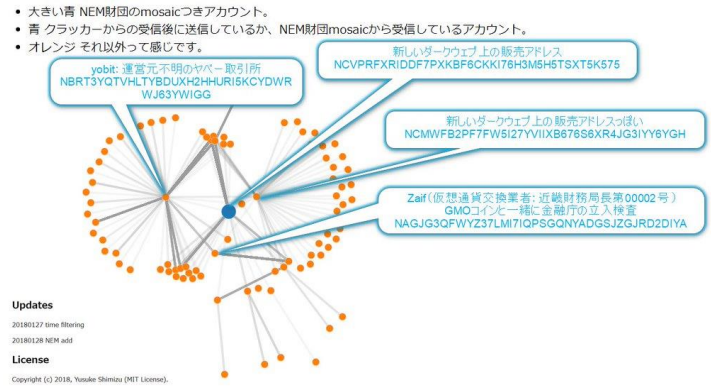
三次流出先アドレスからの資産移動直前	累積入金額	累積出金額	総利用回数/残高
利用回数（トランザクション数）	1,886	2,362	4,248
XEM	4,849,660	3,682,062	1,167,599
円（88.549 円/XEM）	¥429,432,570	¥326,042,888	¥103,389,681

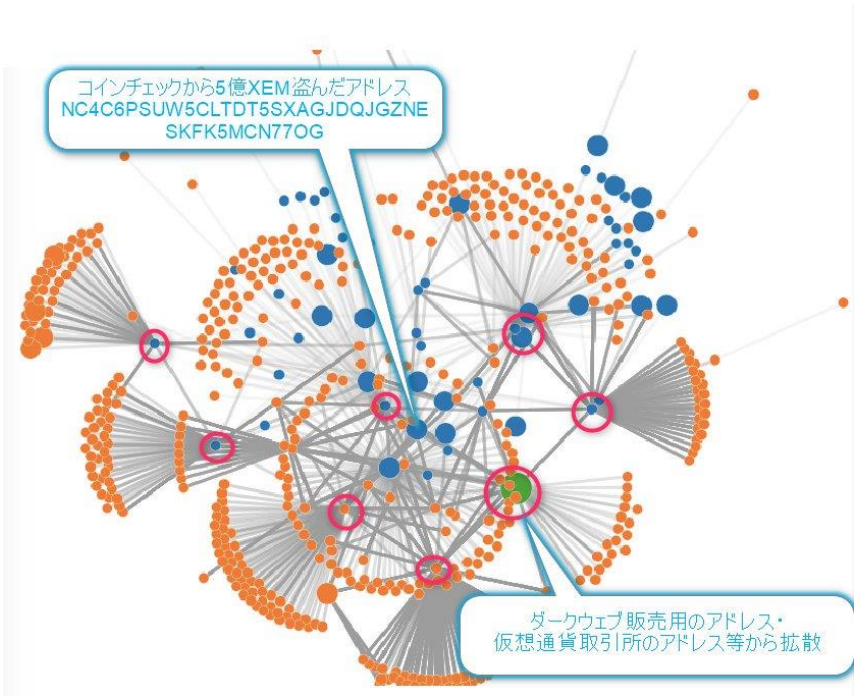
資金洗浄で用いられた仮想通貨取引所としては「HitBTC」、「Yobit」、「Livecoin」[379]や仮想通貨決済代行業者「Coinpayments」等を経由した上で「Zaif」に送金されたことなどが報道されている[380]。実際にこれらの取引所において、ビットコイン・NEM 間の取引が増加したことも指摘されており、例えば「Zaif」では 3 月中旬に取引量が急増している（図表 149）。ダークウェブ上の交換サイトで得た NEM が、様々な交換所等を経由した上で、ビットコイン等に換金されていた可能性が推察される（図表 150）。

図表 149 仮想通貨取引所 Zaif での XEM/BTC の取引量の推移[381]

378 うち 45 回は自身のアドレスから自身のアドレスへの送金となっているため、送金回数／入金額／総金額ともその分重複している。
379 tracker-ournem, "2/7 HitBTC, Yobit, Livecoin へ送金 コインチェックから盗まれた XEM のゆくえ", http://tracker-ournem.hatenablog.com/entry/2018/02/07/073151, 2019/1/7
380 読売新聞ウェブサイト, "コインチェック流出NEM、ダークウェブで4割販売済み", https://www.yomiuri.co.jp/science/goshinjyutsu/20180308-OYT8T50016.html, 2019/1/7
381 Fisco Cryptocurrency Exchange Inc., TradingView, "XEM/BTC", https://www.tradingview.com/x/tCxhLxDA, 2019/1/10

図表 150 取引アドレスの拡散の推移（上、下の順に推移）[382]

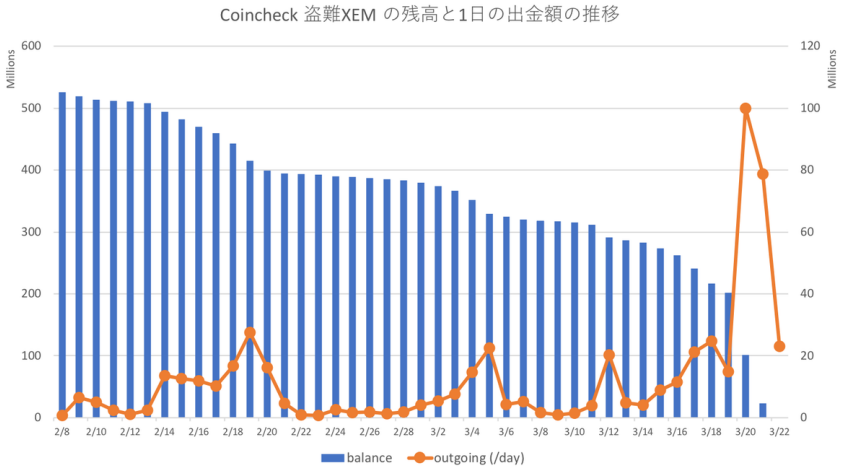




2018 年 3 月 20 日に NEM 財団が追跡を停止したことを公表すると、未換金額約 40%が速やかにバイヤーに転売され、犯行者は不正流出額の全額をバイヤーに転売することに成功したと報道されている（図表 151）。実際に、図表 151 では、NEM 財団が追跡を停止した 2018 年 3 月 20 日以後に、犯行者の残高が急激に減少している。

382 上：単眼愛（モノアイ）@mono_i_love, Twitter, https://pbs.twimg.com/media/DVmuKpYV4AEDt__.jpg, 2019/1/7
下：単眼愛（モノアイ）@mono_i_love, Twitter, https://pbs.twimg.com/media/DWZBnsKVQAAeE-F.jpg, 2019/1/6

図表 151 ダークウェブ上の交換サイトで示されていた残高の推移[383]



3.7.2.4.1 第三段階（暗号資産拡散）にかかる考察

本事件で実施されたマーキングによる追跡は、そのモザイク名（ts:warning_dont_accept_stolen_funds）が示す通り、取引所等での換金を防ぐためのものであった。そのため、取引所や仮想通貨決済代行業者等が当該 XEM を受け入れてしまった時点で追跡の試みは失敗したといえる[384]。

2018 年 3 月 6 日時点で流出額の約 38%が換金済みとの報道もあり[380]、ダークウェブ上の交換サイト開設以降、追跡する側は有効な手立てがないまま、換金を抑え込めない状況に至っていたと考えられる。

今後、犯行者に送金されたビットコインやライトコインから犯行者が特定される可能性が考えられる。ただし、（当局から自身に嫌疑をかけられる可能性があるため）バイヤーが犯行者との取引で用いたアドレスを公開することは考えにくく、他方で犯行者も危険性は十分承知していることから、犯行者が特定される可能性は低いことが予想される[385,386]。

---

383 Masafumi Negishi@MasafumiNegishi, Twitter, https://pbs.twimg.com/media/DY4sd86VwAAgVuf.png, 2019/1/10

384 ただし「Livecoin」も、2018 年 2 月 20 日時点で、誤ってモザイクが付与されてしまったユーザが入金することができないと訴えている事例がある（muhammet_emin, Nem Forum, "Koineks tag problem", https://forum.nem.io/t/koineks-tag-problem-solved/14320, 2019/1/7）。そのため、当初はモザイクが付与されたトランザクションも受け入れていたが、途中から受け入れないように対応方針が変わったことが推察される。

385 暗号資産追跡ツールを提供している会社によると、ビットコイン上のアドレスは数個に特定されており、今後取引所へ入る場合に備えて監視を行っているとのこと。取引所で行う本人確認などにより、今後何らかの形で犯行者が特定される可能性も考えられる。

386 事件から約一年後に犯行者が海外の取引所で換金を図る内容が報道された。産経新聞ウェブサイト, "流出仮想通貨、現金化の動き　海外交換所に持ち込み", https://www.sankei.com/affairs/news/190122/afr1901220004-n1.html, 2019/1/23

3.7.3 仮想通貨取引所「Zaif」における暗号資産追跡事例

3.7.3.1 経緯概要

テックビューロ株式会社が運営する仮想通貨取引所「Zaif」に対して、2018 年 9 月 14 日に、同社が管理する自社資産および顧客資産合わせて約 70 億円（うち顧客資産約 45 億円）が不正に外部へ流出する事件が発生した（図表 152）。

図表 152 仮想通貨取引所 Zaif の不正流出額[387]

種類	レート（2018/9/18 の終値ベース）	不正流出額			
		仮想通貨量	円	うち顧客資産	
				仮想通貨量	円
ビットコイン	（712,565 円/BTC）	5,966.1	4,251,234,047	2,723.4	1,940,662,281
ビットコインキャッシュ	（49,795 円/BCH）	42,327.1	2,107,677,945	40,360.0	2,009,729,689
モナコイン	（107.7 円/MONA）	6,236,810.1	671,704,448	5,911,859.3	636,707,257
合計			7,030,616,439		4,587,099,227

2018 年 1 月の仮想通貨取引所「Coincheck」の暗号資産不正流出事件に続く、大手仮想通貨取引所における不正流出事件として、社会的に大きな注目を集めた。

当該事例は大きく、①犯行者がテックビューロ社の管理するアドレスから自身のアドレスへビットコイン・ビットコインキャシュ・モナコインを送金、②犯行者がミキシングサービス等を利用して当該資金を拡散、というニフェーズに分けられる（図表 153）。

図表 153 主な時系列の推移

No	発生日時		事象
1	2018/9/14	17:33 頃	テックビューロ社のアドレスからのビットコインキャッシュ不正流出開始
2	2018/9/14	17:33 頃	テックビューロ社のアドレスからのビットコイン不正流出開始
3	2018/9/14	17:39 頃	テックビューロ社のアドレスからのモナコイン不正流出開始
4	2018/9/14	18:54 頃	テックビューロ社のアドレスからの不正流出の大半が終了
5	2018/9/14	20:09 頃	不正流出されたビットコインの資産移動が開始
6	2018/9/14	21:00 頃	不正流出されたビットコインの資産移動が終了
7	2018/9/15	10:47 頃	不正流出されたビットコインの資産移動が活発化（拡散が加速）
8	2018/9/15		不正流出されたビットコインの一部が仮想通貨取引所「Binance」に入金と推定
9	2018/9/17		テックビューロ社がサーバ異常を検知
10	2018/9/17	16:57 頃	テックビューロ社がビットコインとモナコインの入出金を停止
11	2018/9/17	20:48 頃	テックビューロ社がビットコインキャッシュの入出金も停止
12	2018/9/18	11:48 頃	テックビューロ社が顧客資産の安全を確認とツイート
13	2018/9/18		テックビューロ社がハッキング被害を確認、財務局へ報告

387 PRTIMES, "テックビューロ株式会社 仮想通貨流出事件に関する状況報告、及び顧客対応状況について", https://prtimes.jp/main/html/rd/p/000000094.000012906.html, 2019/1/7

14	2018/9/20	02:15 頃	テックビューロ社が仮想通貨の入出金停止について公表

3.7.3.2 第一段階（暗号資産流出）

テックビューロ社の管理するアドレス（以下、流出元アドレス）から犯行者の管理するアドレス（以下、一次流出先アドレス）への不正送金について、ビットコインブロックチェーン上では計 16 回、ビットコインキャッシュブロックチェーン上では計 11 回、モナコインブロックチェーン上では計 163 回のトランザクションにより不正送金が行われたことが把握できる[388]（図表 154、図表 155、図表 156）。

図表 154 ビットコインブロックチェーン上の不正流出の記録[389]

No	時刻	送金額（BC）	手数料（BC）	送信元アドレス数	送信先アドレス
1	2018/9/14 17:33	5,000.0	0.00163	131	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
2	2018/9/14 17:33	0.1	0.00004	3	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
3	2018/9/14 17:49	470.0	0.00013	66	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
4	2018/9/14 17:49	20.0	0.00050	42	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
5	2018/9/14 17:49	460.0	0.00001	2	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
6	2018/9/14 18:05	1.0	0.00002	9	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
7	2018/9/14 18:05	1.0	0.00001	流出元アドレス	1FmwHh6 一次流出先アドレス 571f9w
8	2018/9/14 18:05	1.0	0.00002	9	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
9	2018/9/14 18:19	5.0	0.00033	27	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
10	2018/9/14 18:42	2.5	0.00016	22	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
11	2018/9/14 20:31	1.5	0.00000	1	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
12	2018/9/15 7:07	1.0	0.00003	13	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
13	2018/9/15 9:55	1.0	0.00006	28	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
14	2018/9/15 13:32	1.0	0.00120	595	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
15	2018/9/15 13:33	0.5	0.00085	420	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
16	2018/9/15 13:33	0.5	0.00071	352	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w
合計		5,966.1	0.00570	1,726	

図表 155 ビットコインキャッシュブロックチェーン上の不正流出の記録 [389]

No	時刻	送金額（BCH）	手数料（BCH）	送信元アドレス数	送信先アドレス
1	2018/1/14 17:33	0.1	0.00000	1	1N4Gz8QqVs3yXfKos46G8JJwW8Mpcb41YJ
2	2018/1/14 17:33	5,000.0	0.00031	208	1N4Gz8QqVs3yXfKos46G8JJwW8Mpcb41YJ
3	2018/1/14 17:33	5,000.0	0.00054	367	1N4Gz8QqVs3yXfKos46G8JJwW8Mpcb41YJ
4	2018/1/14 17:33	10,000.0	0.00020	136	1N4Gz8QqVs3yXfKos46G8JJwW8Mpcb41YJ
5	2018/1/14 17:33	10,000.0	0.00047	315	1N4Gz8QqVs3yXfKos46G8JJwW8Mpcb41YJ
6	2018/1/14 17:36	1,290.0	0.00001	流出元アドレス	1N4G 一次流出先アドレス 8Mpcb41YJ
7	2018/1/14 17:36	3,000.0	0.00069		1N4G 8Mpcb41YJ
8	2018/1/14 17:36	3,000.0	0.00070	475	1N4Gz8QqVs3yXfKos46G8JJwW8Mpcb41YJ
9	2018/1/14 17:36	5,000.0	0.00086	583	1N4Gz8QqVs3yXfKos46G8JJwW8Mpcb41YJ

388 piyolog, HatenaBlog, "Zaif で発生した不正送金事案についてまとめてみた", http://d.hatena.ne.jp/Kango/20180920/1537414861, 2019/1/7

389 BITCOIN.COM, "Bitcoin Core (BTC) Block Explorer", https://explorer.bitcoin.com/btc, 2019/1/7

10	2018/1/14 17:51	7.0	0.00000	1	1N4Gz8QqVs3yXfKos46G8JJwW8Mpcb41YJ
11	2018/1/14 17:51	30.0	0.00001	8	1N4Gz8QqVs3yXfKos46G8JJwW8Mpcb41YJ
合計		42,327.1	0.00380	2,565	

図表 156 モナコインブロックチェーン上の不正流出の記録[390]

No	時刻	送金額（MONA）	手数料（MONA）	送信元アドレス数	送信先アドレス数
1	2018/9/14 17:39	0.1	0.00	2	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV 他 1
2	2018/9/14 17:55	105,700.0	0.10	212	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV 他 1
3	2018/9/14 17:55	105,700.0	0.10	93	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV 他 1
4	2018/9/14 17:55	25,700.0	0.00	7	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV 他 1
5	2018/9/14 17:55	205,700.0	0.10	150	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV 他 1
6	2018/9/14 17:55	105,700.0	0.02	流出元アドレス	MBEYH8 一次流出先アドレス 9JbitV 他 1
7	2018/9/14 17:55	15,700.0	0.00	6	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV 他 1
8	2018/9/14 17:55	205,700.0	0.10	182	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV
…					
160	2018/9/14 18:53	500.0	0.10	381	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV 他 1
161	2018/9/14 18:53	500.0	0.10	353	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV 他 1
162	2018/9/14 18:53	500.0	0.10	419	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV 他 1
163	2018/9/14 18:54	500.0	0.10	332	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV 他 1
合計		6,236,810.1	11.67	25,142	313

不正送金の理由として、詳細は非公表としつつ、以下の見解がテックビューロ社より公表されている[391]。

- 入出金用のホットウォレットを管理するサーバに対し、外部からの不正アクセスが行われ、当該ホットウォレットで管理している暗号資産（BTC、MONA、BCH）が不正に送金された。

3.7.3.2.1 第一段階（暗号資産流出）にかかる考察

暗号資産不正流出を招いた主な要因としては、コインチェック社と同じくマルチシグやコールドウォレットが運用されていなかったことが挙げられる。

テックビューロ社では、コインチェック社の暗号資産不正流出事件を受けて、セキュリティ対策室を設置してマルチシグ強化やコールドウォレット優先を掲げていたが[392]、マルチシグについては、流出元アドレスのうち、ビットコインでは約 93.5%、ビットコインキャッシュおよびモナコインでは全てのアドレスでマルチシグは用いられていなかっ

390 mona.chainsight, "mona insight", https://mona.chainsight.info/api/, 2019/1/7 より三菱総研作成（他のアドレスへ送金された流出資金も一次流出先アドレス（MBEYH8JuAHynTA7unLjon7p7im2 U9JbitV）へ移動したと考えられる。）

391 PRTIMES, "テックビューロ株式会社 仮想通貨の入出金停止に関するご報告、及び弊社対応について", https://prtimes.jp/main/html/rd/p/000000093.000012906.html, 2019/1/7

392 Zaif, "テックビューロ（Zaif）セキュリティ対策室設置について", https://corp.zaif.jp/info/8517/, 2019/1/7

た（図表 157）。

図表 157 流出元アドレスの内訳（左：ビットコイン、右：ビットコインキャッシュ）[393]

マルチシグ有無	アドレス数	割合（%）
無し	1,614	93.5%
有り	112	6.5%
合計	1,726	100.0%

マルチシグ有無	アドレス数	割合（%）
無し	2,565	100.0%
有り	0	0.0%
合計	2,565	100.0%

また、自己資金で不正流出額を全額補填したコインチェック社と異なり、テックビューロ社の場合はフィスコ社の金融支援が補填の前提となる[394]。そのため、自己資金で弁済できない額をコールドウォレットで運用していた点については、様々な指摘がなされている[22]。

最後に、2018 年 9 月 14 日に不正流出が発生し、2018 年 9 月 17 日にサーバ異常を検知、2018 年 9 月 18 日に顧客資産の安全を確認とした[395]後に、ハッキング被害を確認し財務局へ報告を行うというテックビューロ社の対応の遅れについても多くの報道で問題があると指摘された[396]。

3.7.3.3 第二段階（暗号資産拡散）

ビットコインにおいては、犯行者は大半の不正流出を終えた 1 時間後（2018 年 9 月 14 日 20:09 頃）から他のアドレスへの資産移動を開始し、不正流出額の約 99%（5955.6BTC）を移動させ（図表 158）、複数回の資産移動を繰り返しながら、別なアドレスへ資金を移動した（図表 159）。

図表 158 一時流出先アドレスからの移動

No	時刻	送金額（BC）	手数料（BC）	送信元アドレス	送信先アドレス数
1	2018/9/14 20:09	1.1	0.00004	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w	2
2	2018/9/14 20:09	5,954.5	0.00011	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w	2
3	2018/9/14 20:31	1.5	0.00005	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w	2
4	2018/9/14 20:31	5.0	0.00005	1FmwHh6pg 一次流出先アドレス 71f9w	2

393 マルチシグの有無はアドレスの先頭文字で判断した。具体的には、マルチシグアドレスは、ビットコインではアドレス先頭が「3」の場合、ビットコインキャッシュではアドレス先頭が「q」の場合、モナコインではアドレスの先頭が「p」ないし「3」である。Bitcoin Wiki, "Address", https://en.bitcoin.it/wiki/Address, 2019/1/7

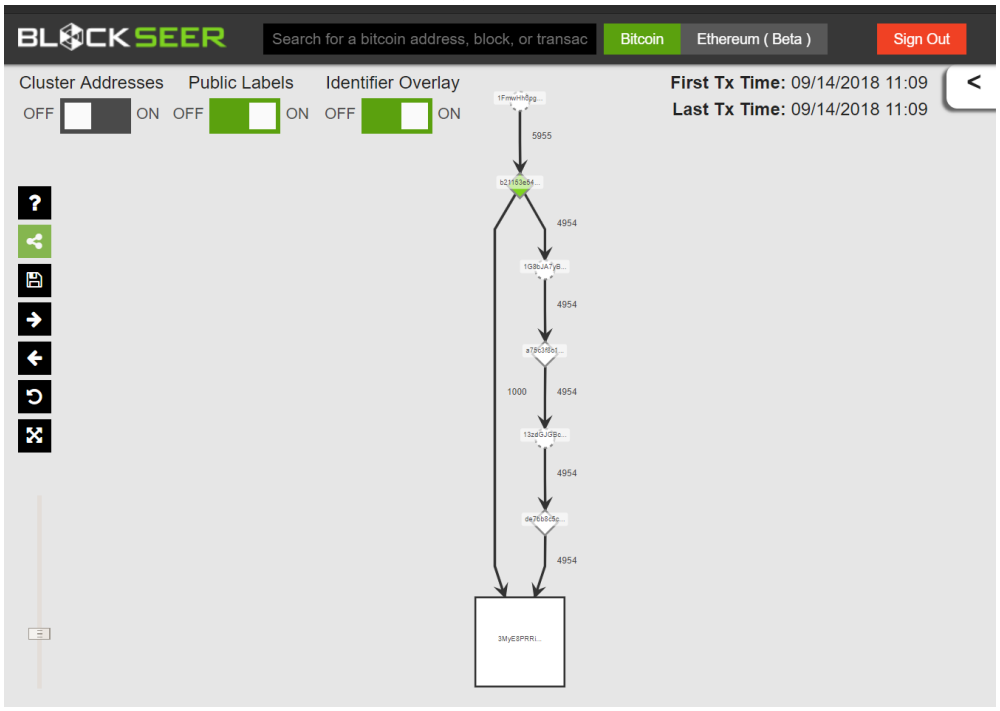
394 PRTIMES, "テックビューロ株式会社 お客様預かり資産に関する金融支援 正式契約締結のお知らせ", https://prtimes.jp/main/html/rd/p/000000098.000012906.html, 2019/1/7

395 Zaif - 暗号通貨取引所@zaifdotjp, Twitter, https://twitter.com/zaifdotjp, 2019/1/7

396 CoinPost, "金融庁が「Zaif 仮想通貨流出事件」の記者ブリーフィングを開催、最新の見解が明らかに", https://coinpost.jp/?p=47950, 2019/1/7

5	2018/9/14 7:07	1.0	0.00004	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w	1
6	2018/9/15 9:55	1.0	0.00004	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w	1
7	2018/9/15 13:32	1.0	0.00004	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w	1
8	2018/9/15 13:33	0.5	0.00004	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w	1
9	2018/9/15 13:33	0.5	0.00004	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w	1
合計		5,966.1			13（重複含む）

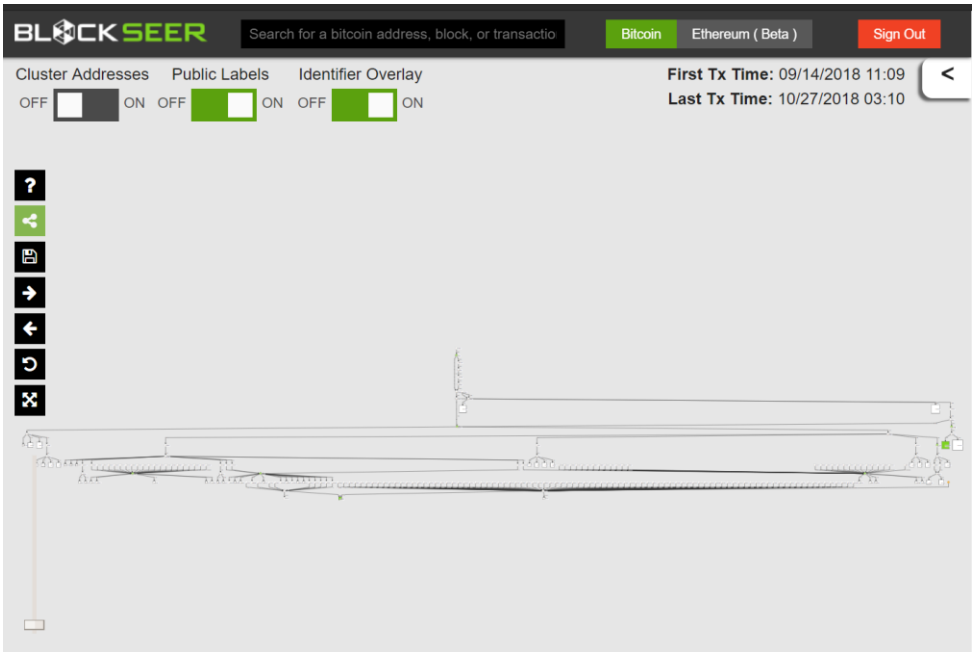
図表 159 2018 年 9 月 14 日末時点の移動状況（最上段が一次流出先アドレス、最下段が移動先のアドレス）[397]



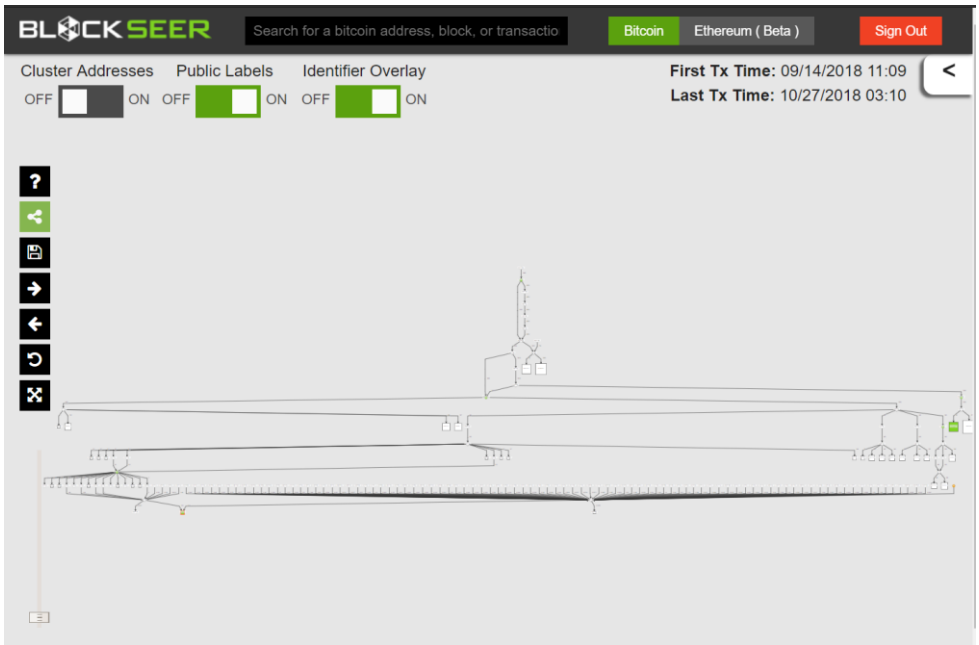
犯行者は翌日（2018 年 9 月 15 日 10:47 頃）から更なる資産移動を活発化させる。ここではミキシングサービスが用いられたと報道されている[398]（図表 160）。流出した資金は、その後、2BTC 程度の少額なアドレスに分けられて、世界でも有数の取引量を持つ仮想通貨取引所「Binance」[399]と思われるアドレス[400]へ移動したと指摘されている[401]（図表 161）。

397 DMG Blockchain Solutions Inc., BlockSeer website, "BlockSeer", https://www.blockseer.com/, 2018/10/26
398 毎日新聞ウェブサイト, "匿名化サービス悪用、追跡困難か Zaif仮想通貨流出", https://www.asahi.com/articles/ASL9N56MYL9NULFA02C.html, 2019/1/7
399 CoinMarketCap, coinmarketcap.com, "Top 100 Cryptocurrency Exchanges by Trade Volume", https://coinmarketcap.com/rankings/exchanges/, 2019/1/7
400 Binance@binance, Twitter, https://twitter.com/binance/status/961666467325358081, 2019/1/7
401 cheena, "Zaif の仮想通貨不正流出で見えてきた「正しいお金の洗い方」", 無能ブログ, https://blog.cheena.net/1910, 2019/1/7

図表 160 少額への分割状況（抜粋）[397]

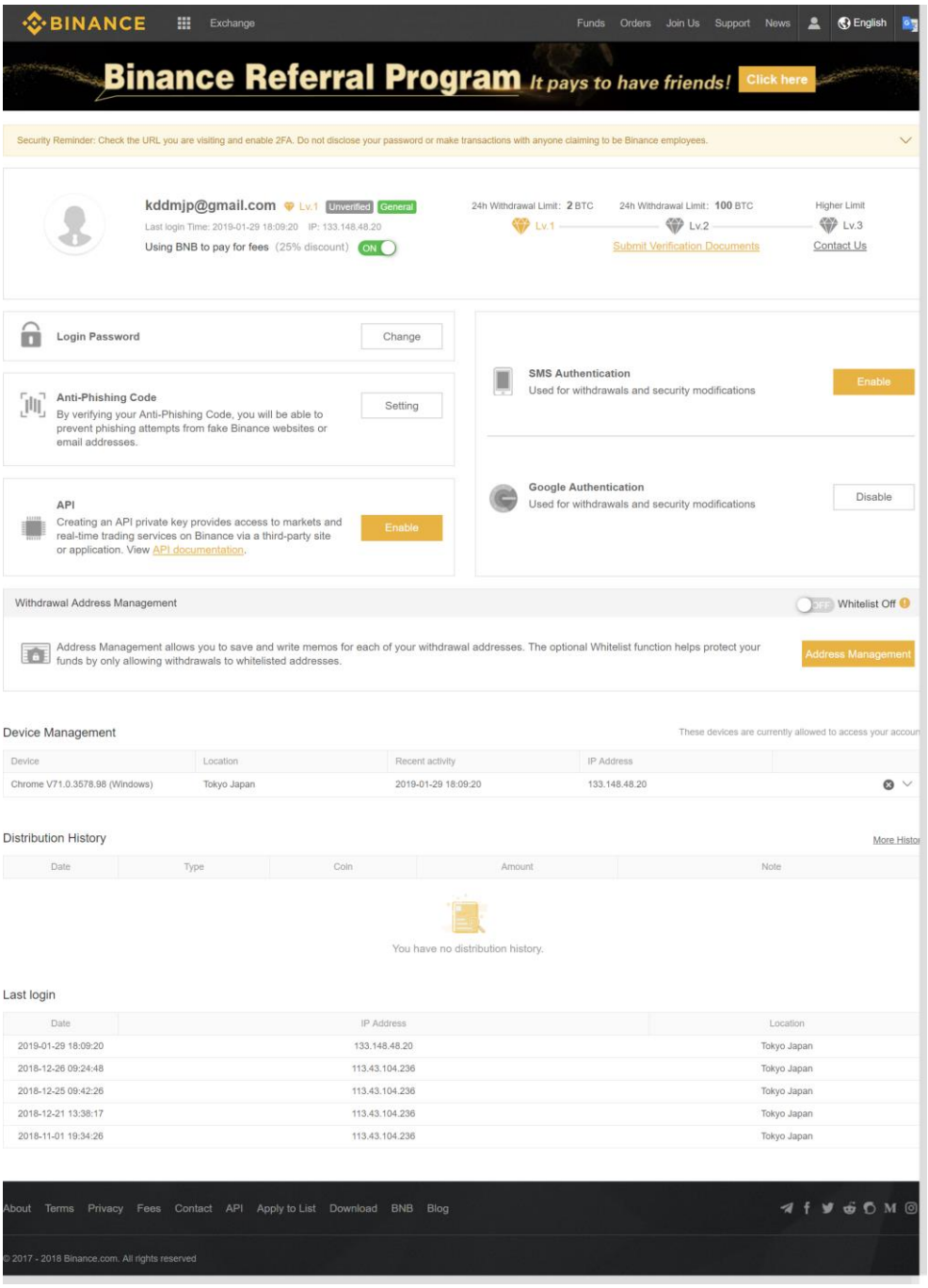


図表 161 仮想通貨取引所「Binance」と思われるアドレスへの移動経路（最下段の左から二番目が Binance とされるアドレス）[397]



ここで、2BTC 程度に分割された理由としては、「Binance」では 24 時間内に 2BTC までの出金であれば本人確認がない点が指摘されている[401]（図表 162）。

図表 162 仮想通貨取引所「Binance」のアカウント画面[402]（画面右上のダイヤモンドのマークで、本人確認を行うと出金制限が 2BTC から 100BTC に変わる）



3.7.3.3.1 第二段階（暗号資産拡散）にかかる考察

仮想通貨取引所「Coincheck」における暗号資産追跡事例と比較して、以下の三点が違いとして挙げられる（図表 163）。

402 Binance, Binance.com, https://www.binance.com/, 2019/1/7

図表 163 仮想通貨取引所「Coincheck」における追跡事例との差異

No	主な差異
1	犯行者（ないし犯行者グループ）が仮想通貨を拡散させたこと
2	ミキシングサービスが利用されたこと
3	本人確認が不要な限度額の範囲で仮想通貨取引所が利用されたこと

- No1「犯行者による拡散」については、暗号資産の不正流出から比較的短時間に当該資金が移動したこと、その間一般に広く報道がなされてはいなかったことによる。

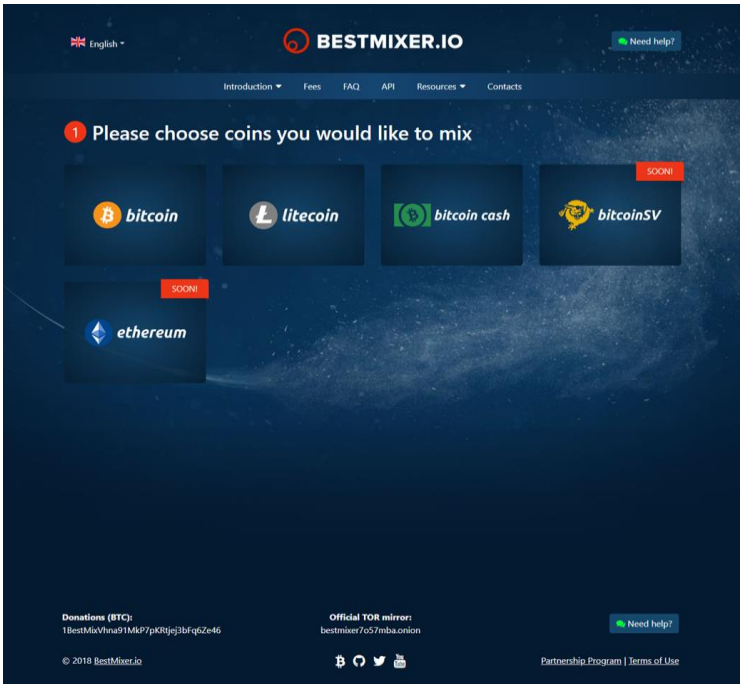
- No2「ミキシングサービス」については、従前よりミキシングサービスのマネーロンダリングへの悪用の可能性が指摘されていたが[403]、実際の利用事例が一般に報道されるところとなった。

  本事例ではミキシングサービス BestMixer[404]や ChipMixer[405]が用いられたと一部で指摘されているが[406]、当該サービスへのアクセスは容易であった（図表 164、2018 年 12 月 18 日時点）。

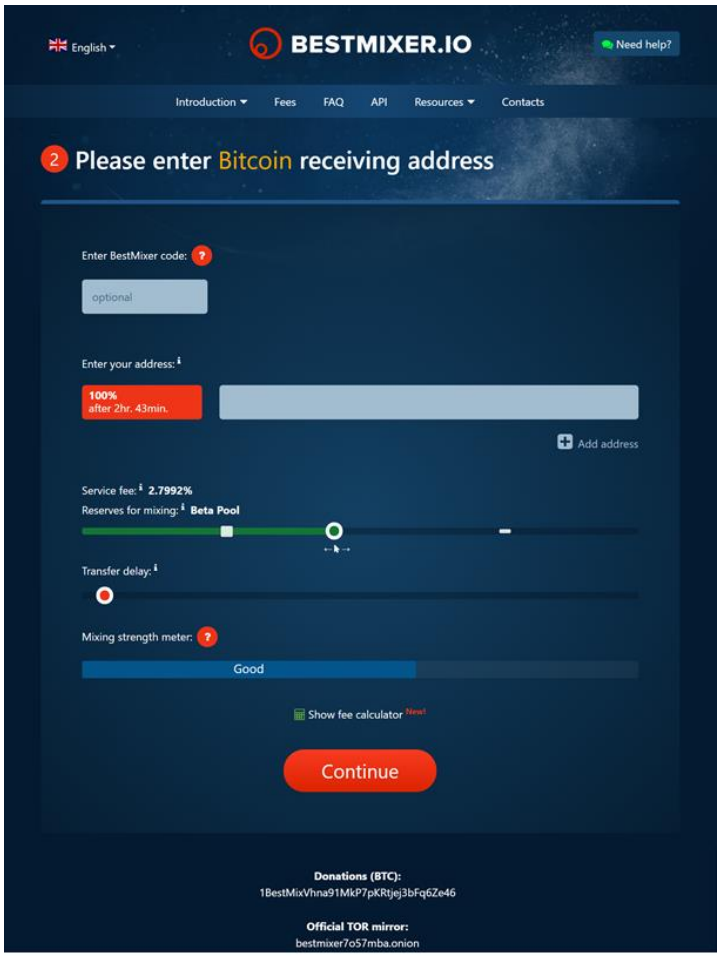
  例えば、BestMixer では、プライバシー・セキュリティポリシーにより、ユーザ登録などの顧客情報の取得は一切行わず、処理終了後 24 時間以内に注文履歴を削除、72 時間以上経過した取引データは廃棄等の対応をうたっている[407]。ビットコインの他、ビットコインキャッシュやライトコインも扱っており、また、受取先アドレスは複数指定することが可能であり、それぞれに遅延時間を設けられることから、第三者がブロックチェーン上のデータから送金元アドレスと送金先アドレスを紐付けるのは困難と考えられる（図表 165）。

403 The Financial Action Task Force, "FATF REPORT Professional Money Laundering", http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf, 2019/1/7
404 BESTMIXER.io, bestmixer.io, https://bestmixer.io/, 2019/1/7
405 ChipMixer, ChipMixer.io, http://ChipMixer.io/, 2019/1/7
406 Cheena@CheenaBlog, Twitter, https://twitter.com/cheenablog/status/1055706764862210048, 2019/1/7
407 送金先アドレスへの送金は 24 時間以内に 1 回のみとされており、（指定した遅延時間によるが）最大でも 72 時間以内に処理が完了する。

図表 164 ミキシングサービス「BestMixer」[408]



図表 165「BestMixer」受取先アドレス入力画面 [404]



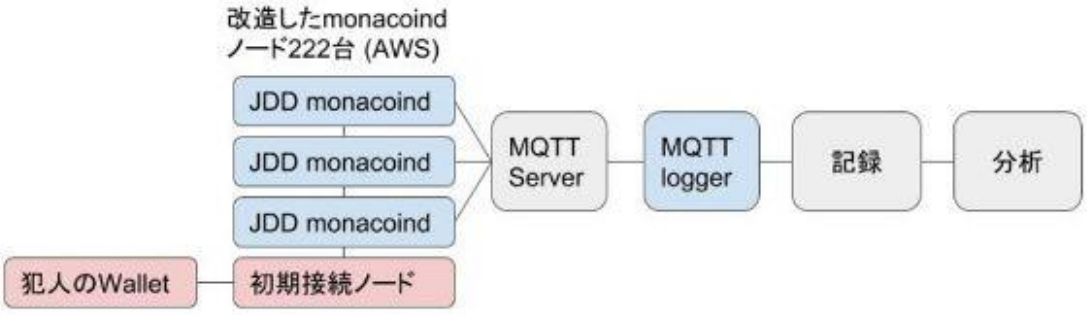
408 Bestmixer.io, "Start new mixing", https://bestmixer.io/en#start_new_mixing, 2018/12/18

- No3「取引所」については、「Coincheck」の事例と同じく仮想通貨取引所が出口の一つとなったが、（本人確認等の緩い）比較的小規模の取引所ではなく、世界最大の取引所を用いた点が特徴といえる。

3.7.3.4 犯行者に関係するノードの追跡（再識別）

2018 年 11 月 5 日に、Japan Digital Design 株式会社は、不正流出したモナコインの送金指示元 IP アドレスの特定したことを公表した[334]。比較的ノード数の少ないモナコインを対象に、全体ノード数の過半数を占める 222 ノードを用意し[409]、犯行者が送金指示に用いる送金指示元ノードと、直接ないし 2 ホップ（間に 1 ノード挟む状況）で接続する可能性を高めることで、送金指示元ノードの IP アドレスを推定した。具体的に、2018 年 10 月 20 日に犯行者が送金指示に用いたノードを推定したところ、送金指示元の 5 件中 4 件はフランス、1 件はドイツであった。

図表 166 追跡システムの概要[410]



図表 167 2018 年 10 月 22 日の資産移動の記録

No	時刻	送金額（BCH）	手数料（BCH）	送信元アドレス	送信先アドレス
1	2018/10/20 14:22	1,000	0.05182	MBEYH8JuAHynTA7unLjon7p7im2U9JbitV	MNykxRZo7x7LeHhFDQN3WeHK3nMahk8ooL
2	2018/10/20 14:22	1,735,810		MBEYH8JuAHynTA7unLjon7p7im2U9JbitV	MDDfvnKnk7AbGU7vdFBBTn1ZuTQJdKAA7L
3	2018/10/20 14:22	1,800,000		MB[redacted]2U9JbitV	MHQ[redacted]Eo8hy
4	2018/10/20 14:22	2,700,000		MBEYH8JuAHynTA7unLjon7p7im2U9JbitV	MQJ4TkGpEVYn6wd45gmYv3XSGbMMR5h4wv
合計		6,236,810	0.05182		

一次流出先アドレス

二次流出先アドレス群

ただし、犯行者は Tor などの匿名化通信を使用した可能性もあり、今回特定された IP アドレスは犯行者とは関係のない場合もあり得る点には留意の必要がある。

409 Amazon Web Services の提供する EC2 を利用しており、メモリ 0.5GB（t3.micro）やメモリ 1GB（t3.small）などのインスタンスが用いられた。

410 Japan Digital Design, "仮想通貨取引所 Zaif から流出した仮想通貨の追跡について", https://static1.squarespace.com/static/59c0ccc39f745604cff71409/t/5bdab4418a922d1e357e4dde/1541137249094/1.png?format=1500w, 2019/1/7

3.7.4 考察

ここでは、仮想通貨取引所「Coincheck」及び「Zaif」における暗号資産追跡事件において、関係者が行った対応等について、事前・事後の観点から評価を行う。

3.7.4.1 事前の対応

まず何よりも「流出を未然に防ぐこと」が極めて重要である。取引所は顧客の資産（具体的には秘密鍵）を預かるカストディ・サービスも提供しているため、外部からの不正アクセスを招かないことに加え、内部犯行が行われないように、各取引所は万全の対策を備える必要がある。

技術面では、コールドウォレットでの運用や、顧客の発信元 IP アドレスの制限（少なくとも Tor や I2P からの接続を遮断する等）、カストディ・サービスのアウトソースなどの手段をとることや、制度面でもそれらを義務付けることが考えられる。

あわせて、流出が発生した場合に速やかに対応できる体制をとる必要がある。特に Coincheck および Zaif のいずれの事件ともに、週末を迎える金曜日に発生しており、週末で取引所の対応が手薄になる一方、顧客の需要に備えてホットウォレットに多額の暗号資産を移動していることを狙っていた可能性が考えられる。技術面では即応体制を整備し、常時監視を徹底する必要があると考えられる。また、制度面においても、公表を含めた迅速な報告の義務付けや、流出に備えた弁済原資の保持の義務付けなどが考えられる[411]。

総じて、両事件においては、これらの対応は徹底されていなかったと考えられる。

3.7.4.2 事後の対応

次に「流出発生後に速やかに拡散を防ぐ」ことが重要となる。プログラム取引等で数百万アドレスに分割するなどは容易に行えるため、一旦拡散してしまうと、流出先を事後的に特定するのは事実上不可能になる可能性があるからである[412]。特に、取引所やミキシングサービス、ギャンブルサイトなど、暗号資産の資金洗浄に用いられるサービスに送金されてしまうと、それ以降は足跡を追うことが極めて難しくなるた

411 金融庁の設置した「仮想通貨交換業等に関する研究会」においても、ここに挙げたものと同様の提言がまとめられている。金融庁, 金融庁ウェブサイト, "仮想通貨交換業等に関する研究会報告書", https://www.fsa.go.jp/news/30/singi/20181221-1.pdf, 2019/2/8

412 岩沢明信, 日本経済新聞, "巨額の仮想通貨流出、2 つの事件は何が違ったのか", https://r.nikkei.com/article/DGXMZO42477140U9A310C1CC1000?s=0, 2019/3/19

め、そのようなサービスへ送金される前に対応する必要がある。報道をみる限り、Coincheck 事件においては当局の初動体制が万全であったと考えることは難しく、Zaif 事件においてはそもそも当局への申告自体が遅れていた。

ただし、拡散を防ぐことに成功したとしても、流出資産を取り返すことは極めて困難であるという点には留意する必要がある。これは、現在までに発生した仮想通貨取引所の不正流出被害において（図表 13）、その後に被害額が取り返された事例は（今回調査した範囲では）非常に限られていたことからも分かる[413]。基本的に事後にできることは、流出資産の凍結など、犯行者が他に換金するコストを上げる程度であるため、「流出額の規模」と「拡散を防ぐためのコスト」などの兼ね合いで判断されることになっていくと考えられる。

拡散防止にあたっては、一つの取引所だけで対応することは困難であり、マイナーや他の取引所、ホワイトハッカーなどの協力を仰ぐ必要がある。具体的には、業界横断ないし国際的に犯罪データを共有する体制を整備し、ある取引所の不正流出に絡んだ暗号資産の受け入れ停止を各取引所に徹底させることやマイナーにも当該トランザクションの受け入れ停止を徹底させることなどが考えられる。

しかし、特に Coincheck 事件において明らかになったように、マイナーや取引所が世界中に散らばる中、上記の徹底を推し進めることは極めて難しいと考えられる。Coincheck 事件では、全ての取引所が流出した NEM の受け入れ停止を行ったということはなく、また、NEM 財団や有志によるマーキングにより流出した NEM を受け取る先に注意換気も行われたが、それでも拡散を防ぐことはできなかった。

以上より、速やかな拡散防止が必要なものの、実際に拡散防止を行うことは現状では様々な限界があると考えられる。

3.7.4.3 その他の対応

より根本的には、暗号資産の技術的なデザインや制度的な対応を、流出することを前提として設計することも考えられる。

技術的なデザインについては、例えば現状のビットコインでは秘密鍵の保有と暗号

413 仮想通貨取引所 Bitfinex は 2016 年 8 月に 12 万 BTC が不正に流出したが、2019 年 1 月にそのうち 27.7BTC（流出額の 0.02%）を回収できたと報告しているが、回収額は極僅かに留まる。Jeffrey Gogo, Bitcoin.com, "Bitfinex Recovers $106,000 of Stolen BTC With US Government Help", https://news.bitcoin.com/bitfinex-recovers-106000-of-stolen-btc-with-us-government-help/, 2019/2/8

資産の所有権は同じことを指すが、この対応関係を分ける（アドレスなどの識別子と秘密鍵・公開鍵の対応関係を変更できるようにする）ことで、秘密鍵が流出しても、資産を窃取できないようにする仕組みが提案されている[414]。他にも、当局など信頼できる第三者からマークされた取引が、マイナーによるブロック生成の際に排除される仕組みや、Zcash のように取引内容を秘匿するものの閲覧キーを渡すことで取引内容を把握できるようにする仕組み（キーエスクローの一種）なども考えられる。

制度的な対応については、資金洗浄に利用される可能性のある取引所やギャンブルサイトにおいて、資産移動経路が事後にも分かるように、同じアドレスを複数の利用者で使い回すのではなく、利用者個別にアドレスを用意するように義務付けることなども考えられる。

いずれにせよ、不正アクセスを完全に防ぐこと（事前の観点）や、流出した資産の拡散を完全に防ぐこと（事後の観点）はできないという前提に立って、暗号資産取引の望ましいデザインについて、当局・エンジニア・アカデミアなどが協働して議論を深めていくことが重要だと考えられる。

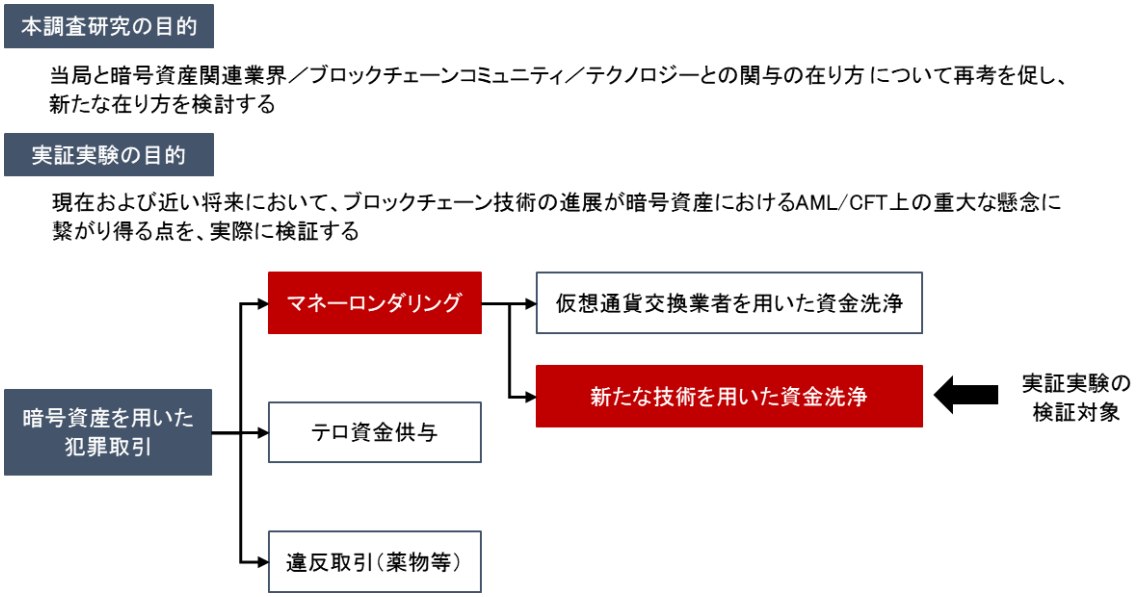
414 Saito, K., et al, "BBc-1 : Beyond Blockchain One", file:///C:/Users/2070621/Desktop/BBc-1_design_paper.pdf, 2019/3/1

4. 実証実験

4.1 概要

本調査研究は、近年のブロックチェーン技術の進展を踏まえて、当局と暗号資産関連コミュニティやテクノロジーとの関わり方を検討することを目的とする。そのため、実証実験では、現在および近い将来におけるブロックチェーン技術の進展が暗号資産における AML/CFT 上の重大な懸念に繋がり得る点を実際に検証することを目的とした（図表 168）。

図表 168 本調査研究の目的と実証実験の検証対象



暗号資産を用いた犯罪取引としては、マネーロンダリング、テロ資金供与、違法取引などが挙げられ、それぞれに最適な技術とその対応策は異なり得ることが考えられるが[415]、我が国においては現在までにマネーロンダリングが犯罪取引の大半を占めることから[416]、マネーロンダリングを本実証実験で扱うシナリオの対象とした。具体的には、不正に得た暗号資産を資金洗浄する場合を考えた[417]（図表 169）。

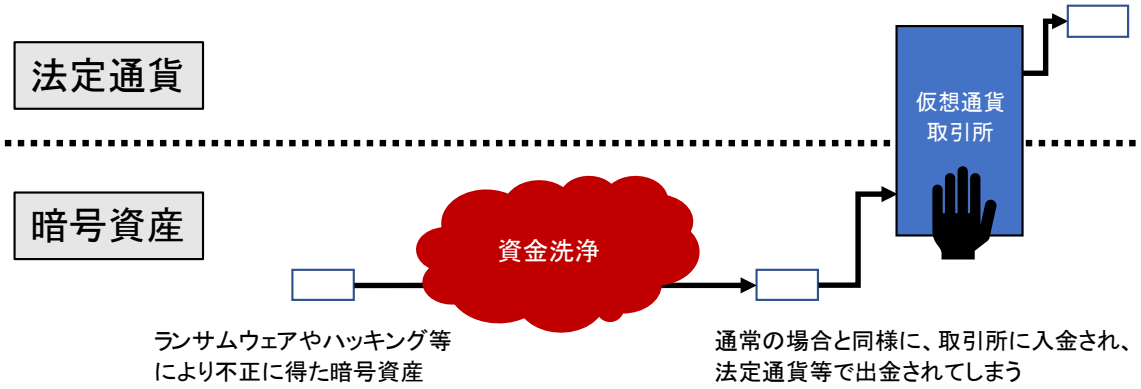
---

415 例えば、マネーロンダリングでは、不正資金を正当な理由のある資金とプーリングさせることなどにより両者を区別できないようにすることが重要になるが、テロ資金供与や違法取引では取引を隠密に行うとともに取引の記録自体を残さないことが重要となると考えられる。

416 以下では、報告書の時点までにテロ資金供与に係る事件検挙はなく、テロ資金の供与元／供与先に係る大きな脅威は認められない（P7）とされている。
警察庁ウェブサイト, FATF勧告実施に関する関係省庁連絡会議 国が実施する資金洗浄及びテロ資金に関するリスク評価に関する分科会, "犯罪による収益の移転の危険性の程度に関する評価書", https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/risk/risk261218.pdf, 2019/1/7

417 仮想通貨交換業者によるマネーロンダリング対策が十分に行われていると考えると、不正に得た法定通貨を

図表 169 取引所規制に対する暗号資産の資金洗浄のインパクト



本調査研究では、専門家等の意見を踏まえ、三つの実証実験を行った（図表170）。以降ではそれぞれ節に分けて記載する。

図表 170 実証実験の一覧

No	名称	実験内容
1	ライトニングネットワークを用いた資金洗浄	ライトニングネットワークを用いて、複数の中継ノードを経由する形で送金する
2	ミキシングを用いた資金洗浄	ミキシングサービスを用いて送金する
3	リスクスコアリングツールによる評価	複数のリスクスコアリングツールを用いて、実際に使われたビットコインアドレスを評価する

敢えて暗号資産に交換した上で資金洗浄を行う必要性が乏しいことや、ランサムウェアの送金先やハッキングなどでは犯行者にとって法定通貨よりも暗号資産の方が利便性が高い等の理由による。

4.2 実証実験1. ライトニングネットワークを用いた資金洗浄

4.2.1 概要

犯行者が何らかの形で得た不正な暗号資産の資金洗浄を図る場合を考える。ここで、犯行者が、ライトニングネットワークを用いて、複数の中継ノードを経由する形で自分自身が管理する他のアドレスへ送金することで、第三者からの追跡がどの程度困難になるかを検証する。ここで、特に、以下の二点を念頭に検証を行った。

- ブロックチェーン上に送金記録が残るか否か
- 通信経路を流れるデータに送金記録が残るか否か

4.2.2 実験環境等

4.2.2.1 各種環境

ソフトウェア構成は図表 171 の通り。ここで、ライトニングネットワークのソフトウェアとして、c-lightning、ptarmigan、eclair、LND の 4 種類を用いた（ソフトウェアの挙動の違い等は「実証実験再現のために必要となるリソース一式」のファイルを参照のこと）。ハードウェア構成は図表 172 の通りであり、同構成のマシンを 4 台用意した。以降ではそれぞれのノードをノード A、ノード B、ノード C、ノード D と記載する。ネットワーク構成は図表 173 の通りである。

図表 171 ソフトウェア構成

名称	バージョン
OS	Ubuntu 18.04.1 LTS
ビットコイン	v0.17.1.0-gef70f9b52b851c7997a9f1a0834714e3eebc1fd8
ライトニングネットワーク	① c-lightning[418]、リポジトリ：arowser[419]、リビジョン番号：9946209b5bcf04093483c84793b6905b400e8327

418 Blockstream 社が 2015 年から開発している、C 言語で実装された、ライトニングネットワークの仕様に準拠したクライアント。

419 暗号化されたパケットを解析するために、c-lightning がメモリ上に保持している復号鍵をファイルに書き出すためのパッチをあてたもの。arowser, Github, "lightning", https://github.com/arowser/lightning/tree/dissector, 2019/2/8

	② ptarmigan[420]、リビジョン番号： b8d7d6bedb11e5d97b2b946201d5c8d26875493b ③ eclair[421]、バージョン：v0.2-beta9 ④ LND[422]、リポジトリ：nakajo2011[423]、リビジョン番号： 4c1ce439a7b77fed09c9b5b01b2f00de22988fa3
Wireshark	TShark (Wireshark) [424] バージョン：2.6.4
Wireshark プラグイン（ライトニングネットワーク用）	lightning-dissector[425]、リビジョン番号： 5f528691b44bccabfd676f15eb5e74fa28936fc4

図表 172 ハードウェア構成

リージョン	モデル	vCPU	メモリ(GB)	ストレージ(GB)	台数
東京	t2.large	2	8	50	4

図表 173 ネットワーク構成

名称	内容
ビットコインネットワーク	testnet3
ライトニングネットワーク	ノード A～ノード D の 4 台のノードで構成されたライトニングネットワーク

4.2.2.2 パケットデータの確認内容

lightning-dissector プラグインで取得が可能なライトニング・ネットワーク・プロトコル・データの一覧は図表 174 の通り。本実験では、こののうち、通信先のチャンネル

420 株式会社 Nayuta が 2017 年 7 月頃から開発している、C++言語で実装された、ライトニングネットワークの仕様に準拠したクライアント。nayutaco, Github, " ptarmigan", https://github.com/nayutaco/ptarmigan, 2019/2/8

421 ACINQ 社が 2015 年 8 月より開発している、Scala 言語で実装された、ライトニングネットワークの仕様に準拠したクライアント。ACINQ, Githbu, eclair, https://github.com/ACINQ/eclair/, 2019/2/8

422 Lightning Labs 社が 2015 年から開発している、Go 言語で実装された、ライトニングネットワークの仕様に準拠したクライアント。

423 暗号化されたパケットを解析するために、LND がメモリ上に保持している復号鍵をファイルに書き出すためのパッチをあてたもの。nakajo2011, Github, " Lightning Network Daemon", https://github.com/nakajo2011/lnd, 2019/2/8

424 著名なパケットキャプチャ・プロトコル解析ソフトであり、リアルタイムでパケット情報を確認できる。

425 株式会社 Nayuta が 2018 年 8 月頃から開発している Lightning Network ノード間の通信を分析するための Wirehark プラグイン。nayutaco, GitHub, "lightning-dissector", https://github.com/nayutaco/lightning-dissector, 2019/1/7

ID（channel_id）、ペイメントチャネルを開くために発行したトランザクション ID（funding_txid）、送金経路情報（onion_routing_packet）、HTLC を作成するときの用いるハッシュ値（payment_hash）、HTLC での支払いを完了するために用いるシークレット（payment_preimage）の値を評価した。

図表 174 パケットデータから取得可能な項目の一覧（青地は評価に使用した項目）

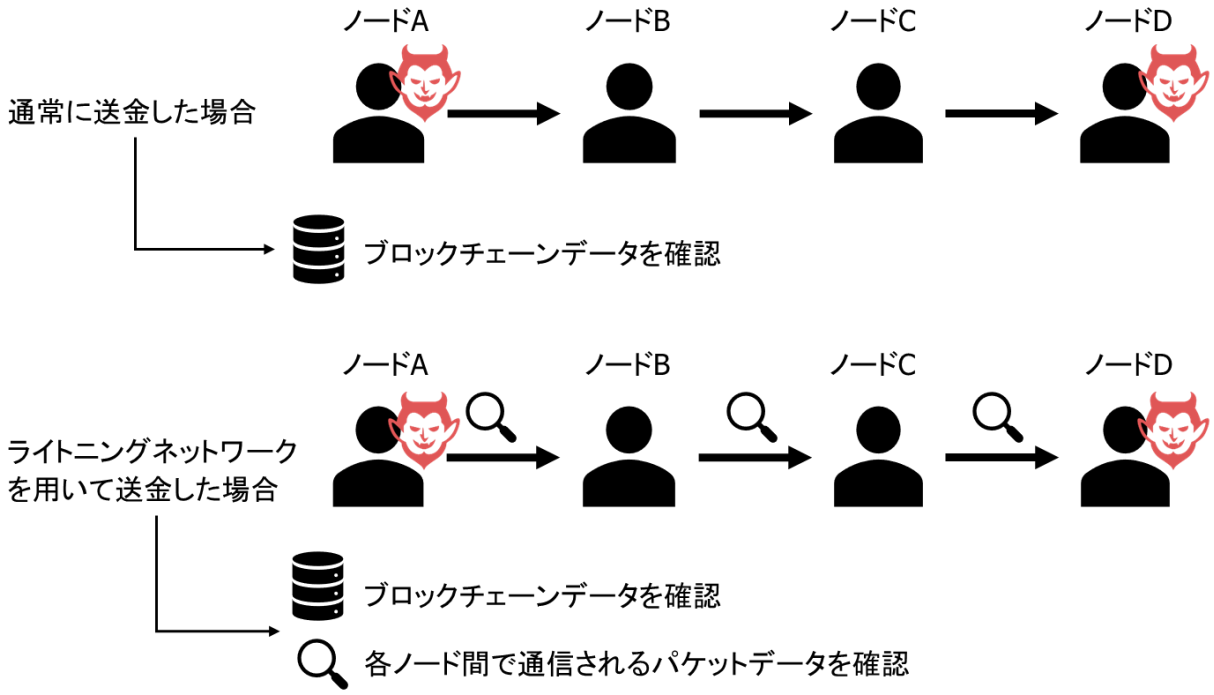
secret.key	secret.nonce	length	length.mac	payload.mac
type.name	type.number	gflen	global_features	lflen
local_features.optional	local_features.required	channel_id	first_timestamp	timestamp_range
chain_hash	temporary_channel_id	funding_satoshis	push_msat	dust_limit_satoshis
max_htlc_value_in_flight_msat	channel_reserve_satoshis	htlc_minimum_msat	minimum_depth	feerate_per_kw
to_self_delay	max_accepted_htlcs	funding_pubkey	revocation_baseponit	payment_baseponit
delayed_payment_basepoint	htlc_basepoint	first_per_commitment_point	channel_flags	funding_txid
funding_output_index	signature.der	next_per_commitment_point	short_channel_id	timestamp
message_flags	cltv_expiry_delta	fee_base_msat	fee_proportional_millionths	node_signature.der
bitcoin_signature.der	node_signature_1.der	node_signature_2.der	bitcoin_signature_1.der	bitcoin_signature_2.der
len	features	node_id_1	node_id_2	bitcoin_key_1
bitcoin_key_2	flen	node_id	rgb_color	alias
addrlen	id	amount_msat	payment_hash	cltv_expiry
onion_routing_packet	num_pong_bytes	byteslen	ignored	num_htlcs
per_commitment_secret	htlc_signature.der	payment_preimage	scriptpubkey	fee_satoshis

4.2.3 実験内容

ノード A からノード B、ノード C を経由して、ノード D へ送金を行う。ここで、ライトニングネットワークを使わずに通常通り送金する場合と、ライトニングネットワークを用いて送金する場合の二パターンを実施した（図表 175）。

ここで、両端のノード A およびノード D は犯行者が管理する場合を想定しており、犯行者が資金洗浄を行って自分自身の他のアドレスへ送金する場合を想定している。

図表 175 実験内容



4.2.4 実験結果

4.2.4.1 通常に送金した場合

ノード A からノード B、ノード C を経由してノード D に 0.000300 BTC (30,000 satoshi)送金した時のブロックチェーンデータ上の送金履歴（図表 176）からは、トランザクション ID（TransactionID 列、From 列）を見ることで、送金元のアドレスから送金先のアドレスを特定することが可能であり、送金経路は図表 177 のように分かる。

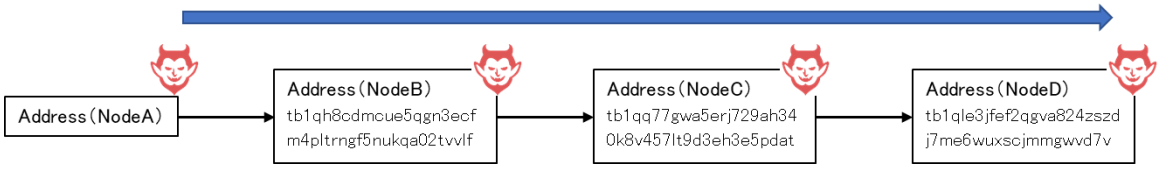
図表 176 ブロックチェーンデータ上の送金履歴（bitcoind を用いた結果）

No	Route	Transaction ID	From (Transaction ID)	To (Address)	Value (BTC) ※手数料除く[426]
1	NodeA → NodeB	fd09b6bf0b5cb3b73df8578f77fc3d3ae6eb3da64e4e37df6dbcb9beeae55eda	99c3aa1c711e9386c9638e4811e92d63e084fd71938d273b051ef98e1952cfc3	tb1qh8cdmcue5qgn3ecfm4pltrngf5nukqa02tvvlf	0.000304

426 手数料のレートは随時変動するが、ここでは手数料を除いて、宛先アドレス（To 列のアドレス）に送金された額を記載している。

2	NodeB → NodeC	62641378ad66ff13ea721644177be24a1c094810bc071d14cc11c8062b9839c1	fd09b6bf0b5cb3b73df8578f77fc3d3ae6eb3da64e4e37df6dbcb9beeae55eda	tb1qq77gwa5erj729ah340k8v457lt9d3eh3e5pdat	0.000302
3	NodeC → NodeD	ae8ee966d4b4bc55aa3dc4d34c001f40d6b72ffcb07b34f37a59541fcdad691f	62641378ad66ff13ea721644177be24a1c094810bc071d14cc11c8062b9839c1	tb1qle3jfef2qgva824zszdj7me6wuxscjmmgwvd7v	0.000300

図表 177 ブロックチェーンデータから分かる送金経路



4.2.4.2 ライトニングネットワーク（c-lightning）を用いて送金した場合

本節では c-lightning を用いた結果を例に、実験結果について記載する。なお、ptarmigan、eclair、LND を用いた実験でも同じ結果が得られた。

4.2.4.2.1 ブロックチェーンデータ上の送金履歴

ノード A からノード B、ノード C を経由してノード D に 0.000300 BTC (30,000 satoshi)送金した時のブロックチェーンデータ上の送金履歴につき[427]、ペイメントチャネルが開いている場合と閉じた場合に分けて記載する。

(i) ペイメントチャネルが開いている場合

ブロックチェーンデータ上の送金履歴（図表 178）からは、ノード A のビットコインは、あるアドレス（実際にはノード A とノード B のマルチシグアドレス）へ送金されたことしか分からない（図表 179）。ここで、ペイメントチャネルを開くのに 0.001 BTC（100,000satoshi）デポジットしている。

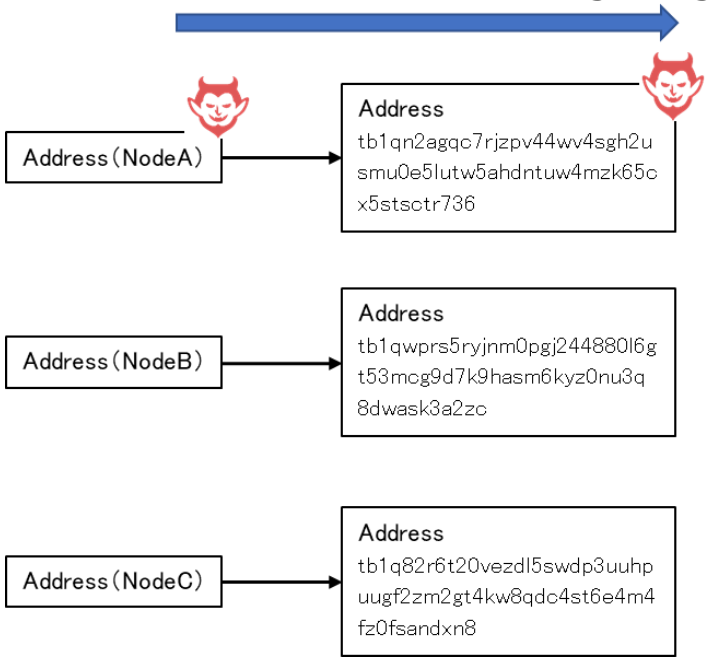
図表 178 ブロックチェーンデータ上の送金履歴（c-lightning を用いた結果）

No	Channel	Route	Transaction ID	From (Transaction ID)	To (Address)	Value (BTC) ※手数料除く
1	NodeA and NodeB Channel Open	NodeA → Script	f80415b238c03346998f2b38552f029cf3a37c1e2401720cb915d7a40cc23b99	4f20c7a9839d3a3f5181809b248dff288bc72bea62358c43703e8f49b01e7d12	tb1qn2agqc7rjzpv44wv4sgh2usmu0e5lutw5ahdntuw4mzk65cx5stsctr736	0.001

427 図表 180 の No9 に記載の通り、c-lightning を用いた場合のみ、0.000300 BTC (30,000 satoshi)を指定したにも関わらず、実際に送金された額は僅かに異なっていた。中継ノードへの手数料の計算等が影響した可能性が考えられる。

2	NodeB and NodeC Channel Open	NodeB → Script	7278f3bfb8f7f6ab8f39829fd4bf2bf66bf199f3d53452e0e9695c3b4e34ad23	3c5d3355f40bb6917a42b2626e313830a3e92dd769ea0d03c7161fa99979bd1b	tb1qwprs5ryjnm0pgj244880l6gt53mcg9d7k9hasm6kyz0nu3q8dwask3a2zc	0.001
3	NodeC and NodeD Channel Open	NodeC → Script	f901fd4a2521b962f500670b05e0df12b87415e7b3a02a7731fdc9c225957aa4	8e2f1c7eb9bd6adb064f9b66aef60f38dc5b306ed3cc8c57e7d1d74c966b1e74	tb1q82r6t20vezdl5swdp3uuhpuugf2zm2gt4kw8qdc4st6e4m4fz0fsandxn8	0.001

図表 179 ブロックチェーンデータから分かる送金経路（c-lightning を用いた結果）



(ii) ペイメントチャネルがクローズされた場合

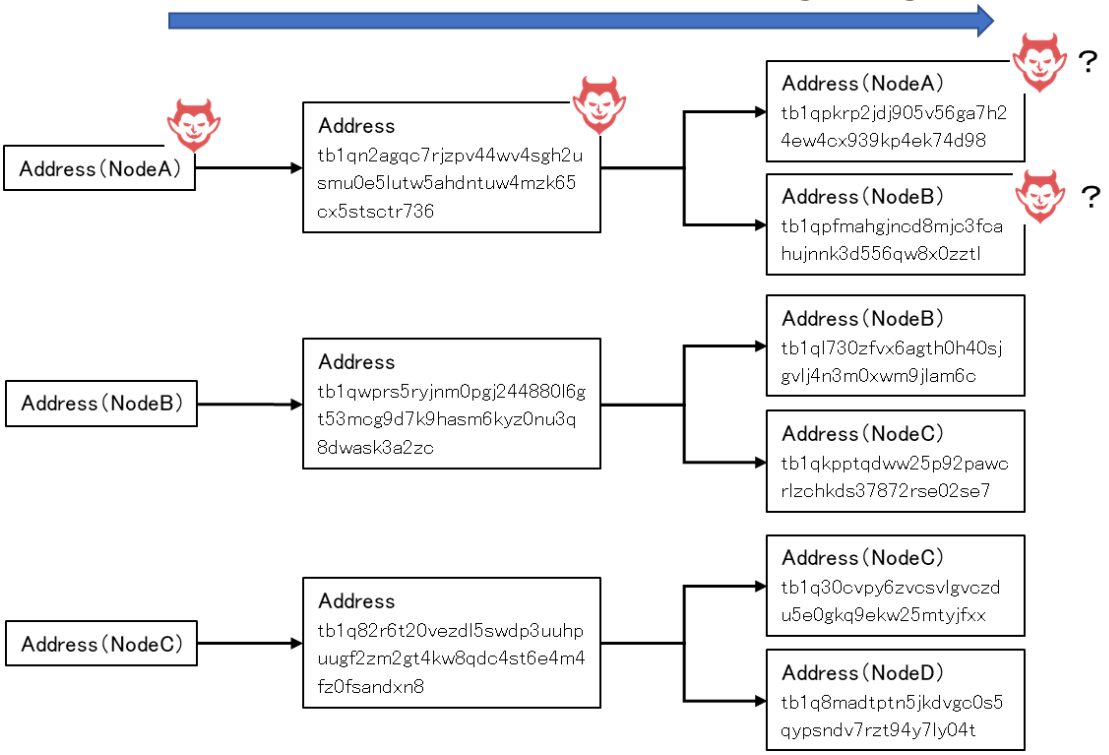
ブロックチェーンデータ上の送金履歴（図表 180）からは、ノード A の BTC は二つに分割して送金されたことしか分からない（図表 181）。

図表 180 ブロックチェーンデータ上の送金履歴（c-lightning を用いた結果）

No	Channel	Route	Transaction ID	From (Transaction ID)	To (Address)	Value (BTC) ※手数料除く
1	NodeA & NodeB Channel Open	NodeA → MutiSig	f80415b238c03346998f2b38552f029cf3a37c1e2401720cb915d7a40cc23b99	4f20c7a9839d3a3f5181809b248dff288bc72bea62358c43703e8f49b01e7d12	tb1qn2agqc7rjzpv44wv4sgh2usmu0e5lutw5ahdntuw4mzk65cx5stsctr736	0.001
2	NodeB & NodeC Channel Open	NodeB → MultiSig	7278f3bfb8f7f6ab8f39829fd4bf2bf66bf199f3d53452e0e9695c3b4e34ad23	3c5d3355f40bb6917a42b2626e313830a3e92dd769ea0d03c7161fa99979bd1b	tb1qwprs5ryjnm0pgj244880l6gt53mcg9d7k9hasm6kyz0nu3q8dwask3a2zc	0.001
3	NodeC & NodeD Channel Open	NodeC → MultiSig	f901fd4a2521b962f500670b05e0df12b87415e7b3a02a7731fdc9c225957aa4	8e2f1c7eb9bd6adb064f9b66aef60f38dc5b306ed3cc8c57e7d1d74c966b1e74	tb1q82r6t20vezdl5swdp3uuhpuugf2zm2gt4kw8qdc4st6e4m4fz0fsandxn8	0.001

4	NodeA & NodeB Channel Close	MultiSig → NodeA	b9a9cccd5da6113a4efc330820e3efb3cf8cdabe461e6d01329d3a2e3c804db4	f80415b238c03346998f2b38552f029cf3a37c1e2401720cb915d7a40cc23b99	tb1qpkrp2jdj905v56ga7h24ew4cx939kp4ek74d98	0.00069747
5		MultiSig → NodeB			tb1qpfmahgjncd8mjc3fcahujnnk3d556qw8x0zztl	0.00030069
6	NodeB & NodeC Channel Close	MultiSig → NodeB	533c7cdef21edbf961c2bf9eb696d664d053938ecc6c2f895c3a629431357357	7278f3bfb8f7f6ab8f39829fd4bf2bf66bf199f3d53452e0e9695c3b4e34ad23	tb1ql730zfvx6agth0h40sjgvlj4n3m0xwm9jlam6c	0.00069748
7		MultiSig → NodeC			tb1qkpptqdww25p92pawcrlzchkds37872rse02se7	0.00030068
8	NodeC & NodeD Channel Close	MultiSig → NodeC	6196b93beb0a9553527b7f9654e0e4b2d9a9e0fb288ec319bc078c76c2bcc9ef	f901fd4a2521b962f500670b05e0df12b87415e7b3a02a7731fdc9c225957aa4	tb1q30cvpy6zvcsvlgvczdu5e0gkq9ekw25mtyjfxx	0.00069748
9		MultiSig → NodeD			tb1q8madtptn5jkdvgc0s5qypsndv7rzt94y7ly04t	0.00030068

図表 181 ブロックチェーンデータから分かる送金経路（c-lightning を用いた結果）



4.2.4.2.2 パケットデータ上の送金履歴

ノード A からノード B、ノード C を経由してノード D に送金した時の各ノード間のパケットデータ上の送金履歴を評価する。

ここで、ライトニングネットワークでは、匿名化されたメッセージを中継するためのプロトコル（Sphinx[428]）をベースとした Onion Routing により経路上のデータは暗号化され、各中継ノードのみが復号鍵を保持する。そのため、以降の節では、暗号化されたままの場合と、復号鍵を用いて復号化された場合に分けて記載する。

(i) 暗号化された状態の場合

各ノード間でペイメントチャネルを開いた際のパケットデータの一部は図表 182 の通りである。ライトニングネットワーク上のパケットデータは暗号化されているため、外部からは、その内容を把握することができない。

図表 182 ライトニングネットワークを用いた場合のパケットデータ（暗号化された状態、c-lightning を用いた結果）

No	Route	tcp.payload
1	NodeA → NodeB	aaa7172631ae79475a4165f287d628dbcb6a0296fe3f9c329025255d19fa91ab1f167f1606aa0ac20337f7c618a11be058d2ac3b161a899f2b3d5e2fac016392e1bf98053e7f929474caddff8aafe4da1c9ab711f33c5cae367e0d9edb694fa0c9c79740f37d78ba42ba331b059a2d22101622268046fe3d21e253139c7578cd69272ccbf1609958dcb4b778794f5224144117210cb48e5d9f0e121a8b2eca3e6a8bacf18d10
2	NodeB → NodeC	ef72fba3f1ddf9d6308d57fde16c7df1c4583e4d085c99aead9493cf10d7765a88e4f5ca9d9524445127eee97ac858b4f1cb165380741fb80e2ebaa2f2f1e76ef8300b4893f74f062909a4ac9c9d7c0264ac1f21e792498ad7ea1f8de58f9aab81257b248f4c8f7d0ba6106386223bbbe0b17ebe84548c34fac7592016465a5d2cff1634fec922e34a053f6e36858c1dcd80ace397d3ddf062b8442a86e7a08ecc5561d820b3
3	NodeC → NodeD	d6b5a2edde00f9d0175d3623c966785b6263715191ac438d0a101af062515567381dbeb524ed96e2c428371e26c04d049ed8b0f1791f5e7ebd4735ba874223115f3a2c7f1e17f3757f9884b19fc2f2ab7813b21e1b712a5d092bbf37b78378fc7540bc008658e55c72bf9161f2ebd36714acd3752b500bd35f0d2f8ccd5661b2961dcd6b70ac161b0596163a21ef2ec12f6c9ab156999e674601635bb0a9aa91a0349f0e47cc
4	NodeD → NodeC	d71d5f5207a16b11791e64e838db391857c5548b8e43590def1243d3af0ab16efb4a5419679acd37daee5052a8d362132ff17c66dea5705f14d02e6c170a5ad826937986124ff4cedb47f4656fb891c267dc3362c7e67deb1e7324098c8156896f97df848cee73c15ec7eedbd0da5c3bca3f0e8dff466d350a4356f331d67d80f09fd184
5	NodeC → NodeB	4d26ab1b4ae23c8d11c7491795fed9e03871b3c713b01ab730a80eb344beb989a4f4d9c875ac322e1e461e1e0f81a8b48f04b69b3b763cf9e2019f6ee4b95e92f09ae5d1306c14aaf809fca6920d3cce9094f8c4a01a9e2a6efdf827df55e25d30d3e7c250de3826b82af13eaa11dc5aac7cdc8edeab45f270a8a826bc03221984a9e183
6	NodeB → NodeA	f9c1f1e8782bfe15052812e6a4eaec03ad433f35b54bc5adf3e668c8e1480ea8123070a6c8b66581cfb92f4c817b287add26792462bff3ec70c4c721212e9413b6cafb480fbc80de718e841a14be70b35019ab7c5afbf88efe0a0b2ea90489c0b068c455ca3007e2b1923f41eeccc44f21b6d11329808ff10c5a74e39cb55fff28215961

(ii) 復号化された状態の場合

中継ノードであるノード B およびノード C それぞれの復号鍵を用いて復元した結果は図表 183 の通りである。パケットデータに含まれるハッシュ値（payment_hash 列）ないしシークレット（payment_preimage 列）をみて、ブロックチェーンデータと組合せ

428 Denezis, G., et al., "Sphinx: A Compact and Provably Secure Mix Format", http://www.cypherpunks.ca/~iang/pubs/Sphinx_Oakland09.pdf, 2019/1/17

て評価すると送金経路を特定することができる[429]（図表 184）。

図表 183 ライトニングネットワークを用いた場合のパケットデータ（復号化された状態、c-lightning を用いた結果）[430,431]

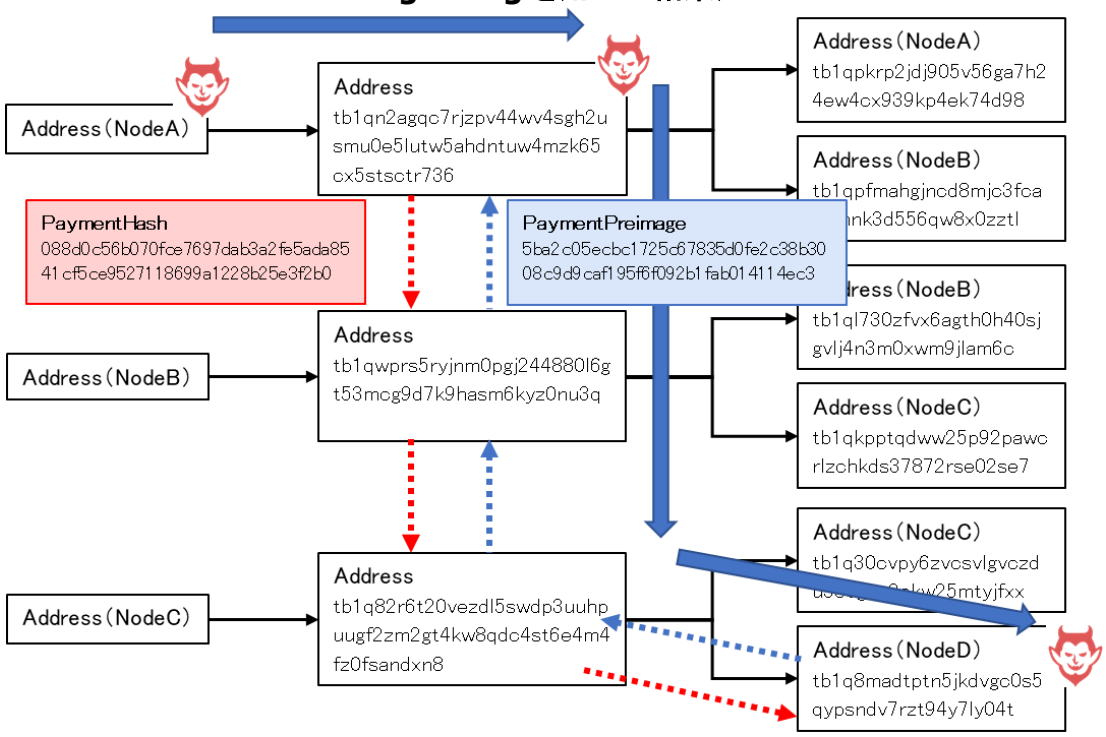
No	Route	channel_id	funding_txid	onion_routing_packet（byte）	payment_hash	payment_preimage
1	NodeA → NodeB	993bc20ca4d715b90c7201241e7ca3f39c022f55382b8f994633c038b21504f8	993bc20ca4d715b90c7201241e7ca3f39c022f55382b8f994633c038b21504f8	1366	088d0c56b070fce7697dab3a2fe5ada8541cf5ce9527118699a1228b25e3f2b0	N/A
2	NodeB → NodeC	23ad344e3b5c69e9e05234d5f399f16bf62bbfd49f823988fabf6f7b8bff37872	23ad344e3b5c69e9e05234d5f399f16bf62bbfd49f823988fabf6f7b8bff37872	1366	088d0c56b070fce7697dab3a2fe5ada8541cf5ce9527118699a1228b25e3f2b0	N/A
3	NodeC → NodeD	a47a9525c2c9fd31772aa0b3e71574b812dfe0050b6700f562b921254afd01f9	a47a9525c2c9fd31772aa0b3e71574b812dfe0050b6700f562b921254afd01f9	1366	088d0c56b070fce7697dab3a2fe5ada8541cf5ce9527118699a1228b25e3f2b0	N/A
4	NodeD → NodeC	a47a9525c2c9fd31772aa0b3e71574b812dfe0050b6700f562b921254afd01f9	N/A	N/A	N/A	5ba2c05ecbc1725c67835d0fe2c38b3008c9d9caf195f6f092b1fab014114ec3
5	NodeC → NodeB	23ad344e3b5c69e9e05234d5f399f16bf62bbfd49f823988fabf6f7b8bff37872	N/A	N/A	N/A	5ba2c05ecbc1725c67835d0fe2c38b3008c9d9caf195f6f092b1fab014114ec3
6	NodeB → NodeA	993bc20ca4d715b90c7201241e7ca3f39c022f55382b8f994633c038b21504f8	N/A	N/A	N/A	5ba2c05ecbc1725c67835d0fe2c38b3008c9d9caf195f6f092b1fab014114ec3

429 図表 183 の「funding_txid」列は、図表 178 や図表 180 の「Transaction ID」列の値をバイト反転させた値となっている。これは歴史的な経緯から、ビットコインではバイト反転させた値を用いているからである。Greg, learnmeabitcoin.com, learn me a bitcoin, "TXID", http://learnmeabitcoin.com/glossary/txid, 2019/3/18

430 ルーティング情報である onion_routing_packet はデータサイズが非常に大きく、また暗号化されているため、ここではデータサイズ（バイト数）のみを記載している。

431 チャネル ID（channel_id）とペイメントチャネルを開く際にデポジットしたトランザクションの ID（funding_txid）は必ず一致するものではない。これは channel_id が、funding_txid とデポジットに用いたトランザクションの順番（funding_output_index）の排他的論理和で生成されるためである。そのため、保有しているビットコインを全てデポジットに用いる場合は、channel_id と funding_txid は一致するが、保有しているビットコインの一部のみを用いる場合は両者が異なる場合が生じる。channel_id の詳細な仕様は以下を参照のこと。
lightning-rfc, Github, "BOLT #2: Peer Protocol for Channel Management", https://github.com/lightningnetwork/lightning-rfc/blob/8516beb2c4fe6fc19bb4b1824b1635ae13805f49/02-peer-protocol.md#the-funding_signed-message, 2019/2/12

図表 184 パケットデータとブロックチェーンデータから分かる送金経路（c-lightning を用いた結果）



4.2.4.3 その他のライトニングネットワークを用いて送金した場合

本節では、ptarmigan、eclair、LND を用いた実験結果について記載する。実験結果は c-lightning の場合と全く同様であるので、ブロックチェーンデータ上の送金履歴およびパケットデータ上の送金履歴の結果のみを記載する。

4.2.4.3.1 ptarmigan の場合

ブロックチェーンデータ上の送金履歴を図表 185、パケットデータ上の送金履歴を図表 186 に記載する。

図表 185 ブロックチェーンデータ上の送金履歴（ptarmigan を用いた結果）

No	Channel	Route	Transaction ID	From (Transaction ID)	To (Address)	Value (BTC) ※手数料除く
1	NodeA & NodeB Channel Open	NodeA → MutiSig	665b54d58328150db3b6b4e67de012fa4331889a1100ccc89d911d612f545a75	0431d7a88fb982e841f29e95baf4b025d55034b7f0fe46a22e44bc322af4f550	tb1qrhuhdgx4vv3g9yqjkjwnyl2txukdtmlt6sn0x6cuylfnz6tfwljq7k96ha	0.001
2	NodeB & NodeC Channel Open	NodeB → MultiSig	93d756833de7d10ddbbf234ef6ceaa56f90fa11f2434641bd738ea197594cea8	f4a9d730817d53b4d373a7aecd70b644dfb413fced81100437eff1488fc24393	tb1qljrlm553pw038w6s3kdszgjulmxy9ktvlr78h0pz7m998ellgwuq4mtlpv	0.001

3	NodeC & NodeD Channel Open	NodeC → MultiSig	a42a773aa29497af444b8ade314d4cf3fcee9509bed6d33937f58c1da46fb544	6a4c675606e341cec1236bb5ca2e98fc08e75037bffe6e83285759ca2ac0f6a9	tb1qdhk80rdn8y2pzrqtgvvgpvlq9a07er0ve4p8xctqp9ex4l0gz0gq454k9r	0.001
4	NodeA & NodeB Channel Close	MultiSig → NodeA	2d6412b67505800de802cc78462d149f4c89e1a10e55f919b210a9b2a1f9d489	665b54d58328150db3b6b4e67de012fa4331889a1100ccc89d911d612f545a75	2MwNWtr4KEoN6Let8F1sfLcUoXjaJCeTxqK	0.0006981
5		MultiSig → NodeB			2MsJ6fjnyXSuQN8GNzcZfZLdKxfASCCQkpW	0.00030006
6	NodeB & NodeC Channel Close	MultiSig → NodeB	81b3a2ae0a2cd01d350b1f624d49f78fe3f1994227a017b49f09254553750da1	93d756833de7d10ddbbf234ef6ceaa56f90fa11f2434641bd738ea197594cea8	2MskQPPfnsP14GJS4nnVwDEHbbZQr1neBCj	0.00069813
7		MultiSig → NodeC			2NFeH8R3hqVBu9JaQiYgPJrd2PT9uN4ibKt	0.00030003
8	NodeC & NodeD Channel Close	MultiSig → NodeC	3f8d13b350a94695d3e7c6ec57aada55e7e8a42fabe9ffe1284b130a9669951c	a42a773aa29497af444b8ade314d4cf3fcee9509bed6d33937f58c1da46fb544	2N1g8FHM3bzRQxX9FVE1ptrE8LJueAbKvxf	0.00069817
9		MultiSig → NodeD			2MvVZYsXuUTzvdDyFPNQxWZeG1ZdVF6ZDa9	0.0003

図表 186 ライトニングネットワークを用いた場合のパケットデータ（復号化された状態、ptarmigan を用いた結果）

No	Route	channel_id	funding_txid	onion_routing_packet（byte）	payment_hash	payment_preimage
1	NodeA → NodeB	755a542f611d919dc8cc00119a883143fa12e07de6b4b6b30d152883d5545b66	755a542f611d919dc8cc00119a883143fa12e07de6b4b6b30d152883d5545b66	1366	309ed207d4ef8c1a998e27363c62e2912dc96f71fe69cacfd3429a1da78dcdab	N/A
2	NodeB → NodeC	a8ce947519ea38d71b6434241fa10ff956aacef64e23bfdb0dd1e73d8356d793	a8ce947519ea38d71b6434241fa10ff956aacef64e23bfdb0dd1e73d8356d793	1366	309ed207d4ef8c1a998e27363c62e2912dc96f71fe69cacfd3429a1da78dcdab	N/A
3	NodeC → NodeD	44b56fa41d8cf53739d3d6be0995eefcf34c4d31de8a4b44af9794a23a772aa4	44b56fa41d8cf53739d3d6be0995eefcf34c4d31de8a4b44af9794a23a772aa4	1366	309ed207d4ef8c1a998e27363c62e2912dc96f71fe69cacfd3429a1da78dcdab	N/A
4	NodeD → NodeC	44b56fa41d8cf53739d3d6be0995eefcf34c4d31de8a4b44af9794a23a772aa4	N/A	N/A	N/A	f50bd34249bc73502846b6d126fd1090c1eb1f3c30d1787b48d66c9e4bfc53ff
5	NodeC → NodeB	a8ce947519ea38d71b6434241fa10ff956aacef64e23bfdb0dd1e73d8356d793	N/A	N/A	N/A	f50bd34249bc73502846b6d126fd1090c1eb1f3c30d1787b48d66c9e4bfc53ff

6	NodeB → NodeA	755a542f611d919dc8cc00119a883143fa12e07de6b4b6b30d152883d5545b66	N/A	N/A	N/A	f50bd34249bc73502846b6d126fd1090c1eb1f3c30d1787b48d66c9e4bfc53ff

4.2.4.3.2 eclair の場合

ブロックチェーンデータ上の送金履歴を図表 187、パケットデータ上の送金履歴を図表 188 に記載する。

図表 187 ブロックチェーンデータ上の送金履歴（eclair を用いた結果）

No	Channel	Route	Transaction ID	From (Transaction ID)	To (Address)	Value (BTC) ※手数料除く
1	NodeA & NodeB Channel Open	NodeA → MutiSig	7249c2530688e9383992795f147f05dc378cfdfce9b307d0e1b57518aadf0dee	d3250a22aa57fd5c6057e04563e0604ade087a6fdcffb0ea9c402e766f6fbac9	tb1qhx57v3utqn7w9y9ls005r9fr3xksfs6xl4f7635chfgvcj9gnahqgq47ww	0.001
2	NodeB & NodeC Channel Open	NodeB → MultiSig	a95365545a6d4a3c6c9047c43677cad526e57f883bd49256b045da2a7f953c38	b013e6537e960aaa6feb60c206e0d44ccfaa71dd7e3fae822cb6f57f7fb02e2a	tb1q6gv43s5vd8lwvm0pv3ul6vjw7nm97ckg7m3dkxgaryugsku0fjws2wygzz	0.001
3	NodeC & NodeD Channel Open	NodeC → MultiSig	d9110a431d992c28a795d6a64265314597e8d05fc95330cc116191a99ca43e2c	d3250a22aa57fd5c6057e04563e0604ade087a6fdcffb0ea9c402e766f6fbac9	tb1qm7txqhxny405xc4kxcscjdgqn5yzppl6am50872zj75pm7xplvqq82ya5s	0.001
4	NodeA & NodeB Channel Close	MultiSig → NodeA	223e29409faf84c89ebb414baffe7df32ee5088b73118ac741f9c9f5e737bafd	7249c2530688e9383992795f147f05dc378cfdfce9b307d0e1b57518aadf0dee	2MtPyqPH5cZkXU5JjhkByCPr8jNM3PsXpUB	0.00069652
5		MultiSig → NodeB			2MvypqgdXetcUPukF8sqJ1D6ue64DDp7KFX	0.00030008
6	NodeB & NodeC Channel Close	MultiSig → NodeB	002edd56d0ad18adeca9aed67c4c3d0a7361cccb256515b7f9a8d4154cfd25a3	a95365545a6d4a3c6c9047c43677cad526e57f883bd49256b045da2a7f953c38	2N5joDFvE8XFTWNW1mhXeoCnYr8gYN7Ytvc	0.00069656
7		MultiSig → NodeC			2NArPC7XRFFXV3rwsib77Sysak4rfRhcZaP	0.00030004
8	NodeC & NodeD Channel Close	MultiSig → NodeC	ae6dbd1f6827c557d6a63d1eee28bc6d7e0a5e936842e2f21fce0908d0fed912	d9110a431d992c28a795d6a64265314597e8d05fc95330cc116191a99ca43e2c	2N2qAP4BiSLC7323ds7qXhN6aPncgw9sDAu	0.0006966
9		MultiSig → NodeD			2NCn3Bu66n2qVAtHEt4hGznBxdHYhHWGJCy	0.0003

図表 188 ライトニングネットワークを用いた場合のパケットデータ（復号化された状態、eclair を用いた結果）

No	Route	channel_id	funding_txid	onion_routing_packet（byte）	payment_hash	payment_preimage
1	NodeA → NodeB	ee0ddfaa1875b5e1d007b3e9fcfd8c37dc057f145f79923938e9880653c24972	ee0ddfaa1875b5e1d007b3e9fcfd8c37dc057f145f79923938e9880653c24972	1366	a51f7716acce5ea5aed984ef976d004989c77b0ef2d1e58791d94bf1fea93810	N/A
2	NodeB → NodeC	383c957f2ada45b05692d43b887fe526d5ca7736c447906c3c4a6d5a54565 53a9	383c957f2ada45b05692d43b887fe526d5ca7736c447906c3c4a6d5a54565 53a9	1366	a51f7716acce5ea5aed984ef976d004989c77b0ef2d1e58791d94bf1fea93810	N/A
3	NodeC → NodeD	2c3ea49ca9916111cc3053c95fd0e89745316542a6d695a7282c991d430a11d9	2c3ea49ca9916111cc3053c95fd0e89745316542a6d695a7282c991d430a11d9	1366	a51f7716acce5ea5aed984ef976d004989c77b0ef2d1e58791d94bf1fea93810	N/A
4	NodeD → NodeC	2c3ea49ca9916111cc3053c95fd0e89745316542a6d695a7282c991d430a11d9	N/A	N/A	N/A	01b2ed7e670165f4307b04e492b160e8b643bc2ca8e95d65504427ba0197e448
5	NodeC → NodeB	383c957f2ada45b05692d43b887fe526d5ca7736c447906c3c4a6d5a54565 53a9	N/A	N/A	N/A	01b2ed7e670165f4307b04e492b160e8b643bc2ca8e95d65504427ba0197e448
6	NodeB → NodeA	ee0ddfaa1875b5e1d007b3e9fcfd8c37dc057f145f79923938e9880653c24972	N/A	N/A	N/A	01b2ed7e670165f4307b04e492b160e8b643bc2ca8e95d65504427ba0197e448

4.2.4.3.3 LND の場合

ブロックチェーンデータ上の送金履歴を図表 189、パケットデータ上の送金履歴を図表 190 に記載する。

図表 189 ブロックチェーンデータ上の送金履歴（LND を用いた結果）

No	Channel	Route	Transaction ID	From (Transaction ID)	To (Address)	Value (BTC) ※手数料除く
1	NodeA & NodeB Channel Open	NodeA → MutiSig	f015fab26d8fc191c98543ce6e9ea91b5f105c26bc27c18c49a13eeeca9ea782	c746278fd5e5c0ab19c06e4ef066dc4baea30ade85162203227c7dc84b0cb1b5	tb1qzl8fchrkxc2rzxr3q3aluwfaw7fpa53gynhdul0tsn4geeyc2ttsur8l2p	0.001
2	NodeB & NodeC Channel Open	NodeB → MultiSig	ed3ecc0c25f48e16e479cda057a5a7443ea2491e69c642687c781de4d6bb139a	13cf0151dfe9addd878c569706591036f44d5b1f3fd4bd566054d4cabbfd179c	tb1q9wws8wzd8gzzps2n673jxuzmg2zhydsg4ce3khl6cyd4kdfq2hxsuwd6jw	0.001

3	NodeC & NodeD Channel Open	NodeC → MultiSig	8667f0e8adc182315012e5e875a73eadf48579c8b5e31148614b8417ce75c274	c9133ab8e43893ab668da2086fc89e08f9772af5951657e55c11479ce34ae704	tb1qrffqngefx96xddwfuc6ljdljp6q97zk0uy9479jlauep5dulje8sqfns4j	0.001
4	NodeA & NodeB Channel Close	MultiSig → NodeA	c45fc49c96320bf57c2dd8cbd4440233e0b525bdb6bcee0fac01d396fe7e7796	f015fab26d8fc191c98543ce6e9ea91b5f105c26bc27c18c49a13eeeca9ea782	tb1qafekgn28pfvlrt9jetjtuucyc7e30muxmpxdx3	0.00069814
5		MultiSig → NodeB			tb1qlv442w3gqakuq29tz3vfpham3kez0c32dzndf8	0.00030002
6	NodeB & NodeC Channel Close	MultiSig → NodeB	0a817a6617a29c2b7508f672946964ca0d5a0a3bb162635e427ff776f9559e89	ed3ecc0c25f48e16e479cda057a5a7443ea2491e69c642687c781de4d6bb139a	tb1qhy7j4fr0naxvq2wgc2sjxyr0pcgt29c6saekau	0.00069815
7		MultiSig → NodeC			tb1q8jaw93hvhzrum0gv4u922mdzduw0dpwmf8mmhk	0.00030001
8	NodeC & NodeD Channel Close	MultiSig → NodeC	05e680f2cfee3cee970875146d238a48212b2a07de07386ecb361ff45bf244f2	8667f0e8adc182315012e5e875a73eadf48579c8b5e31148614b8417ce75c274	tb1qtcrs35jeafy8y9eqhr7ucu37zmqa0sw8tm0djc	0.00069817
9		MultiSig → NodeD			tb1q3vy9fp5l0fgsyxmtyjsw780plqmu3mg8tsc3ww	0.0003

図表 190 ライトニングネットワークを用いた場合のパケットデータ（復号化された状態、LND を用いた結果）

No	Route	channel_id	funding_txid	onion_routing_packet（byte）	payment_hash	payment_preimage
1	NodeA → NodeB	82a79ecaee3ea1498cc127bc265c105f1ba99e6ece4385c991c18f6db2fa15f0	82a79ecaee3ea1498cc127bc265c105f1ba99e6ece4385c991c18f6db2fa15f0	1366	b23a34f73a0d52e3228e7acdd4689faa8e20edb2b9fce607e756b02f52afa8c9	N/A
2	NodeB → NodeC	9a13bbd6e41d787c6842c6691e49a23e44a7a557a0cd79e4168ef4250ccc3eed	9a13bbd6e41d787c6842c6691e49a23e44a7a557a0cd79e4168ef4250ccc3eed	1366	b23a34f73a0d52e3228e7acdd4689faa8e20edb2b9fce607e756b02f52afa8c9	N/A
3	NodeC → NodeD	74c275ce17844b614811e3b5c87985f4ad3ea775e8e512503182c1ade8f06786	74c275ce17844b614811e3b5c87985f4ad3ea775e8e512503182c1ade8f06786	1366	b23a34f73a0d52e3228e7acdd4689faa8e20edb2b9fce607e756b02f52afa8c9	N/A
4	NodeD → NodeC	74c275ce17844b614811e3b5c87985f4ad3ea775e8e512503182c1ade8f06786	N/A	N/A	N/A	e311a06f4165d4ab6e109f9fcdd9306e7c943ae9ff04e71fa1b675734217c69e
5	NodeC → NodeB	9a13bbd6e41d787c6842c6691e49a23e44a7a557a0cd79e4168ef4250ccc3eed	N/A	N/A	N/A	e311a06f4165d4ab6e109f9fcdd9306e7c943ae9ff04e71fa1b675734217c69e

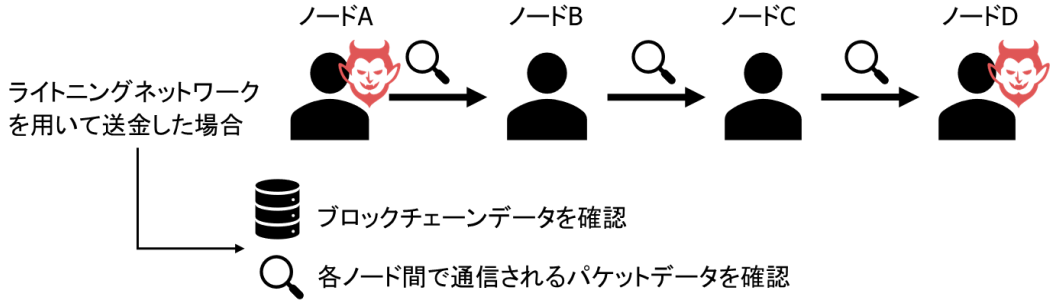
6	NodeB → NodeA	82a79ecaee3ea1498cc127bc265c105f1ba99e6ece4385c991c18f6db2fa15f0	N/A	N/A	N/A	e311a06f4165d4ab6e109f9fcdd9306e7c943ae9ff04e71fa1b675734217c69e

4.2.5 考察

4.2.5.1 匿名化の度合い

犯行者が、不正に得たコインを、自身の保持するノード A から、第三者のノード B、ノード C を経由して、再び自身の保持するノード D へ送金を行う場合の匿名化の度合いについて考察する。ここで、通常通り送金する場合、送金経路は容易に特定可能であるため、以下ではライトニングネットワークを用いた場合について記載する（図表 191）。

図表 191 ライトニングネットワークを用いた送金のイメージ



4.2.5.1.1 ブロックチェーンデータからみた匿名化の度合い

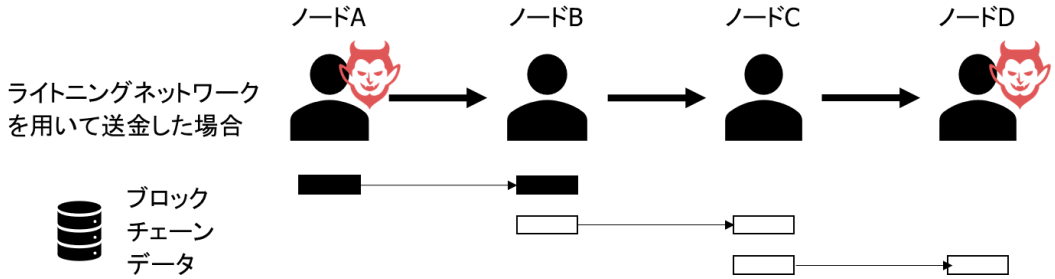
ノード A に着目した場合、ブロックチェーンデータから取得できるのは、以下の送金経路である。

- ノード A･B 間のファンディングトランザクションの経路（ノード A からノード A･B 間のファンディングアドレスへの送金経路）
- ノード A･B 間のクロージングトランザクションの経路（ノード A･B 間のファンディングアドレスからノード A･B それぞれのアドレスへの送金経路）

中継ノード B･C は、A から送金されたコインではなく、それぞれ自身が既に保持しているコインを用いて送金する。そのため、ノード A から、中継ノード B･C を経て、ノード D へ至る、一連の送金経路はブロックチェーンデータからは把握することができない（図表 192）。

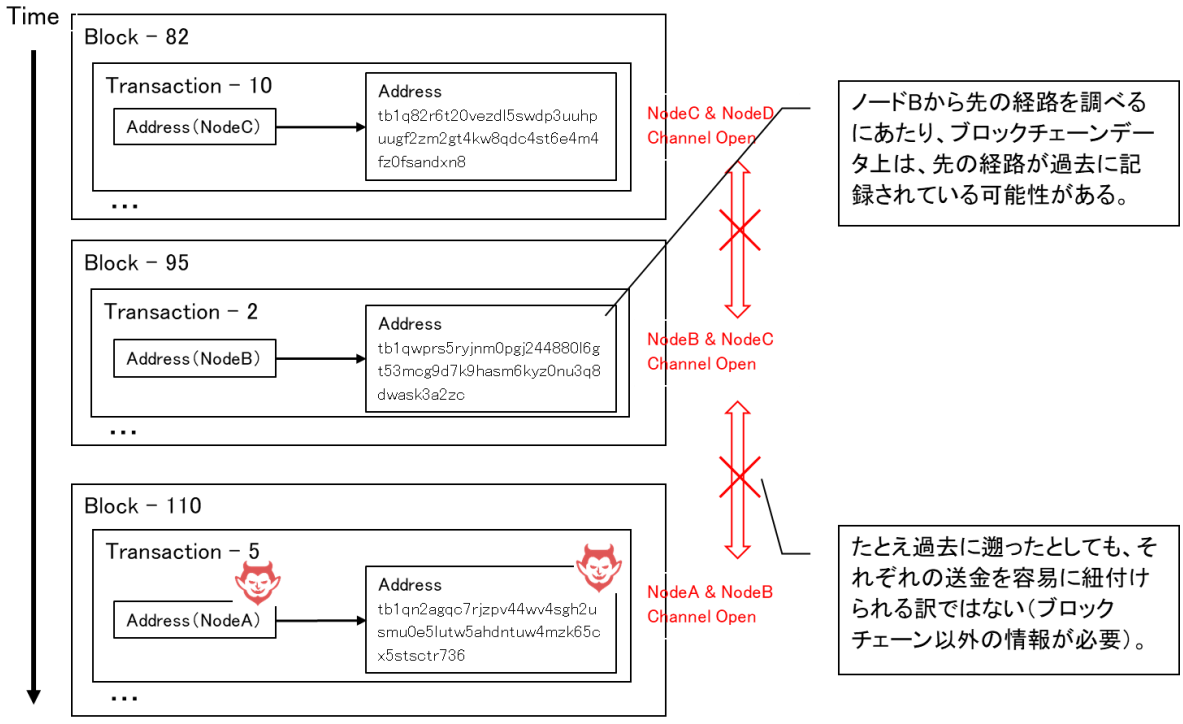
ライトニングネットワークを用いたこのような資金洗浄方法は、本質的には、第三者に不正なコインを送金し、代わりに同額を第三者から送金してもらう、ということで成り立つ。そのため、資金洗浄を行うためには、必ず第三者をいずれかの中継ノードに含めることが必要となる。

図表 192 ライトニングネットワークを用いた送金のイメージ



ブロックチェーン上のデータでは、ファンディングトランザクションやクロージングトランザクションが唯一の手がかりとなるが、各ペイメントチャネルのオープン・クローズは任意のタイミングで行える。そのため、ノード B から先の送金経路を調査しようとする場合は、時系列的に過去に遡って取引を調査する必要も生じる（図表 193）。また、ノード A・B 間のファンディングトランザクションとノード B・C 間のファンディングトランザクションを紐付ける情報はブロックチェーンデータにはないため、過去に遡っても、あくまで送金経路の候補が得られるに留まる。

図表 193 ブロックチェーンデータ上での送金経路探索イメージ

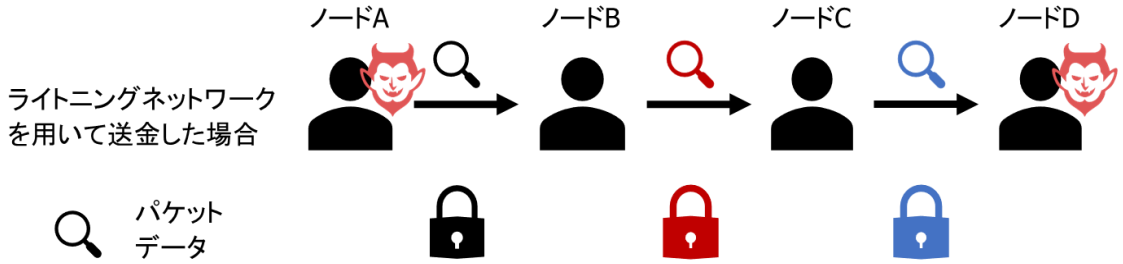


4.2.5.1.2 パケットデータからみた匿名化の度合い

送金情報や経路情報を格納したパケットデータは BOLT((Basis of Lightning Technology)にしたがい暗号化されているため[432]、経路上の情報を見ても第三者がその内容を把握することはできない(図表 194)。

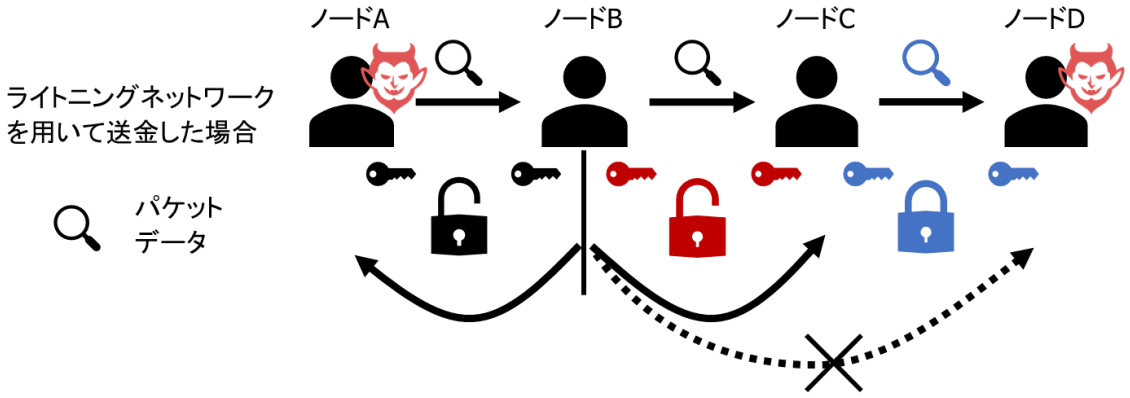
また、送金経路情報を格納したパケットのデータサイズはどのノード間でも一定であるため、パケットデータのサイズなどから終端ノードを推測することもできない。

図表 194 経路上のパケットデータのイメージ



各中継ノードは暗号データの複合鍵を保持しているものの、復号化した内容から得られる情報は限定的である。すなわち、ノード A からノード D までの全体の送金経路は起点となる送金元のノード A によって決定されており、中継ノードが把握できるのは前後 1 ホップのノードの情報、送金額、手数料、シークレット、ハッシュ値等の情報に限られる(図表 195)。そのため、各中継ノードだけでは、起点となる送金元と終点となる受取先を特定することはできない。

図表 195 中継ノード B が把握できる範囲のイメージ



以上より、ライトニングネットワークが資金洗浄に用いられた場合、送金経路の特

432 ライトニングネットワークでは Onion Routing が定義されている。詳しい仕様は次を参照:lightningnetwork, "BOLT #4: Onion Routing Protocol", https://github.com/lightningnetwork/lightning-rfc/blob/master/04-onion-routing.md, 2019/1/7

定は極めて困難であり、匿名性は高いと考えられる。

4.2.5.1.3 （参考）犯行にあたっての制約条件

二者間のペイメントチャネルで一度に送金可能な額は、そのペイメントチャネルにデポジットした金額以下という制約がある。そのため、複数のペイメントチャネルを組合せた場合、一度に送金可能な額は全てのペイメントチャネルのデポジット額の最小値となる。ここで、ライトニングネットワーク上のペイメントチャネルの平均デポジット額は 0.026BTC（約 1 万円）[433]ほどである。

そのため、多額の資金を送金するには、資金を小額に分割した上で、多数のチャネルを用意し分散して送金する必要がある。ただし、この点に関しては、今後の機能追加により、複数の経路を組合せた送金を可能にする Atomic Multipath Payments などが導入されると解消されると見込まれる。

4.2.5.2 再識別方法

送金経路の再識別にあたっては、全ての中継ノードを押さえるか、全てのネットワークを監視する必要があると考えられる（図表 196）。

- 全ての中継ノードを押さえる場合

  経路上では共通のハッシュ値やシークレットに基づいて、ノード A からノード D までの送金経路を特定することが可能である。ただし、特定にあたっては、各中継ノードがライトニングネットワーク上のあらゆるデータ（送金情報や経路情報）を保持していることが前提である[434]。

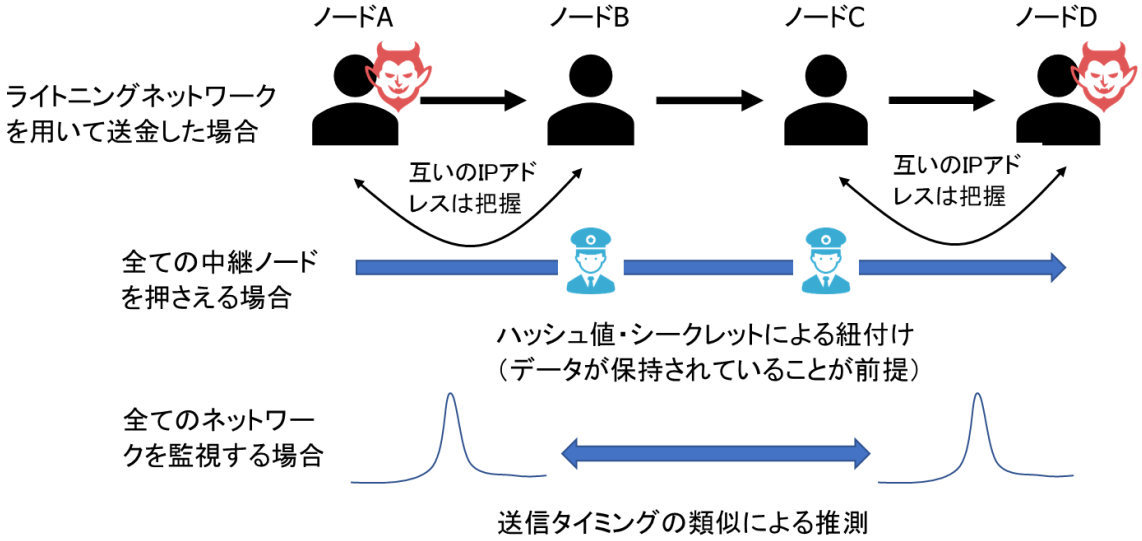
- 全てのネットワークを監視する場合

  ノード A・B 間でやり取りされるパケットデータの送信タイミングとノード C・D 間のパケットデータのタイミングを見て、両者を紐付ける推測が可能である。

433 2019 年 1 月 18 日現在。1ML.com, "Real-Time Lightning Network Statistics", https://1ml.com/statistics, 2019/1/18

434 今回用いた c-lightning などの実装では、復号鍵をメモリ上で保持しておき、ペイメントチャネルをクローズする際に廃棄する形となっていた。そのため、実験では、中継ノードが明示的にデータを残すようにパッチをあてる、ビルドし直すなどの処理を行う必要があった。

図表 196 再識別方法のイメージ



その他にも、ライトニングネットワークではペイメントチャネルを開く際に、以下の情報を公開するか否かを選択できる。

- ノード情報

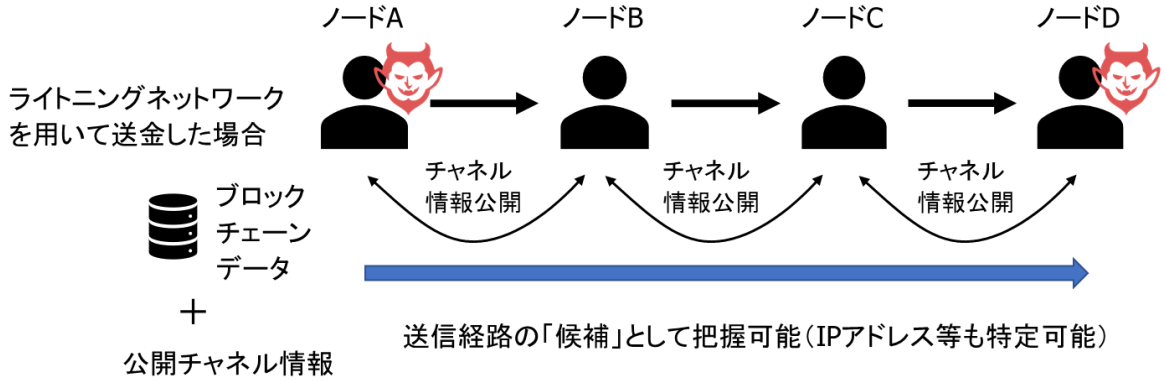
  各ノードは node_announcement メッセージを介して自身のノードの略称名（エイリアス名）や IP アドレス等を公開することが可能である。外部からの接続を受け入れる場合は自身のノード情報を公開する必要がある。

- チャネル情報

  各チャネルの情報は channel_announcement メッセージを介して公開することができ、このメッセージを用いて channel_update メッセージで手数料や有効期間を通知することができる。

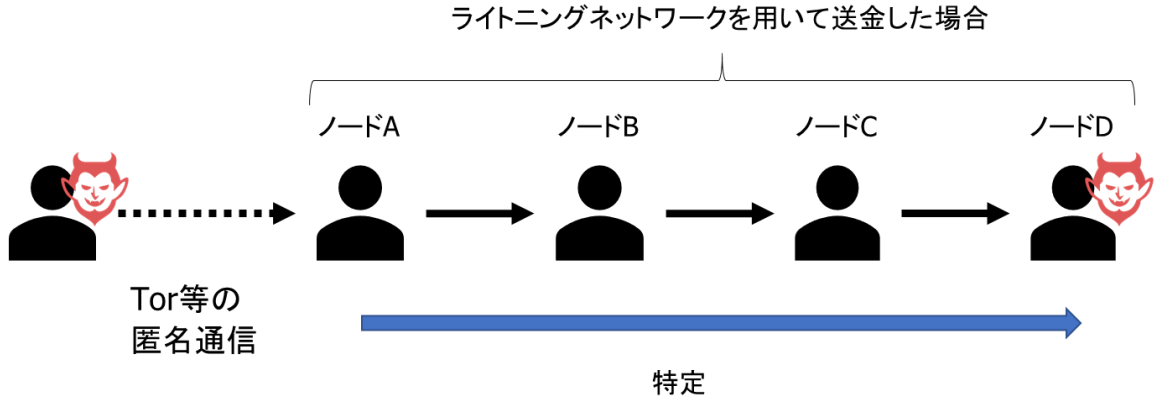
そのため、全てのペイメントチャネルが公開されていた場合、ノード間のファンディングトランザクションを紐付けることが可能となり、ブロックチェーンデータから送金経路の候補を調べることが可能となる（図表 197）。ただし、各中継ノードでペイメントチャネルが複数開かれている場合、どの組合せが実際に使われたかまでは分からないため、送金経路を「特定」するまでには至らない点に留意が必要である。

図表 197 公開チャネル情報を用いた再識別方法のイメージ



なお、上記のいずれの場合においても、ノード A が Tor の出口ノード等の場合は起点となる送金元を特定することは極めて困難となる（図表 198）。

図表 198 匿名通信とライトニングネットワークを組合せたイメージ



4.2.5.3 その他の匿名性の向上手法

再識別手法を踏まえて、犯行者がさらに匿名性を向上させるその他の手法について記載する。

4.2.5.3.1 経路長を長くすることによる匿名性の向上

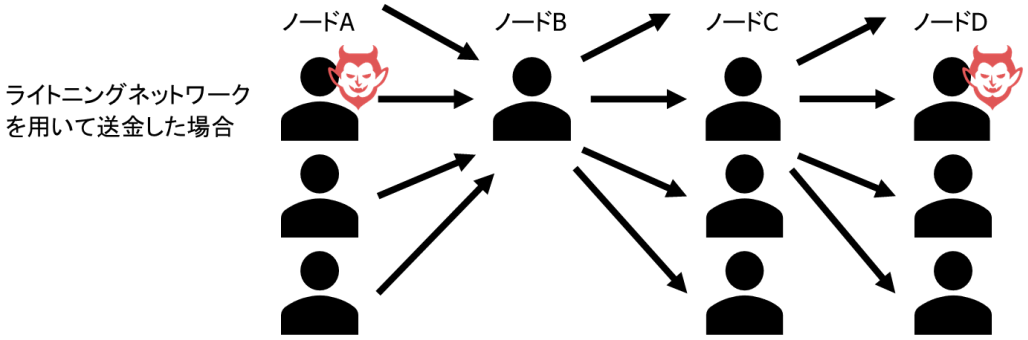
決済を中継する中継ノードの数が多いほど、再識別する際に押さえる先が増えることになり、匿名性が向上すると考えられる。

4.2.5.3.2 ミキシングによる匿名性の向上

中継ノードとして、多数のペイメントチャネルを持つハブとなっているノードを経由すると、ミキシングサービスと同様に複数のペイメントチャネルをプーリングすることになるため、匿名性が向上すると考えられる（図表 199）。図表 199 では、ノード B が多数

のペイメントチャネルを保持しているため、第三者が、その中からノード A→ノード B→ノード C という組合せを特定するのは極めて難しいと考えられる。

図表 199 中継ノードによるミキシング効果のイメージ



4.2.5.3.3 ハッシュ値やシークレットを置き換えることによる匿名性の向上

同一経路上で、異なるハッシュ値やシークレットを用いることにより、送金経路の特定を極めて困難にすることが可能である（図表 200）。現在までに、大きく以下の二通りの手法が提案されている。両者ともに本稿執筆時点までにライトニングネットワークにはまだ実装されていないが、これらを導入したライトニングネットワークも今後現れてくると考えられる。

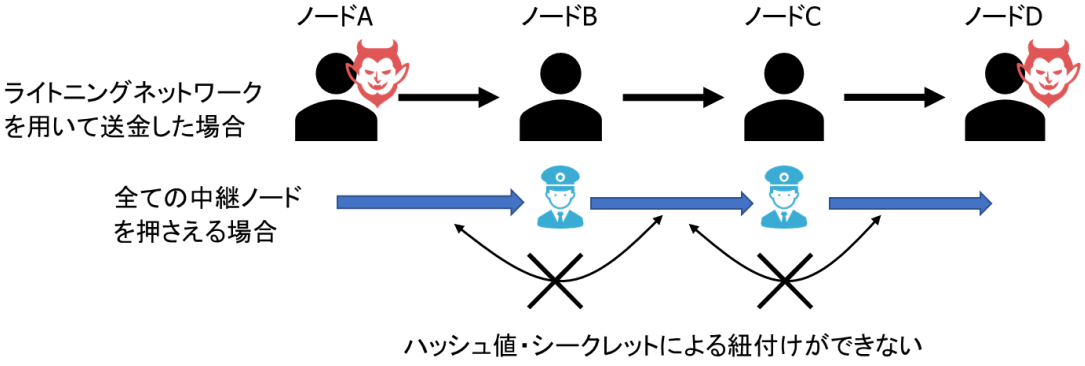
- スクリプトレススクリプト

  ハッシュ値やシークレットを署名に含める技術であり、起点となる送金元以外からは経路を特定することは極めて困難となる。

- Multi-Hop Locks

  経路上のノード間ごとに異なるハッシュ値やシークレットを用いる技術であり、起点となる送金元以外からは経路を特定することは極めて困難となる。

図表 200 ハッシュ値やシークレットを置き換える効果のイメージ

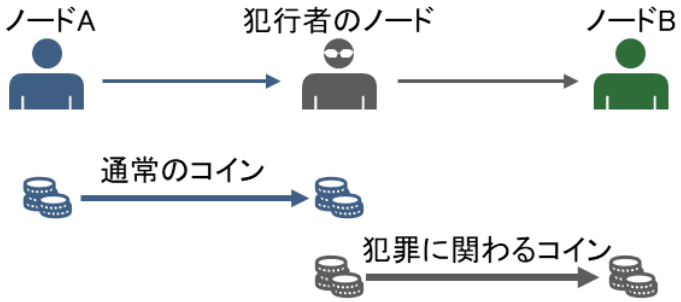


4.2.5.4 その他の論点

4.2.5.4.1 犯行者が中継ノードを運営した場合

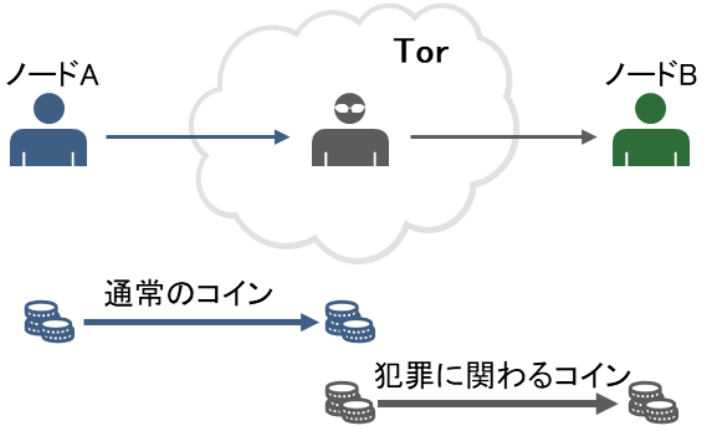
犯行者は送金の起点となる以外に、中継ノードになる場合も考えられる。この場合は、第三者から正規のコインを受け取る代わりに、自身の持つ不正なコインを他者へ送金することで、資金洗浄を図ることが可能となる（図表 201）。図表 201 の場合、自身の犯罪収益をノード B へ送金し、代わりに同額の通常のコインをノード A から受けることで、犯行者は資金洗浄を図ることができる。

図表 201 犯行者が中継ノードの場合



ただし、このような資金洗浄にあたっては、（1）送金元（ノード A）が通常のコインを保持している必要がある、（2）犯行者は自身の身元を隠すため Tor 秘匿サービスなどを併用することが望ましい、（3）犯行者はハブとなることが望ましい、など、実利用にあたってのハードルは複数存在する。なお、（2）については、多くの先から接続を受け入れる中継ノードとなるためには、IP アドレス等を含めた自身のノード情報などを公開する必要があるため、自身の匿名性を担保するには、Tor 秘匿サービスなどの匿名通信と組み合わせるのが望ましいということである（図表 202）。

図表 202 犯行者が中継ノードの場合（Tor 秘匿サービスを用いた場合）



4.2.5.4.2 中継ノードのビジネスモデル

3.2.2.1 節「ミキシング」のその他の論点でも記載した通り、経済的インセンティブの観点からは、中継ノードのビジネスモデルは手数料ビジネスとなる可能性が高いと考えられる。

多くの先とペイメントチャネルを開くためには、その分多くのデポジット額が必要となり（初期コスト）、ノード情報等を公開するため、デポジット額が多額になるほど、ハッキングなどの被害を受ける可能性も高まる。デポジット額はチャネルを開いている限り、他へ転用することもできない（機会コスト）。

そのため、収入と費用の兼ね合いから、小規模なハブとなる中継ノードが複数生じる可能性も考えられる。この場合、複数の中継ノードがダウンしても他の中継ノードを経由できるためライトニングネットワーク全体としての頑健性は高まるが、中継ノードの規制対応コストが高まると、廃業する先も多数生じる可能性が考えられる。

4.2.5.5 当局の視点

ライトニングネットワークを用いた送金は匿名性が高いということから、暗号資産のAML/CFT 上、中継ノードは重要な役割を果たすと考えられるため、これに対する規制の必要性が考えられる。

例えば米国では、暗号資産が通貨代替物（convertible virtual currency）とすれば、中継ノードは Money Transmitter と解釈される可能性があるが、詳細は州により異なると考えられる。

> "In addition, a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency."[435]

我が国では、ビットコインなどの暗号資産が、本稿執筆時点では一般には為替取引上の資金に該当しないと解釈されているため、中継ノード運営主体が資金移動業

435 The Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering, 2019/1/24

者としての登録および AML/CFT の対応が必須であるか明確ではない[436]。

「仮想通貨の交換等を行う者が、金銭の移動を行うことを内容とする依頼を受けて、これを引き受けること、又はこれを引き受けて遂行する場合には、為替取引を行っているとして、法第 37 条に基づく資金移動業者の登録が必要となり得ることに留意する。」[437]

こうしたライトニングネットワークを用いた送金が一般に普及した場合、暗号資産交換業者等は、ライトニングネットワークの中継ノード経由という新たな資金洗浄ルートに対してもモニタリングを行う必要が生じる。しかし、今回の実験結果から明らかなように、ブロックチェーン上からは不正を把握できないため、疑わしい取引として判断するのは極めて困難になると考えられる。これは従来の取引所のみを対象とする規制では不十分になる可能性があるということを示している。

436 法的な解釈を巡っては、中継ノードが、反復性や継続性の観点から「業」として行っているかもポイントになると考えられる。また、たとえ、資金移動業者であり、AML/CFT 上の対応の必要があると解釈された場合でも、非常に多数の中継ノードが生じた場合には、当局にとってそれら中継ノードの監督にあたっては多大な労力がかかることが懸念される。

437 金融庁, 金融庁ウェブサイト, "16 仮想通貨交換業者関係", https://www.fsa.go.jp/news/28/ginkou/20161228-4/29.pdf, 2019/1/24

4.3 実証実験2. ミキシングを用いた資金洗浄

4.3.1 概要

犯行者が何らかの形で得た不正な暗号資産の資金洗浄を図る場合を考える。ここで、一般に利用可能な、暗号資産のミキシングサービスを利用した場合に、どのような経路をたどるかを検証する。

立命館大学上原研究室で行われたミキシングサービスの実験結果[438]をもとに、上原研究室の了解の下、実験に用いたアドレス等を用いて評価した結果を記載する。

4.3.2 実験条件等

ミキシングサービスのうち、最低金額が低いサイト等で選定した以下の二つのサービスを用いた（図表 203）。いずれも、複数の受取アドレスを指定したり、着金遅延を指定したりすることが可能となっている。

- Bitcoin Blender (http://bitblendervrfkzr.onion/)

  2014 年から開始しており、ダークウェブ上のサイトでのみミキシングの申し込みが行える。5BTC 以上デポジットした場合は 0.5%手数料が下がること、友人紹介制度や二段階認証などが提供されている。手数料は匿名性を高めるため 1-3%のランダムな値となる。送付先アドレスは最大 5 つまで一度に指定できる。

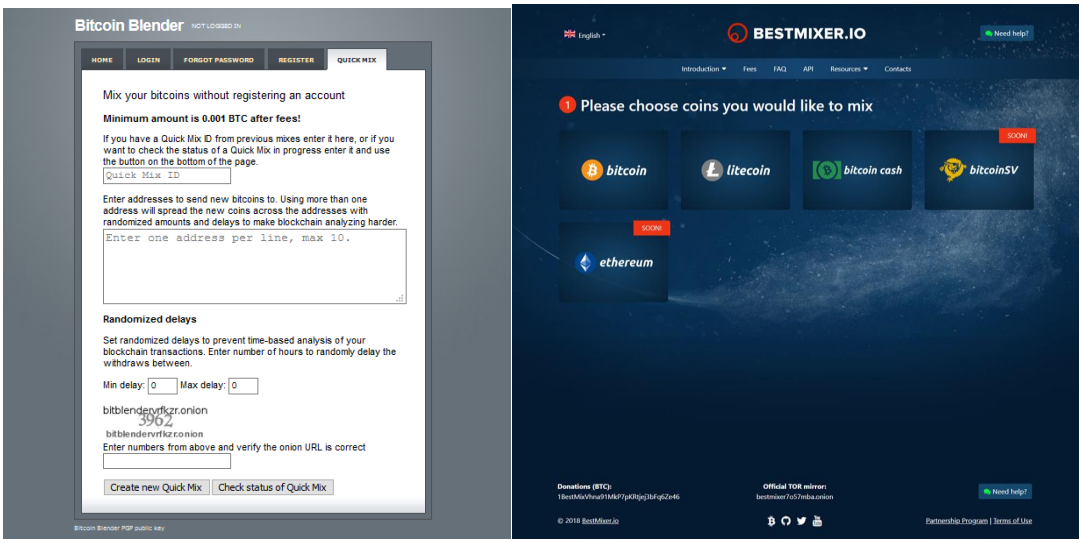
- BestMixer (https://bestmixer.io/en)

  2018 年から開始しており [439]、ウェブサイトは 11 ヶ国語に対応し、通常のウェブ上のサイトおよびダークウェブ上のミラーサイトからミキシングの申し込みが行える。Youtube にも 11 ヶ国語で利用方法を示した動画をアップロードしており、ビットコインの他、ライトコイン、ビットコインキャッシュを扱う [440]。手数料は基本手数料に加え、受取アドレス毎に固定額が加算される。基本手数料はビットコインの場合 1%～5%の間で指定可能であり、基本手数料率に応じてミキシングを行う資金プールの属性が変わる。

---

438 廣澤龍典, 立命館大学 大学院, "ミキシング結果 報告書", 2018 年 12 月 13 日に基づく。
439 bestmixer, Bitcoin Forum, "[ANN] BESTMIXER.IO THE FUTURE OF BITCOIN MIXING! TECHNOLOGY IS HERE", https://bitcointalk.org/index.php?topic=3140140.0, 2019/1/29
440 本稿執筆時点のもの。今後、イーサリアムおよびビットコイン SV にも対応する予定とされている。

図表 203 対象としたミキシングサービスのページ（左：Bitcoin Blender[441]、右：BestMixer[442]）



4.3.3 実験結果

4.3.3.1 ミキシングサービスの手数料

Bitcoin Blender、BestMixer それぞれを二回ずつ利用したところ、返金率は概ね 95%～97%であった（図表 204）。

ミキシングサービス事業者は返金時にトランザクション手数料を支払う必要がある。最終的な返金時のトランザクション手数料のみを考慮すると、ミキシングサービス事業者の手数料収入は概ね 1%～3%の範囲であった。

ただし、実際には、他のユーザの暗号資産とプーリングした上で、相当回数のトランザクションを経て資産を移動しているため、ミキシングサービス事業者の実際の手数料収入はこれよりも下がることが見込まれる。

図表 204 ミキシングサービスへの入金額と返金額[443]

サービス名	試行回数	単位	入金額	返金額		手数料		サービス側の手数料収入率（最大値）
				返金額	返金率	サービス側が返金時に支払う手数料	サービス側の手数料収入（最大値）	
			A	B	B/A	C	D=A-B-C	D/A

441 anonymous Bitcoin enthusiast and software developer, bitblender.io, "Bitcoin Blender", http://bitblendervrfkzr.onion/?p=quickmix, 2019/2/5

442 Best Mixer, Bestmixer.io, "Start new mixing", https://bestmixer.io/en#start_new_mixing, 2018/12/18

443 円換算は、ミキシングサービスを実施した 2018/11/13 のレートである、717,100 円/BTC を用いた。

Bitcoin Blender	1 回目	BTC	0.00180000	0.00173262	96.3%	0.00002082	0.00004656	2.59%
		円	1,291	1,242		15	33	
	2 回目	BTC	0.00400000	0.00382459	95.6%	0.00005705	0.00011836	2.96%
		円	2,868	2,743		41	85	
BestMixer	1 回目	BTC	0.00190000	0.00181310	95.4%	0.00006057	0.00002633	1.39%
		円	1,362	1,300		43	19	
	2 回目	BTC	0.00300000	0.00292954	97.7%	0.00020516	-0.00013470	-4.49%
		円	2,151	2,101		147	-97	

4.3.3.2 送金から返金までの時間差

入金から返金までの時間差を計測すると 2 時間～20 時間の範囲であった（図表 205）。Bitcoin Blender では最小遅延時間と最大遅延時間を指定することができ、BestMixer では 72 時間までの範囲で返金アドレス毎に 1 分単位で指定できた。

図表 205 ミキシングサービスへの送金時刻と返金時刻

サービス名	試行回数	入金時刻	返金時間			
			片方のアドレス		もう片方のアドレス	
			返金金時刻	時間差	返金金時刻	時間差
Bitcoin Blender	1 回目	2018/11/13 17:03	2018/11/13 19:40	2 時間 37 分	-	-
	2 回目	2018/11/14 18:57	2018/11/15 14:48	19 時間 50 分	-	-
BestMixer	1 回目	2018/11/13 18:46	2018/11/13 21:40	2 時間 54 分	2018/11/13 22:23	3 時間 37 分
	2 回目	2018/11/14 19:20	2018/11/15 13:49	18 時間 29 分	2018/11/15 14:34	19 時間 14 分

Bitcoin Blender、BestMixer ともに途中経路の時刻をみると、基本的に入金時刻よりも後に入金された資産が移動されている。Bitcoin Blender では入金された資産が移動するのは 8 日～10 日後である（図表 206）。したがって、返金された暗号資産は入金された暗号資産とは別のものであると考えられる。

図表 206 ミキシングサービスへの入金時刻と次の資産移動の送金時刻

サービス名	試行	入金時刻	送金先アドレス

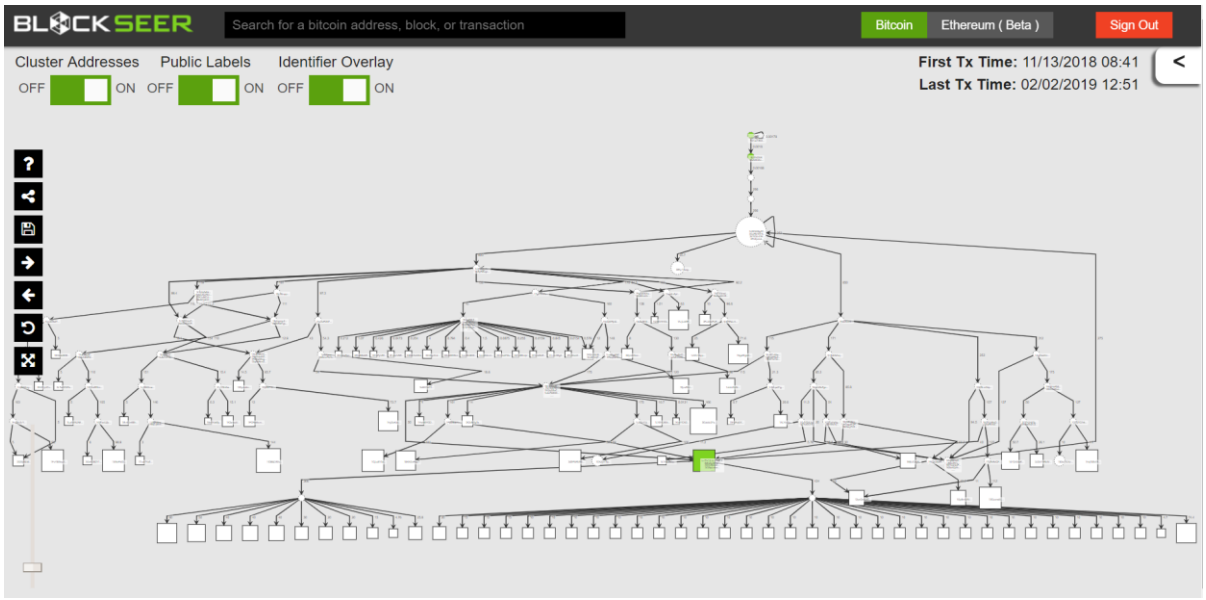
	回数		（ミキシングサービス事業者の受取アドレス）	
			送金時刻	時間差
Bitcoin Blender	1 回目	2018/11/13 17:03	2018/11/21 20:56	8 日 3 時間 52 分
	2 回目	2018/11/14 18:57	2018/11/25 7:29	10 日 12 時間 31 分
BestMixer	1 回目	2018/11/13 18:46	2018/11/14 0:27	5 時間 41 分
	2 回目	2018/11/14 19:20	2018/11/15 13:36	18 時間 16 分

4.3.3.3 ミキシングの程度

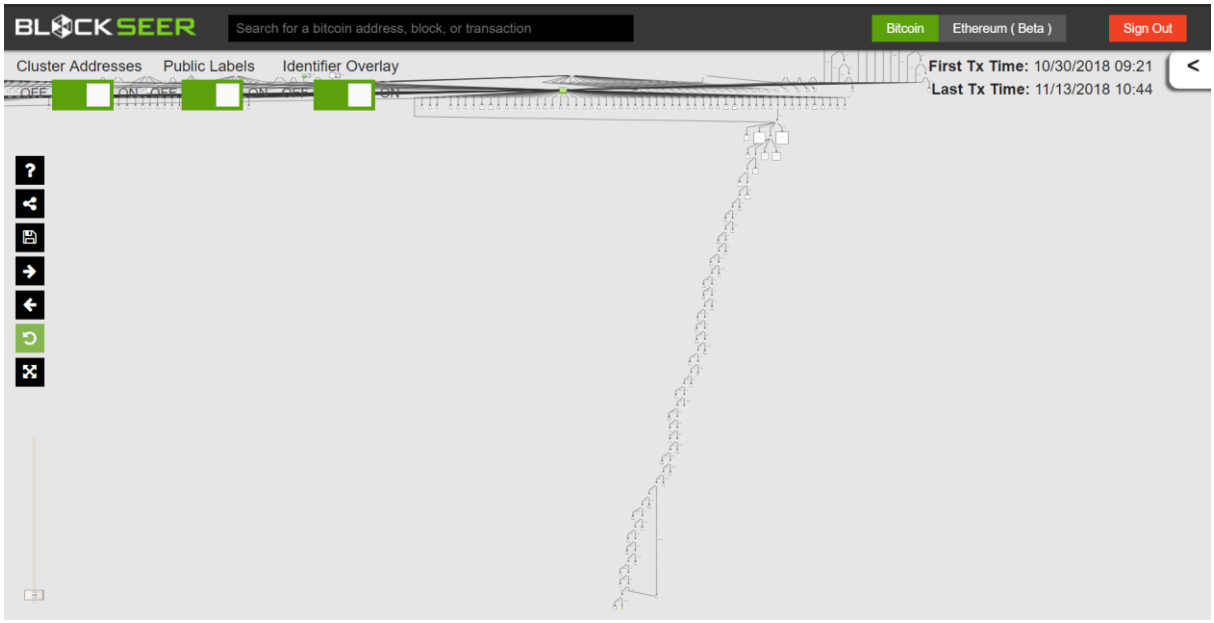
送金した際のアドレスおよび返金された際のアドレスを用いて、それぞれ上流からの経路および下流からの経路を、BlockSeer を用いて確認したが、資産移動経路は極めて複雑であり、また、途中で Binance や Huobi と推測されるアドレスを経由していた（図表 207、図表 208、図表 209、図表 210）。

なお、Bitcoin Blender では、二回の実験ともに返金受取アドレスを二つ指定したが、片方のアドレスにしか返金されなかった。また、Bitcoin Blender では SegWit 形式のアドレスが積極的に使用されていた。

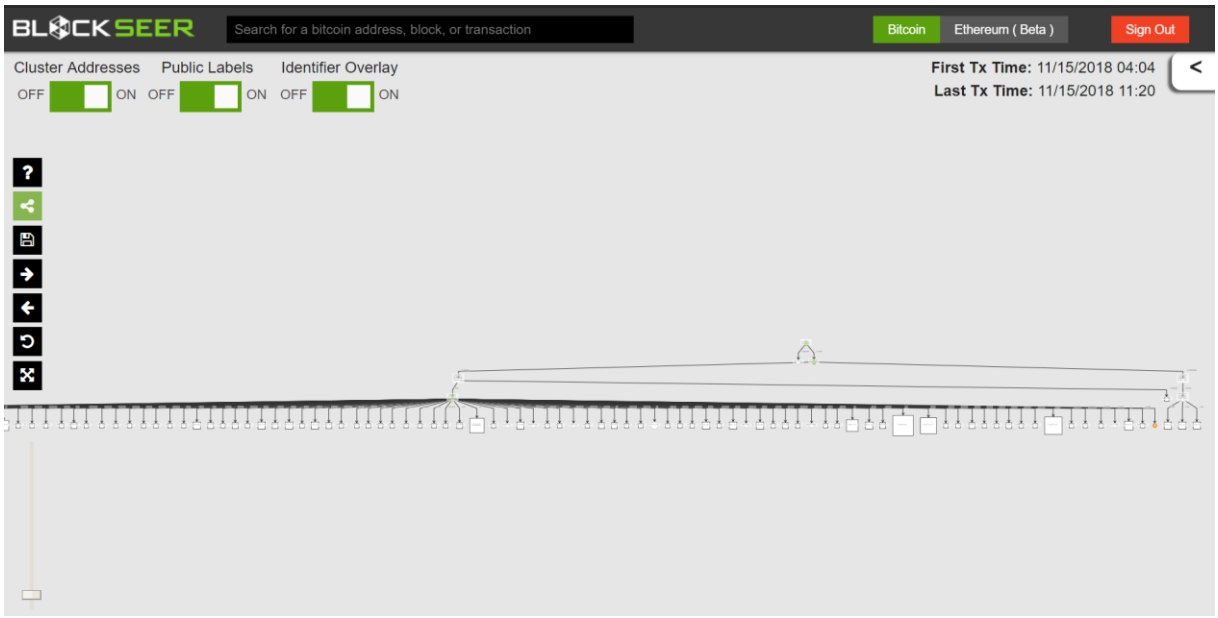
図表 207 Bitcoin Blender 一回目の送金アドレスからの経路（一部、最上段が送金元アドレス）[397]



図表 208 Bitcoin Blender 一回目の返金アドレスからの経路（一部、最下段が返金先アドレス）[397]



図表 209 BestMixer 一回目の送金アドレスからの経路（一部、最上段が送金元アドレス）[397]

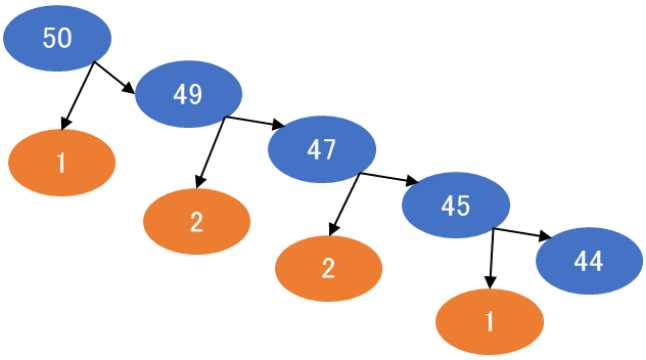


図表 210 BestMixer 一回目の返金アドレスからの経路（一部、最下段が返金先アドレス）[397]

4.3.3.4 ミキシングの特徴なパターン

各種文献等でも記載されている通り、今回の実験でも Peeling chain という特徴的なパターンが見られた（図表 208、図表 210）。これは少しずつ皮がむかれていくように、相対的に大きな金額（実）と小さな金額（皮）の 2 つに分離（peeling）することが繰り返されるパターンである（図表 211）。

図表 211 Peeling Chain のイメージ（青はミキシングサービス事業者の暗号資産、橙は利用者への返金用の暗号資産を指す）[444]



4.3.4 考察

4.3.4.1 匿名化の程度

入金資産の移動時刻と返金時刻の比較から、ミキシングサービス事業者は入金された資産とは全く別の資産プールから、利用者が指定した時刻に返金を行うことが分かる。すなわち、第三者が、返金された資産から本来の入金元を追跡することは基本的には不可能だと考えられる。

ミキシングサービス事業者のみが入金元と返金先の紐付けが可能であるが、一定期間経過後はデータが廃棄されるため[445]、データ廃棄後はミキシングサービス事業者も含めて紐付けが不可能になると考えられる。

4.3.4.2 ミキシングサービス事業者のビジネスモデル

一回のミキシングにかかる手数料収入は、ビットコインの場合 1%～3%程度の範囲と考えられる[446]。Bitcoin Blender のようにトランザクションサイズを削減する SegWit の利用は、ミキシングサービス事業者において今後さらに普及すると考えられる。

なお、例えばダークウェブからしか申し込めない Bitcoin Blender の経路の一部に

444 Balthasar, T., ResearchGate, "An Analysis of Bitcoin Laundry Services", https://www.researchgate.net/profile/Julio_Hernandez-Castro2/publication/319944399_An_Analysis_of_Bitcoin_Laundry_Services/links/5a045d410f7e9beb177883af/An-Analysis-of-Bitcoin-Laundry-Services.pdf?origin=publication_detail, 2019/2/7 より三菱総研作成。
445 利用者の問合せ対応のために一定期間のみデータを保持するとされており、データ保持期間は Bitcoin Blender では 10 日間、BestMixer では最大 72 時間となる。
446 例えば、BestMixer では、ライトコインやビットコインキャッシュなどでは基本手数料が 3%～15%であり、ビットコインよりも割高になる。

おいても今回確認する限り約 12 億円が移動しており、ミキシングサービス事業者の保有する全体の資産は相当な規模であることが予想される。また、途中経路に取引所と思われるアドレスも複数含まれており、資産移動経路を隠蔽する以外に、何らかの暗号資産取引を行うために取引所アドレスが含まれていた可能性も考えられる。

以上より、事業者は、ミキシング手数料という手数料ビジネス以外に、自己勘定取引や、暗号資産建て信託への投資などの預かり資産ビジネスも手掛けている可能性が考えられる。

4.3.4.2.1 ミキシングサービス事業者の行動原理

ミキシングサービスの入金と返金には時間差が存在し、全ての単位時間において、入金額が返金額を上回る場合、残高は単調増加する。そのため、ミキシングサービス事業者が何らかの資産ビジネスを行っている場合、BestMixer のように常に広報活動を行い、入金を増やし続けるよう取り組むのが望ましい。データを蓄積して、入金額・時間差のぶれを考慮して将来残高を適切に予測するように取り組む必要もあると考えられる。

また、BestMixer のように複数の暗号資産を扱っている場合、ビットコインの入金を他の暗号資産で返金するという販売所ビジネスも行うことが可能と考えられる[447]。例えば、TransferWise 社（英）のようにマッチングビジネスを行う（ビットコインをイーサに変換したい利用者と、イーサをビットコインを変換したい利用者とをマッチングさせて、取引所を介さずに暗号資産の変換を行うなど）ことで、一般の取引所よりも安価なサービスを提供できる可能性も考えられる。

447 本稿執筆時点では BestMixer は販売所機能は提供していない。

4.4 実証実験3. リスクスコアリングツールの評価

4.4.1 概要

犯行者が何らかの形で得た不正な暗号資産の資金洗浄を図る場合を考える。ここで、一般に利用可能な、ビットコインにおけるリスクスコアリングツールが、不正な経路を経たアドレスを正しく評価できるかを検証する。

今回は、不正な経路としてミキシングサービスを経た経路を考えることにした。

4.4.2 実験条件等

4.4.2.1 実験データ

実際にビットコインの送金に用いられた以下のアドレスについて、リスクスコアリングツールの結果を評価した（図表 212）。それぞれのアドレスの内容については、図表 213、図表 214、図表 215、図表 216、図表 217 を参照のこと。

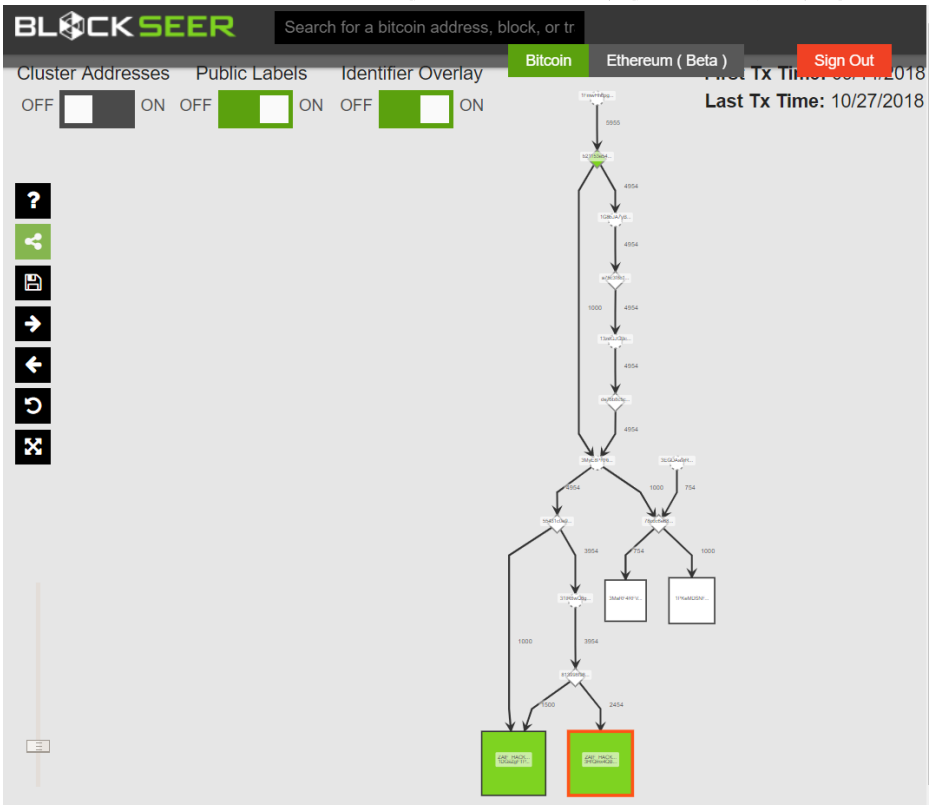
図表 212 リスクスコアリング対象アドレスの一覧[448]

No	ビットコインアドレス	送金・着金回数	内容
1	1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w	25	仮想通貨取引所「Zaif」からの一次流出先アドレスとされるアドレス
2	3HfQmx4QBBVB6699mhSpdbVnYq19pxPWsu	4	No1 からビットコインが送金されたアドレス
3	16YrELPzCnVY5Sgc7ridQAR7yXjZJvx89r	2	No1 からビットコインが送金されたアドレス
4	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	380,485	No1 からビットコインが最終的に送金されたとみられる仮想通貨取引所「Binance」のアドレス
5	14ZQKTpaWwMe9xeLxZkdhfijdn2z97pV4b	2	実証実験 2「ミキシングを用いた資金洗浄」で使用した、Bitcoin Blender への送金元アドレス
6	bc1qdfgtezjucd583k0d90mg939f7nfrkehmm8pz8l	243	実証実験 2「ミキシングを用いた資金洗浄」で使用した、Bitcoin Blender のアドレス ※No5 のアドレスの送金先アドレスである Bitcoin Blender の受けアドレスから最初に送金された先のアドレス
7	17uLLWiNNLBS6HnTF2n3rVYypCAGWig4og	2	実証実験 2「ミキシングを用いた資金洗浄」で使用した、BestMixer への送金元アドレス

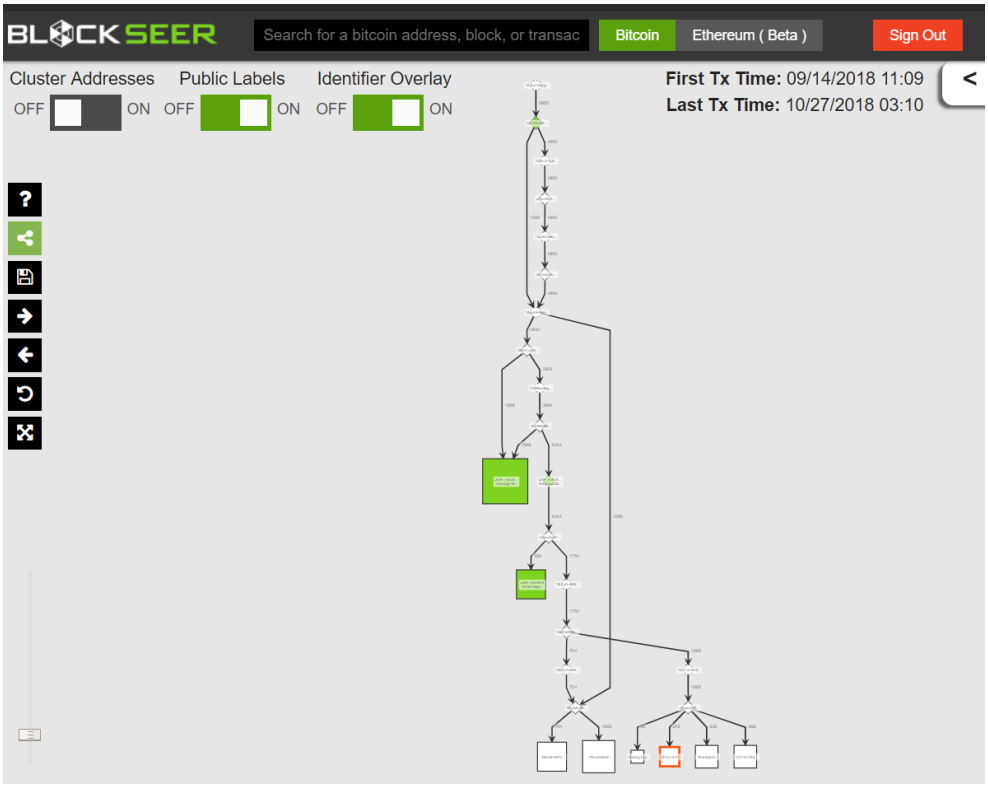
448 「送金・着金回数」列は、本稿執筆時点までに、当該アドレスが含まれるトランザクション数を示す。

8	3DWxRFQCUiJpnqGUNVH1srD5QPdJZv1R22	2	実証実験 2「ミキシングを用いた資金洗浄」で使用した、BestMixer のアドレス ※No7 のアドレスの送金先アドレスである BestMixer の受けアドレス
9	34Yan6SyDpYKQXi8q8epeHMUBVjWi7wbye	2	実証実験 2「ミキシングを用いた資金洗浄」で使用した、、BestMixer のアドレス ※No7 のアドレスの送金先アドレスである BestMixer の受けアドレスから最初に送金された先のアドレス

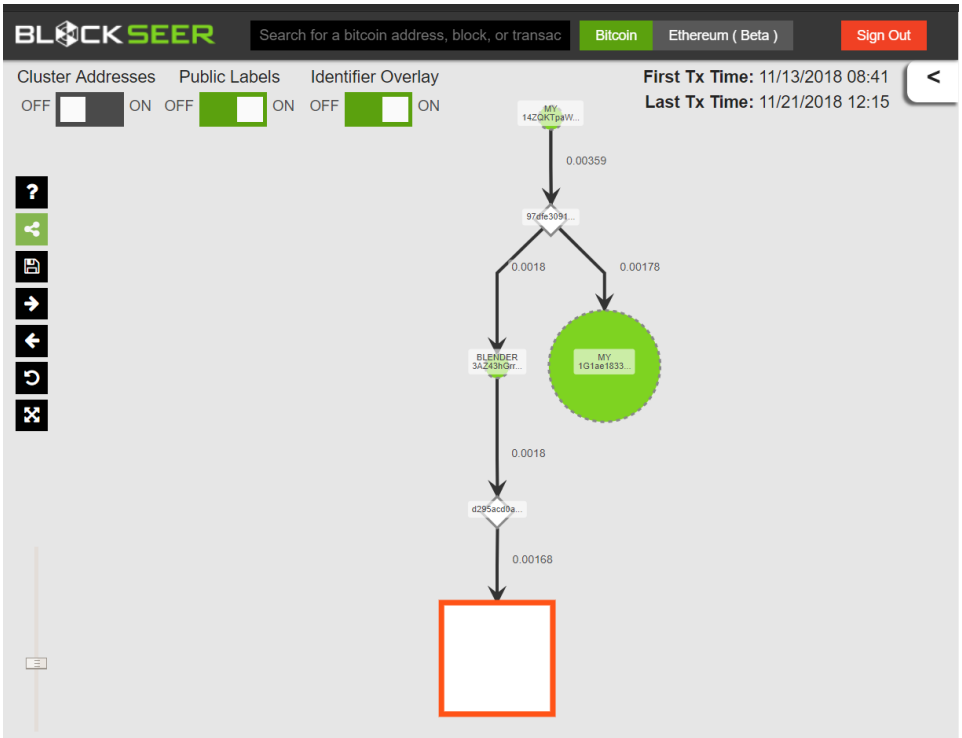
図表 213 対象アドレス No1・No2（最上段が No1、最下段のうち赤枠が No2）[397]



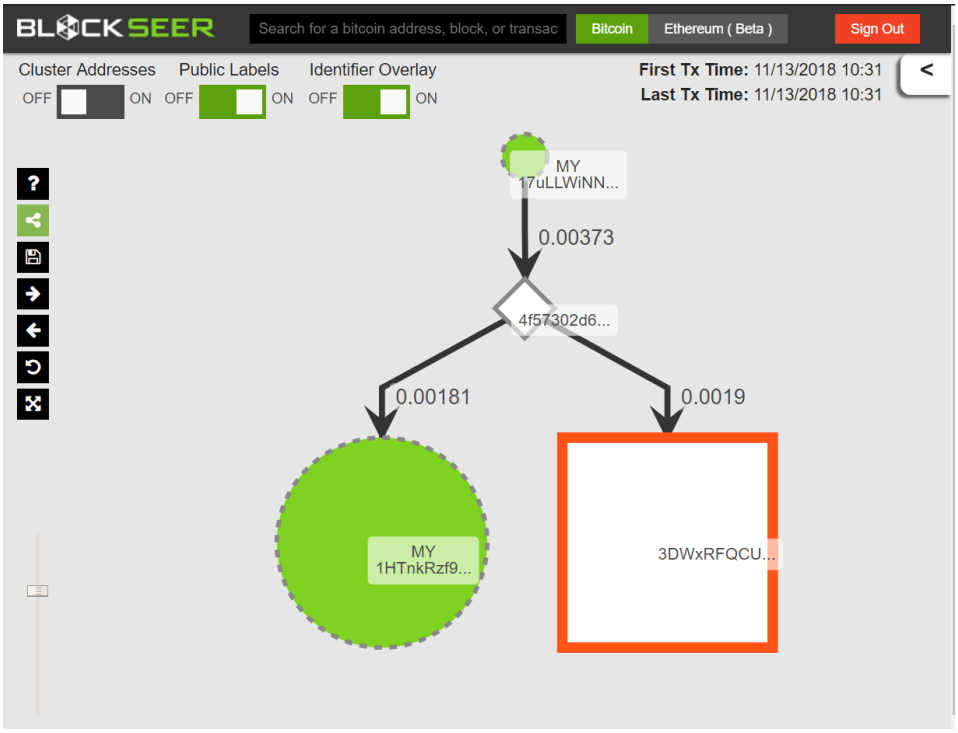
図表 214 対象アドレス No3（最下段のうち赤枠が No3）[397]



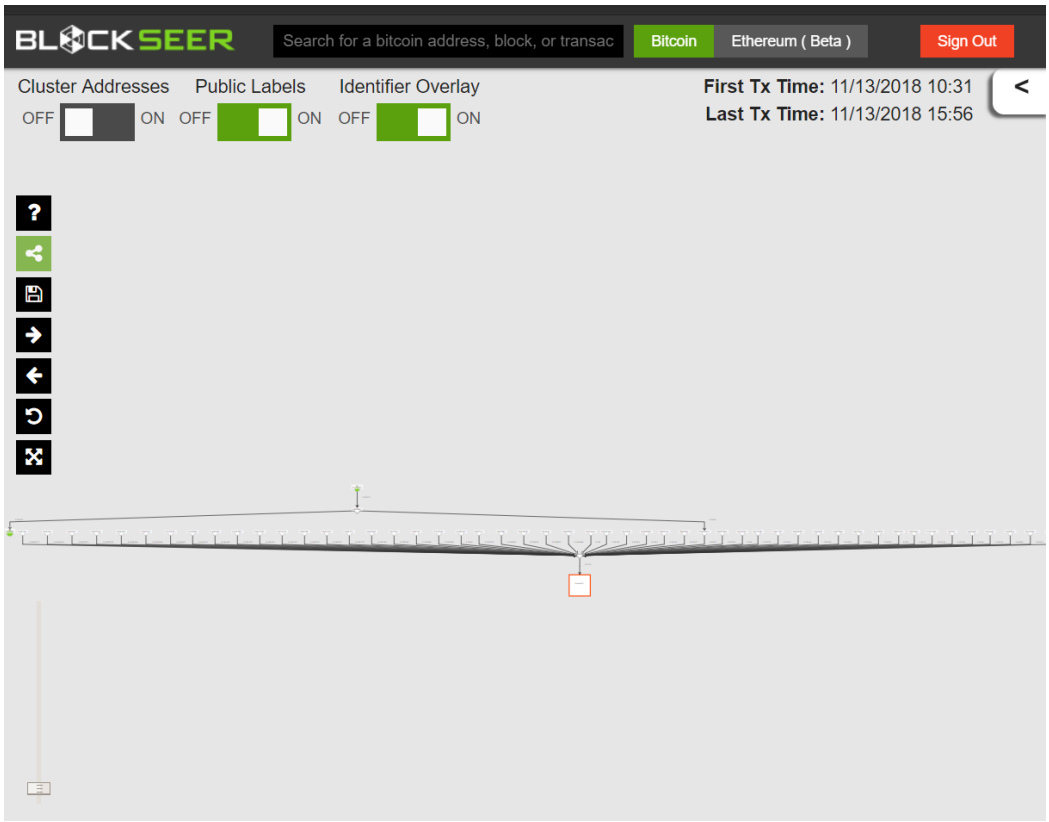
図表 215 対象アドレス No5・No6（最上段が No5、最下段の赤枠が No6）[397]



図表 216 対象アドレス No7・No8（最上段が No7、最下段の赤枠が No8）[397]



図表 217 対象アドレス No7・No9（最上段が No7、最下段の赤枠が No9）[397]



4.4.2.2 実験に用いたツール

暗号資産のリスクスコアリングツールを提供している企業（以下、追跡ベンダ）4 社

の協力を得て、それらのスコアを比較した。

4.4.3 実験結果

- No1 の仮想通貨取引所「Zaif」からの不正流出先アドレスは、いずれのツールにおいても、リスクが極めて高いと正しく評価された。
- No4 の仮想通貨取引所「Binance」のアドレスは、いずれのツールにおいても、わずかにリスクが高いと評価された。
- 上記以外のアドレスについて、いずれのツールにおいても、ニュートラル～わずかにリスクが低いと評価された。
- No6 の SegWit アドレスについては、いくつかのツールでは未対応のためスコアが算出されなかった。

4.4.4 考察

4.4.4.1 リスクスコアの精度

本調査研究でヒアリングした限りでは、各追跡ベンダとも、リスクスコアリング上、ミキシングサービスは脅威であり、ミキシングサービスを経たアドレスは一律リスクが高いとみなす等の対応をしているとのことであった。しかし、実際のスコアでは、リスクは正しく評価されていなかったと言える。これはビットコインではアドレスを無限に生成できるため、ウェブやダークウェブなどの外部情報を使わない限り、あるアドレスがミキシングサービスのものかどうかの判断が非常に難しいからではないかと推察される。

4.4.4.2 リスクスコアの特徴

No1～No4 までのアドレスに対するスコアから明らかな通り、各追跡ベンダが保持している不正アドレス等を含むデータベースに当該アドレスが存在するかどうかがリスクスコアに大きく影響を与えており、実験結果を見る限り、当該アドレスが不正アドレスから派生したかどうかはあまり影響を与えていないのではないかと考えられる。

また、たとえアドレスの経路を重視して評価できるようになったとしても、アドレス毎にリスクを見積もるという考え方自体が不適切な場合もあると考えられる。例えば、No4 の仮想通貨取引所「Binance」のアドレスなど、送金・着金件数が極めて大きいアドレスについては、疑わしい経路を経たビットコインと正常な経路を経たビットコインが

混ざってしまい、全体としてみると当該アドレスのリスクは薄まって評価されてしまう懸念がある。この場合、犯行者からみると、送金・着金件数が極めて大きいアドレスを経由すれば、それ以降のアドレスのリスクスコアを下げる（リスクが低いと評価させる）ことが可能になってしまう問題が生じる。

4.4.4.3 その他

また、No4 の仮想通貨取引所「Binance」のアドレスなど、送金件数が多いアドレスについては計算処理も大きくなることが予想され、当該アドレスではスコアが出力されるまでの時間が相当長くなる場合もあった。そのため、リスクスコアリングツールは、パフォーマンスの面でもさらに改善の余地があると考えられる。

5. 当局としての対応策

本章では、前章までの理論的考察及び実証実験を通じて把握された課題の対応策について記載する。

5.1 理論的考察及び実証実験を通じて把握された課題

3.1 節「調査結果の全体像」で示したレイヤー毎に、匿名化技術と再識別技術を比較すると、巧妙に匿名化された場合は「事後の犯行者特定は技術的には極めて困難」と言わざるを得ないと考えられる。主な結論は以下の通りである。

- 資金洗浄方法は既にある程度確立されていると考えられる。

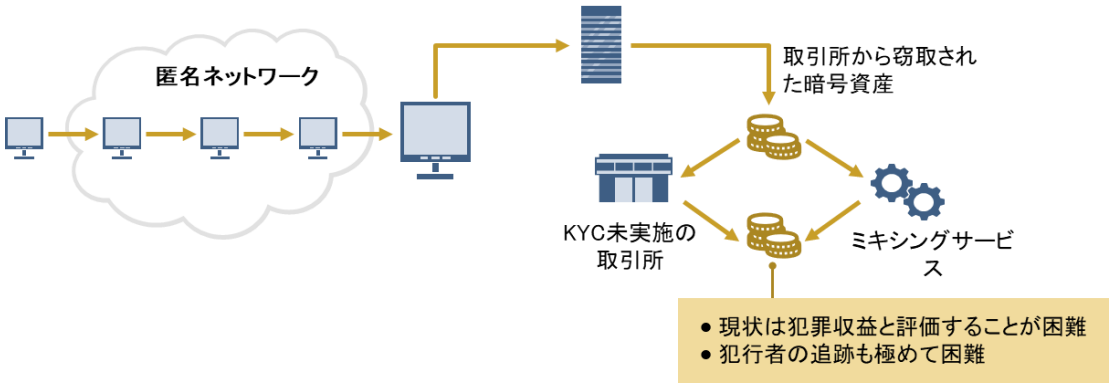
  暗号資産の資金洗浄には、(1)規制遵守が徹底されていない仮想通貨取引所や仮想通貨決済代行業者、(2)ミキシングサービス、(3)オンラインギャンブルサイト等が用いられるが、これらは容易に利用が可能である。例えば、ミキシングサービス最大手の Bitmixer.io が閉鎖(2017 年 8 月)した後も、BestMixer などのクローンサイトが数多く出現しており、また、海外に所在していること等から、こうしたサービスの取締を徹底することは極めて難しいと考えられる。

- 現状利用可能な非識別技術は限界を抱えている(図表 218)。

  再識別化にあたっては、大きく(1)レイヤー毎のプロトコルに基づく追跡、もしくは(2)外部データベースに基づく追跡という二通りのアプローチを組合せて行われるが、基本的には、犯行者のミスをつく／実装上の脆弱性をつくなどに留まる。また、現状利用可能なリスクスコアリングツールでは、リスクを正しく評価できているとは言い難いと考えられる。

図表 218 事後的な再識別の技術的限界のイメージ

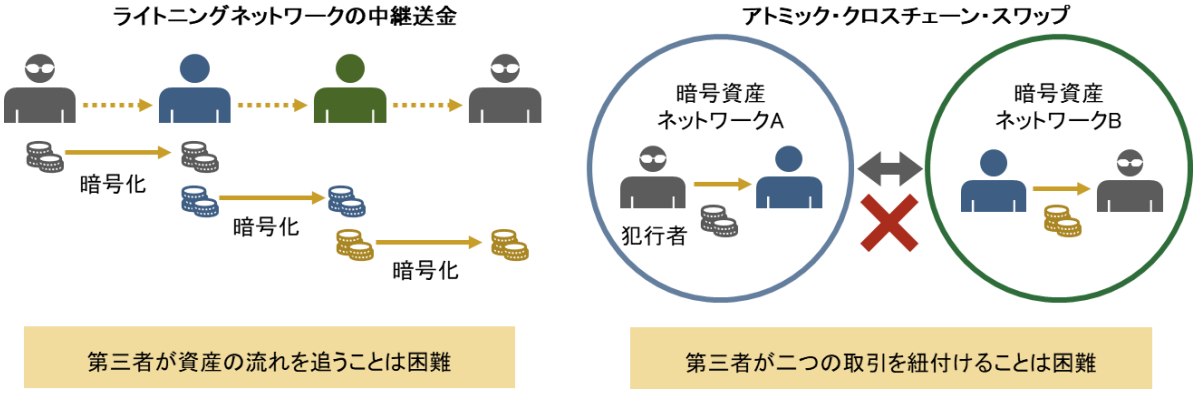
例えば、匿名通信が利用された上で、ミキシングサービスやKYCを行わない取引所等を経由された場合、その適切なリスク評価や犯行者の追跡は現状極めて難しい。



➢ 匿名化技術はさらに進展を見せている。

3.2 節「ブロックチェーン要素技術にかかる調査」に記載した通り、足元様々な匿名化技術が開発されている。例えばライトニングについては、4.2 節「実証実験1．ライトニングネットワークを用いた資金洗浄」でも確認した通り、中継送金が行われると、その資産移動経路を把握することは極めて困難となる。また、暗号資産の交換に、アトミック・クロスチェーン・スワップが行われると、交換された資産の移動経路を第三者が把握することは極めて困難となる（図表 219）。他に、ゼロ知識証明（zk-SNARKs）や MimbleWimble なども、極めて強力な秘匿性を有すると考えられる。

図表 219 新たな技術を用いた資金洗浄のイメージ



上記を踏まえると、極めて匿名性の高い資金洗浄は既に可能であり、今後さらに様々な手法が利用可能になると考えられる。一般にこうした技術はオープンソースの形で公開され、スマートフォン用のアプリなども提供されるため、利用にあたっての技術的・心理的なハードルは低いことも予想される。また、匿名化技術は、匿名通貨（モネロ、ジーキャッシュ等）だけでなく、ビットコインを中心に積極的に開発が進められている。

以上より、法定通貨と暗号資産の接点である暗号資産取引所を規制するだけでは不十分となる懸念があるとともに、一部の暗号資産（匿名通貨等）を規制するだけでは不十分となる懸念があると考えられる。

今後、更なる技術革新の進展や暗号資産内で完結した金融取引が増えていくにつれ、クリプトロンダリング等のリスクは拡大・深刻化する懸念がある。

5.2 他国の参考事例

暗号資産の資金洗浄リスクへの対応策を検討するにあたり、専門家等の意見を踏まえ、過去の類似の事例の調査を行った。本節では、ロシア連邦政府による Telegram ブロッキングの事例、中華人民共和国政府によるビットコイン取引取締の事例、アメリカ合衆国連邦政府による特定のビットコインアドレス排除の事例について記載する。

5.2.1 ロシア連邦政府による Telegram のブロッキング

5.2.1.1 経緯概要

Telegram（詳細は 3.5.1.1 節「Telegram」を参照のこと）は、近年、テロを計画するプラットフォームとしての使用が指摘されており[449]、またロシア当局による Telegram ユーザの暗号化されたメッセージ閲覧を許可する裁判所命令を遵守しなかったとして、ロシア政府はロシアでの Telegram の使用を禁止している[450]。

5.2.1.2 IP アドレスブロッキング

ロシア当局は 2018 年 4 月に IP アドレスブロッキングを開始した[450]。Telegram 側は Domain Fronting[451]と呼ばれる技術を用いてブロック対象先を人為的に増加させた[452]ために、ブロック対象先となる IP アドレスが 1900 万近くに膨れ上がったという報告もある[453]（図表 220）。数十の無関係なサイトへのユーザアクセスを誤ってブロ

449 The New York Times, "What Is Telegram, and Why Are Iran and Russia Trying to Ban It?", https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html, 2018/11/7

450 Reuters, "Russia tries more precise technology to block Telegram messenger", https://www.reuters.com/article/us-russia-telegram/russia-tries-more-precise-technology-to-block-telegram-messenger-idUSKCN1LF1ZZ, 2018/11/7

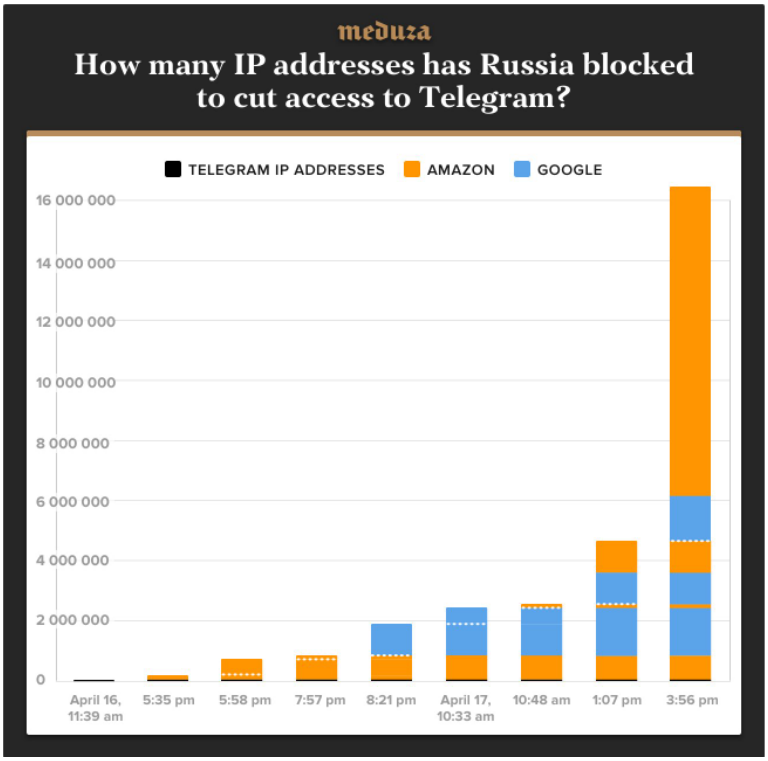
451 ブロッキングされていないウェブドメインに紐づくトラフィックに見せかけてブロッキングされることを回避する技術。トラフィックを一度 CDN(Content Delivery Network)に送信、CDN 上の Domain Fronting サーバを経由して目的地に到達するため、CDN 上でホストされている Web サイトのトラフィックのように見せることができる。Medium, " Domain fronting—A technique used to circumvent internet censoring", https://medium.com/@pmvk/domain-fronting-a-technique-used-to-circumvent-internet-censoring-10ef1bb3db84, 2018/11/7

452 MATT BURGESS, Wired, "This is why Russia's attempts to block Telegram have failed", https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google, 2018/11/7

453 Techcrunch.com, "Russia’s game of Telegram whack-a-mole grows to 19M blocked IPs, hitting Twitch, Spotify and more", https://techcrunch.com/2018/04/19/russias-game-of-telegram-whack-a-mole-grows-to-19m-blocked-ips-hitting-twitch-spotify-and-more/, 2018/11/7

ックするという事象が発生し、ロシア当局による IP アドレスブロッキングは中断している。（同時期の 2018 年 4 月に、Google と Amazon は Domain Fronting を禁止するためのインフラ変更を実施している[454]。）

図表 220 ロシア当局がブロッキングを実施した IP アドレス数と当該 IP アドレスを保有する組織の推移[455]



5.2.1.3 DPI ブロッキング

ロシア当局は、2018 年 8 月から、Deep Packet Inspection（DPI）[456]のテストを開

454 The verge, "A Google update just created a big problem for anti-censorship tools", https://www.theverge.com/2018/4/18/17253784/google-domain-fronting-discontinued-signal-tor-vpn, 2018/11/7
Amazon.com, "Enhanced Domain Protections for Amazon CloudFront Requests", https://aws.amazon.com/it/blogs/security/enhanced-domain-protections-for-amazon-cloudfront-requests/, 2018/11/7
455 Meduza, meduza.io, "Here's how many IP addresses Russia has blocked to cut access to Telegram", https://meduza.io/image/attachments/images/002/947/294/large/EgbMx5yQxHOIZmMA02tP_Q.jpg, 2018/11/8
456 インターネット経由で送信されたパケットの詳細（パケットの中身、どのアプリケーションのパケットか）を検査すること。検査のレベルごとに、Shallow Packet Inspection (SPI), Medium Packet Inspection (MPI), Deep Packet Inspection (DPI) がある。DPI は ISP (Internet Service Provider) によるネットワークトラフィックの最適化（VoIP トラフィックを識別し、優先順位をつけることで遅延を減らす等）にも使用される。
catchpoint, "A Guide to Deep Packet Inspection", http://blog.catchpoint.com/2017/07/19/guide-deep-packet-inspection/, 2018/11/8

始したと報道されている。1回目のテストではブロッキング対象以外のサービスがブロックされる事象が発生したとされる。ロシア当局からの要請に基づき、ロシア国内の 9 つの企業が Deep Packet Inspection を用いたブロッキングソリューションを提出しており、当局側はその中から最も効果的な手法を選択し、必要に応じて改良を加え、実際への適用を企図していると報じられている[450]。一方で、DPI はその技術的な難易度に加え、運用負荷が極めて高いことが指摘されており、実際の運用にあたっては、高負荷の処理に耐えうる高価な専用機器が必要とされている[457]。

5.2.2 中華人民共和国政府によるビットコイン取引の取締

5.2.2.1 経緯概要

中国では 2013 年頃よりビットコインが普及し始め、ビットコインの取引所取引において人民元建ての取引が急速に拡大した[458]。中国当局は、犯罪取引や投機リスクへの懸念を理由に、2013 年 12 月にビットコインへの規制を取り纏めた。中国国内の金融機関ではビットコインの売買が禁止され、仮想通貨取引所では法定通貨との交換が禁止されたが、法の抜け道は多く見られ、またビットコインの保持そのものも違法とはされなかった。その後もビットコインの中国での普及は進み、2016 年 12 月にはビットコインの取引所取引における 98%（トランザクション件数ベース）が人民元建てで行われるまでに至った（図表 221）。

図表 221 人民元建て取引の割合（左）と中国のハッシュパワー（右）の推移[459]

457 上原哲太郎, "IDF 第15期第1回「法務・監査」分科会 Web サイトのブロッキングにおける技術的・運用上の課題", https://digitalforensic.jp/wp-content/uploads/2018/06/law-15-1.pdf, 2019/1/7

458 他のアセットと異なりビットコインへの規制が緩かったことや、電子決済化と相性が良かったこと、背景となる思想が魅力的に捉えられたことなどがその要因として挙げられている。

459 Kaiser, B., et al., Princeton University, "The Looming Threat of China: An Analysis of Chinese

2017 年初頭に、投資家保護と金融リスクの顕在化を未然に防ぐことを目的として ICO (Initial Coin Offering) を禁止した。2017 年 9 月には、仮想通貨取引所における暗号資産と法定通貨の交換、暗号資産の売買、代理店サービスの提供も禁止され、結果として、仮想通貨取引所は中国内で事業を継続ができなくなった。2018 年 2 月には、OTC 取引や Peer to Peer 取引なども禁止され、海外含め、仮想通貨取引所のウェブサイトをブロッキングするという報道がなされている。マイニング事業についても、2018 年 1 月に、マイニング事業者に対する電力価格、税金、土地利用に関する優遇政策等を廃止したために、中国のマイニング事業者が苦境に陥っていることが報道されている[460]。

2017 年以降、中国国内においてビットコイン取引が全般に厳しくなる中でも、VPN (Virtual Private Network)と暗号資産 Tether を経由して、海外での暗号資産取引もしくは OTC 取引は可能との指摘もある[461]。

5.2.2.2 Great Firewall および Great Canon

中国当局はビットコイントラフィックに影響を与え得る様々な手段を保持していると考えられている。例えば、各種規制により、仮想通貨取引所やマイニング事業者へ直接的に影響を及ぼすことも可能であるし、エネルギー価格などを通して間接的に影響を及ぼすことも考えられる。

上記以外に、中国当局は国内の全ての ISP（Internet Service Provider）を管理しており、あらゆるトラフィックのモニタリングと操作が可能と言われる。著名なシステムとしては Great Firewall と Great Canon が挙げられる。Great Firewall は以下のような監視を行っていると指摘されている[462]。

Influence on Bitcoin", https://blockchain.princeton.edu/papers/2018-10-ben-kaiser.pdf, 2019/1/7
図表 221（左）・・・・・ p.5 Fig.1(a)
図表 221（右）・・・・・ p.5 Fig.1(b)
図表 222（左）・・・・・ p.8 Fig.3(a)
図表 222（右）・・・・・ p.8 Fig.3(b)

460 Library of Congress, "Regulation of Cryptocurrency: China", http://www.loc.gov/law/help/cryptocurrency/china.php, 2018/11/8

461 Tether (USDT)は USD と連動しており、他の暗号資産と比較してボラティリティが小さく、また法定通貨と比較して送金手数料が小さい。Bitcurate, Medium, "Tether and VPN Rescue Chinese Crypto Traders to Circumvent The Bans", https://medium.com/@bitcurate/tether-and-vpn-rescue-chinese-crypto-traders-to-circumvent-the-bans-283c6cbdffdd, 2018/11/8

462 Chew, W., Medium, "How It Works: Great Firewall of China", https://medium.com/@chewweichun/how-it-works-great-firewall-of-china-c0ef16454475, 2018/11/8

- URL フィルタリング：ブラックリスト先へのアクセスは拒否される
- DNS キャッシュポイズニング：ドメインと IP アドレスの紐づけを書き換えることで、ユーザが入力した URL に対応する Web サイトとは別の Web サイトに接続させる
- 手作業による検閲：何十万人もの民間人がオンラインコンテンツを監視し、コンテンツ内容が法律や規制に違反した場合に当該企業には罰金や業務停止等の厳しい処罰の対象となりうる（近年の AI 技術の進歩により検閲のプロセスは自動化されようとしている。）
- Deep Packet Inspection：トラフィックの監視やフィルタリングを行う
- 接続元の探査：Tor など匿名通信の中継ノードからの接続を拒否する[463]

ただし、Great Firewall では、既に送信されたパケットを止めることはできないことも指摘されている。

Great Cannon は、Great Firewall に比べ、より能動的なアクションを可能とするシステムであり、通過中のパケットに悪意のあるコードを挿入し、特定のターゲット宛てにパケットの宛先を変更して、当該ターゲットへの DoS 攻撃を仕掛けることができる。

5.2.2.3 Great Firewall と空ブロック

上記の Great Firewall により、中国国内と国外の通信においてはパケットロスが発生するため[464]、パケットの再送等によりレイテンシが増大することが指摘されている。ある研究では、ビットコインの 1 ブロックを転送するのに、中国国内では平均して 3.9 秒かかるのに対し、中国国内と国外では約 17.4 秒に達するとの報告もある。

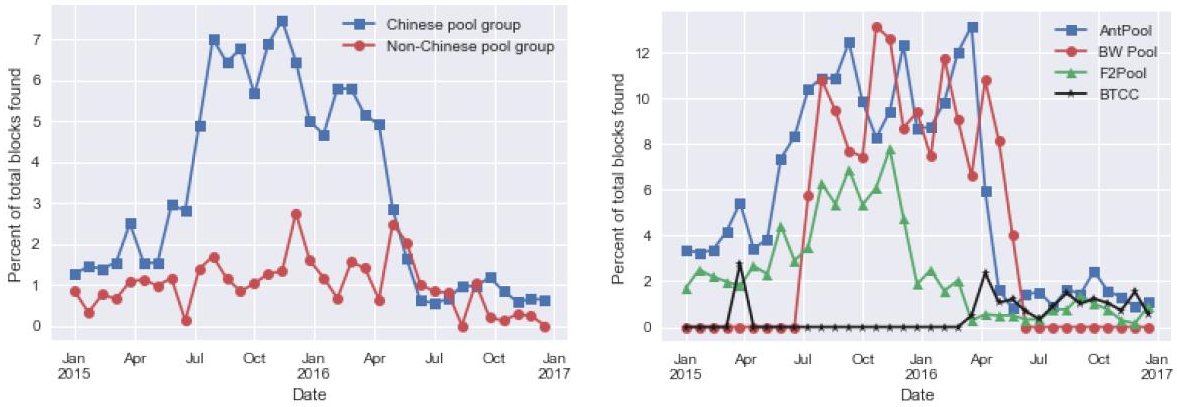
Great Firewall 下のため速やかにブロックを伝播させるにはブロックサイズを小さくした方が良いことやトランザクション手数料よりもブロック報酬の方が遥かに大きいことなどから、中国のマイニングプールでは空ブロックの割合が一時期非常に高かったことが指摘されている（図表 222）。空ブロックの存在は、ビットコインのスループットを下げる効果があり、ビットコインシステムの実効性を著しく低下させることにつながる。

463 Ensafi, R., et al, "Analyzing the great firewall of china over space and time.", https://nymity.ch/pdf/ensafi2015a.pdf, 2019/1/7

464 パケットロス率は、米国と香港間の通信では 0.2%のところ、米国と中国間では 6.9%に達したとの研究もある。

この問題は 2016 年にコンパクトブロックが導入されたことより解消されたが[465]、空ブロックの事例は、当局による大規模な監視の下、中国で独特のインセンティブ構造が形成され得ることを示している。

図表 222 空ブロックの中国国内・国外比較（左）とマイニングプール別内訳（右）の推移 [459]



(a) (b)

5.2.2.4 再識別手段

中国当局は国内に対して多大な影響力を行使し得る立場にあるが、中国当局がビットコインの再識別（非匿名化）を行う際には、以下の手段などが想定されている [459]。

- ヒューリスティックに基づくクラスタリング
- トラフィック解析：ビットコインネットワークのトラフィックを監視し、DPI などを用いてトランザクションがどの IP アドレスから生成されたのかを特定する
- サービス事業者の顧客情報提出の義務化：ビットコインを扱う商店や取引所に、アドレスとそれに紐づく顧客情報を提出させる。
- Web トラッキング情報の収集：E-commerce 等のビットコインアドレスと購入者情報の両方が分かるサイトのトラフィックからのトラッキング情報の取得、トラッカーの投入等
- 利用者による申告義務化

465 BIP152 として 2016 年 6 月 22 日にビットコインへ導入された。

5.2.3 アメリカ合衆国連邦政府による特定のビットコインアドレスの排除

5.2.3.1 経緯概要

米国財務省外国資産管理室（Office of Foreign Assets Control、以下 OFAC）は、2018 年 11 月 28 日に、SamSam ランサムウェアの身代金をイラン・リヤルに変換するのを手伝ったとして、イラン出身の二名（Ali Khorashadiza deh、Mohammad Ghorbaniyan）を制裁対象者リスト（Specially Designated Nationals and blocked Persons、以下 SDN）に登録するとともに、関連する二つのビットコインアドレス（149w62rY42aZBox8fGcmqNsXUzSStKeq8C と 1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V）を SDN に登録した[466]。SDN に個人に紐づく情報として暗号資産アドレスが登録されたのは初めてとなる。

米国政府は 2018 年 11 月からイラン制裁を再開しており、その一環の取組となる。登録されたアドレスは、SamSam ランサムウェアの身代金（被害者は 200 人以上）を含め、40 超の取引所とのやり取りし 7,000 回以上利用され、計 6,000BTC 扱っていた。もし取引所等がこれらのアドレスを含むウォレットを管理していた場合、（1）ウォレットを停止させるか、（2）凍結対象ウォレットを用意して、そこへ集約するかのいずれかで、制裁対象者がウォレットにアクセスできないようにする必要があり、いずれの場合も、監査証跡を保持し、10 営業日以内に OFAC に報告する必要がある[467]。

5.2.3.2 ビットコインコミュニティ等の反応

米国政府の対応に対する反応について、本稿執筆時点で大きな報道はなされていないが、取引所等はより一層コンプライアンスに努める一方、暗号資産コミュニティは反発して、より高度な匿名化技術の開発に進むことや匿名通貨の活発な利用などを通して、より地下に潜る危険性が懸念されている[468]。

466 U.S. Department of the Treasury, "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses", https://home.treasury.gov/news/press-releases/sm556, 2018/12/10

467 U.S. Department of the Treasury, "OFAC FAQs: Sanctions Compliance（646. How do I block digital currency? ）", https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#646, 2019/2/8

468 Kayla Izenman, "Crypto at the Crossroads: Exploring the Impact of the US Treasury's Bitcoin Sanctions", https://rusi.org/commentary/crypto-crossroads-exploring-impact-us-treasury%E2%80%99s-bitcoin-sanctions, 2019/3/19

5.2.4 まとめ

5.2.1 節「ロシア連邦政府による Telegram のブロッキング」の事例からは、クラウドサーバを介する中央集権型のサービス（Telegram）であっても、一国の当局がブロッキングすることは難しいことが分かる。IP 制限は偽装で容易に回避することが可能であり、また、Deep Packet Inspection も、技術的な難易度や運用負荷が高いため、大規模に行うのは難しいのではないかと考えられる。

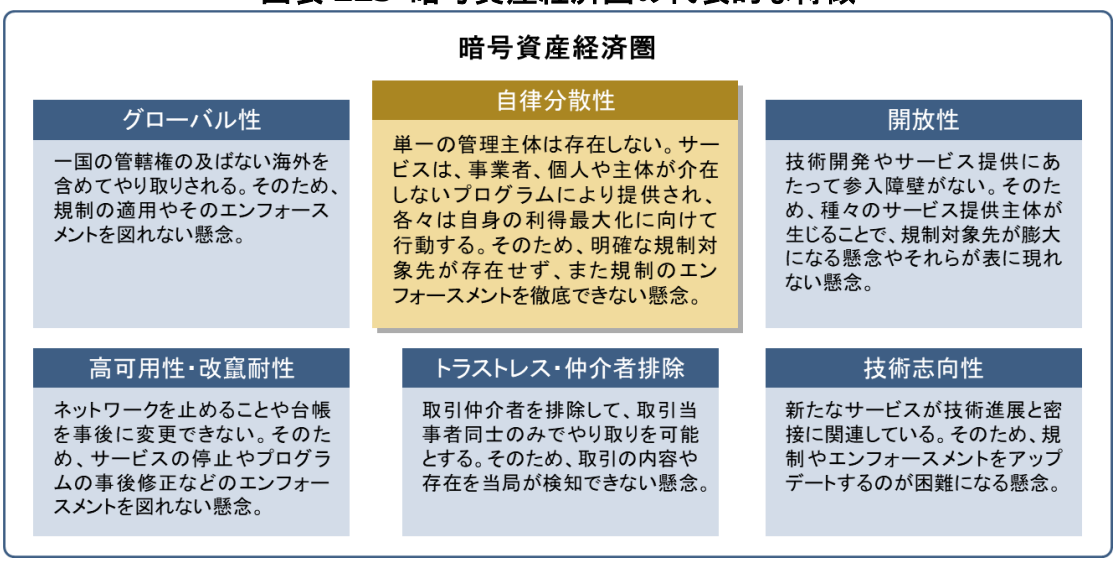
5.2.2 節「中華人民共和国政府によるビットコイン」の事例からは、Great Firewall や Great Canon などの技術的な対応では限界があることが予想される。最終的には、技術的な対応の他に、「利用者の申告義務化」や「顧客情報提出の義務化」などの制度的な対応も組み合せる必要があると考えられるが、その有効性については現時点では未知数である。

暗号資産取引を念頭に考えると、たとえ当局が規制をかけたとしても、暗号資産取引を制限することは技術的には極めて難しいことが予想される、また、制度的に制限したとしても、そのエンフォースメントの徹底も難しいと予想される。この場合、技術的に回避可能である限り、当局がいくら制度的に制限をかけても、5.2.3 節「アメリカ合衆国連邦政府による特定のビットコインアドレスの排除」で懸念されているように、暗号資産取引が地下に潜るだけの危険性が存在する。

5.3 課題への対応策

政策立案上の観点からは、自律分散性に代表される暗号資産経済圏固有の特性により、従来の規制アプローチは暗号資産経済圏には必ずしも有効でない懸念がある（図表 223）。すなわち、規制の強化は、脱法行為でなく適法行為のみを減少させるリスク濃縮など、意図せざる結果を招く危険性がある。また、暗号資産経済圏は、技術的な進展が極めて早く、法令等の実効性確保が技術的に難しい部分も存在する。

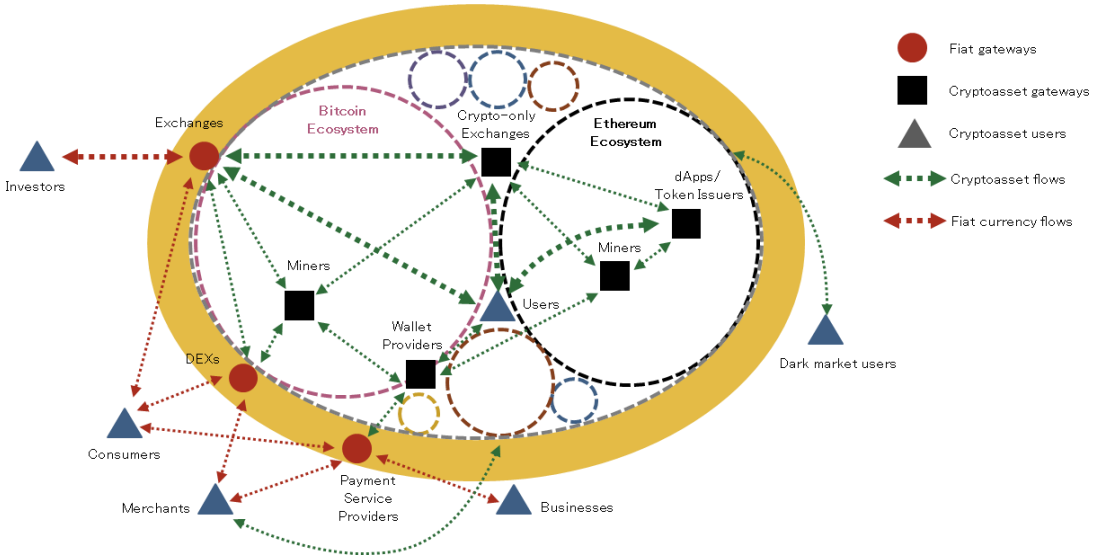
図表 223 暗号資産経済圏の代表的な特徴



例えば、AML/CFT の観点からは広く網をかけた上で抜け道を塞ぐことが肝要であるが、以下に挙げるような犯罪収益の資金洗浄経路を全て塞ぐことには困難が予想される（図表 224）。これは、一国からみて、 FATF 勧告の未遵守国の取引所、個人やプログラムなどにも法令対応を徹底させることは難しいと考えられるからである。

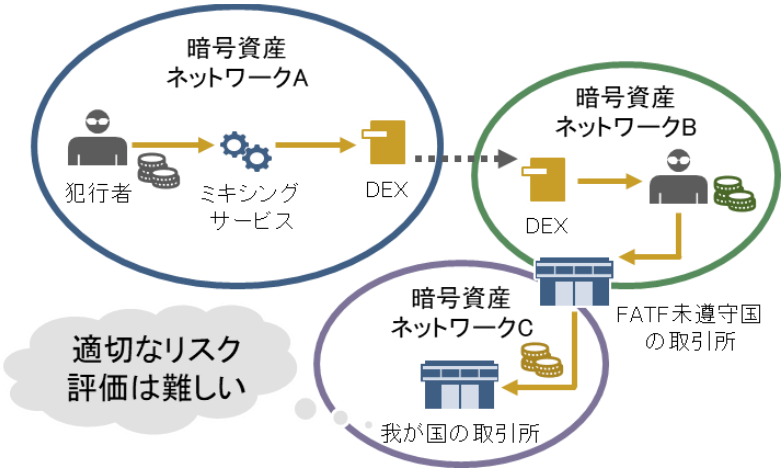
- 海外取引業者、ウォレット業者や個人
- 海外販売業者、決済代行業者や個人（ShapeShift、CoinPayments 等）
- ミキシングサービス・DEX 等運営事業者や個人（Bestmixer.io、IDEX 等）
- ライトニングネットワーク等の中継ノード運営業者や個人
- FATF 未遵守国の業者や個人
- デプロイ済みのプログラム（DEX 等）

図表 224 暗号資産経済圏内外の資産移転のイメージ



法令の対象先からみても、疑わしい取引を検知するにあたって、様々な先を経由して匿名化された取引のリスクを適切に評価することは非常に難しい（図表 225）。

図表 225 法令等の実効性確保が技術的に難しい例



上記を踏まえると、暗号資産経済圏に対しては、まず、予め法令等で明確に定める部分（法令等の実効性が確保できる部分）とそれ以外の部分に分けて考えることが必要と考えられる。

その上で、①法令等で定める部分についてはその実効性をしっかりと確保することが重要であり、②境界を含むそれ以外の部分については、暗号資産経済圏に関わるコミュニティが規制のゴールを理解し、そのゴールへ向けて自主的に取り組むように当局が促していく取組が重要になってくるのではないかと考えられる。

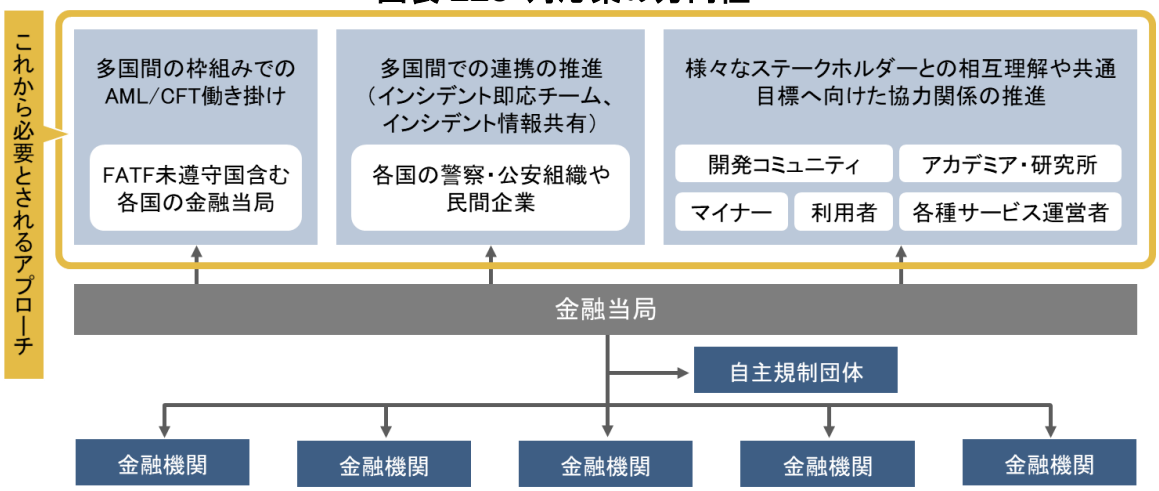
① 法令等で定める部分とは、主に暗号資産取引所や暗号資産決済代行事業

者が考えられる。ここでは、適格な事業者とそうでない事業者を峻別していくことが必要になっていくとともに、場合によっては、(i)取引所の入出金先を、適格な取引所の KYC 情報取得済みの先のみに絞る(安全な取引を囲い込む)ことや(ii)個人利用者も利用にあたっては登録制とすることなどの措置をとっていくことも選択肢として考えられる。

② それ以外については、当局が規制を指示し、それを監督するアプローチは、暗号資産経済圏に対しては必ずしも有効でなく、また、また技術的にも難しいことを踏まえると、仮想通貨経済圏に関わる様々なプレーヤーに向けた、多面的な対応が必要になる可能性がある。例えば、(i)業界横断ないし国際的に犯罪データを共有すること[469]や、(ii)非識別技術の開発を促進させること[470]、(iii)自身のアドレスを自己申告制とすること、(iv)警察・公安等と協力し即応態勢を構築すること[471]などが考えられる。

特に、②それ以外の部分への対応については、当局にとって従来のアプローチと大きく異なる取組になることが予想される。そのため、社会的厚生の増大という共通の目標、すなわち、適切な利用者保護や取引の適正化など、透明性が高く公平で信頼できる暗号資産経済圏の実現へ向けて、当局は様々なステークホルダーと相互理解を深め、共通目標へ向けた協力関係となるよう取り組むことが望ましいと考えられる(図表 226)。

図表 226 対応策の方向性



469 犯罪データを構築する際は当局主導か民間主導かが論点になると考えられる。
470 米国国土安全保障省は、法執行機関での活用を念頭に、匿名通貨であるモネロ、ジーキャッシュの追跡技術確立へ向けた事前引き合い書(pre-solicitation document)を公表している。Nikhilesh De, coindesk, "US Government Interested in Tracking Privacy Coins, New Document Shows", https://www.coindesk.com/us-homeland-security-is-interested-in-tracking-privacy-coins, 2018/12/11
471 拡散を阻止するため、手数料を意図的に引き上げるなども選択肢として考えられる。