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

2019年3月20日

金融庁
Financial Services Agency

株式会社三菱総合研究所
社会ICTイノベーション本部

目次

目次

用語集

用 語	意 味
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
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
DeFi	Decentralized Finance：分散型金融 ブロックチェーン上のスマートコントラクトを介して提供される金融サービスの総称
DEX	Decentralized Exchange：分散型取引所
FATF	Financial Action Task Force：金融活動作業部会
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、現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
KYC	Know Your Customer：本人確認
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）
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
クリプトロンダリング	Crypto-Laundering：暗号資産を用いた資金洗浄
セキュリティ	Security：犯罪等からの保護や保安
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
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）

用語集

用 語	意 味
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
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
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
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）
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

Pfitzmann, A., et al, Technische Universitat Dresden, “A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management”, https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, 2019/2/7を参考に記載

謝辞・免責事項

謝辞

- 本報告書作成にあたっては、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。

免責事項

- 本報告書の内容は金融庁の公式見解を示すものではない。
- 本報告書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。

1 背景

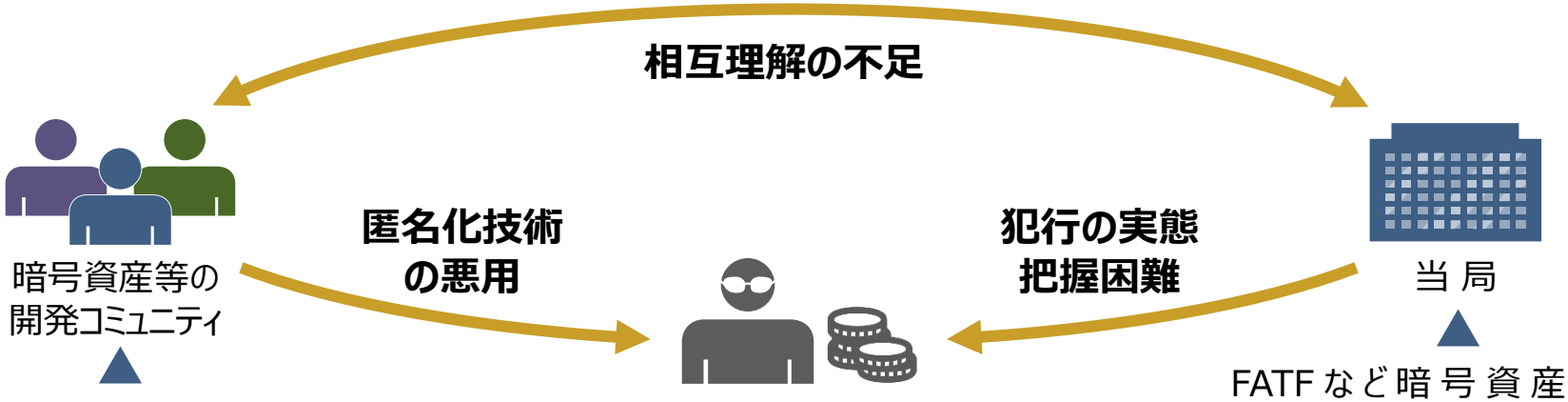
本章の要旨

- 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、各種匿名化技術の急速な進展により、暗号資産取引の把握や追跡は困難な状況になりつつある。そのために、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も困難となりつつある。
- 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。
- 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、クリプトロンダリング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。こうした懸念は既に一部現実化しつつあると言える。
- このような状況は、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。

1.1 暗号資産のAML/CFTを取り巻く状況－現状

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、各種匿名化技術の急速な進展により、暗号資産取引の把握や追跡は困難な状況になりつつある。そのために、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も困難となりつつある。

暗号資産のAML/CFTを取り巻く主なステークホルダーの状況



通貨としての利便性向上やプライバシー保護等の考えに紐付けつつ匿名性向上へ向けた各種取組を進めているところ。
匿名通貨や管理主体なしにサービス提供する分散型取引所、匿名通信技術などの開発が進む。

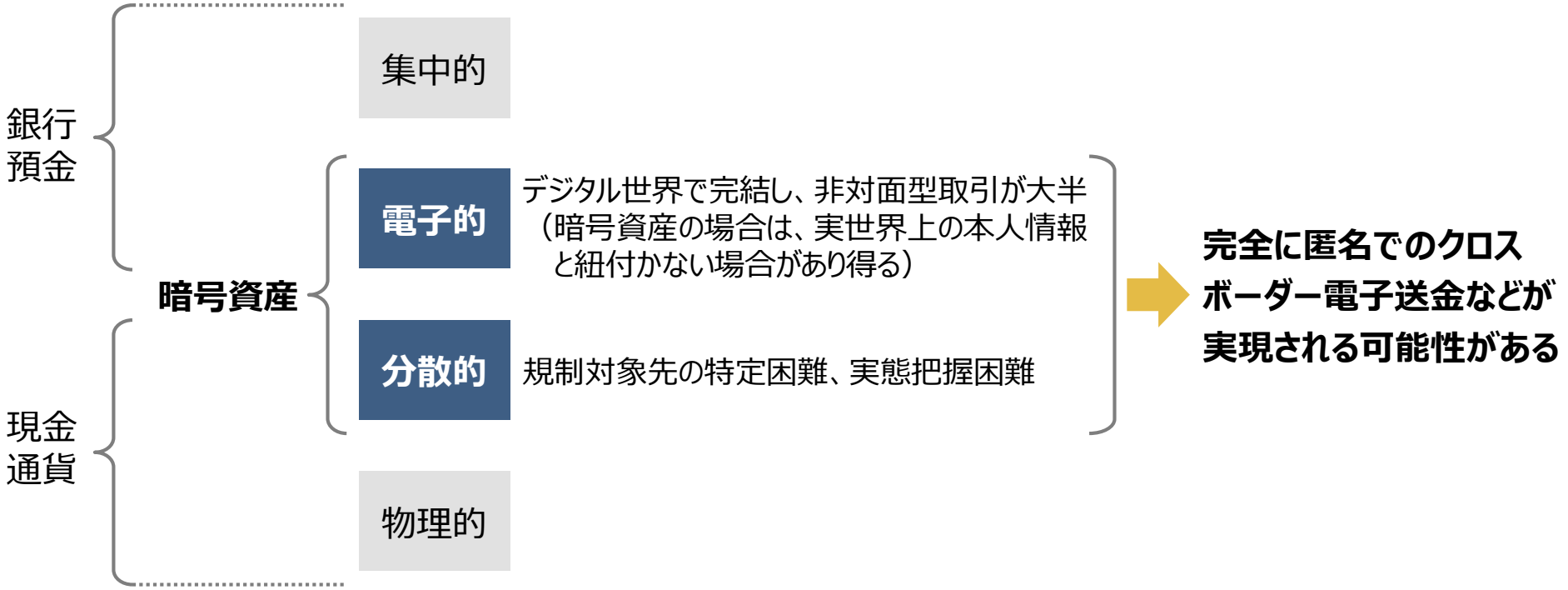
ランサムウェアやクリプトジャック、取引所を狙ったサイバー犯罪など、攻撃頻度の増加、手法の多様化を進めているところ。
こうして得た暗号資産は、匿名化技術を悪用して資金洗浄が行われる。

FATFなど暗号資産を巡るAML/CFTの観点からの議論が国際的に高まる中、 仮想通貨交換業者に対して、本人確認およびマネーロンダリング防止対応により水際で防止すべく制度対応を講じているところ。
ただし、犯行の実態把握や追跡は困難な状況となっている。

1.1 暗号資産のAML/CFTを取り巻く状況－暗号資産の特性

電子的・集中的に処理される銀行預金と物理的・分散的に処理される現金通貨の性質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。

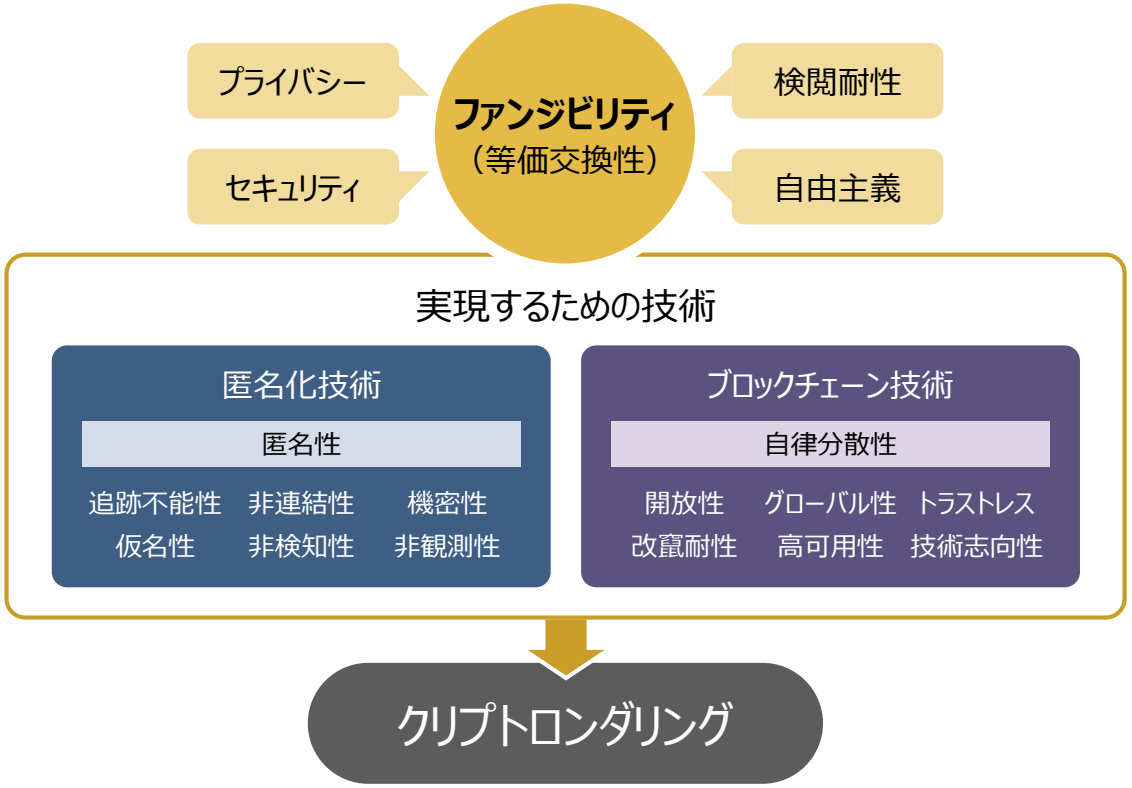
法定通貨と比較した場合の、暗号資産の通貨としての特性



1.1 暗号資産のAML/CFTを取り巻く状況－開発動向

前項の特性に加え、ファンジビリティ（等価交換性、過去の取引内容や移転経路によらず同額であれば等価で交換可能という性質）の確保やプライバシー保護等の考えに紐付けられつつ、暗号資産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。

暗号資産のファンジビリティを巡る概念とクリプトロンダリングの関係



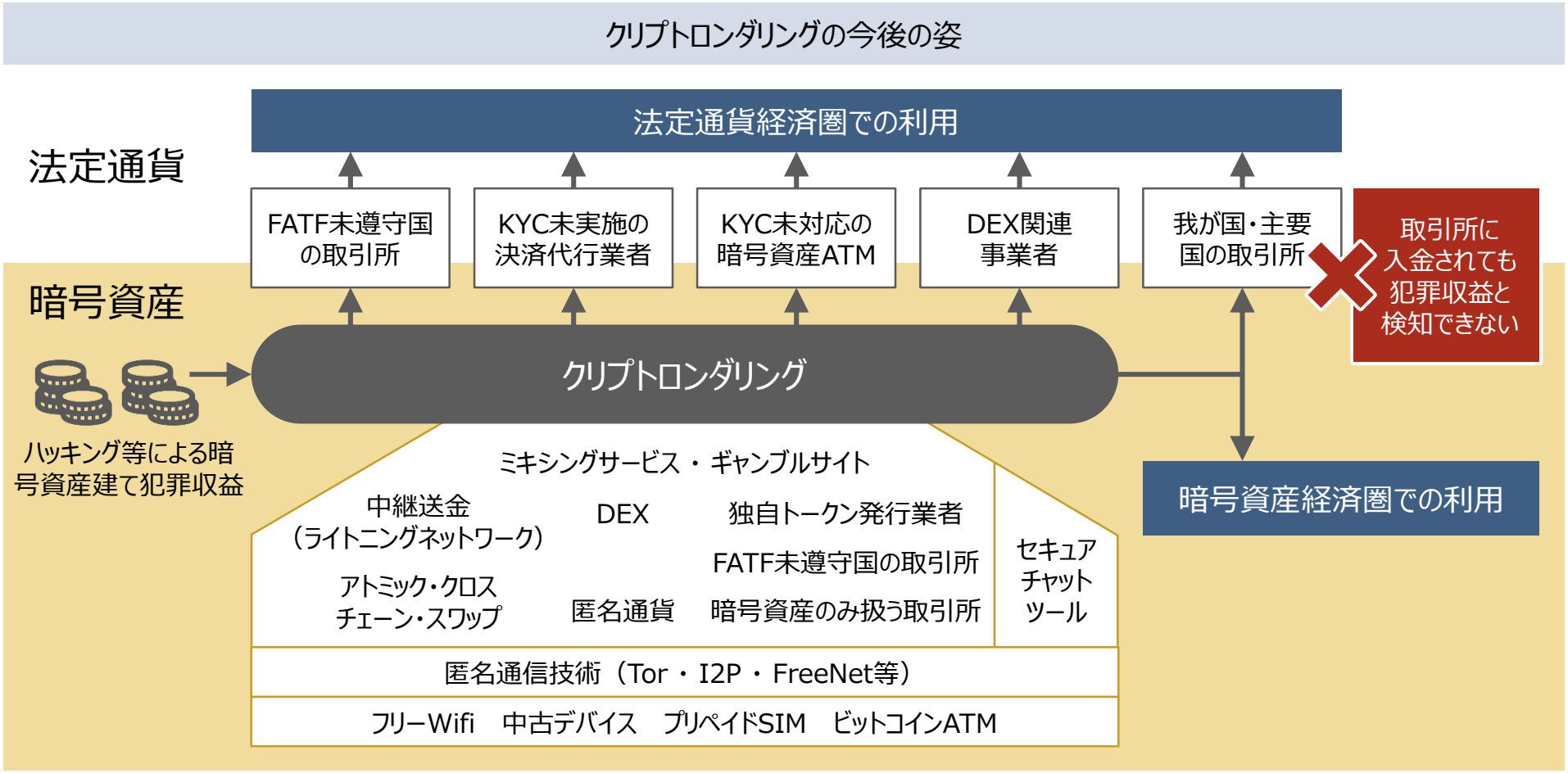
ファンジビリティは、通貨としての重要な性質であり、暗号資産が実現すべき目標と考えられている。

『過去の取引内容やその移転経路によらない』という点を『それらを公にされないこと』と解釈すると、プライバシー、セキュリティ、さらに検閲耐性や自由主義といった考えにも紐付けられ、このような文脈で暗号資産コミュニティでは議論されている。

他方で、ファンジビリティを実現する技術である匿名化技術（匿名性等）とブロックチェーン技術（自律分散性等）が組み合わさると、資金洗浄などの犯罪へ悪用される危険性も生じる。

1.1 暗号資産のAML/CFTを取り巻く状況－将来的な展望

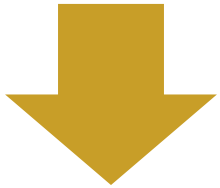
今後、暗号資産経済圏が拡大し、匿名化技術も進展していく中では、クリプトロンダリング等のリスクはさらに拡大・深刻化していくことが懸念される。



1.2 本調査研究の問題意識

暗号資産経済圏のプレーヤーは多岐に渡り、今後も増加が見込まれるが、こうした中で匿名化技術が分散型サービスとして広く普及した場合、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。こうした懸念は既に一部現実化しつつある。

このような状況は、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。

2 暗号資産を取り巻く状況

2.1 暗号資産経済圏の拡大
2.2 暗号資産関連犯罪の拡大
2.3 クリプトロンダリング

本章の要旨

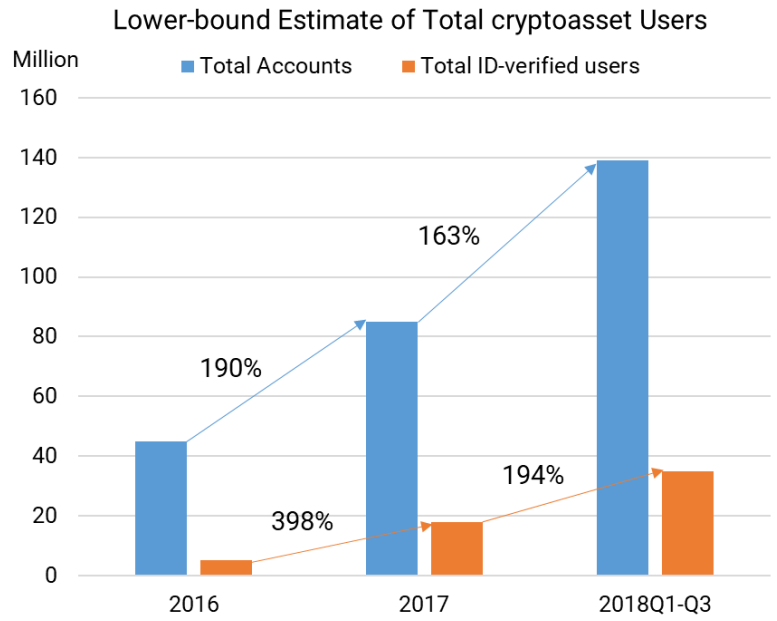
- 暗号資産経済圏は、未だ規模は小さいものの、個人利用を中心に世界的に拡大している。
- 暗号資産の用途も広がりを見せており、物品購入、法定通貨との取引や資本逃避以外に、暗号資産同士の取引やサービス利用手段としての利用も増加している。
- 他方で、暗号資産を用いた犯罪リスクも増加している。ビットコインは匿名ネットワーク上での違法な電子商取引で既に広く利用されているが、近年はビットコイン以外の暗号資産の利用も拡大している。さらに、暗号資産に関連したサイバー犯罪も増加傾向にあり、暗号資産取引所を狙うサイバー犯罪や一般人を狙うクリプトジャックなど手法の多様化とあわせて、被害額の増大を招いている。
-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

2.1 暗号資産経済圏の拡大－利用の拡大

当初は金融危機や高インフレ国における資本逃避手段やダークマーケットの決済手段として注目を集めた暗号資産は、近年急速にその利用が拡大。暗号資産利用者の口座数は全世界で凡そ1.4億弱、利用者の多くが個人と推定されている。

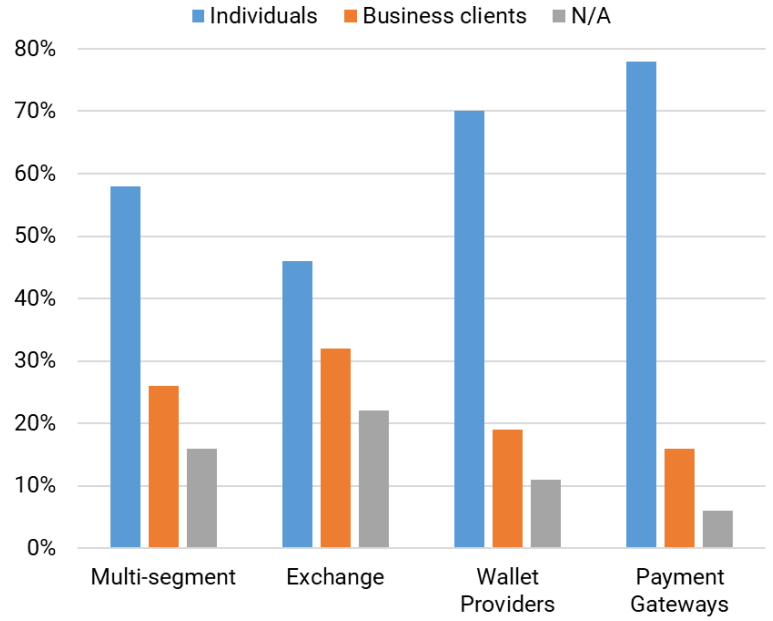
暗号資産利用者の口座数の推移

47ヶ国を対象とした調査では、暗号資産利用者の口座数は2018年に63%の伸び（1.4億）、うち約25%はKYC済みの利用者。



事業種別毎の暗号資産利用者の内訳

いずれの事業種別においても個人利用が中心となる（Multi-segmentとは、それ以外のいずれかを組合せた事業種を指す）。

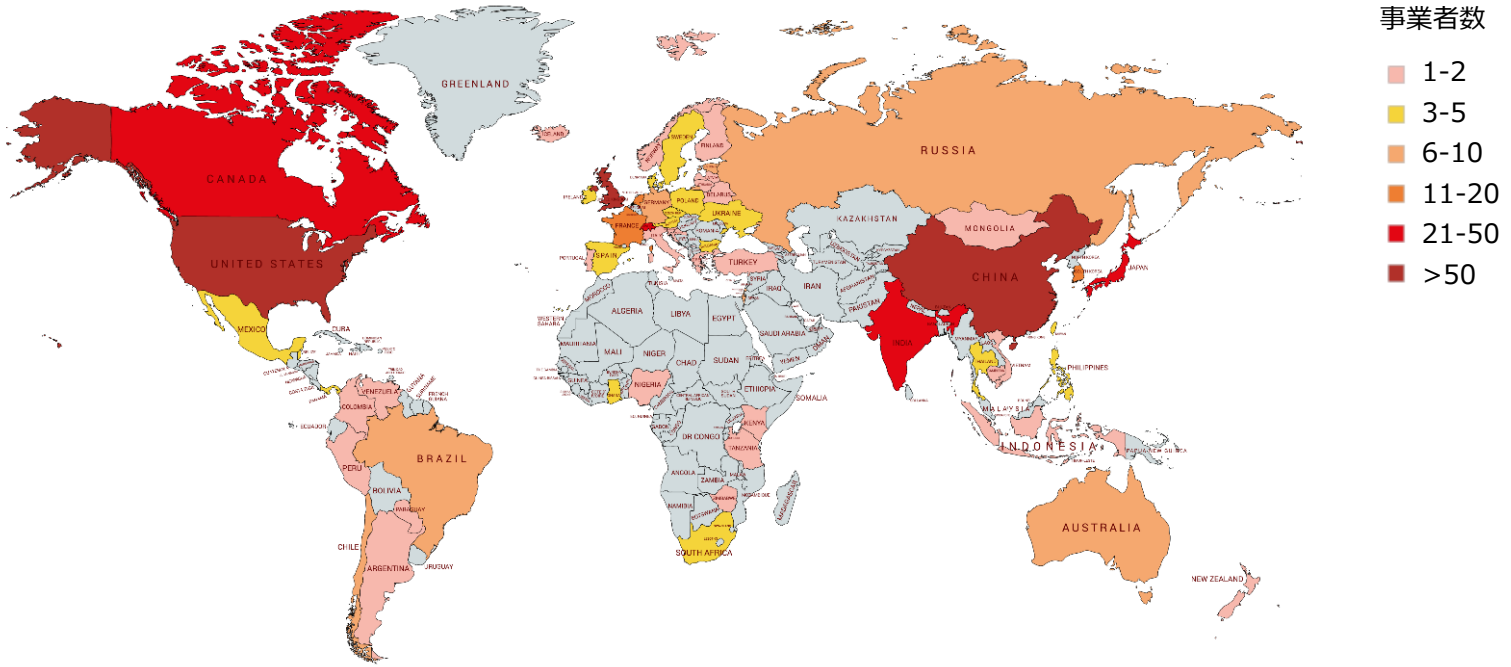


（左・右） Rauchs, M., et al., University of Cambridge Judge Business School, "2nd Global Cryptoasset Benchmarking Study", https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf, 2019/1/9より三菱総研作成

2.1 暗号資産経済圏の拡大－事業者の拡大

暗号資産関連サービスを提供する事業者は世界的に拡大。日本・米国・欧州・カナダにおいては、国民の凡そ2-9%が暗号資産関連事業者等を介して暗号資産を保有していると推定されている。

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）

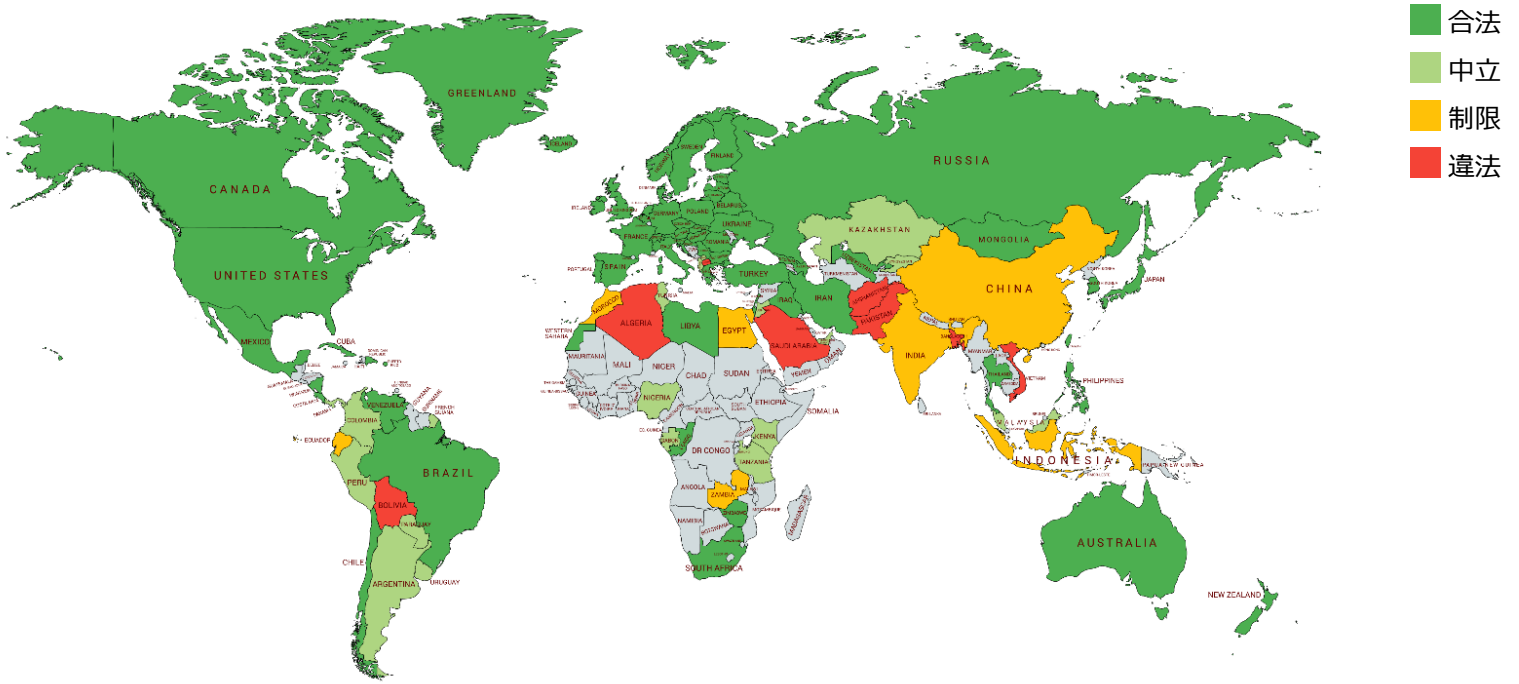


Rauchs, M., et al., University of Cambridge Judge Business School, “2nd Global Cryptoasset Benchmarking Study”, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf, 2019/2/23より
Minas, “mapchart.net”, https://mapchart.net/world.html, 2019/2/23を用いて三菱総研作成

2.1 暗号資産経済圏の拡大－法的な位置付け

ビットコインは110ヶ国において合法ないし中立と報告されているものの、その法的な位置づけは通貨（Currency）以外にも財（Property）やコモディティ（Commodity）など分かれており、各国で規制内容も異なることが考えられる。

ビットコインの法的な扱い

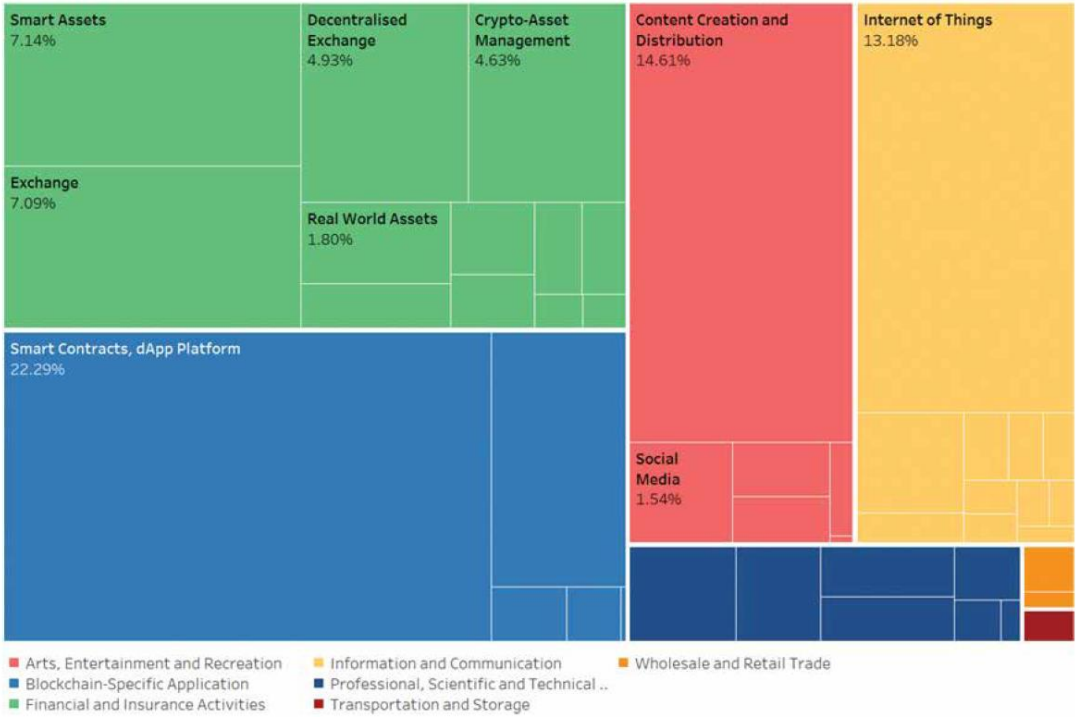


Coin Dance, coin.dance, “Bitcoin Legality by Country”, https://coin.dance/poli/legality, 2019/2/23より
Minas, “mapchart.net”, https://mapchart.net/world.html, 2019/2/23を用いて三菱総研作成

2.1 暗号資産経済圏の拡大－利用用途の拡大

暗号資産の用途として、交換手段（Exchange Token）、投資・資金調達手段（Security Token）、サービス利用手段（Utility Token）の三種類に大別する指摘が多い。交換手段としては特に情報商材との親和性が高く、近年はサービス利用手段としての利用が増加している（SNS、ゲーム、コンテンツ配信等）。

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）



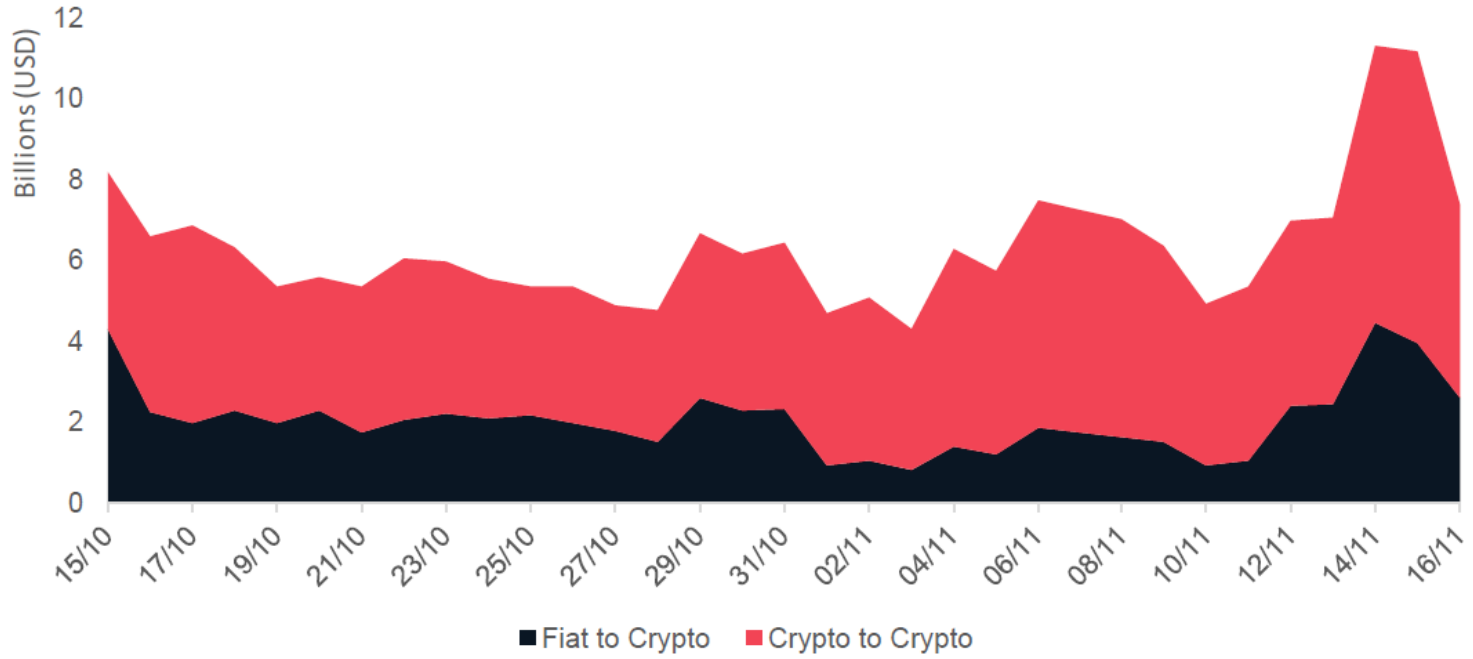
CryptCompare, Crypt Coin Comparison LTD, "Cryptoasset Taxonomy Report 2018", https://www.cryptocompare.com/media/34478555/cryptocompare-cryptoasset-taxonomy-report-2018.pdf, 2019/1/11

2.1 暗号資産経済圏の拡大－暗号資産同士の取引

現在までに1,900種類以上（亜種も含めた調査では16万種以上）の暗号資産が提案されており、暗号資産同士の取引も活発に行われている。

現物取引における暗号資産取引額の内訳（2018年10月～11月）

70以上の取引所のデータを用いた調査では、暗号資産同士の取引額は現物取引額全体の約2/3を占める（暗号資産のみ扱う取引所が全体の4割強）。



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

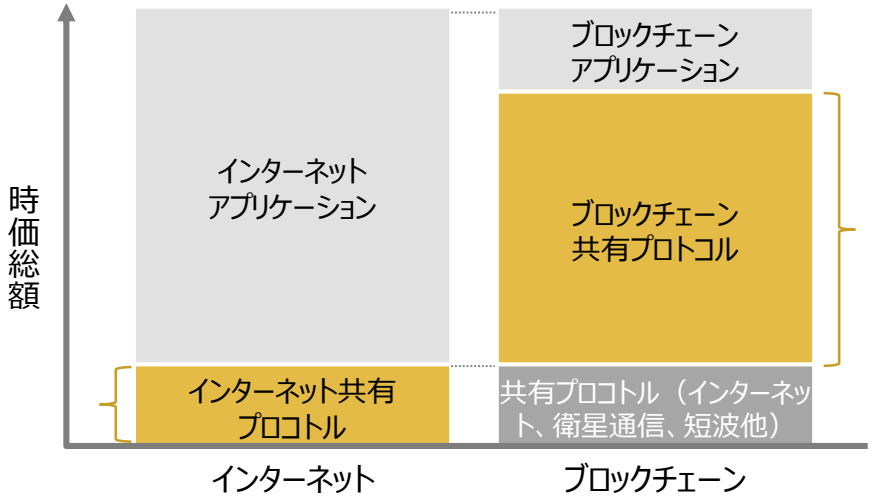
2.1 暗号資産経済圏の拡大－ブロックチェーン技術の可能性

ブロックチェーンは、アプリケーションよりも、共有データ・共有トークンを提供する共有プロトコルの時価総額が早く成長するため、従来のビジネスモデルを変える可能性があるとの指摘がなされている。

また、DApps（分散型アプリケーション）は、特定の管理主体が不要、常時利用可能、プログラムロジックが公開されており透明性が高い、プログラム可能な支払いを実現できるなどの特徴から、その可能性に大きな期待が寄せられている。

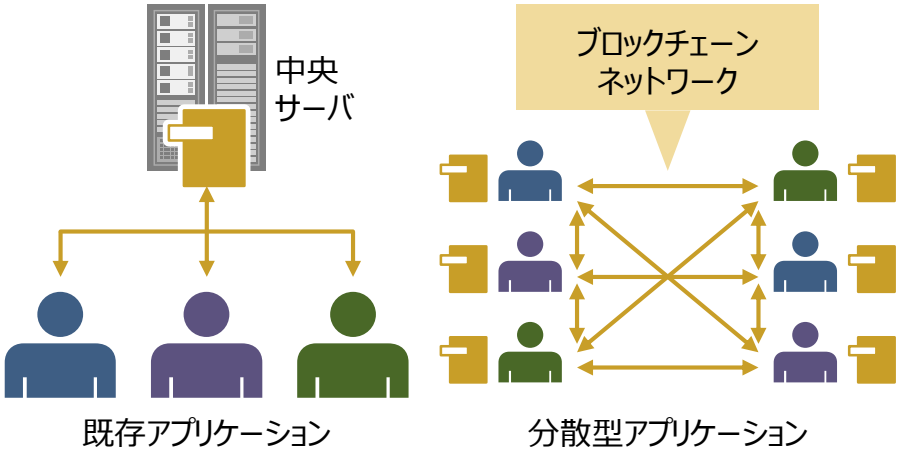
インターネットとブロックチェーンの比較

ブロックチェーンの共有プロトコルは、様々なアプリケーションが利用できる共有データと共有トークンを提供する。そのため、個々のアプリケーションの成功が、トークンやデータの需要や投機を呼び、共有プロトコルの時価総額を上昇させるため、共有プロトコルの方が早く成長すると指摘されている（著名な指摘だが、その妥当性については見解が分かれている）。



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

ブロックチェーン上にデプロイされた分散型アプリケーションは、プログラムのロジックが公開されており、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という特徴があり、こうした透明性や検証性が重要な特徴として考えられている。



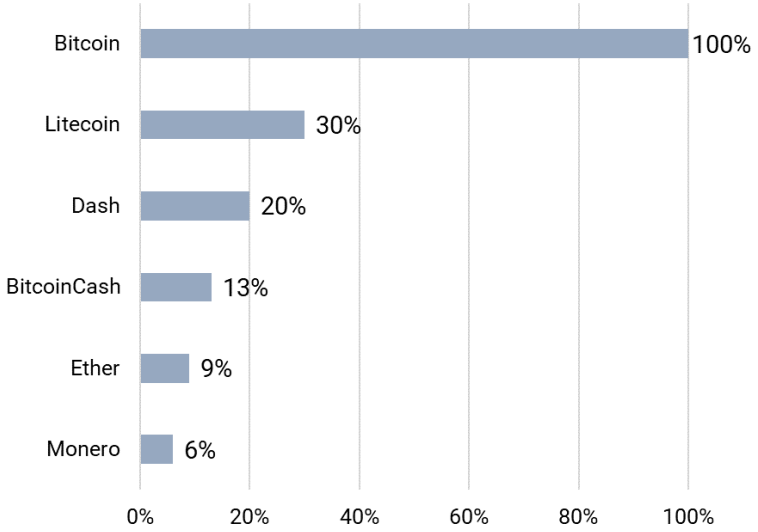
（左）Monegro, J., UNION SQUARE VENTURES, “Fat Protocols”, http://www.usv.com/blog/fat-protocols, 2019/1/11より三菱総研作成

2.2 暗号資産関連犯罪の拡大 – ダークマーケットでの利用

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いるが、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。

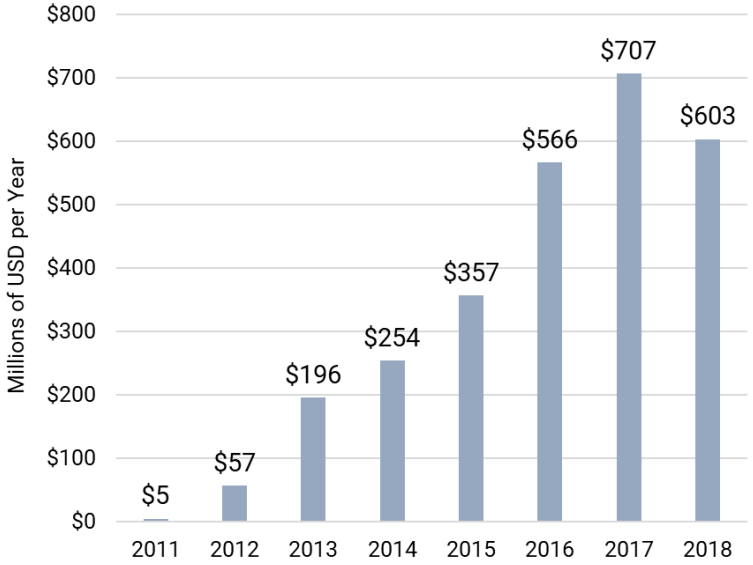
ダークマーケットでの暗号資産の取扱状況（2018年）

ダークウェブ上のマーケットプレイスや掲示板など150サイトを調査したところ、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。なお、英語圏ではモネロ、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。



ダークマーケットへのビットコインの流入量（2011～2018年）

ビットコインに絞っても、ダークマーケットへの流入量は2017年に7億ドルを超えた。2017年中頃からは、ビットコインの手数料の増大、処理遅延の拡大等により、他のコインへ一部流れていると推測されている。



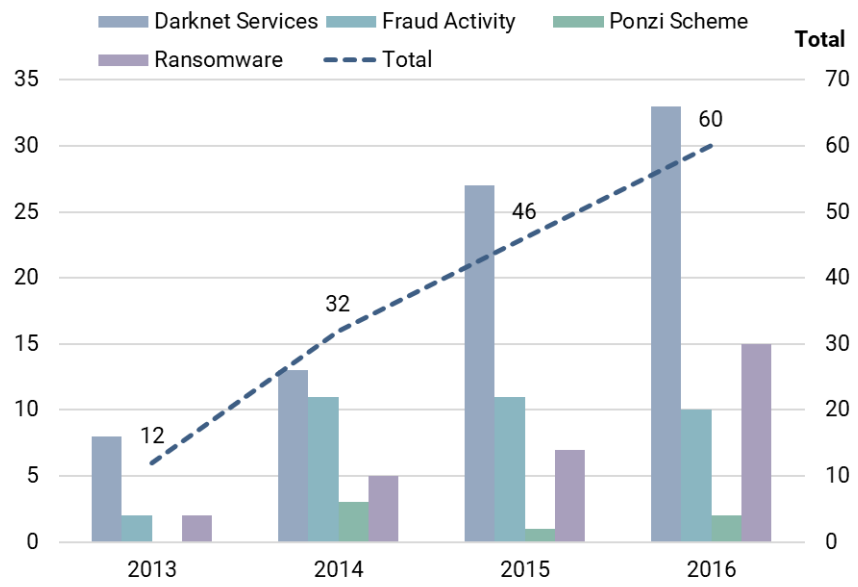
（左）Barysevich, A., et al, Record Future, "Litecoin Emerges as the Next Dominant Dark Web Currency", https://www.recordedfuture.com/dark-web-currency/, 2019/2/23 より三菱総研作成
（右）Chainalysis Team, Chainalysis, "Crypto Crime Report - Decoding increasingly sophisticated hacks, darknet markets, and scams January 2019", https://blog.chainalysis.com/2019-cryptocrime-review, 2019/2/23 より三菱総研作成

2.2 暗号資産関連犯罪の拡大 – ダークマーケットの動向

ダークマーケットは増加傾向にあり、かつ、複数の事業者に分散化しつつある。こうしたダークマーケットで用いられた暗号資産は、次に資金洗浄サービスへ送られると考えられる。

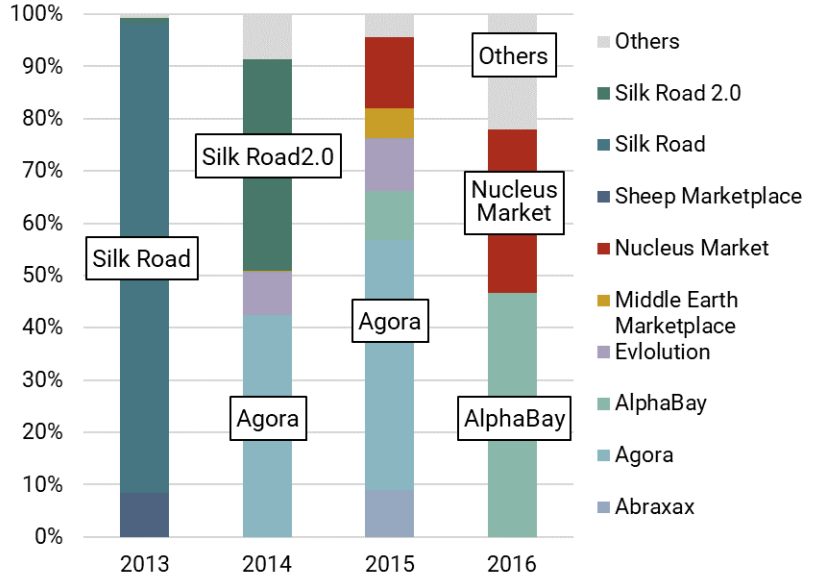
暗号資産建て犯罪収益を扱う違法事業者数の推移（2013～2016年）

暗号資産建て犯罪収益を扱う先はダークマーケットが大半を占める。ランサムウェア等含めて全体としても増加傾向にあり、2013年から2016年にかけて5倍（計60事業者）に拡大している。



ダークマーケットの内訳（資金洗浄サービスへの流入割合、2013～2016年）

主要なダークマーケットは、SilkRoad（2013年閉鎖）、Agora（2015年閉鎖）、AlphaBay（2017年閉鎖）と変遷が見られるが、プレーヤーは徐々に分散化している。



（左・右）Fanusie, Y., et al, Foundation for Defense of Democracies (the Center on Sanctions and Illicit Finance), “Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services”, https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf, 2019/1/18より三菱総研作成

2.2 暗号資産関連犯罪の拡大－サイバー犯罪事件

我が国では、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へ社会的な関心が高まる。

主要なサイバー犯罪事件の例

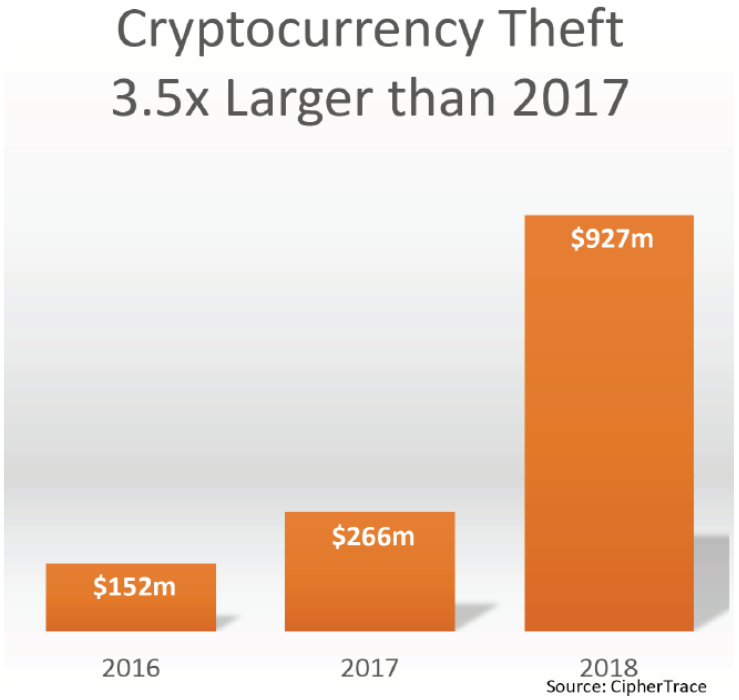
発生時期	取引所／事件の名称	被害額
2014年2月	MtGox（日）	約470億円
2016年6月	The DAO	約65億円
2016年8月	Bitfinex（香）	約65億円
2017年6月	Wanacry	約1600万円（身代金額）
2017年11月	Thether（米）	約50億円
2017年12月	NiceHash（スロベニア）	約68億円
2018年1月	Coincheck（日）	約580億円
2018年2月	BitGrail（伊）	約181億円
2018年6月	Coinrail（韓）	約40億円
2018年6月	Bithumb（韓）	約33億円
2018年7月	Bancor（瑞西）	約15億円
2018年9月	Zaif（日）	約70億円

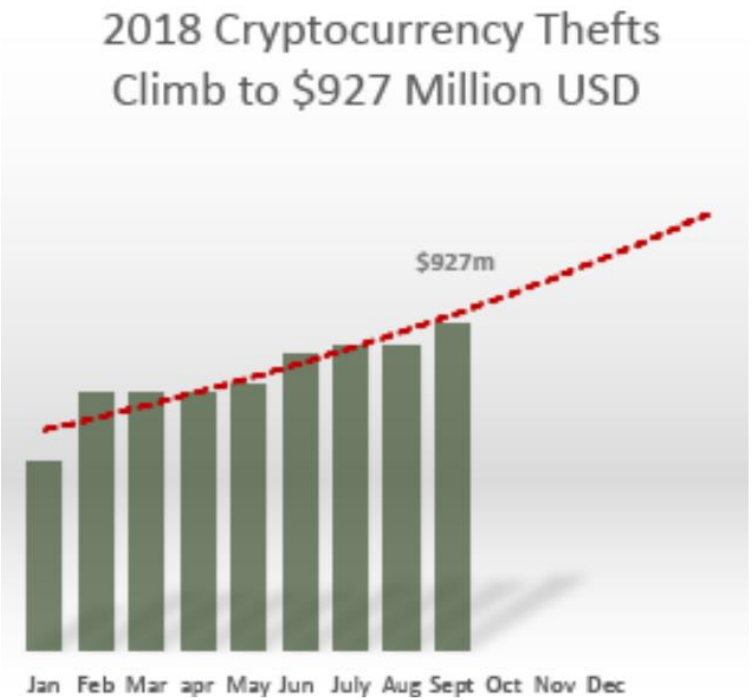
以下の資料を参考に三菱総研にて社会的影響の大きい事例を追記。楠 正憲, 情報処理学会 特別解説, "Zaifからの暗号資産流出 ～仮想通貨交換業者はアントローラブル？～", https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=191952&item_no=1&page_id=13&block_id=8, 2019/1/7

2.2 暗号資産関連犯罪の拡大－サイバー犯罪被害額の拡大

暗号資産取引所等のサイバー犯罪被害額は、2018年第3四半期までに、2017年の約3.5倍（9.27億ドル）に増加し、2018年内に10億ドルを超えると推定されている。こうして窃取された暗号資産も、次に資金洗浄サービスへ送られると考えられる。

暗号資産取引所等の被害額の状況（左：年別、右：2018年の月別）





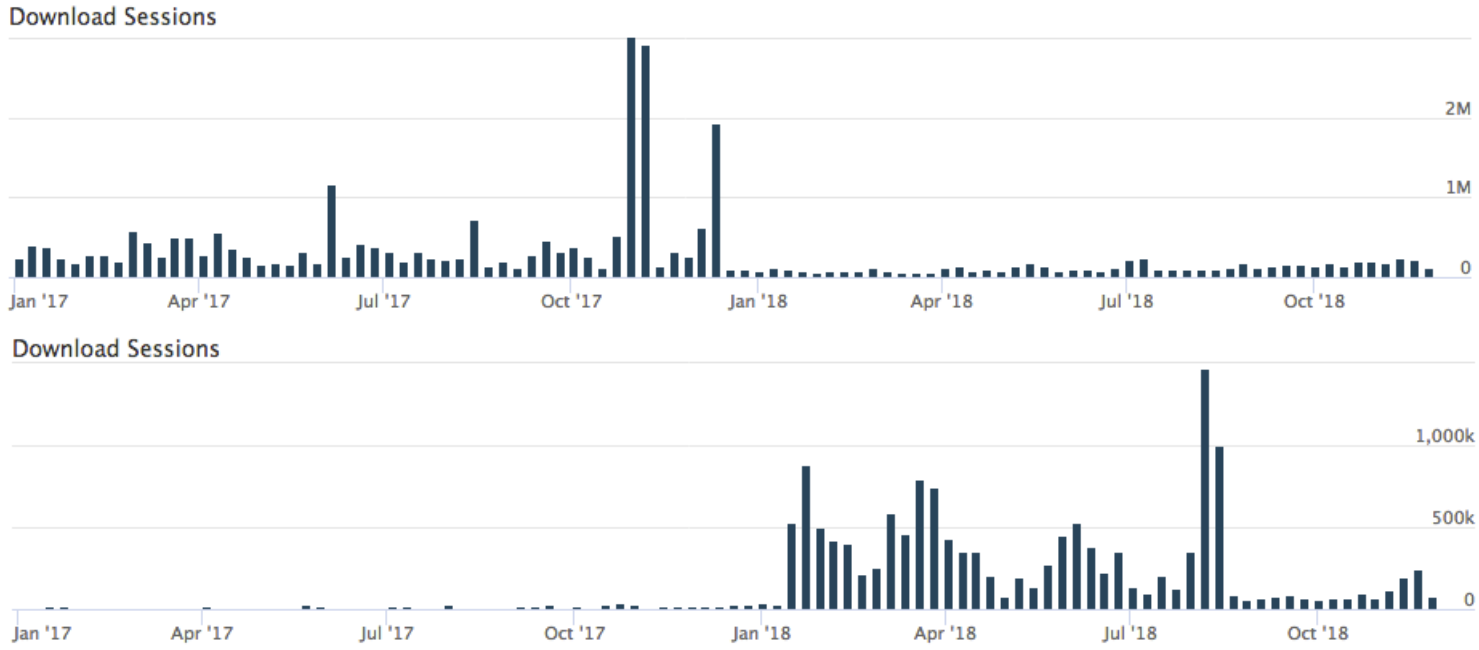
（左・右）CipherTrace, CipherTrace, Inc., "Cryptocurrency Anti-Money Laundering Report - Q3 2018", https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf, 2019/1/11

2.2 暗号資産関連犯罪の拡大 – 攻撃手法の変化

近年は、暗号資産取引所を狙うサイバー犯罪以外に、ブロックチェーン再編成を悪用した犯罪や、一般人を狙うランサムウェア、フィッシング詐欺、クリプトジャックなど、攻撃頻度の増加や手法の多様化が見られる。

ランサムウェア検出数（上）とクリプトジャックマルウェア検出数（下）の推移

暗号資産の高騰した2017年末から、攻撃手法が変化したと考えられる。

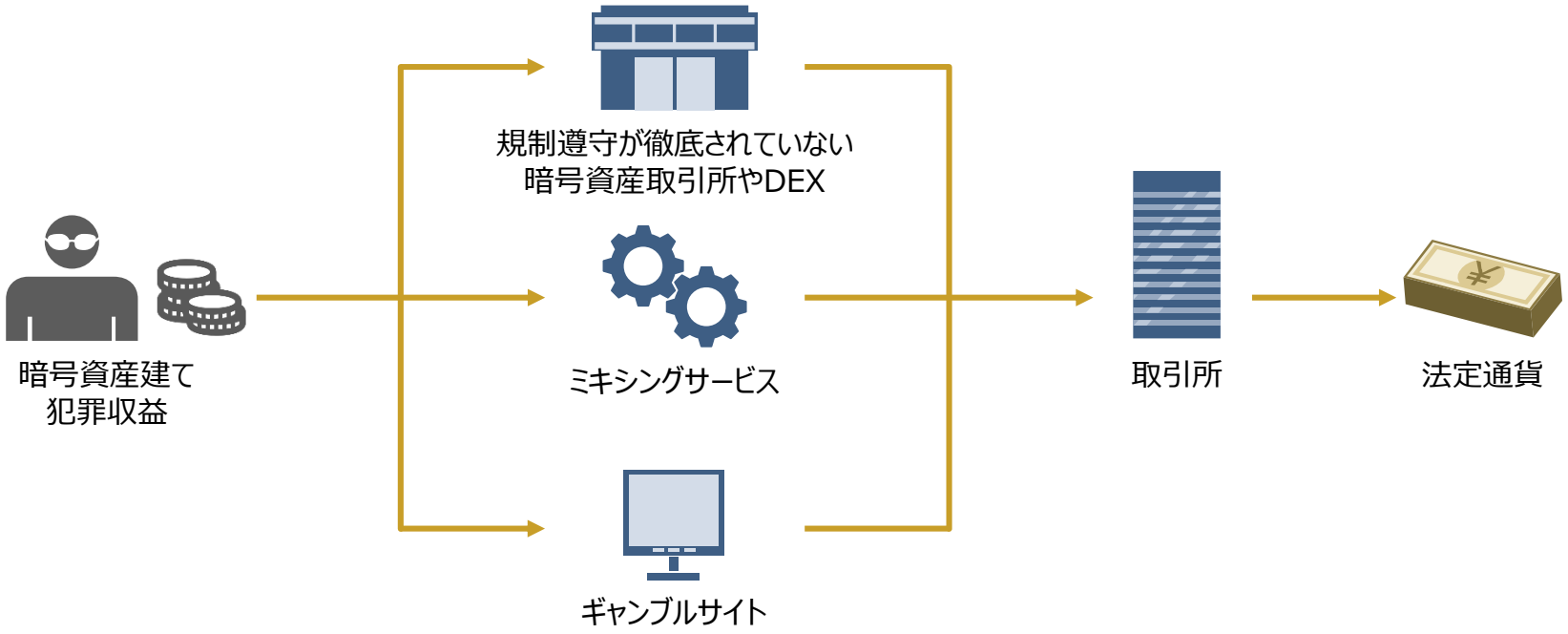


（上）林 薫, Palo Alto Networks, Inc., "2018年のサイバー脅威の振り返りと2019年の予測", https://www.paloaltonetworks.jp/content/dam/pan/ja_JP/Images/blog/2018/126525/picture-02.png, 2019/1/30
（下）林 薫, Palo Alto Networks, Inc., "2018年のサイバー脅威の振り返りと2019年の予測", https://www.paloaltonetworks.jp/content/dam/pan/ja_JP/Images/blog/2018/126525/picture-03.png, 2019/1/30

2.3 クリプトロンダリング

暗号資産建て犯罪収益の資金洗浄にあたっては（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が一般に良く利用されると考えられている。

クリプトロンダリングのイメージ（一例）

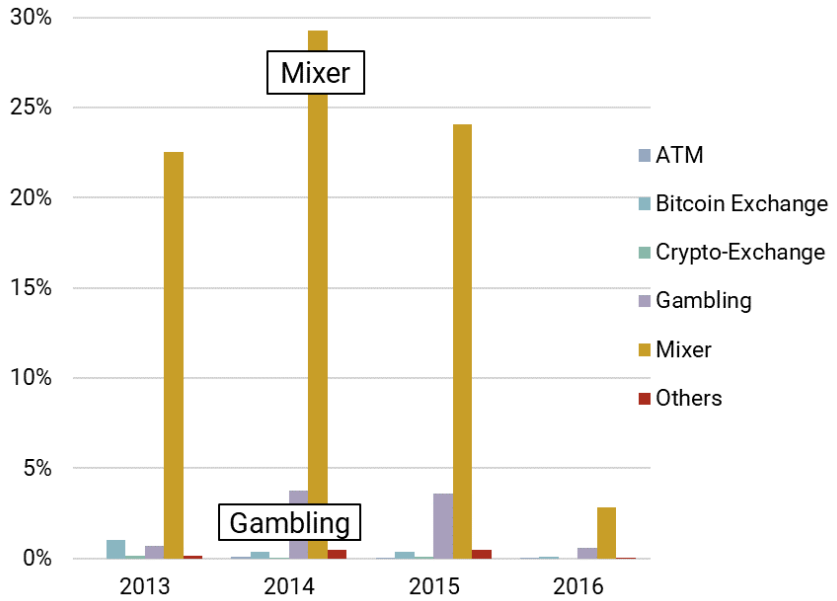


2.3 クリプトロンダリング – 資金洗浄に利用されるサービスの内訳

資金洗浄に利用されるサービスの内訳としては、一般の暗号資産取引所に加え、ミキシングサービスやギャンブルサイト、DEXなどが考えられている。

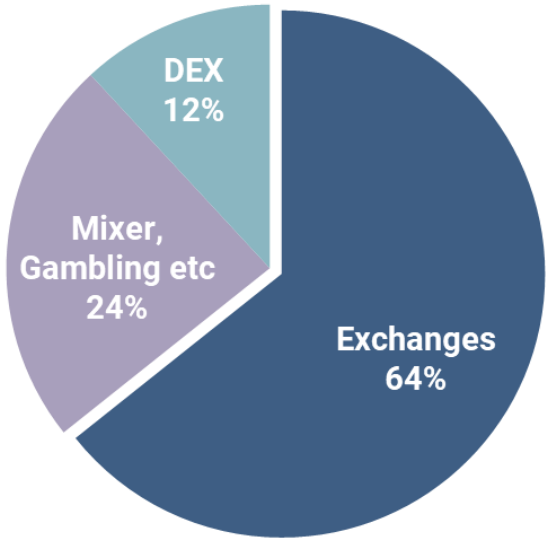
犯罪収益の割合の推移（2013～2016年）

例えば、ミキシングサービスに入金されるビットコインの約1/4～1/3が犯罪に紐づくものであった（2016年は取引量が急増したため、割合は全般に低下している）。



資金洗浄に利用されるサービスの内訳（2018年）

ダークマーケット等から資金洗浄のために送金されるサービスの内訳は、通常の取引所、ミキシングサービスやギャンブルサイト、DEXの順となる。



＊ 左・右ともに全ての暗号資産犯罪やダークマーケット取引を網羅していない点に留意。

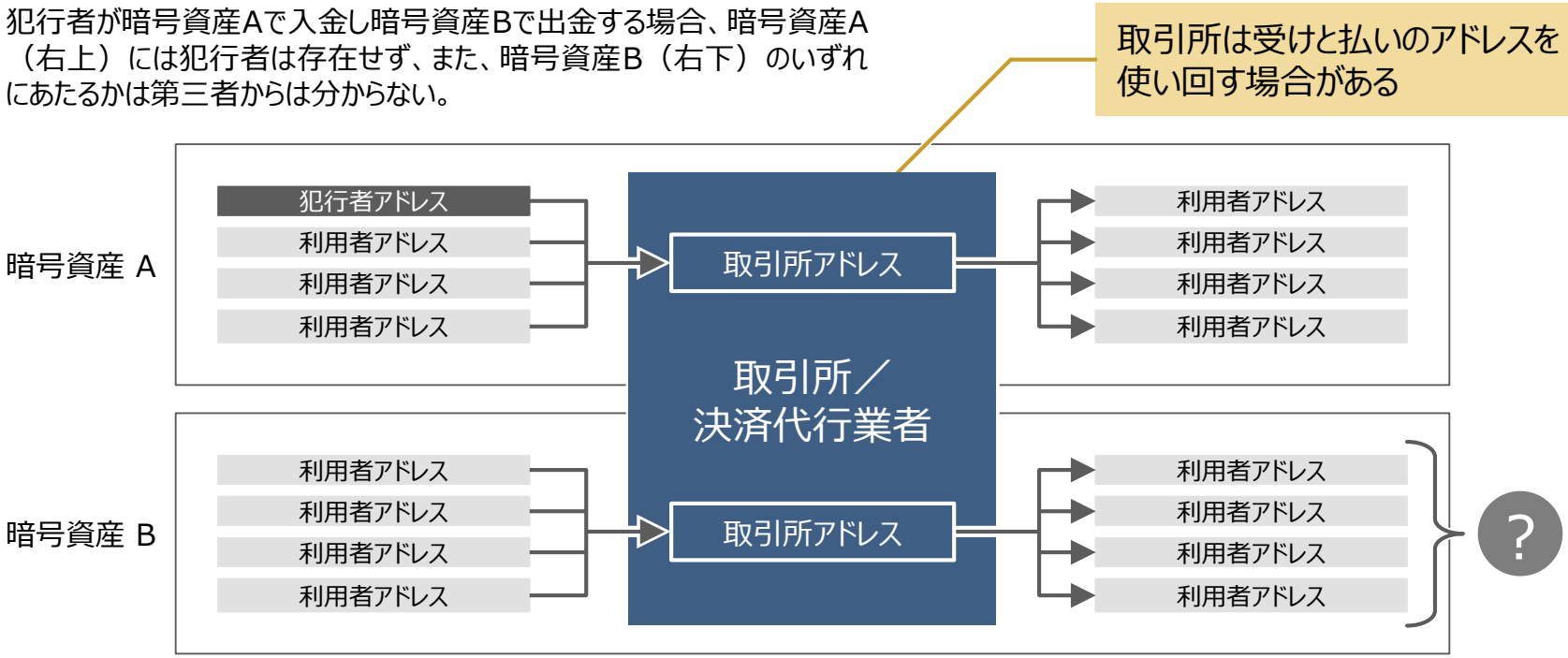
（左） Fanusie, Y., et al, Foundation for Defense of Democracies (the Center on Sanctions and Illicit Finance), “Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services”, https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf, 2019/1/18より三菱総研作成
（右）Chainalysis Team, Chainalysis, "Crypto Crime Report - Decoding increasingly sophisticated hacks, darknet markets, and scams January 2019", https://blog.chainalysis.com/2019-cryptocrime-review より三菱総研作成

2.3 クリプトロンダリング – 暗号資産取引所

暗号資産取引所は、法定通貨や他の暗号資産と交換できることや取引所に入った後の移動経路が第三者からは分からないことなどから資金洗浄に利用されやすい。民間の調査では、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～2018年9月までで約25億ドルに上ると推定されている。

取引所を用いた暗号資産の資金洗浄のイメージ（一例）

犯行者が暗号資産Aで入金し暗号資産Bで出金する場合、暗号資産A（右上）には犯行者は存在せず、また、暗号資産B（右下）のいずれにあたるかは第三者からは分からない。



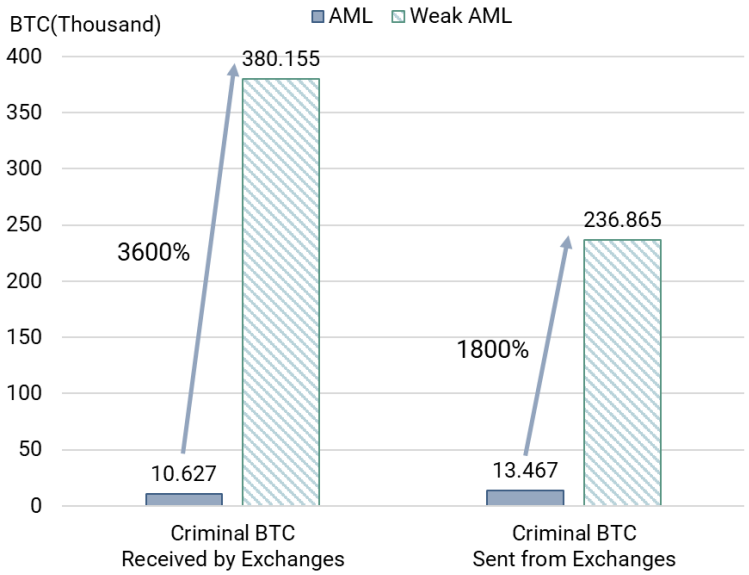
被害額の推定は以下の資料に基づく; CipherTrace, CipherTrace, Inc., “Cryptocurrency Anti-Money Laundering Report - Q3 2018”, https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf, 2019/1/11

2.3 クリプトロンダリング – 暗号資産取引所への規制の効果

規制遵守が徹底されていない国の暗号資産取引所へ犯罪収益に関わる取引が集中する傾向が指摘されている。これは逆に言えば、暗号資産取引所へのAML/CFTの規制の効果があるということを意味すると考えられる。

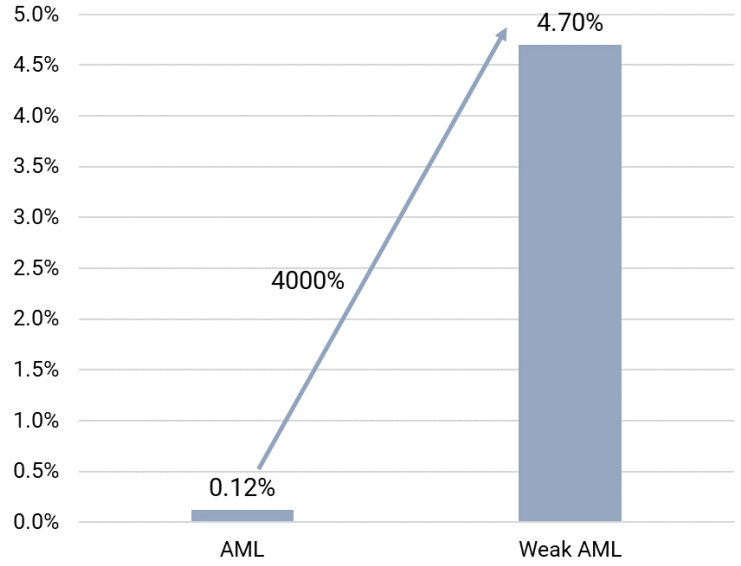
AML規制の強弱と暗号資産取引所の犯罪収益取引額
（2009年1月～2018年9月）

AML規制が弱い国の取引所は、徹底している国の取引所に比べ、暗号資産関連犯罪に関わるビットコインを36倍多く受領し、18倍多く送金すると推定されている。



AML規制の強弱と暗号資産取引所における疑わしい取引の割合
（2009年1月～2018年9月）

AML規制が弱い国の取引所では、全入金の凡そ4.7%が犯罪収益に関連したものと推定されている（AML規制を徹底している国の取引所では凡そ0.12%）。



（左・右）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 より三菱総研作成

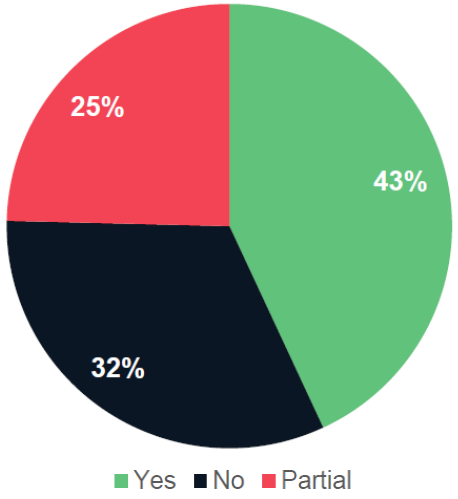
2.3 クリプトロンダリング – 暗号資産取引所の状況

AML/CFTの対応を行っていない暗号資産取引所も多く、欧州・米国等の25の暗号資産取引所等の7割弱においてKYCが徹底されていないという報告や、上位130取引所のうち約1/3はKYCを行っていないという報告がなされている。

また、FATF勧告の未遵守国等に本拠地を置く暗号資産取引所も多く、こうした取引所へ規制対応を徹底させることには困難が予想される。

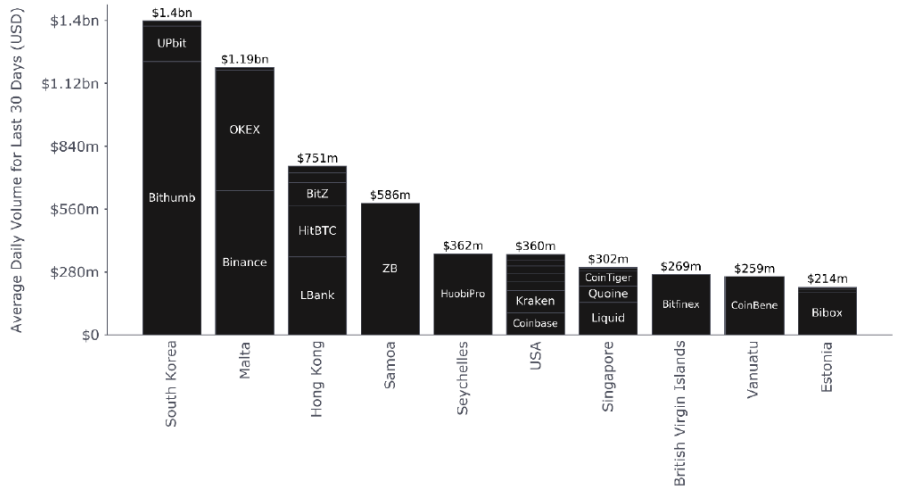
暗号資産取引所（上位130）のKYC対応状況

全体の約1/3（32%）の取引所はKYC未対応。



上位10取引所の所在国の内訳
（取引高は2018/10/15～2018/11/15まで）

取引高上位の取引所は韓国、マルタ、香港、サモア、セーシェル、米国、シンガポール、バージニア諸島、バヌアツ、エストニアに存在する。



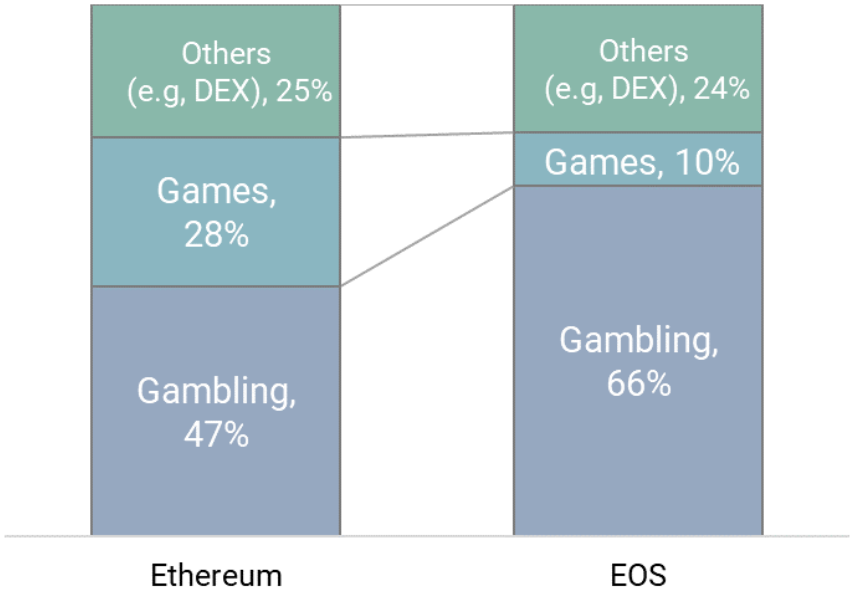
（左・右） CryptoCompare, Crypt Coin Comparison LTD, "CCCAGG Exchange Review, November 2018", https://www.cryptocompare.com/media/35308846/cryptocompare_exchange_review_2018_11.pdf, 2019/1/14

2.3 クリプトロンダリング – ギャンブルサイト

ギャンブルサイトなど、取引所と同じように預け入れ・引出しができるサービスは、暗号資産がプールされることや、入金された後の移動経路が第三者からは分からないことなどから、資金洗浄に利用されやすいと考えられる。

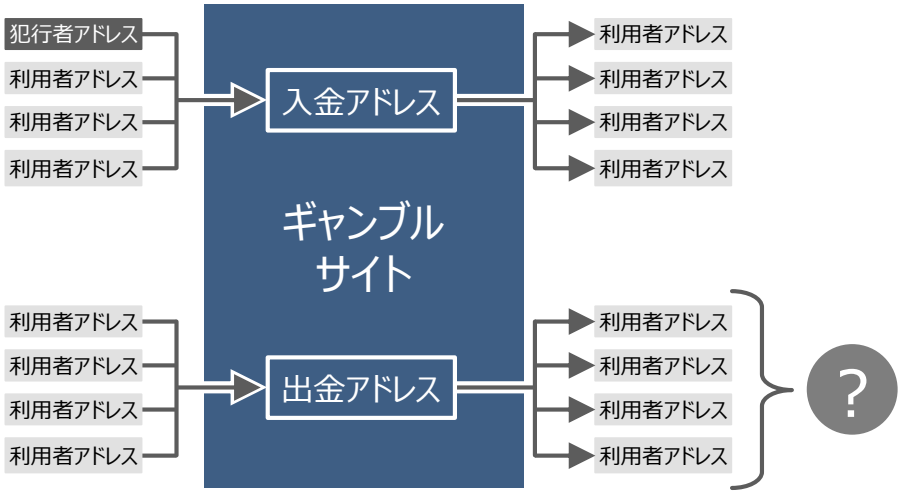
DAppsのカテゴリ内訳

DAppsの大半はギャンブルに分類される。



ギャンブルサイトを用いた資金洗浄のイメージ

預け入れ・引出しができる場合、取引所と同様の理由で、移動経路を第三者から隠蔽することが可能（ギャンブルサイト内でのユーザ間送金なども行われると、移動経路はさらに複雑となる）。



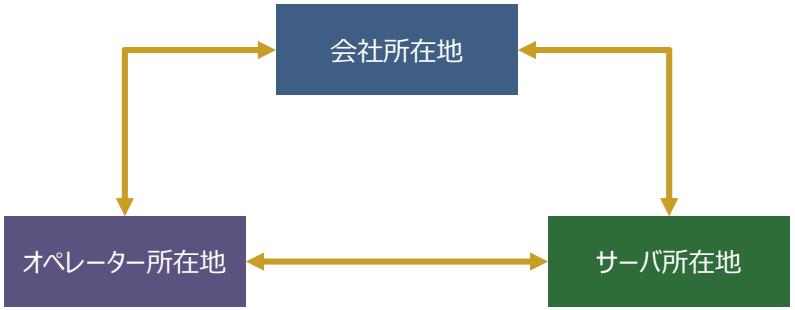
（左）diar, Diar Ltd, “EOS, Tron Lure Betting Crowd to Decentralized Applications”, https://diar.co/volume-3-issue-3/, 2019/2/8より三菱総研作成
（右）Fiedler, I., ResearchGate, “Online Gambling as a Game Changer to Money Laundering?”, https://www.researchgate.net/publication/254969899_Online_Gambling_as_a_Game_Changer_to_Money_Laundering, 2019/2/8を参考にした

2.3 クリプトロンダリング – 資金洗浄サービス事業者の所在地

資金洗浄に利用される事業者の実際の所在地は不明な場合が多く（ダークウェブ上のサイト以外に、通常のWebサイトであっても所在地の把握は困難）、また、それらを閉鎖させることも難しいとみられている。

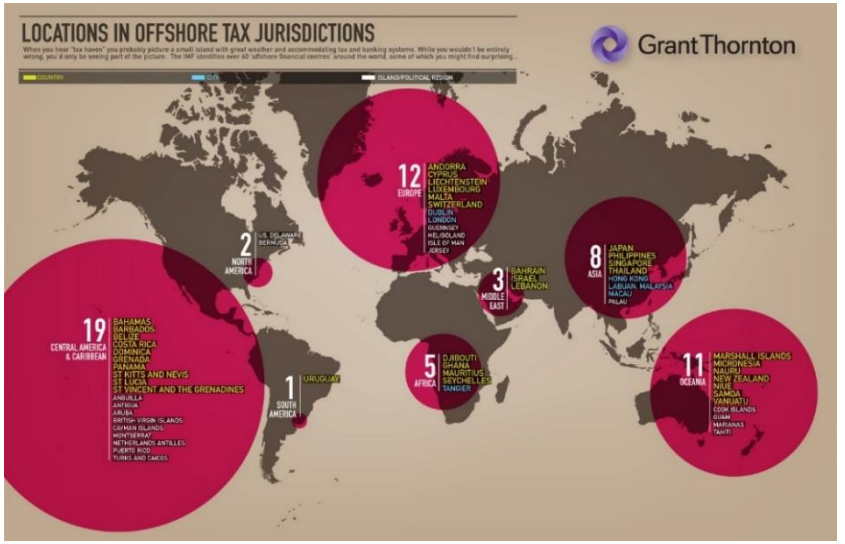
違法サイトの所在地のイメージ

資金洗浄に利用される事業者の運営形態を考えるにあたって、フィッシング詐欺サイトなどの通常の違法サイトの例が参考になる。
こうした違法サイトの事業者は、オフショア法人を安価に設立した上で、一般に ”Bulletproof hosting”と呼ばれる違法コンテンツを許可するホスティングサービスを用いてサービスを提供し、定期的にサイトを閉鎖して別な法人でやり直すことが指摘されている。この場合、登記上の法人所在地、サーバ所在地やオペレーター所在地などが分かれており、規制のエンフォースメントには困難が予想される。



オフショア法人の所在地の例

違法サイトが設立するオフショア法人は、ベリーズ、ケイマン諸島、キュラソー島などのオフショア金融センターに置かれる場合が多いと指摘されている。



（左） Brown, S., et al, HITB SECURITY CONFERENCE, “Privacy and Protection for Criminals: Behaviors and Patterns of Rogue Hosting Providers”, https://conference.hitb.org/hitbsecconf2018ams/materials/D1%20COMMSEC%20-%20Dhia%20Mahjoub%20and%20Sarah%20Brown%20-%20Privacy%20and%20Protection%20for%20Criminals%20-%20Behaviors%20and%20Patterns%20of%20Rogue%20Hosting%20Providers.pdf, 2019/2/25 より三菱総研作成
（右） Grant Thornton, "Locations of offshore tax jurisdictions (infographic)", https://www.grantthornton.co.uk/globalassets/1.-member-firms/united-kingdom/images/insights/2010/locations_in_offshore_tax_jurisdictions_large.jpg, 2019/2/19

3 暗号資産取引を巡る匿名化技術等にかかる調査

3.1 匿名化技術・再識別技術の全体像
3.2 アプリケーションレイヤー（ブロックチェーン）
3.3 P2Pレイヤー/インターネットレイヤー
3.4 実世界レイヤー

本章の要旨

- 様々な匿名化技術や再識別技術について、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。
- 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。
  - 例えば、従前からあるミキシングにおいても、信頼できる仲介者に委託する中央集権型から、仲介者に対する資産移動経路の秘匿化、送金金額の秘匿化、トランザクションの存在自体の秘匿化へと発展しつつある。
  - 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、カストディリスクの削減、データ量の削減等の観点からも、こうした技術の開発が行われている。こうした技術は、パブリック型ブロックチェーン特有の制約の下で、独自の進化を遂げつつあると考えられる。
- 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。

本章の要旨

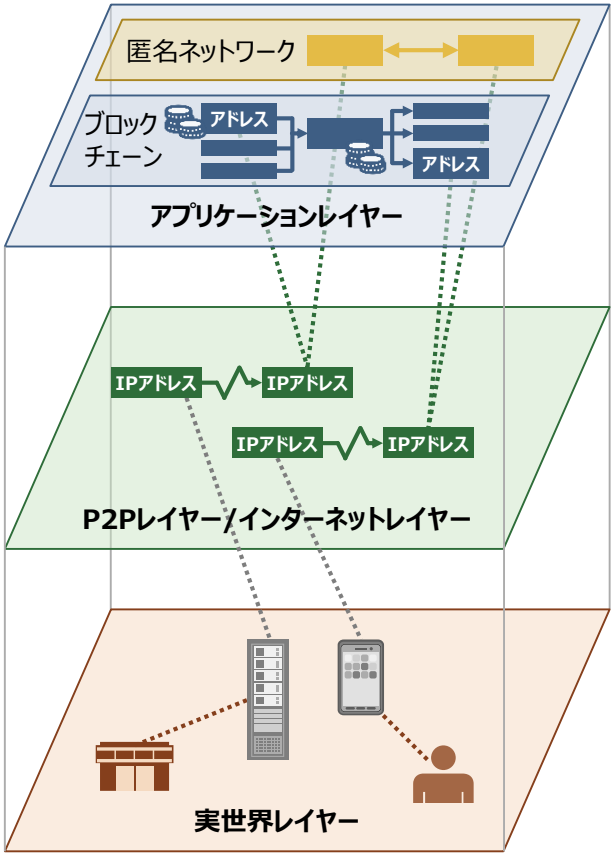
- P2Pレイヤー/インターネットレイヤーの匿名通信においては、利用の裾野が拡大しつつあり、今後はビットコインやセキュアチャットツールなど他のアプリケーションと組合せた場合の全体としての匿名性の確保などが図られていくと考えられる。
- 実世界レイヤーでは、フリーWifi、プリペイドSIM、中古デバイスなどで、本人情報なしにインターネットに接続することが既に可能な状況になっている。
- こうした状況に対し、再識別技術は（1）各層毎の技術的な推測、（2）外部のデータを用いた特定という二通りのアプローチを組合せて行われるが、基本的には犯行者のミスをつく等の対応に留まる。KYC情報やEC購入履歴情報、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。

3.1 匿名化技術・再識別技術の全体像

3.1.1 全体像
3.1.2 匿名化技術の例
3.1.3 再識別技術の例
3.1.4 本調査研究で明らかになった論点の例

3.1.1 全体像

様々な匿名化技術や再識別技術について、インターネット・プロトコルスイートを参考に、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。



アプリケーションレイヤー

各アプリケーション上のアドレス※が存在する。
（例. ビットコインアドレス、ダークウェブアドレス）

P2Pレイヤー/インターネットレイヤー

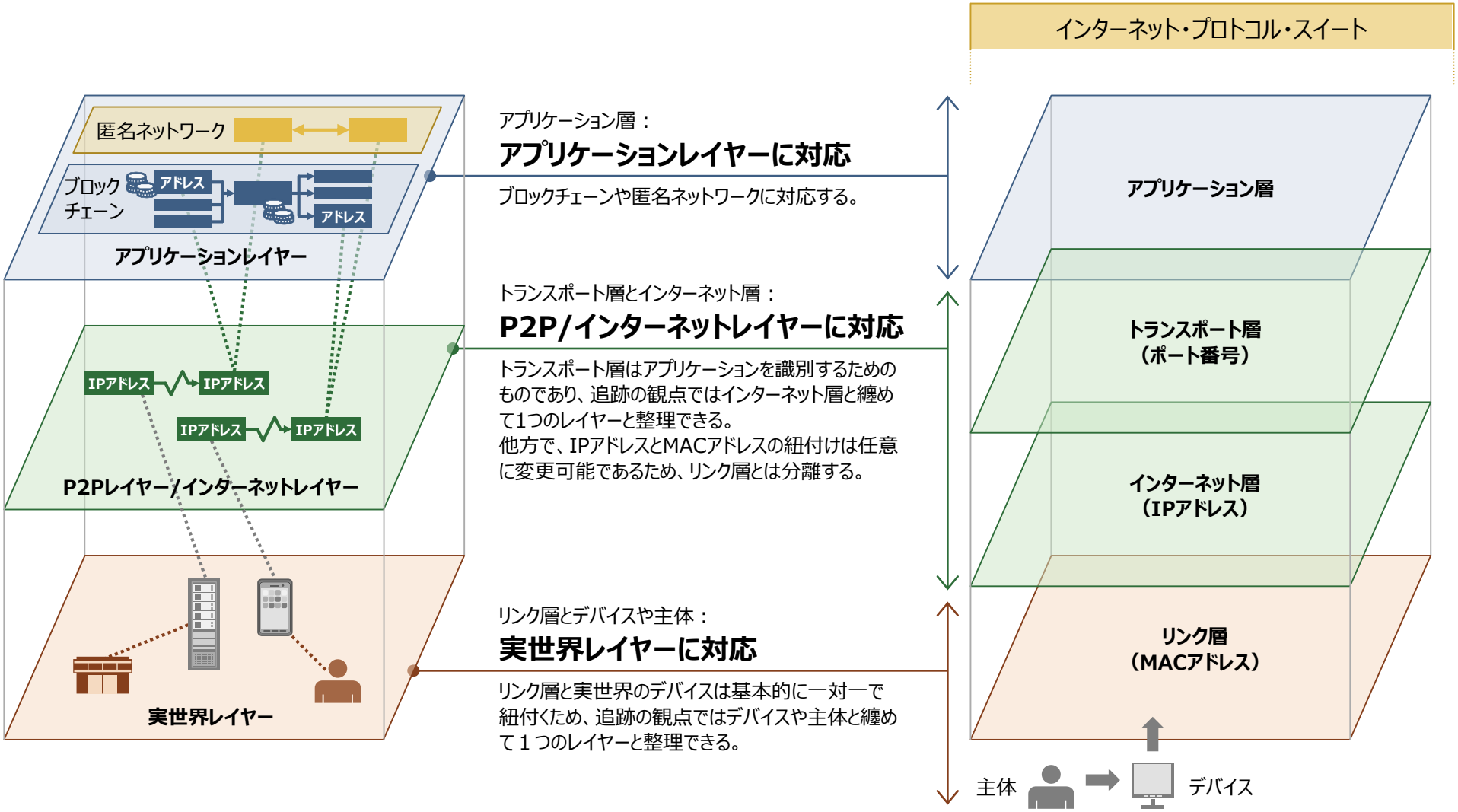
IPアドレス※1が存在する。

実世界レイヤー

デバイスや組織・個人などの物理的主体が存在する。

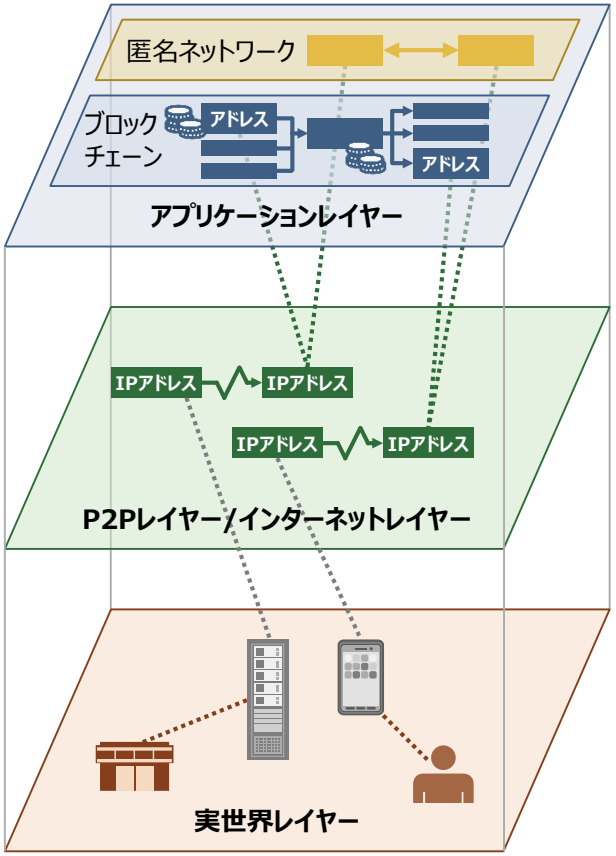
※ アドレスとはネットワークやアプリケーション上での所在地にあたる識別子である（例. 電子メールアドレス）。

3.1.1 全体像 – インターネット・プロトコルスイートとの比較



3.1.2 匿名化技術の例

各層毎に匿名化技術が存在するが、それらの利用にあたっての技術的・心理的なハードルは低い。



アプリケーションレイヤー

ブロックチェーン：ミキシング、匿名通貨等
匿名ネットワーク：Tor秘匿サービス、匿名チャットツール等

P2Pレイヤー/インターネットレイヤー

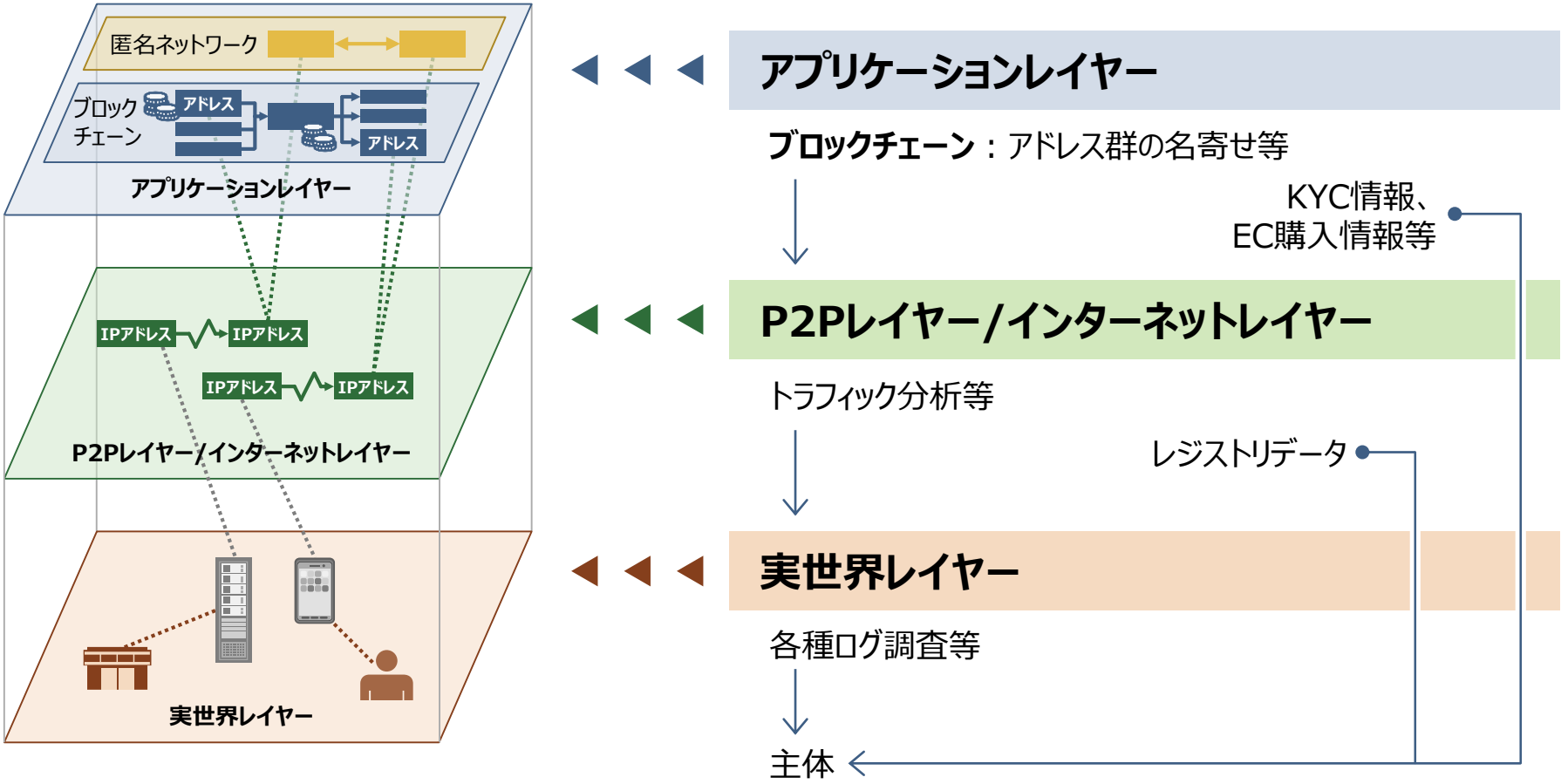
Torオニオンルーティング、I2P、FreeNet等

実世界レイヤー

フリーWifi、プリペイドSIM、中古デバイス、ビットコインATM等

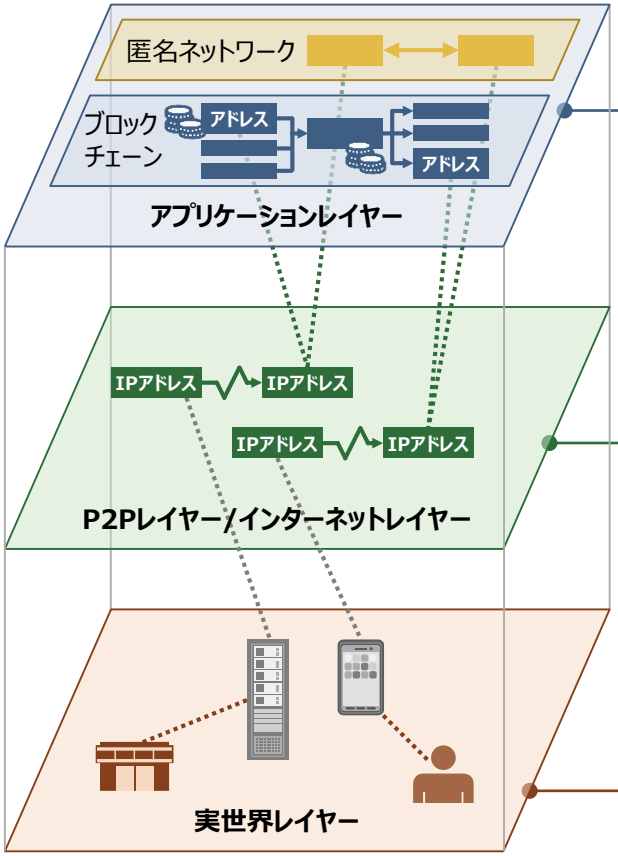
3.1.3 再識別技術の例

再識別技術については、各層毎の技術的な推測および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。



3.1.4 本調査研究で明らかになった論点の例

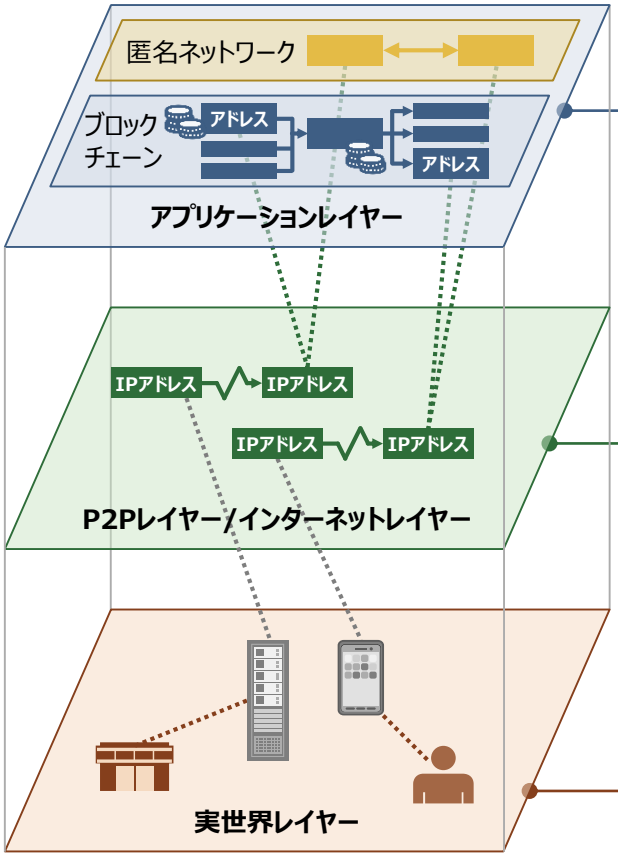
暗号資産にかかる規制の議論の土台として、技術的にできること／できないことの正しい認識が重要である。



論点

1. ビットコインでは送金経路が記録されるので、追跡しやすいのではないか？
2. 暗号資産の追跡技術は、ある程度確立されているのではないか？
3. 取引データの発信元となるIPアドレスを特定できるのではないか？
4. IPアドレスが分かれば、犯行者を特定できるのではないか？
5. P2Pレイヤー/インターネットレイヤーで止めれば良いのではないか？
6. 正しいIPアドレスが分かれば、犯行者を特定できるのではないか？
7. 法定通貨と暗号資産の接点（暗号資産取引所等）を押さえれば十分ではないのか？

3.1.4 本調査研究で明らかになった論点の例



論点に対する回答

1. 例えばミキシングが行われると、候補先が指数関数的に増える等により、送金元と送金先の紐付けが行えず、追跡が困難となる。
2. 学術的な有効性評価はなされていない状況にある。また、あくまで確率的な推測であり、ケースバイケースになる。
3. ノード間の転送にランダムな遅延時間を入れたりダミーの発信元を用意することで、発信元の特定を困難にすることが可能である。
4. 匿名通信等により送信元IPアドレスを第三者から秘匿することが可能である。
5. パケット暗号化やプロトコル偽装等により、暗号資産の取引データと識別することが困難。また、IPアドレス制限では全てをカバーしきれない。
6. フリーWifiと中古デバイス等の組み合せにより、KYCなしにインターネット接続が可能であり、犯行者の特定は容易ではない。
7. 極めて匿名性の高いクリプトマネーロンダリングは既に可能であるため、取引所を押さえるだけでは不十分となる。

3.2 アプリケーションレイヤー（ブロックチェーン）

3.2.1 ブロックチェーンの匿名化技術
3.2.2 ブロックチェーンの再識別技術

3.2.1 ブロックチェーンの匿名化技術

3.2.1.1 ブロックチェーン要素技術

3.2.1.2 DEX

（参考）セキュアチャットツール

3.2.1.1 ブロックチェーン要素技術

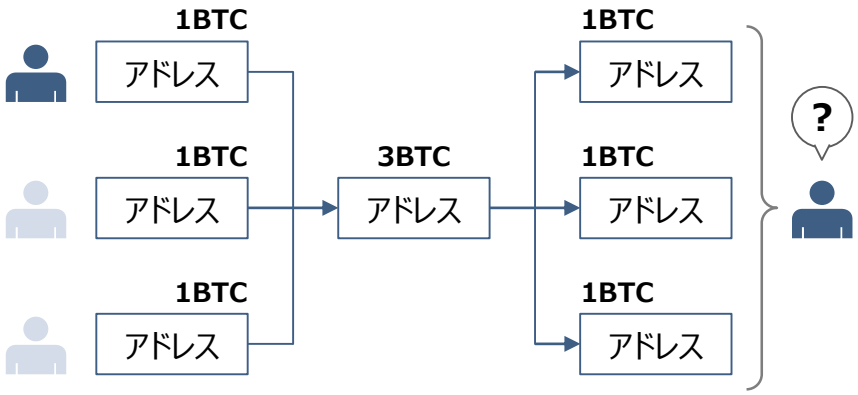
3.2.1.1.1 調査対象技術の一覧－匿名化の考え方

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。そのため、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。
- トランザクションの発信元は、ここでは必要な秘密鍵の保有者を指し、ネットワーク全体にトランザクションが伝播する経路から推測される可能性がある。そのため、匿名化にあたっては、伝播経路を複雑にする、ダミーの発信元を用意するなどにより、「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。

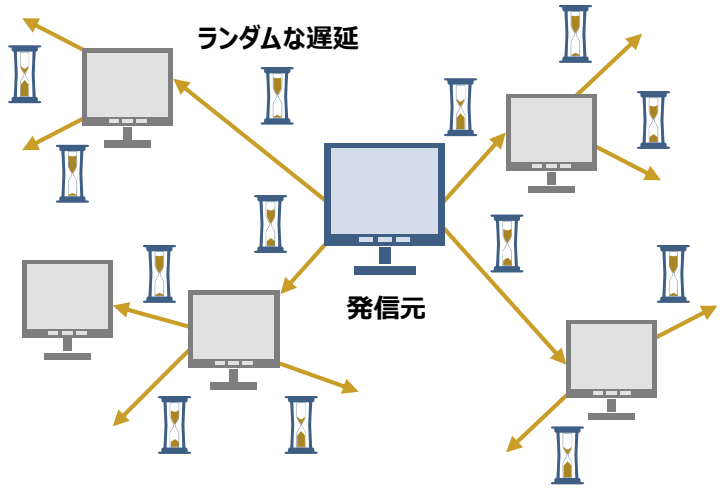
トランザクションの内容（資産移動経路）の匿名化の例

コインを一度プーリングすることで、実際の資産移動経路を第三者から隠蔽する（ミキシング）。



トランザクションの発信元の匿名化の例

各ノードは接続先毎にランダムな遅延時間をおくことで、伝播経路の推測を困難にし、トランザクションの発信元を第三者から隠蔽する。



3.2.1.1.1 調査対象技術の一覧

専門家等の意見を踏まえ、暗号資産取引の匿名性を高める技術として、以下に挙げる技術について記載する。

本調査研究で対象とした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）	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）	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、ライトコイン、ディクレッド、イーサリアム	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。

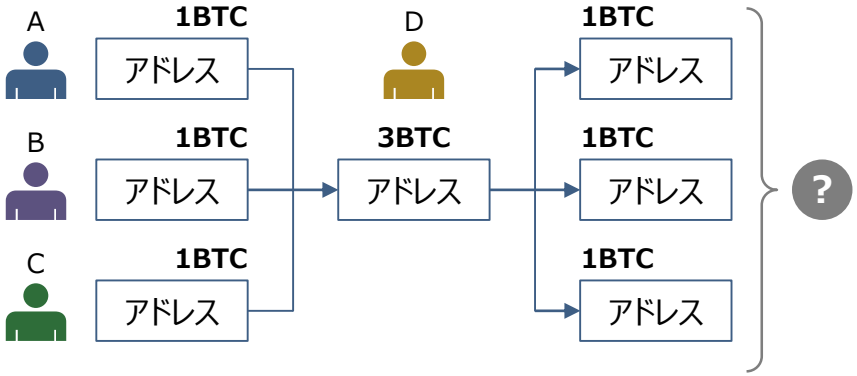
3.2.1.1.2 ミキシング

ミキシングとは、第三者から資産移動経路（送金元と送金先のつながり）を秘匿する場合に用いる仕組みであり、ビットコインやイーサリアム等で利用可能である。具体的には、複数の送金元からのコインをプールした上で、それを再分配する。

中央集権型のミキシング

利用者はミキシングサービス事業者へ送金して、プールされたコインを受け取る。ただし、取引所と同様、ミキシングサービス事業者に関連した被害（持ち逃げ被害、ハッキング被害、サーバ障害による被害等）やミキシングサービス事業者へのプライバシー漏洩といった問題がある。

※ 実際にはミキシングサービス事業者は全く異なる資金プールから返金する。

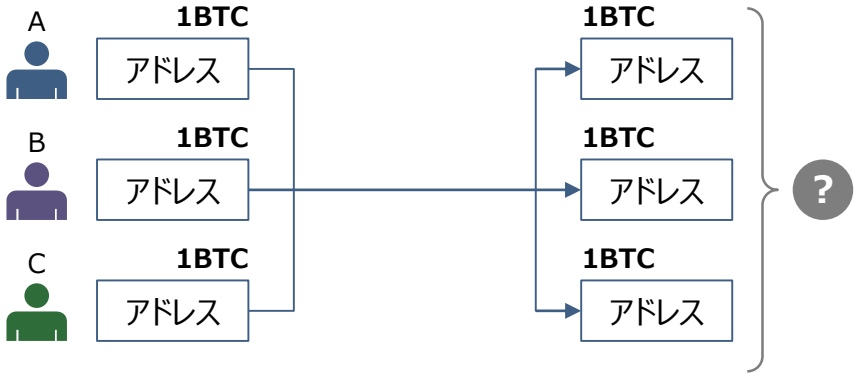


Input	Output		Signature
A（1BTC）	D	3BTC	A
B（1BTC）			B
C（1BTC）			C

Input	Output		Signature
D	E	1BTC	D
	F	1BTC	
	G	1BTC	

分散型のミキシング（CoinJoin）

利用者は同額を持ち寄り、分配額が同額となるトランザクションを作成し、順に署名を行う。ここで、全員の署名が揃わないと有効にならないため、持ち逃げ被害はない。ただし、同額を出す利用者をタイミング良く集めることは実際には難しい。金額が不均一になる場合、資産移動経路をある程度推測されてしまう問題が生じる。

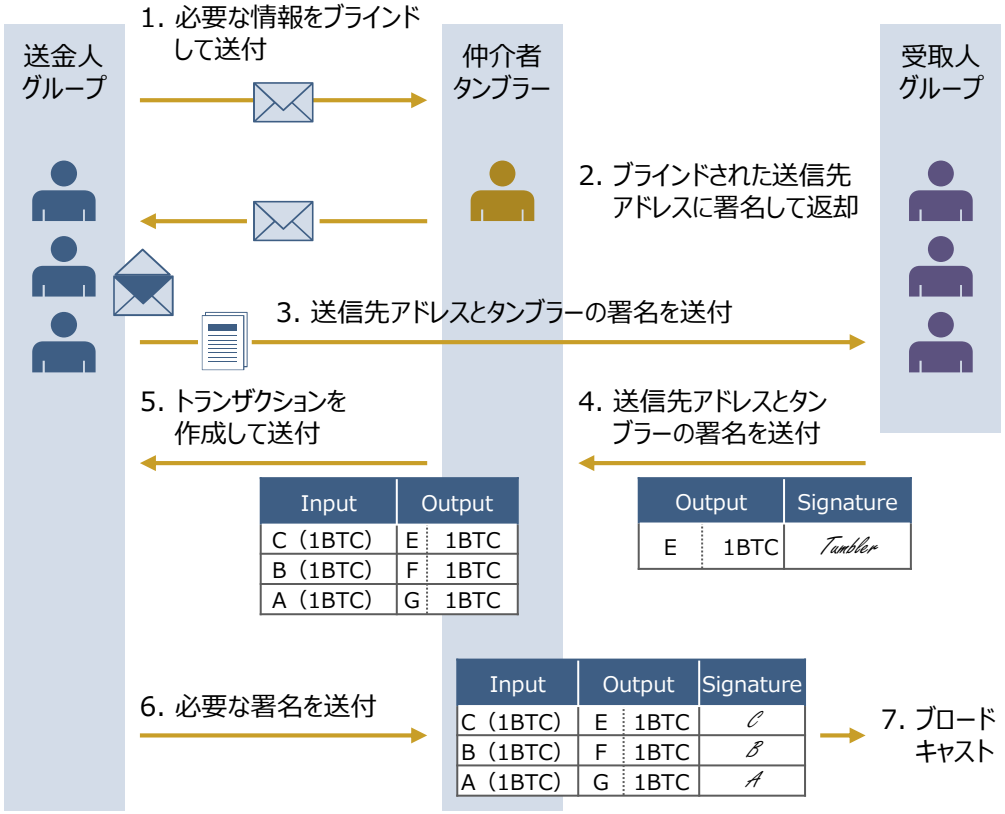


Input	Output		Signature
A（1BTC）	D	1BTC	A
B（1BTC）	E	1BTC	B
C（1BTC）	F	1BTC	C

3.2.1.1.2 ミキシング－Chaumian CoinJoin

ミキシングにおいても、中央集権型から、仲介者に対する資産移動経路の秘匿化（CoinShuffle、Tumblebit、Chaumian CoinJoin）、送金金額の秘匿化（ValueShuffle）、トランザクションの存在自体の秘匿化（CoinJoinXT）へと発展しつつある。

Chaumian CoinJoinの処理の流れ



Chaumian CoinJoinは、第三者以外に、仲介者（タンブラーと呼ばれる）からも資金移動経路を秘匿する。そのため、中身を明らかにしない状態で署名を行う技術（ブラインド署名）を利用する。 Hidden WalletやWasabi Wallet、 Samourai Walletなど一部のウォレットでサポートされている。

1. 送金人は必要な取引情報を仲介者（タンブラー）へ送付する。ここで、送信先アドレスはブラインドされており、タンブラーは中身を見ることができない。
2. タンブラーは送信元アドレスの情報を見て未使用かどうかなどを確認し、問題なければブラインドされた送信先アドレスに署名をして、送金人に返す。
3. 送金人は送信先アドレスとタンブラーの署名をアンブラインドして取り出し、受取人へ送付する。
4. 受取人は、送信先アドレスとタンブラーの署名をタンブラーへ送付する。
5. タンブラーは、自身の署名があることを確認した上で、1.の送信元アドレスと4.の送信先アドレスからトランザクションを作成し、送金人へ送付する。
6. 送金人はトランザクションの内容を確認して、問題なければ自身の署名をタンブラーへ送付する。
7. タンブラーは、受領した署名をトランザクションに追加して、ブロックチェーン上にブロードキャストする。

3.2.1.1.2 ミキシング – 課題と新たな取組

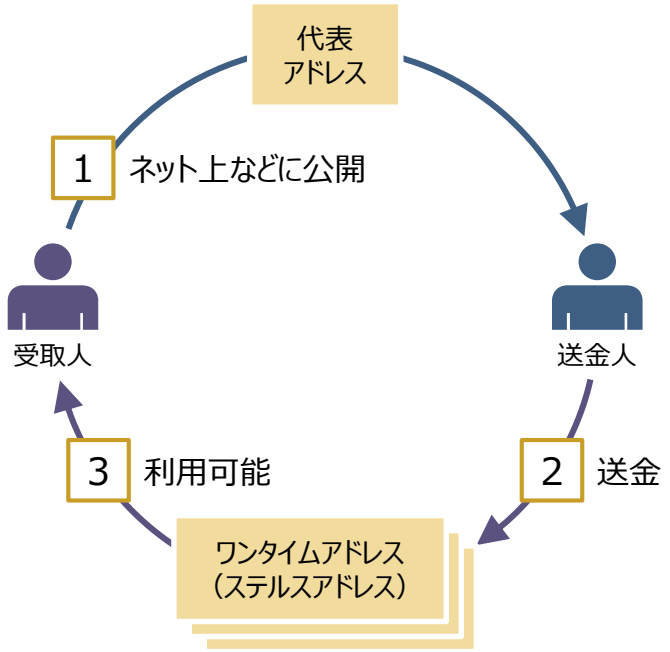
コインをプールするアプローチでは匿名性と利便性などのトレードオフがあることから、取引内容や取引の存在自体の秘匿化へと進展していく可能性が考えられる。

課題	内容	関連した新たな取組
匿名性と利便性のトレードオフ	● 第三者や仲介者に対する匿名性を上げるには、十分な数の利用者を確保する必要がある（予め配ったコインを追跡するというアクティブな攻撃に対してはミキシングは脆弱であると指摘されている）。 ● 他方で、利用者が多数では、ミキシングの都度、他の参加者を待つ必要があり、利便性の点で問題がある。	● モネロはダミー送金元を使う（リング署名）など他の手段を用いることで回避している。
匿名性とミキシングが露呈するリスクのトレードオフ	● 匿名性を上げるために送金元と送金先の数を多くするほど、逆に、その特徴からミキシングが行われたと推測される可能性がある。	● ミキシングを行うトランザクションをブロックチェーンの外（オフチェーン）で扱うCoinJoinXT（未だ提案段階）で解消される可能性がある。 ● 入金と出金のコインを別にするTumblebitでは、入出金間の関係を断つなど他の手段を用いることで回避している。
匿名性とトランザクションサイズのトレードオフ	● 匿名性を上げるために、匿名セットのサイズを増やすほど、トランザクションサイズが増大する（トランザクションサイズの制約から、一度にミキシングできる匿名セットのサイズはビットコインでは350～470に制限される）。	【一部解決済み】 ● 複数の公開鍵や署名を1つの公開鍵や署名に集約できるSchnorr署名（暗号資産グリンやビームで導入済み）で一定程度軽減されるが、完全には解消されない。
匿名性と利便性のトレードオフ（送金額）	● 第三者や仲介者に対する匿名性を上げるには、送金額を極力均一化する必要がある。	【解決済み】 ● 送金額の秘匿化とCoinJoinを組合せたValueShuffle（ブロックチェーン基盤Stegosで導入済み）で解消されている。
カストディリスク	● 中央集権型のミキシングでは、仲介者が秘密鍵を管理するため、カストディリスクが存在する。	【解決済み】 ● 分散型ミキシングであるCoinJoin等で解消されている。
単一障害点	● 仲介者を必要とするミキシングでは、仲介者が単一障害点となる。	【実用上問題は少ない】 ● 中央集権型以外のミキシングでは、仲介者は秘密鍵は管理しないため、ある仲介者に障害が発生しても他の仲介者を利用すれば済むと考えられる。

3.2.1.1.3 ステルスアドレス

ステルスアドレスとは、寄付など受取人のアドレスを広く公開する必要があるものの、第三者から受取人の実際のアドレスを秘匿する場合に用いる仕組みであり、モネロ等で導入されている。具体的には、代表となるアドレスは公開するものの、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。

ステルスアドレスを用いた取引イメージ



1. 受取人は2つの公開鍵***A***, ***B***を公開する。
2. 送金人は受取人の2つの公開鍵***A***, ***B***に、ランダムに生成した自身の秘密鍵***r***を加えてワンタイムアドレスを生成して、そこへ送金する。この際、生成した秘密鍵***r***に対応する公開鍵***R***もトランザクションに含めておく。
3. 受取人は自身の2つの公開鍵***A***, ***B***に対応する秘密鍵***a***, ***b***と、送金人の公開鍵***R***から、ワンタイムアドレスに対応する秘密鍵を生成し、当該アドレスに送金されたコインを利用する。

送金人が協力して、都度、受取人だけが使えるワンタイムアドレスへ送金する仕組みであり、ディフィー・ヘルマン鍵共有を用いて送金人と受取人の間で共有鍵を生成することを利用している。

3.2.1.1.3 ステルスアドレス – 課題と新たな取組

ステルスアドレスは既に概ね課題が解決されている。ビットコインでは採用されなかったが、ウォレットなどのアプリケーションレベルで導入可能であるため、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。

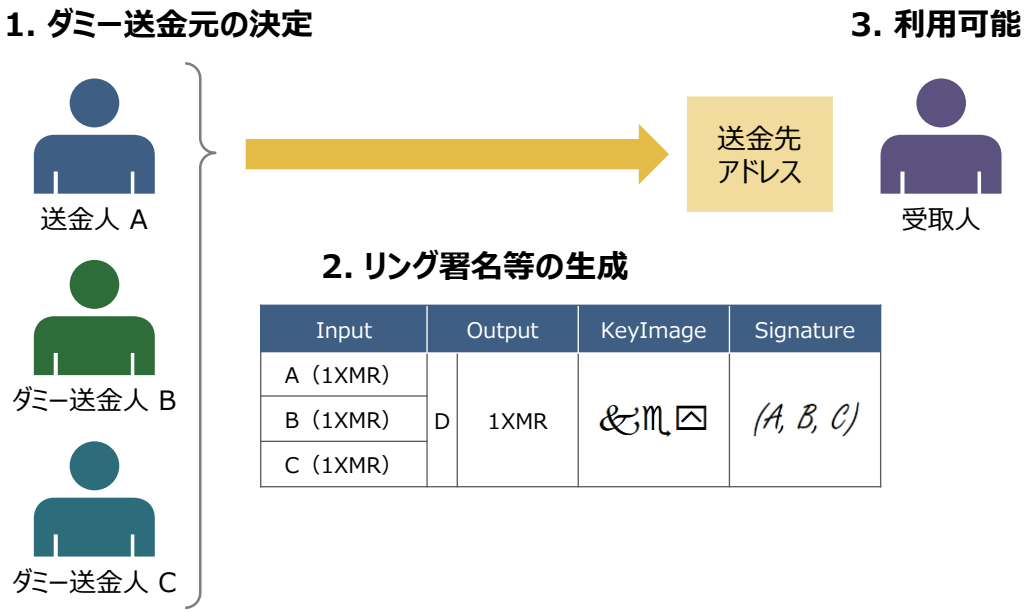
課題	内容	関連した新たな取組
利用の必要性	● 受信側が都度アドレスを作成すればステルスアドレスと同じ効果が得られる。	● ミンブルウィンブルでは、送金にあたって送金人と受取人が協力するため、アドレスという識別子自体が不要である。
入金確認の必要性	● 受取人は、入金されるアドレスが受動的には分からないため、（1）送金人から連絡をもらうか、（2）自身ないし信頼できる第三者がブロックチェーン上の取引を走査する必要がある。	–
秘密鍵の使い回し	● 当初の提案では、受取人が公開する代表アドレスには１つの公開鍵しか含まれていなかった。この場合、入金を検知するために秘密鍵を常時用いる必要があり、安全性の点で問題がある。	【解決済み】 ● 「入金検知で用いる鍵」と「コインの利用で用いる鍵」の２つを使い分ける現在の方式が採用されることになった（現在の方式では、入金検知で用いる鍵を第三者へ預けることで、入金監視を第三者に委託することも可能になった）。

3.2.1.1.4 リング署名

リング署名とは、第三者から送金元を秘匿する場合に用いる仕組みであり、モネロ等で導入されている。具体的には、実際の送金元以外にダミーの送金元を加えることで、送金人以外に実際の送金元が分からないようにしている。

（なお、実際の送金元の秘密鍵から生成したユニークな値（キーイメージ）をトランザクションに含めることで、実際の送金元が分からない場合に生じ得るコインの二重使用問題を解決している。）

リング署名を用いた取引イメージ



Input		Output	KeyImage	Signature
A（1XMR）	D	1XMR	&ℳ囚	(A, B, C)
B（1XMR）				
C（1XMR）				

1. 送金人は、実際の送金元に加え、送金額が同額となるダミー送金元をN個選択し、N+1個の送金元をトランザクションに含める。
2. 送金人は、実際の送金元に対応する秘密鍵からキーイメージを生成し、トランザクションに含める。次に、当該トランザクション、実際の送金元の秘密鍵、ダミー送金元の公開鍵やキーイメージ等からリング署名を生成し、それもトランザクションに含めてブロードキャストする。
3. 受取人は自身のアドレスに送金されたコインを利用可能となるが、署名を検証してもどの送金元のコインかは分からない。

3.2.1.1.4 リング署名 – 課題と新たな取組

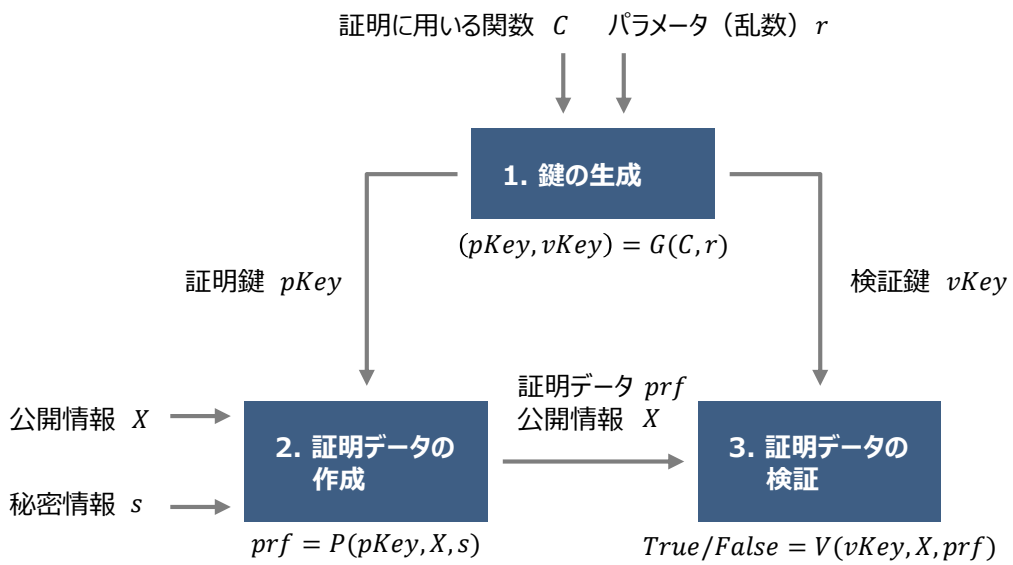
リング署名では、ダミー送金元の選定方法が重要であり、ダミー送金元の属性と実際の送金元の属性を極力近づける必要がある。

課題	内容	関連した新たな取組
ダミー送金元の属性	● 以下の偏りにより、実際の送金元を推測される場合がある。 ✓時系列の偏り 過去に使われた送金元ほどその後も利用される可能性が高いため、最新のものほど実際の送金元である可能性が高い。 ✓トランザクションの偏り 複数の送金元が単一のトランザクションから選ばれる場合は、そのような可能性は低いため、実際の送金元である可能性が高い。	【一部解決済み】 ● 時系列の偏りについてはダミー送金元を選定する確率密度関数の変更により対処可能と報告されている（本稿執筆時点ではモネロには導入されていない）。
匿名性とトランザクションサイズのトレードオフ	● モネロでは匿名性を上げるために、数次に渡って匿名セットの必要数が引き上げられたが、匿名セットのサイズが大きくなるほどトランザクションサイズが増大する。	【一部解決済み】 ● 複数の公開鍵や署名を1つの公開鍵や署名に集約できるSchnorr署名（暗号資産グリンやビームで導入済み）で一定程度軽減されるが、完全には解消されない。
匿名セットのサイズ	● モネロの初期バージョンではダミー送金元を含めないトランザクションが非常に多かったため、送金元の凡そ95%を追跡可能であった。	【解決済み】 ● モネロでは、ダミー送金元の必要数を引き上げる対応が数次に渡って行われた（本稿執筆時点のv0.13.0.4で、ダミー送金元の必要数は10）。

3.2.1.1.5 ゼロ知識証明（zk-SNARKs）

ゼロ知識証明とはある情報を秘匿したまま、相手にその情報を知っていることを証明する仕組みであり、ゼロ知識証明の一種であるzk-SNARKs（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge）はジーキャッシュやイーサリアム等に導入されている。具体的には、暗号化した状態で計算が可能である準同型暗号等を利用して、送信元、送金先や送金額などではなく、それらの証明データのみをブロックチェーン上に記録することで、取引内容を第三者から秘匿する。

zk-SNARKsを用いた取引のイメージ



1. 信頼できる第三者が、証明に用いる関数***C***（出力は真偽値のみのブール値関数）およびパラメータ***r***から、証明鍵***pKey***、検証鍵***vKey***を生成する。***pKey***および***vKey***は暗号化されており、広く公開される。
2. 証明者は、証明鍵***pKey***、公開される情報***X***と秘密情報***s***から証明データ***prf***を生成する。
3. 検証者は、証明データ***prf***を、検証鍵***vKey***と公開される情報***X***を用いて検証し、真偽値の判断をする。

送金の場合、一般に、証明者は送金人および受取人であり、検証者は中継ノードやマイナーとなる。なお、イーサリアムでは「3.証明データの検証」のスマートコントラクトが提供されておりオンチェーンで実行されるが、「1.鍵の生成」や「2.証明データの作成」は独自にオフチェーンで実行する必要がある。

3.2.1.1.5 ゼロ知識証明（zk-SNARKs）－課題と新たな取組

鍵生成時のパラメータを漏洩してはならないという制約の克服や計算量削減を中心に改善が試みられているが、イーサリアムではスケーラビリティ改善の観点からも検討が進められている。

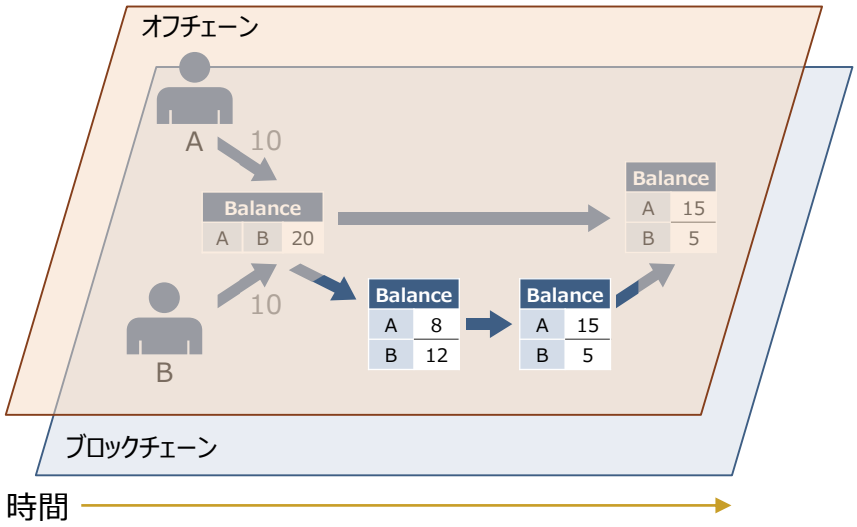
課題	内容	関連した新たな取組
利用の必要性	● ブロックチェーン外で処理することなどでも同じ効果が得られる。 ✓ zk-SNARKsは、送金人・受取人がマイナーと都度やり取りできない（非対話型である必要）、ブロックチェーン上の台帳にデータを記録するコストが高い（簡潔である必要）などのブロックチェーン特有の制約に基づいて発展した手法であるため、前提条件が変わる場合はそれに応じた別な手法が望ましいこともある。	● JPモルガン他の開発するブロックチェーン基盤Quorumでは、取引内容を暗号化したハッシュ値のみをブロックチェーン上に記録し、実際の取引内容はブロックチェーンの外（オフチェーン）で送信することで、zk-SNARKsの利用を回避している。
信頼できる第三者による鍵生成の必要性	● 鍵の生成は信頼できる第三者が行う必要がある（前項のパラメータ***r***が漏洩すると、秘密情報***s***を使わずに検証に成功する、偽の証明データを作成できるため）。そのため、鍵生成部分は一般に『トラステッドセットアップ』とも呼ばれる。 ● このトラステッドセットアップは、秘匿する対象が変わる毎（前項の、証明に用いる関数***C***が変わる毎）に行う必要があり、様々な問題にzk-SNARKsを適用する場合、実運用では難しい場面が生じる。	【一部解決済み】 ● zk-STARKs（Zero-Knowledge Scalable Transparent ARguments of Knowledge、未だに導入事例なし）は以下の課題を解決しているが、逆に証明データのサイズが大きくなる（場合によって200倍以上）等の問題が生じる。 ✓ 鍵生成に用いる情報が公開されても問題ない。 ✓ zk-SNARKsよりも問題の複雑さの影響が少ない。 ✓ 衝突困難ハッシュ関数を用いて量子耐性を備えている。
計算量と証明データのサイズ	● 問題（前項の、証明に用いる関数***C***）が複雑になるほど、特に証明データを作成する時間などが長くなる。	
量子耐性	● 離散対数問題の困難性を利用した楕円曲線暗号などが用いられるが、量子コンピュータへの耐性はない。	

3.2.1.1.6 ライトニングネットワーク

ライトニングネットワークとは、ブロックチェーン上の取引のスケーラビリティ拡充、即時決済、手数料の低減等を実現する仕組みであり、ビットコインやライトコインに導入されている。具体的には、ブロックチェーン上に記録する取引を最小限とし、それ以外の取引をオフチェーンで行う。

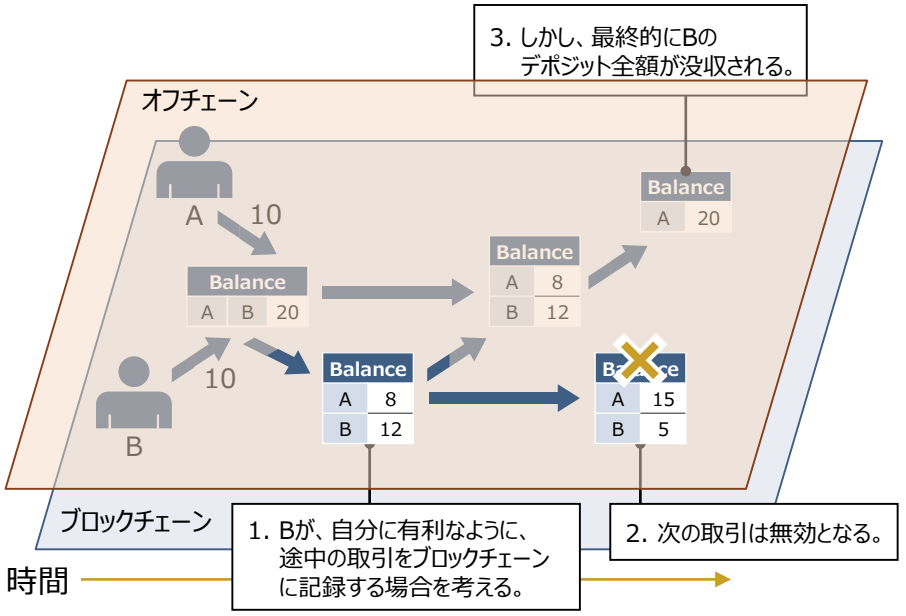
ライトニングネットワークを用いた取引イメージ

ブロックチェーン上には、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。
ただし、オフチェーンでの取引は、最初にデポジットされたコインの範囲内に限られる。また、最初の取引がブロックに格納されるまで待つ必要がある。



トラストレスの実現イメージ

取引仲介者がいないため、取引当事者同士が不正を行わないように、どちらか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に没収される）形としている。

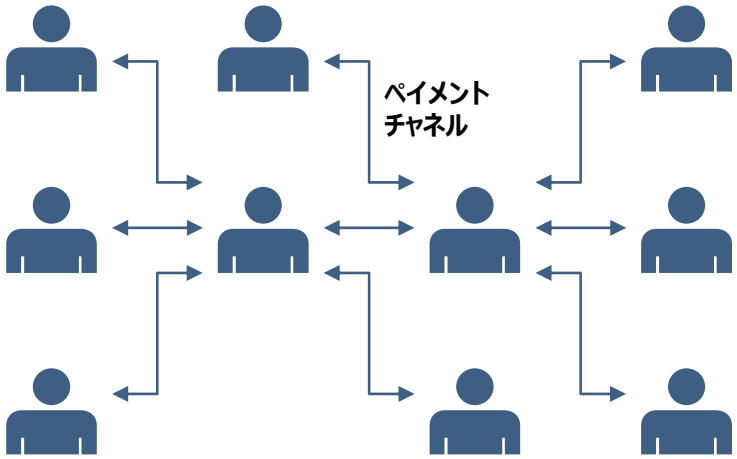


3.2.1.1.6 ライトニングネットワーク

ライトニングネットワークでは、ペイメントチャネル（二者間でのオフチェーン取引を可能とする仕組み）を組み合せることで、直接ペイメントチャネルを開いていない任意の当事者間においても取引を行うことが可能である。

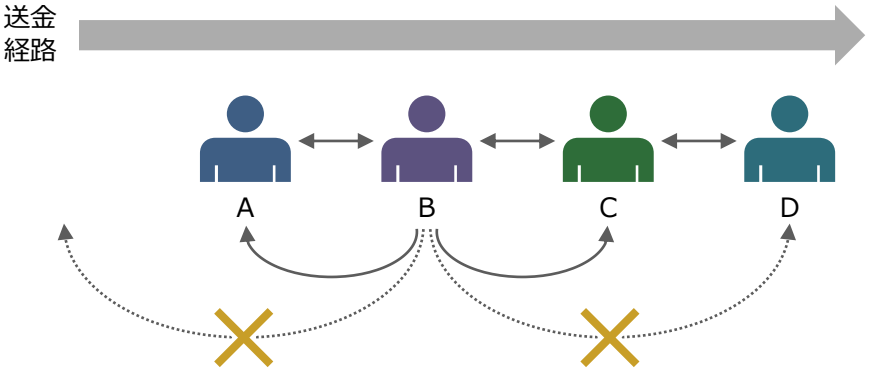
ライトニングネットワークの中継送金のイメージ

ペイメントチャネルを中継することで、任意の当事者間において取引を行うことが可能である。ただし、中継回数が少ないほど手数料が少なくなるため、多くのペイメントチャネルを持つノードにさらにペイメントチャネルが集中し、結果としてハブとなるノードが生じることになる。



中継送金とプライバシーのイメージ

現在の仕様では、ライトニングネットワークの中継送金は3.3.1.3節「Tor」のOnion Routingと同様の仕組みが定められており、送金を中継するノードは前後のノードしか分からない。そのため（送金経路は送金人が決定するが）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。



中継ノードBからみて、ノードDは分からず、また、
ノードAは送金人のノードから中継ノードかは分からない

3.2.1.1.6 ライトニングネットワーク – 課題と新たな取組

オフチェーンを利用する所謂セカンドレイヤー技術は、新たな提案が早期に仕様に組み込まれるなど、ブロックチェーン本体にあたるオンチェーン技術に比べ、進展スピードが非常に早いのが特徴であり、様々な取組が進められている。

課題	内容	関連した新たな取組
ハブの存在	• 多額のコインを保持する特定のノードがハブ化し、ペイメントチャネルの寡占化が進むと、ハブノードの障害やハブノードへの攻撃によりネットワーク全体の安定性が低下することとなる。	–
ルーティング	• 経路情報を管理する特定の主体が存在しない一方、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経路を選択する必要がある。	–
中継ノードのインセンティブ	• 中継ノードを増やす経済的インセンティブを考える必要がある（デポジットという初期コストやデポジットしたコインを他に転用できないという機会コストを払って、手数料収入を得るだけでは利益が出ない懸念があるため）。	–
流動性の分断	• デポジットしたコインは、ペイメントチャネル内の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には利用できないため、利用者の流動性はオンチェーンとオフチェーンに分断されることになる。	【一部解決済み】 ● 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手法（Splicing）が提案されている。
キャパシティ（送金額の上限）	• ペイメントチャネルでは、最初にデポジットした金額（キャパシティ）の範囲内でしか取引が行えない。特に、中継送金の場合は、組合せた複数のペイメント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。	【一部解決済み】 ● 送金額を複数のルートに分割して送金する手法（Atomic Multi-Path Payments、次期仕様に導入される予定）が提案されている。

3.2.1.1.6 ライトニングネットワーク – 課題と新たな取組

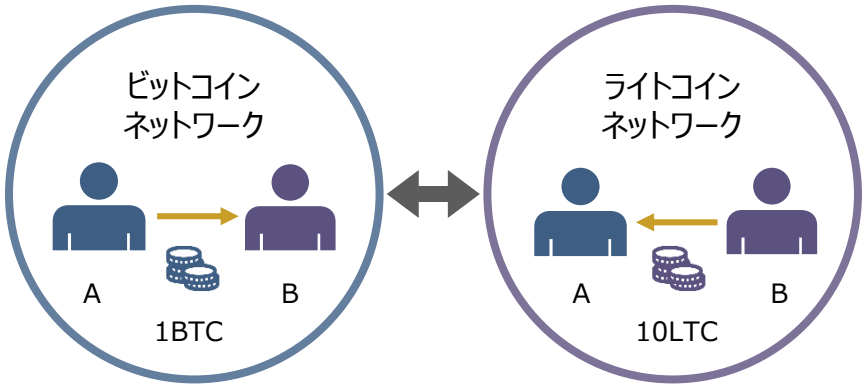
課題	内容	関連した新たな取組
常時監視やバックアップ・リカバリーの必要性	• 相手が不正を行う場合に備えて、常時ブロックチェーンを監視する必要がある。また、障害発生等に備えてペイメントチャネルの状態を適切にバックアップ・リカバーできる必要がある。	【一部解決済み】 • 常時監視のアウトソース（Watchtower）、バックアップ・リカバリー（Data Loss Protection）や全額没収というペナルティ緩和（eltoo）などが提案されている。Watchtowerなど一部は特定のウォレットでサポートされている。
中継送金時の嫌がらせ攻撃	• 最終的な受取人や中継ノードが、中継された資産を受け取らずシークレット（ハッシュ化する対象の値）を開示しないことで、経路上のノードの処理を遅延させる嫌がらせ攻撃が可能である（被害にあったノードは、払い戻しまでの時間、流動性を利用できなくなる）。	【解決済み】 • Ripple Interledgerプロトコルでは、少額の送金を複数回繰り返すことで、嫌がらせ攻撃を受けた際には、すぐにペイメントチャネルを閉じることができるように対応されている。
中継送金時のプライバシー	• 中継送金の場合、経路上の各ペイメントチャネルで、同じシークレットやハッシュ値を用いる必要があり、悪意のある第三者がそれらハッシュ値やシークレットから経路を推定することが可能となる。	【実用上問題は少ない／解決済み】 • TorのOnion Routingと同様に、パケットデータを暗号化することで解決されている。 • 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）や、ハッシュ値やシークレットを署名に含める手法（スクリプトレススクリプト）等も提案されている。

3.2.1.1.7 アトミック・クロスチェーン・スワップ

アトミック・クロスチェーン・スワップとは、二つの異なるブロックチェーン上の暗号資産を、仲介者の介在や相互のネットワークの接続なしに、取引当事者間でのみ交換する仕組みであり、ビットコインやライトコイン等で導入されている。具体的には「ハッシュ・タイムロック・コントラクト」と呼ばれる技術を用いて、相互の暗号資産の受け渡しを条件付けることで実現している。

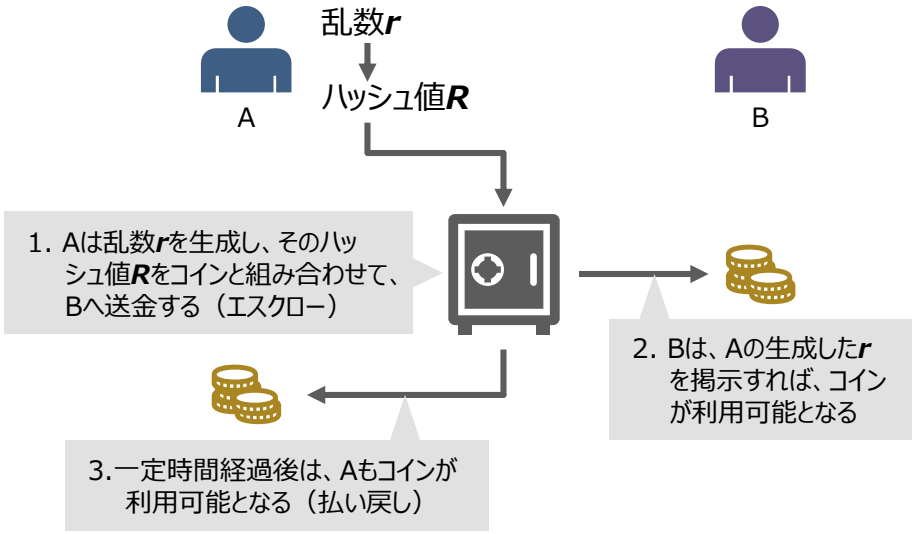
アトミック・クロスチェーン・スワップのイメージ

ビットコインとライトコイン双方の受け渡しを条件付けることで、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。



ハッシュ・タイムロック・コントラクトのイメージ

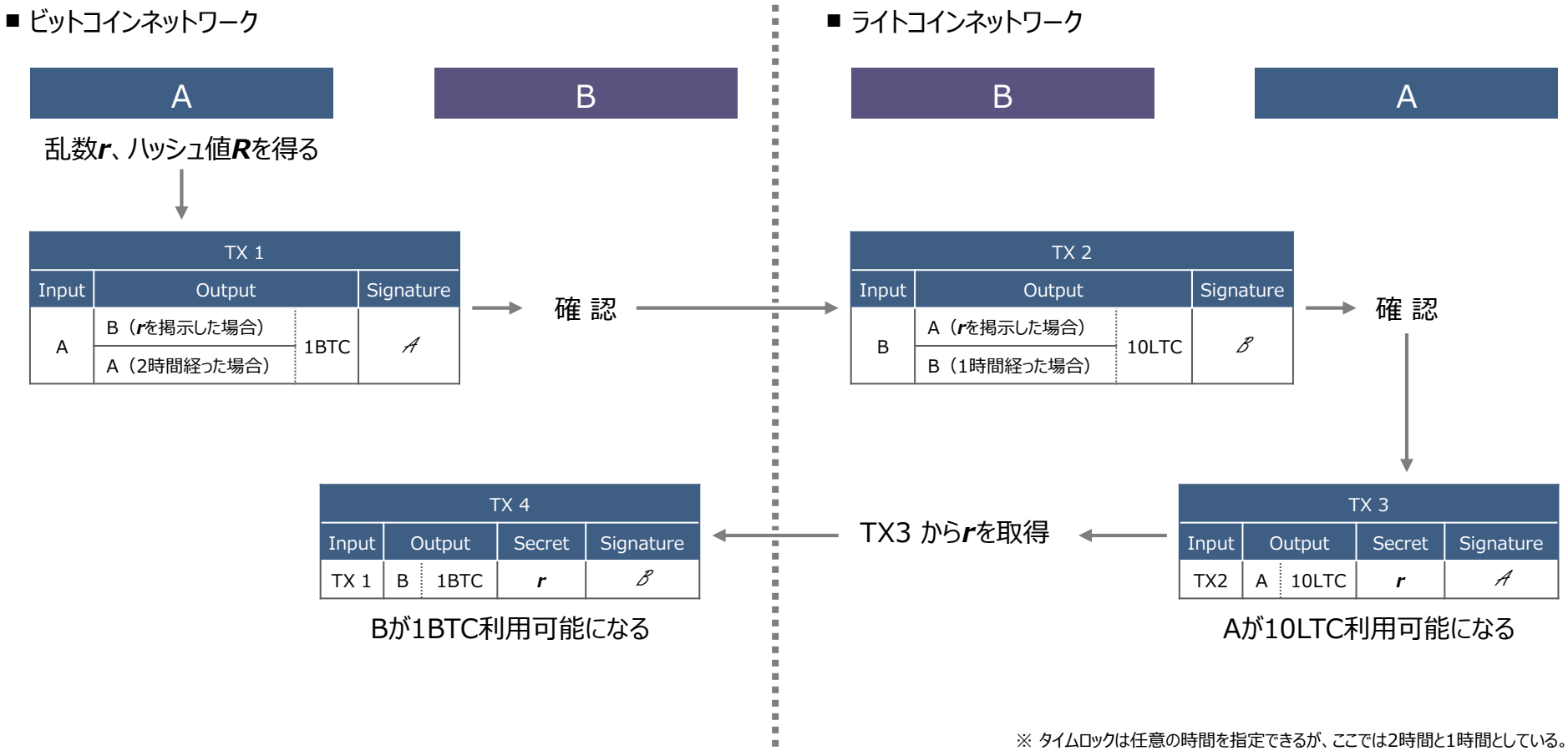
ハッシュ・タイムロック・コントラクトとは、ハッシュ関数とタイムロック機能を組合せて、条件付き支払いを可能にする技術であり、ライトニングネットワークやRipple Interledgerプロトコルなどでも同様の考えが利用されている。



3.2.1.1.7 アトミック・クロスチェーン・スワップ

取引当事者は任意のタイミングで取引を中止することができる。

アトミック・クロスチェーン・スワップの取引イメージ



※ タイムロックは任意の時間を指定できるが、ここでは2時間と1時間としている。

3.2.1.1.7 アトミック・クロスチェーン・スワップ – 課題と新たな取組

ハッシュ・タイムロック・コントラクトを用いるライトニングネットワークの進展と重なる部分も多い。プライバシーの改善が積極的に図られているが、実用化にあたってはアトミック性の担保や処理時間の短縮なども重要と考えられる。

課題	内容	関連した新たな取組
アトミック性の担保	● 最後のトランザクションが送信されない場合（前項ではBの最後のトランザクションが送信されない場合）のみ、アトミック性（一体不可分性を指し、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こと）が成り立たない。	● 信頼できる第三者に委託しておくことなどの運用での対処が提案されている。
常時監視の必要性	● 取引当事者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。	–
処理時間および流動性の利用効率	● 取引が覆らないことを確認するために、トランザクション毎に十分に長い時間を置く必要がある。取引が中止された場合、払い戻しまでに一定時間待つ必要がある。 ● 取引の間、他の取引にコインを利用することができないため、流動性の利用効率が悪化する。	【一部解決済み】 ● ライトニングネットワーク上でアトミック・クロスチェーン・スワップを行う手法が提案されている（ただし、取引が覆らないことを確認する時間が短縮されるが、それ以外のペイメントチャネルを開く時間や払い戻しの時間はかかる）。

3.2.1.1.7 アトミック・クロスチェーン・スワップ – 課題と新たな取組

課題	内容	関連した新たな取組
対応可能なブロックチェーン	● 双方のブロックチェーンともにハッシュ・タイムロック・コントラクトを備えている必要がある。また、ブロックチェーンデータは参加者に開示される必要がある。	【一部解決済み】 ● ハッシュ・タイムロック・コントラクトをマルチシグで代用する仕組みがBarter DEXで用いられている。ただし、片方のブロックチェーンのみに限られる（もう片方のブロックチェーンにはハッシュ・タイムロック・コントラクトが必要）。
プライバシー	● 異なるブロックチェーン上で同じシークレット（ハッシュ化する対象となる値）やハッシュ値を用いる必要があるため、第三者がハッシュ値やシークレットから双方のトランザクションを紐付けることが可能となる。	【解決済み】 ● ハッシュ値やシークレットを署名に含める手法（スクリプトレススクリプト）が提案されている。シュノア署名を用いた手法（2017年）と楕円曲線DSAを用いた手法（2018年）の両方が提案されている（いずれも、未だ未導入）。
オプション性	● 任意のタイミングで取引を中止／継続できることは、市場価格に応じて期限内にいつでも権利行使可能ということであり、アメリカンタイプのコールオプション性を有すると考えられる。この点が取引レートに反映されていない場合、売却側が不利となる。	【実用上問題は少ない／解決済み】 ● 片方に担保を拠出させ、当該当事者が取引を中止した場合に罰則を与える仕組みが提案されている。

3.2.1.1.8 ミンブルウィンブル

ミンブルウィンブルとは、ブロックチェーンデータの削減を行い過去履歴の検証負荷を下げる仕組みであるが、取引内容を秘匿化し、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側面もある。グリンやビームで導入されているが、ビットコインなど従来の暗号資産とは仕組みが大きく異なり、アドレスは存在せず、送金にあたっては受取人の協力が必要である。

トランザクションの構成

送金額はPedersen commitmentを用いて秘匿化される。これは、いわば送金額という値を金庫に入れた状態に相当する（外部から金庫の中の送金額を見ることはできず、また、一度金庫に入れた送金額を事後的に変更することはできない）。Pedersen commitmentは加法準同型性を持つことから、取引内容の検証は、送金額を秘匿化したまま行われる。送金は送金人・受取人双方が協力することで行われ、アドレスなどの識別子は用いられない。

ビットコインのトランザクション

Input	Output		Signature
AのUTXO	Bのアドレス	3BTC	𝒔

ミンブルウィンブルのトランザクション

Input	Output	Signature
c1	c2	c2 - c1という公開鍵に対応する秘密鍵による署名 *s1*

不要な取引履歴の削除

トランザクションカットスルーと呼ばれる仕組みにより、不要な部分は削除され、署名は集約される。例えば、下図では、c2やc3を含む取引はブロックチェーン上には記録されないことになる。

実際のトランザクション

Input	Output	Signature
c1	c2	*s1*

Input	Output	Signature
c2	c3	*s2*

Input	Output	Signature
c3	c4	*s3*

ブロックチェーンに記録されるトランザクション

Input	Output	Signature
c1	c4	*s1* + *s2* + *s3*

※実際の実装（グリン）の仕様では、署名は送金人・受取人双方が協力して作成し、署名は集約しないこととされている。

3.2.1.1.8 ミンブルウィンブル – 課題と新たな取組

グリンやビームは2019年1月にネットワークが稼働したばかりであり、今後利用が増えるにつれ、多面的な観点から課題が洗い出されると考えられる。

課題	内容	関連した新たな取組
スクリプト機能	● ミンブルウィンブルには、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。	【一部解決済み】 ● ハッシュ値などを署名に含める手法（スクリプトレススクリプト）で一部の機能を代替することが可能である。 ● グリンなどでは、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は、スクリプト外（トランザクションの機能）で解消されている。
利便性	● ミンブルウィンブルでは、送金の都度、送金人と受取人が協力する必要がある。送金の仕方が従来と異なるため、利用者に受け入れられるかは未知数な部分がある。	–
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、悪意のある者がコインを任意の量生成したり、取引内容を明らかにされてしまう問題が生じる。	【一部解決済み】 ● グリンやビームではSwitch commitments（量子耐性を備えたElgamal commitmentsと現状のPedersen commitmentsの両方を切り替えて利用できるもの）を用いて、量子コンピュータが実用化された場合も、コインを任意の量生成することができないようにしている。ただし、取引内容を明らかにされてしまう問題は解消されていない。
金額秘匿の弊害	● ミンブルウィンブル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、送金先までの最適な経路を計算できない問題が生じ得る。	–

3.2.1.1.9 シュノア署名

シュノア署名とは、楕円曲線DSAと同じく、離散対数問題の困難性に基づく電子署名方式の一種であり、グリンやビーム等で導入されている。複数の公開鍵や署名を一つに集約できる特徴があり、ブロックチェーンのデータを削減し、取引当事者の数や取引内容を第三者から隠蔽する点に期待されている。ビットコインには、後方互換性のあるソフトフォークで導入可能であり、導入へ向けて検討が続けられている。

データ量を削減するイメージ

AとBのマルチシグアドレス宛にコインを送金し、当該コインを利用する場合（1）AとBの公開鍵が集約できるため、マルチシグアドレスを（通常のアドレスと同じく）1つのアドレスで表現でき、（2）コインを利用する場合も署名を集約できるため、1つの署名で済む。このように、複数の公開鍵や署名を一つの値で置き換えることで、データ量を削減することができる。

Input	Output		Signature		Script
AとBのマルチシグアドレス宛に送金されたUTXO	D	1BTC	A	B	公開鍵Aと公開鍵Bを含むスクリプト本体

Input	Output		Signature
P	D	1BTC	$A+B$

ここで、Pは、*A*と*B*の公開鍵を集約した公開鍵から算出されるアドレスを指す。

取引内容を隠蔽するイメージ

シュノア署名を活用して、複数の支払い条件を一つの公開鍵で置き換える仕組み（Taproot）が提案されている。この場合、コインを送金する際に、いずれの支払い条件もブロックチェーンに記録されない。また、ある条件を満たしてコインを受け取る際も、それ以外の条件はブロックチェーンには記録されないため、公開範囲を最小限に留め、プライバシーを向上することができる。

Input	Output		Signature	Public Key
A	AとBのマルチシグアドレス A（1時間経った場合）	1BTC	A	A

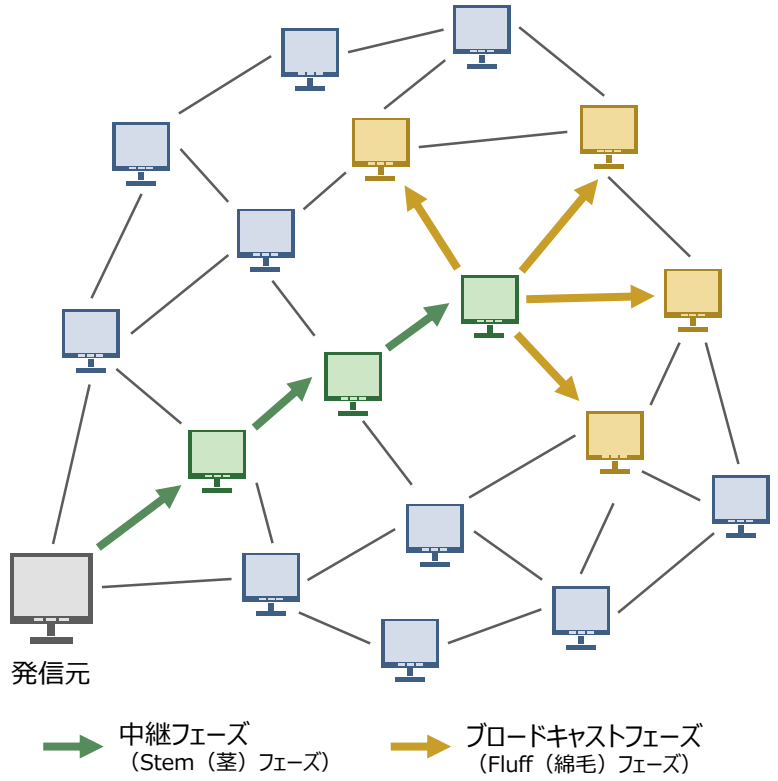
Input	Output		Signature	Public Key
A	P	1BTC	A	A

ここで、Pは、複数の支払い条件を集約した公開鍵から算出されるアドレスを指す。

3.2.1.1.10 ダンデリオン

ダンデリオンとは、P2Pネットワークにおいて、トランザクションの実際の発信元を秘匿する仕組みであり、グリンやゼットコイン等で導入されている。具体的には、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ブロードキャストを行うことで実現している。

ダンデリオンの処理フロー



ダンデリオンは、トランザクションの発信（ブロードキャスト）をダミーノードが行うことで、実際の発信元ノードの存在を秘匿する。具体的には、中継経路構築、トランザクション中継、ブロードキャストという3ステップを踏む。

1. 各ノードは、接続先の中からランダムに中継先ノードを選択する。これは10分毎に更新される。

2. 発信元ノードは、ランダムに選んだ中継先ノードへトランザクションを送信する。中継ノードは、中継するか／ブロードキャストするかを、90%／10%の確率で選択する。この段階はStem（茎）フェーズと呼ばれる。

3. 中継ノードがブロードキャストを選択した場合、もしくはノード毎にランダムに設定された有効期限を過ぎた場合に、当該ノードはトランザクションを近隣ノードへブロードキャストする。この段階はFluff（綿毛）フェーズと呼ばれる。以降は、通常の場合と同様に、ブロードキャストが繰り返されながら、当該トランザクションがネットワーク全体へ伝播していく。

グリンの場合、ミンブルウィンブルとダンデリオンを組合せて、各中継ノードがトランザクションを中継する際に、トランザクションカットスルーにより、複数のトランザクションを集約してから中継する。そのため、いくつかの取引は中継時にその存在自体が削除されることになる。

3.2.1.1.11 匿名通貨

匿名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称され、代表的なものとしてダッシュ、モネロ、ジーキャッシュが挙げられる。

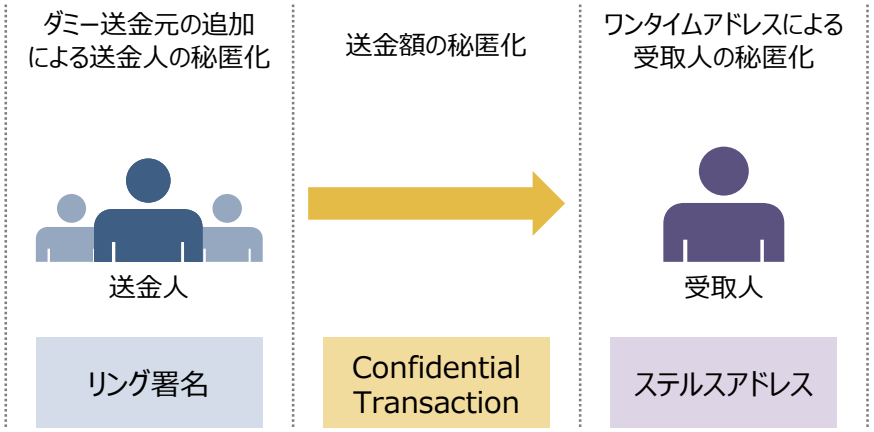
名称	稼働時期	匿名化技術	特徴
ダッシュ	2014年 1月	ミキシング （PrivateSend）	• 利用者が指定した場合に限り、ミキシングが行われる。 ➢ 利用者はPrivateSendと呼ばれる機能を有効化する。 ➢ PrivateSendを有効化した利用者が計3人集まると、4種類の金額種別（0.01／0.1／1／10DASH）毎に、ミキシングが複数回行われる。 • ただし、ミキシングが行われるだけであり、送金人、受取人や送金額等の秘匿化は行われない。
モネロ	2014年 4月	ステルスアドレス、 リング署名 （Ring CT）	• 利用者の指定なしに、送金人の秘匿化を行うリング署名、受取人の秘匿化を行うステルスアドレス、送金額の秘匿化を行うConfidential Transaction（CT）がデフォルトで行われる。 ➢ ステルスアドレスにより、送金先として、都度ランダムなワンタイムアドレスが利用される。 ➢ リング署名により、都度同額のダミー送金元を集めて、実際の送金元が秘匿化される。 ➢ Confidential Transactionにより、送金額も秘匿化される。
ジーキャッシュ	2016年 10月	ゼロ知識証明 （zk-SNARKs）	• 利用者が指定した場合に限り、取引内容（送金元、送金先、送金金額等）の全てを秘匿化するzk-SNARKsが行われる。zk-SNARKsはミキシングやリング署名等よりも秘匿化の度合いが強いと指摘されている。 ➢ アドレスは、取引内容を秘匿する秘匿アドレスと、それ以外の公開アドレスからなる。 ➢ 送金元アドレス・送金先アドレスの秘匿・公開の組合せ（計四通り）で、送金元、送金先、送金額の秘匿の指定が可能となる。 • なお、閲覧鍵（viewing-key）を第三者に提供することで、提供された者は秘匿された場合でも取引内容を確認することができる（利用することはできない）。

3.2.1.1.11 匿名通貨－モネロ

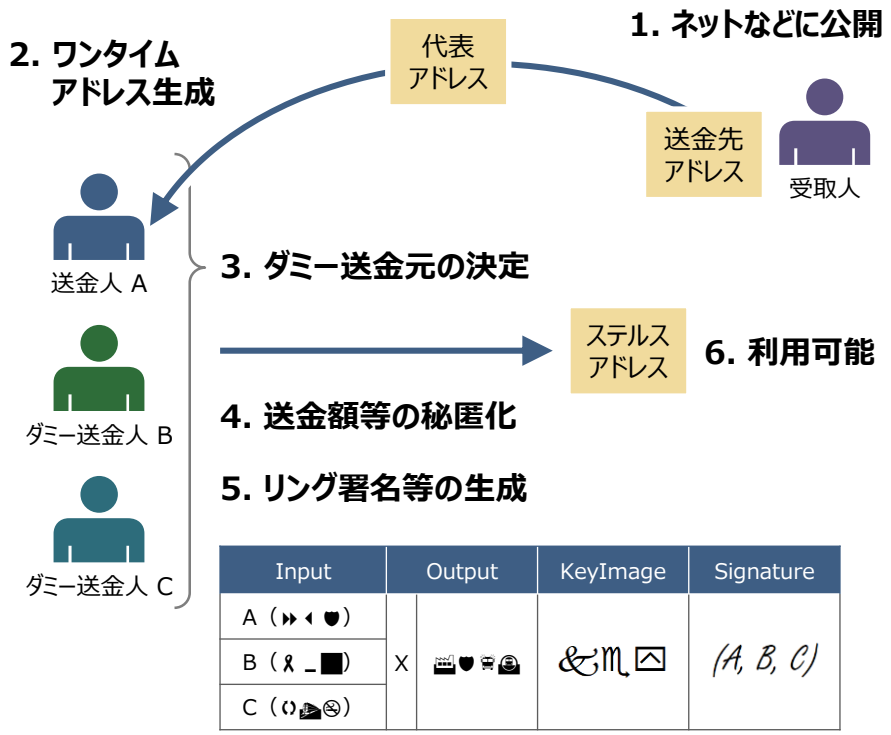
匿名化技術は組合せて用いられる場合もあり、例えばモネロでは送金人、受取人、取引金額それぞれを異なる技術で秘匿化している。モネロは、ビットコインで提案された匿名化技術も積極的に取り入れており、ジーキャッシュとともに代表的な匿名通貨として広く知られている。

秘匿技術の組合せのイメージ

モネロでは、送金人の秘匿化を行うリング署名、受取人の秘匿化を行うステルスアドレス、送金額の秘匿化を行うConfidential Transactionが標準で備わっている。
なお、リング署名とConfidential Transactionの組合せはRing CTと呼ばれ、2017年1月から稼働を開始した。



処理フローのイメージ



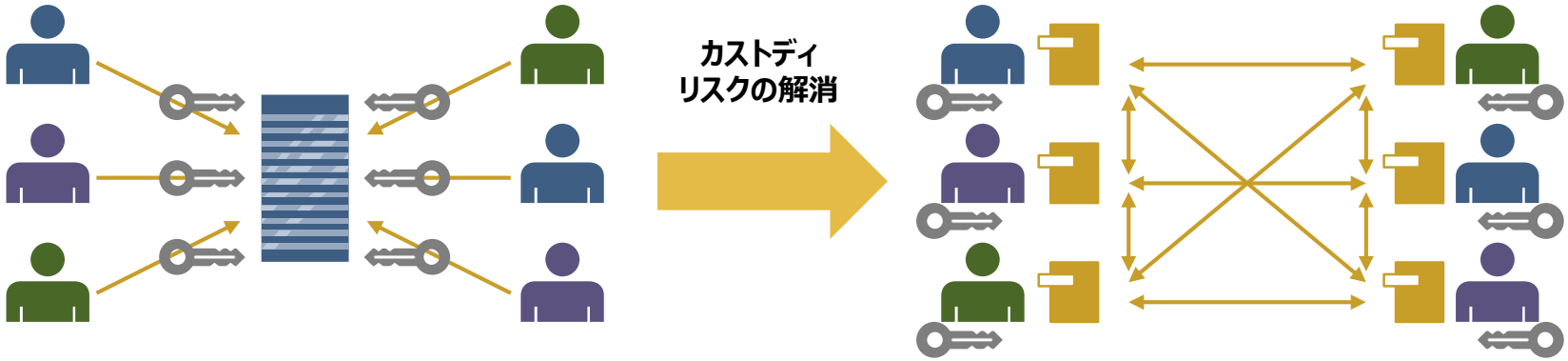
3.2.1.2 DEX

3.2.1.2.1 DEXの概要
3.2.1.2.2 DEXの分類
3.2.1.2.3 主要なDEX
3.2.1.2.4 DEXの課題と方向性

3.2.1.2.1 DEXの概要

分散型取引所（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。

従来の取引所（中央集権型取引所）	DEX（分散型取引所）
利用者は取引所に秘密鍵を預ける。秘密鍵管理やサーバ運用など、取引にあたっては取引所を信頼する必要がある。	利用者は自身で秘密鍵を管理する。取引処理はブロックチェーン上のスマートコントラクトが行う。



取引所にリスクが集中
（単一障害点、単一信頼点）

利用者にリスクが分散
透明性および可用性の向上

3.2.1.2.1 DEXの概要 – メリット

DEXの最大のメリットは、中央集権型取引所に関連した被害（ハッキング被害、価格操作・仮装売買による被害やサーバ障害による被害等）を受けないことであり、それ以外の主なメリットとしては以下が挙げられる。

- 常時取引が可能（高い可用性）
- KYCを経ずに取引が可能（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

	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、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

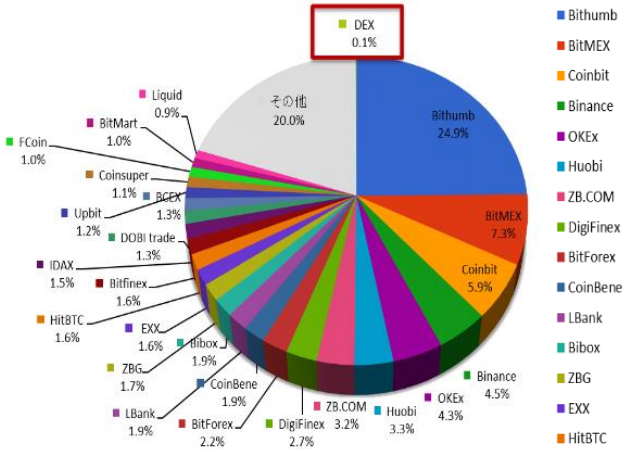
3.2.1.2.1 DEXの概要－取引量等の規模

DEXの取引高は全取引所の取引高の0.1%程度と推測される（2018/11/13時点）。

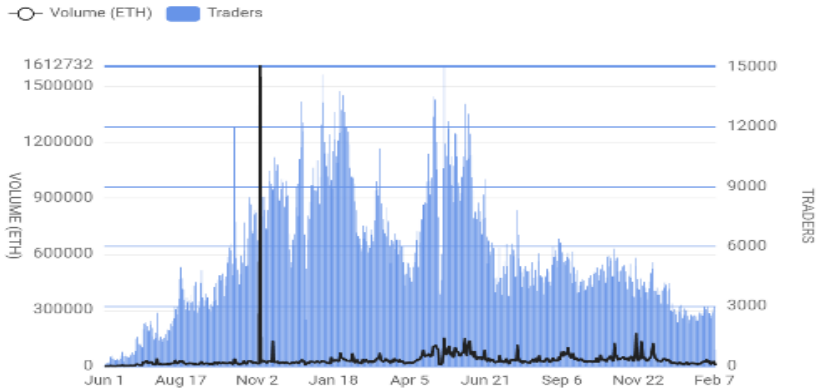
DEXの取引高（2018/11/13）

	過去24時間の取引高（手数料なし取引含まず）	過去7日間の取引高（手数料なし取引含む）
米ドル	7,413,898	39,736,254
円	¥843,701,592	¥4,521,985,705

過去7日間の取引高に占める割合（手数料なし取引含む、2018/11/13）



DEX取引高の推移（2017/6～2019/2）



時価総額の比較（2018/9/17時点）

	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	約1,085億	約12兆	100.00%	–
イーサリアム	約202億	約2.3兆	18.61%	100.00%
0x	約2.9億	約324億	0.27%	1.43%
IDEX (Aurora)	約1,000万	約11億	0.01%	0.05%

（左上･左下）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
（右上）DEXWatch and Alethio, DEX Watch, "DEX Volume and Traders on Ethereum", https://dex.watch/, 2019/2/8
（右下）CoinMarketCap, coinmarketcap.com, "Historical data", https://coinmarketcap.com/ 2018/11/13 より三菱総研作成

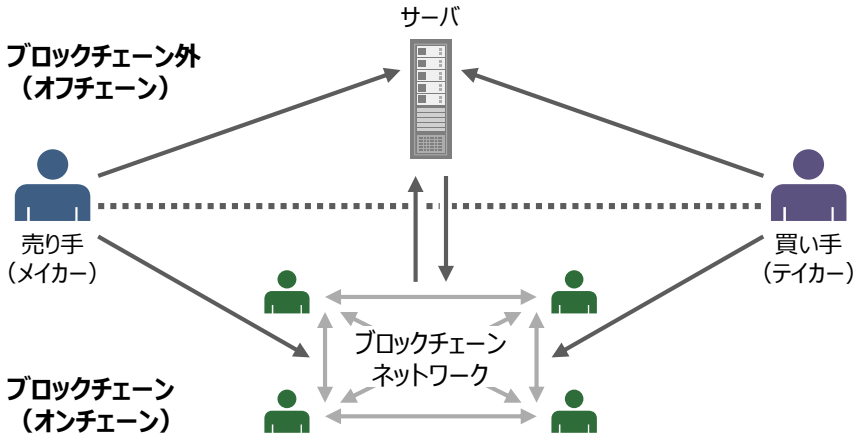
3.2.1.2.2 DEXの分類－分類の軸

本調査研究では、技術的な視点と当局の視点を考慮し、オフチェーン処理の有無、および異種トークンの取扱有無という二軸で整理した。

- オフチェーン処理の有無は、効率性（技術面）や制度対象先の特定（制度面）に関わる。
- 異種トークンの取扱有無は、相互運用性（技術面）、取扱資産の充実度（利便性）やAML/CFT規制上の重要度（制度面）に関わる。

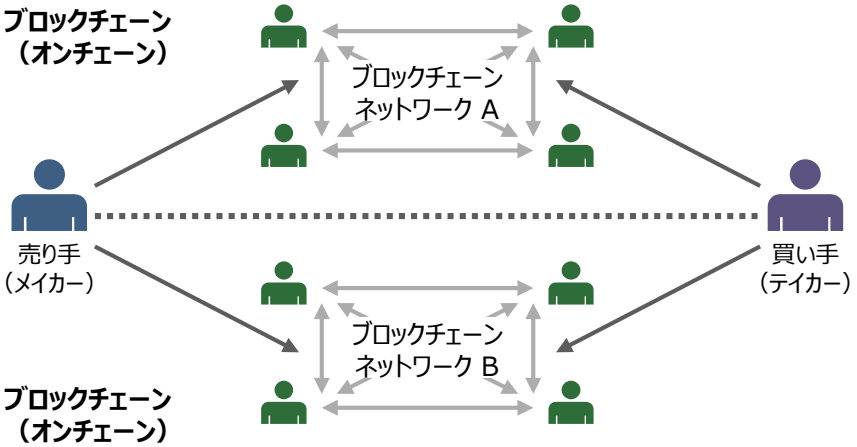
オフチェーン処理の有無

オフチェーン処理を行う場合、特定のノードや主体に処理を集中させるほど、効率的な処理が可能となるが、障害発生リスクやセキュリティリスクを高めることになる。
また、特定の管理主体が必要となるため、規制対象先が存在することになる。



異種トークンの取扱有無

同一ブロックチェーン基盤上の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や法定通貨も扱うかという点は相互運用性や利用者の利便性の点では重要となる。
また、取扱通貨の種別は、AML/CFT上の重要性に関わることになる。



3.2.1.2.2 DEXの分類－一覧表

以降の項で各々のパターンについて記載する。

DEXの一覧表

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 （法定通貨含む）
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）	なし	なし
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）			

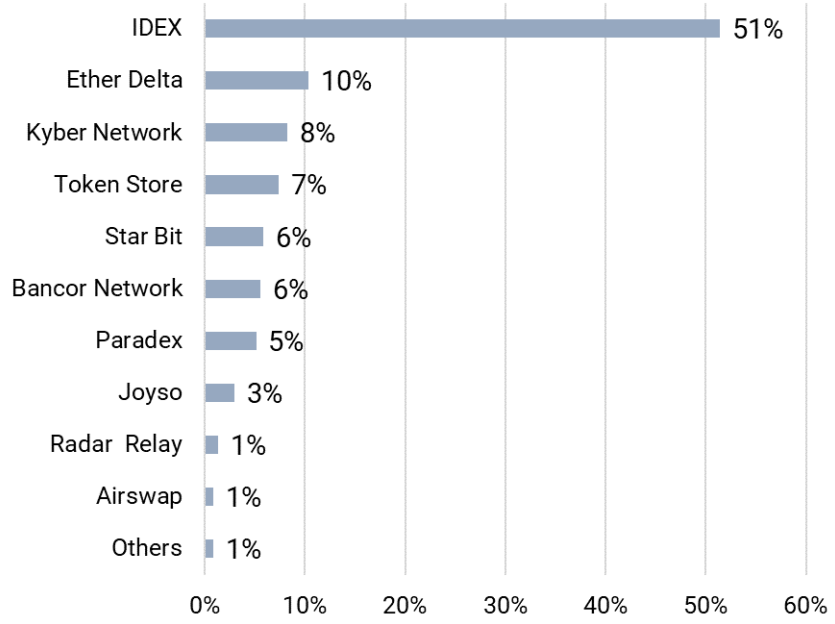
＊ 本調査研究で確認した限り、法定通貨との交換が可能であったもの。

3.2.1.2.2 DEXの分類－主要なDEX

取引所業務には強いネットワーク効果が働き、流動性は更なる流動性を生むと考えられる。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。

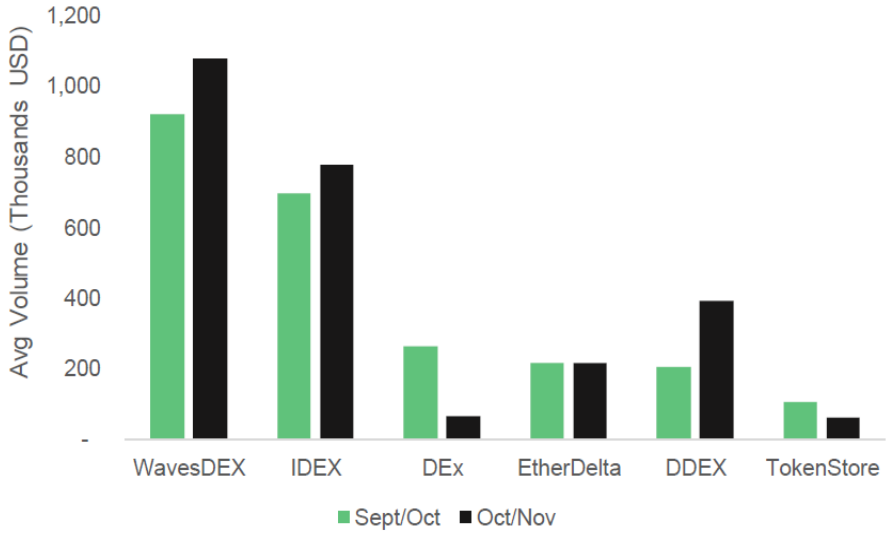
主要なDEX－ERC20トークン（同種トークン）の場合

IDEXが過半を占める（過去30日間が対象、2019/2/1時点）。



主要なDEX－異種トークンも含めた場合

WavesDEXとIDEXが大半を占める（24時間平均取引高、2018/10および2018/11時点）。また、これらDEXの取引高は全体の約0.4%に留まる。



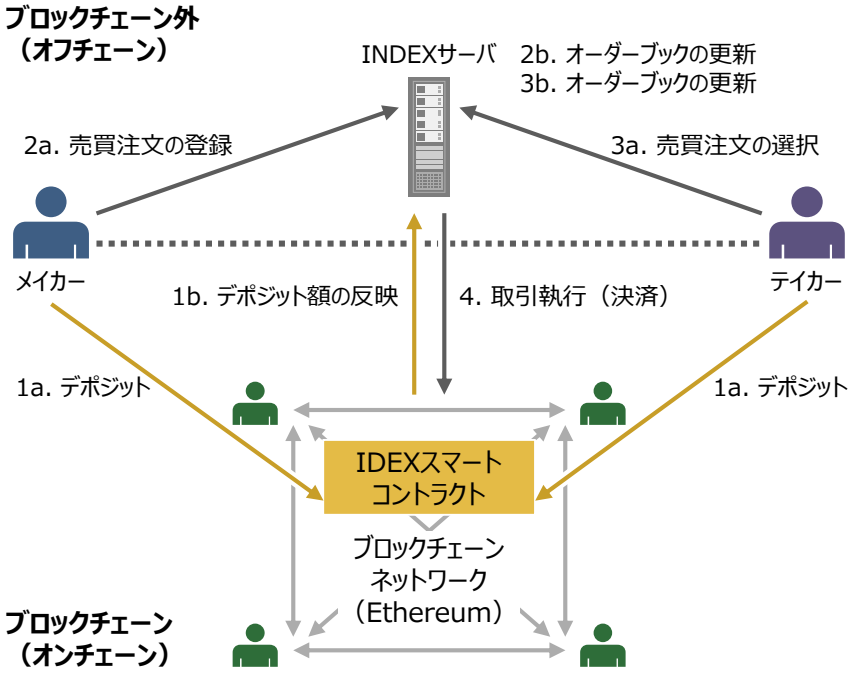
（左）Etherscan, etherscan.io, "Top DEX Pie Chart", https://etherscan.io/stat/dextracker, 2019/2/1より三菱総研作成
（右）CryptoCompare, Crypt Coin Comparison LTD, "CCCAGG Exchange Review, November 2018", https://www.cryptocompare.com/media/35308846/cryptocompare_exchange_review_2018_11.pdf, 2019/1/14

3.2.1.2.3 主要なDEX－（1）管理主体あり、同種トークンのみ

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。

一般に、メイカーとテイカーの「マッチング」および「価格形成」はオフチェーンで管理されるオーダーブックを通して行われる。

IDEXの処理フロー



1. メイカーおよびテ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する。
2. メイカーは、デポジットした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。
3. 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。
4. 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。

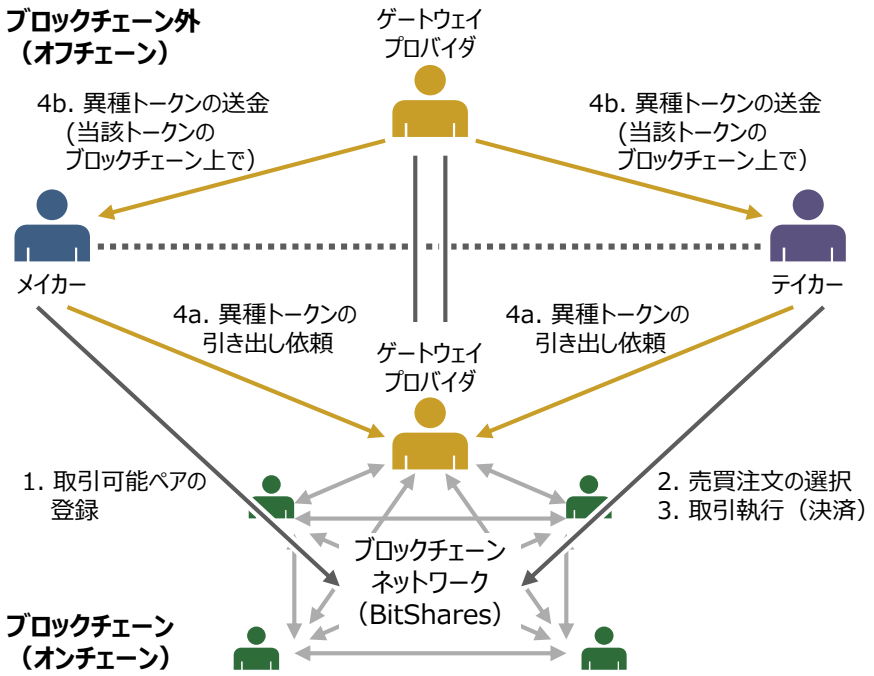
オーダーブックおよび残高情報等をオフチェーンで管理することにより、取引の高速化を実現するとともに、訂正／取消注文等にも手数料のかからない仕組みとなっている。

3.2.1.2.3 主要なDEX－（2）管理主体あり、異種トークンも取扱

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。

一般に、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、当該ブロックチェーン上でそれらを取引する形をとる。メイカー・テイカーの「マッチング」・「価格形成」はオンチェーンで行われ、「決済」はオンチェーンとオフチェーンの両方で行われる。

OpenLedgerの処理フロー



1. メイカーは売り注文をBitShares上にブロードキャストする（BitSharesではブロックチェーンデータがオーダーブックになる）。
2. テイカーは希望する売り注文を選択し、売り応答注文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。
3. メイカー・テイカー双方の応答注文が揃った時点でBitShares上で決済が行われる。
4. 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（特定の運営主体）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。

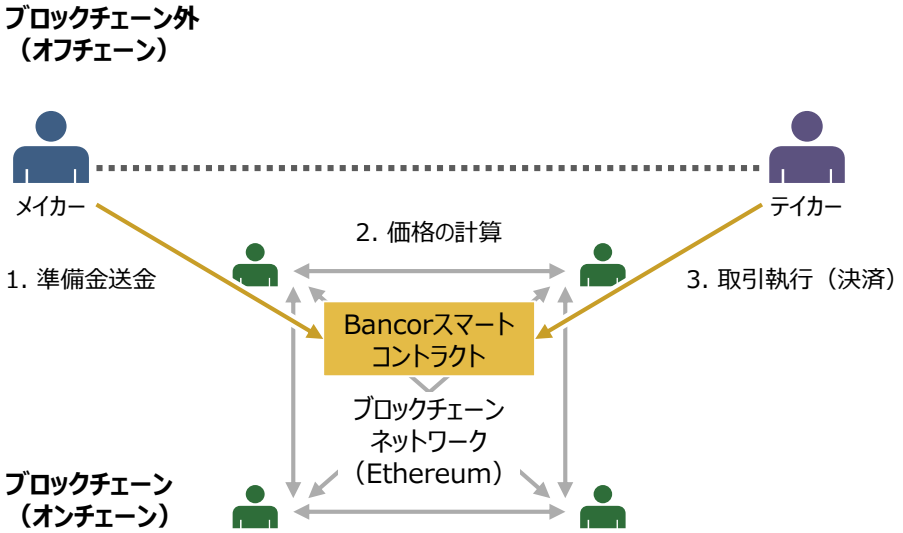
決済に特定の主体が深く関与するため、決済リスク（信用リスクや流動性リスク）が存在すると考えられる。

3.2.1.2.3 主要なDEX－（3）管理主体なし、同種トークンのみ

特定の管理主体は存在せず、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。

一般に、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。

Bancorの処理フロー



1. 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。
2. 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、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。
3. 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。

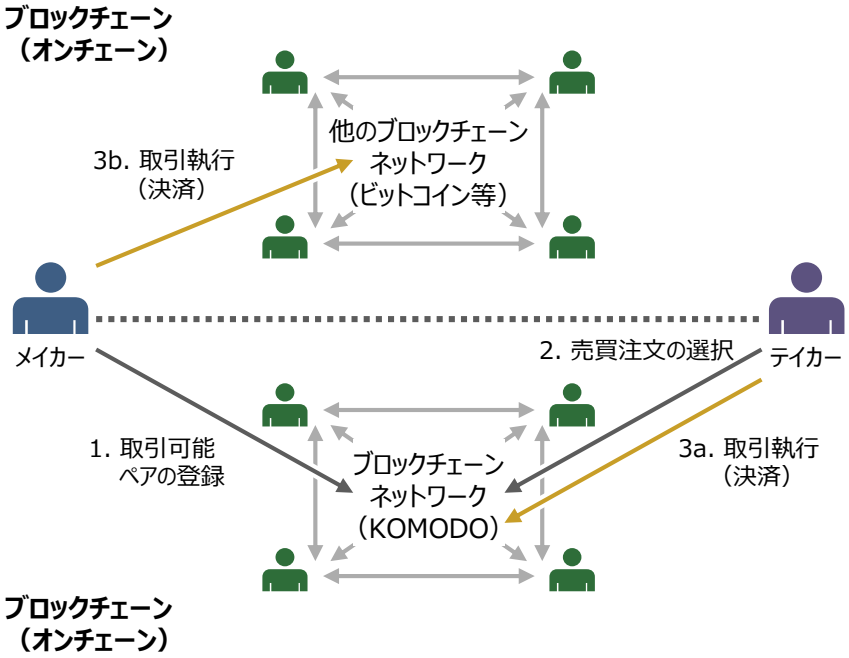
人を排除することによる詐欺行為の撲滅や取引が活発でない暗号資産の流動性リスクの解決を目指している。

3.2.1.2.3 主要なDEX－（4）管理主体なし、異種トークンも取扱

特定の管理主体は存在せず、メイカーとテイカーの「マッチング」・「価格形成」・異種トークンとの「決済」は全て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。

BarterDEXの処理フロー

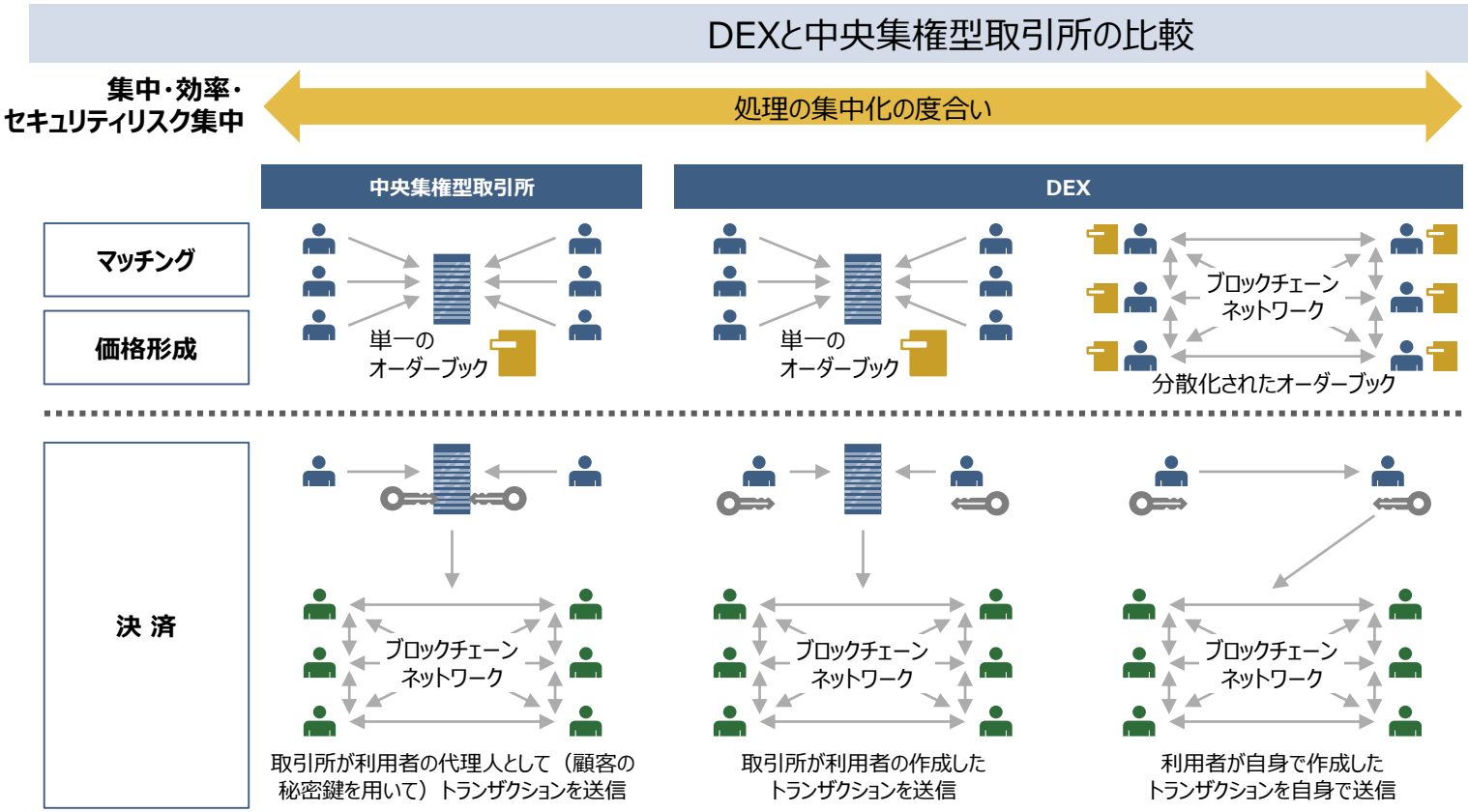


1. 分散保持されるオーダーブックにメイカーが売買注文を登録する。
2. テイカーが自身の希望する注文を選択する。
3. 取引ペアとなる異なるブロックチェーン上でのメイカー・テイカー各々の残高確認を経て、問題なければマッチングが成立する。
4. メイカー・テイカーはアトミック・クロスチェーン・スワッププロトコルに従って取引ペアとした二つのブロックチェーン間でのコインの交換を行う。

利用者は、取引ペアとなるブロックチェーン上の秘密鍵を管理する必要がある、アトミック・クロスチェーン・スワップという複雑な手順を踏む必要がある、長い承認時間を待つ必要があるなど、他のDEXに比べて利用者側の負担が大きい。

3.2.1.2.4 DEXの課題と方向性－技術面

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、全ての機能を分散化させることが望ましい。しかしながら、近年は安全性よりも効率性を重視して一部処理を集中化させる取組が活発化し、中央集権型取引所に戻りつつあるとも言える。DEXにおける効率性と安全性の最適なバランスについては今後さらに検討が進むと考えられる。



- オーダーブック等をオフチェーンで処理することは、処理の高速化、訂正・取消処理への手数料負担の軽減などのメリットがある。
- 他方で、当該処理が単一障害点、単一信頼点となることにもつながり得る

3.2.1.2.4 DEXの課題と方向性－ユーザビリティ面

単に暗号資産の交換を行うだけであれば、既存の中央集権型取引所や販売所の方がユーザビリティの面で優れている。例えば、多様なトークンの取引プラットフォームや他の分散型金融サービス（DeFi）との組合せなど、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。

課題	利用にあたってのDEXの課題
利用者の自己責任の範囲が広い	• 暗号資産の秘密鍵を適切に管理する必要がある。 • 一部のDEXでは複雑な決済手順を適切に行う必要がある。 • スマートコントラクトのバグや予期せぬトラブルなどのリスクを負う必要がある。
マイナーや他のユーザによる攻撃	• フロントランニング（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DEXは設計される必要があるが、マイナーによる攻撃は防げない。 • また、こうした対策は事前に流動性がロックされるなど利用時の不便を生じさせる。
中央集権型取引所に比べて使い勝手が悪い	• 処理速度はオフチェーンで処理する中央集権型取引所よりも遅い。 • 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ものは少ない。 • 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場合が多い。 • 信用取引や証拠金取引が行えるものは限られる。 • 取引手数料は中央集権型取引所に比べ低廉ではない（一部のDEXでは、手数料を上げるほど取引が成立する可能性が高まるため、手数料の上昇を招きやすい可能性がある）。 【特定の管理主体を介在させずに異種トークンも取り扱うDEXの場合】 • 価格変動等により取引が途中で中止されるリスクが存在する。 • 取引相手による詐欺などに備えて、常にブロックチェーン上を監視する必要がある。 • アトミック・クロスチェーン・スワップを行う場合、流動性の利用効率が悪化する。
流動性が低い	• 取引高は全取引所の約0.1%程度に留まる。 • ネットワーク外部性により流動性が低いことはさらに流動性を低下させる懸念がある。

（参考）セキュアチャットツール

セキュアチャットツール

セキュアチャットツール（アプリケーションレイヤー）はブロックチェーンとは異なるものであるが、近年は、ブロックチェーン関連の開発情報やダークマーケットの取引情報がやり取りされることも多い。セキュアチャットツールで通信内容を隠蔽し、匿名通信で全体の伝送経路を隠蔽する、というセキュアチャットツールと匿名通信を組み合わせた使い方が可能である。

代表的なセキュアチャットツール

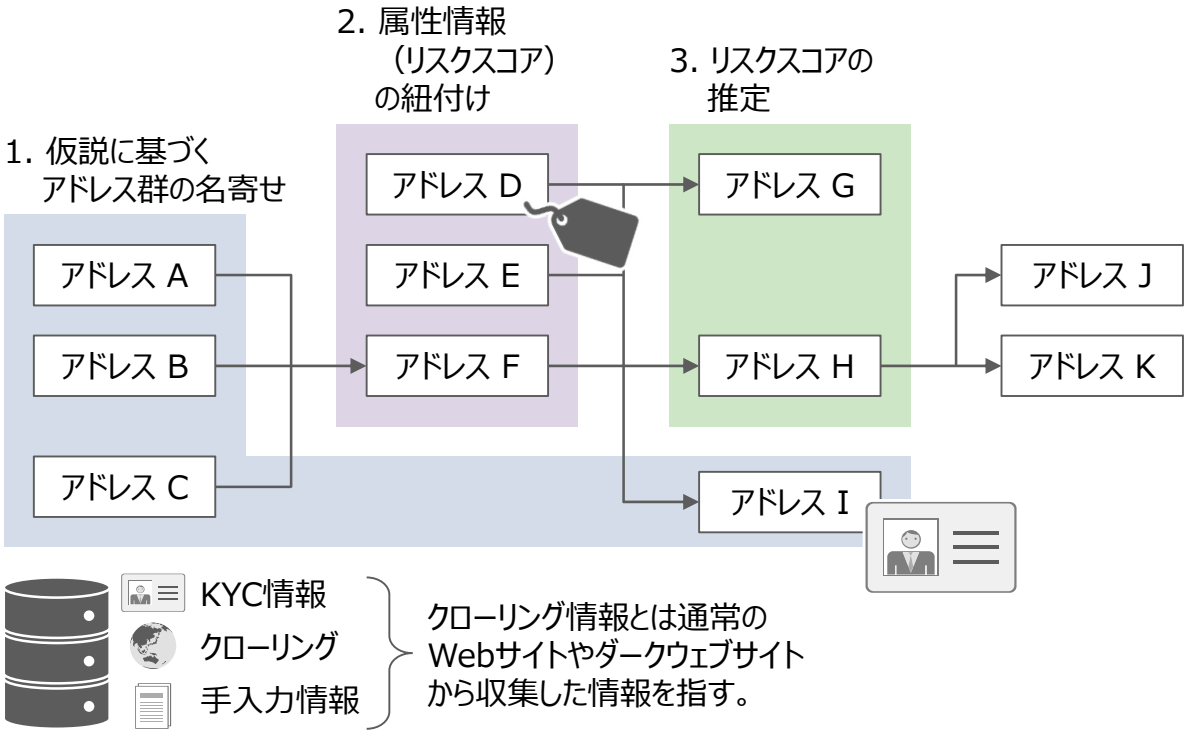
ツール名	Telegram	Signal
概要	月間アクティブユーザ数が2億人超（2018/3/22時点）にのぼる。クライアントはオープンソースだが、サーバのコードは公開されていない。	アメリカ合衆国上院において議員間の連絡のツールとして公式に認可されている。SignalプロコトルはWhatsAppなど他のソフトウェアでも一部用いられており、クライアント・サーバのコードともにオープンソースである。
開発経緯	露のソーシャルネットワークVkontakteの創始者であるNikolai Durov氏とPavel Durov氏の兄弟（露）を中心に2013年に開始。	前身は2010年頃よりTextSecureやRedphone等として開発が進められ、2014年からSignalという名称に移行。
匿名化の仕組み・程度	MTProtoという独自プロトコルだが、その安全性については議論が分かれている。エンドツーエンド暗号化は1対1のシークレットチャットの場合のみに行われる。	Signal Protocolという独自プロトコルであり、拡張トリプル・ディフィー・ヘルマン鍵合意プロトコルなどが用いられている。エンドツーエンド暗号化は全ての通信で行われる。
政府要請への対応	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ことがあったが、これを拒否しており、ロシア国内で使用禁止となった。イランでも使用禁止になったと報じられている。	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、2016年に米政府が犯罪の疑いのある通信データを提出させた際も有用なデータは保持されていなかった。

3.2.2 ブロックチェーンの再識別技術

3.2.2 ブロックチェーンの再識別技術

ブロックチェーン上のアドレスのリスク評価にあたっては、アドレス群を名寄せし、別途収集した外部データをアドレス群に紐付けて属性情報を付与し、紐付いたアドレス群に基づいて、紐付かなかったアドレスのリスクを推測する手法などがとられる。しかし、これらはあくまで推測に留まり、またデータベースの質や量にも大きく依存する（匿名化技術も再識別技術も、学術的な有効性評価はなされていない状況にある）。

ブロックチェーンアドレスの再識別のイメージ



1. 一定の仮説に基づいてアドレス群の名寄せを行う。
2. ウェブやダークウェブから収集した外部データと照らし合わせて合致したアドレスには属性情報（リスクスコア）を割り振る。
3. 合致しないアドレスには、既に振られたリスクスコアをもとに、リスクスコアの推定を行う。

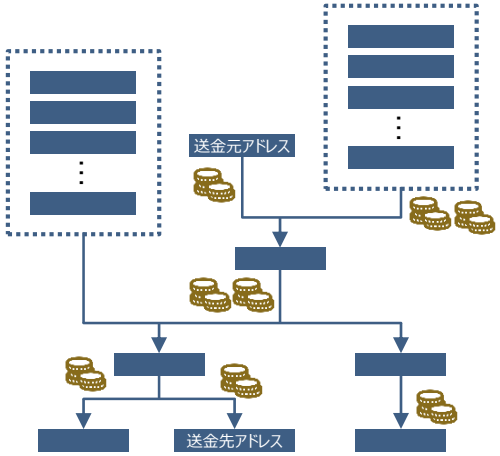
しかし、そもそも名寄せにあたっての仮説の妥当性についてコンセンサスが得られているわけではない。

3.2.2 ブロックチェーンの再識別技術

ミキシングなどの高度な匿名化技術に対しては、特徴的な振る舞いの検知などが進められている。また、外部データとして、ブラウザのクッキー情報やSNSの情報などを活用する手法も提案されている。

ミキシングサービスの振る舞いによる検知

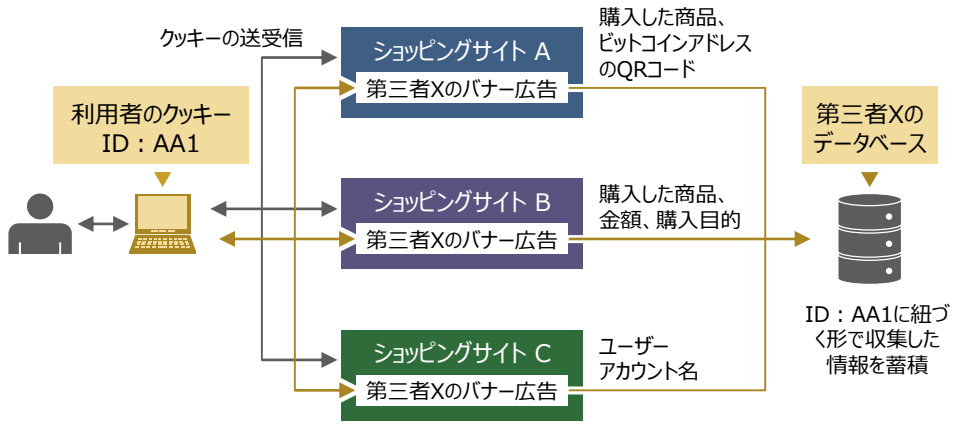
ミキシングサービスについては、送金元と送金先の紐付けは極めて困難であり、また、（アドレスは無限に生成できるため）ミキシングサービス自体の検知も困難である。
そこで、ミキシングサービスに特徴的な振る舞いに着目した検知が取り組まれている。



特徴	検知内容
アドレスの使い回し	● 毎回特定のアドレス（Central address）へ送金される ● 複数の送金経路上に同じアドレスが存在する
特徴的な取引パターン	● 送金元への支払いとなる少額とそれ以外という二分割を繰り返す（Peeling Chain） ● 複数の送金経路で送金回数が一定、ないし時間間隔が一定 ● 送金元一つに対して複数の送金先が存在する

外部データの活用

ビットコイン決済の可能なECサイトに掲載されているバナー広告等のクッキーをアドレスの名寄せに活用する方法が提案されている。他には通常のSNSサイトやダークウェブサイトのアカウントとビットコインアドレスの情報を紐付ける方法なども提案されている。



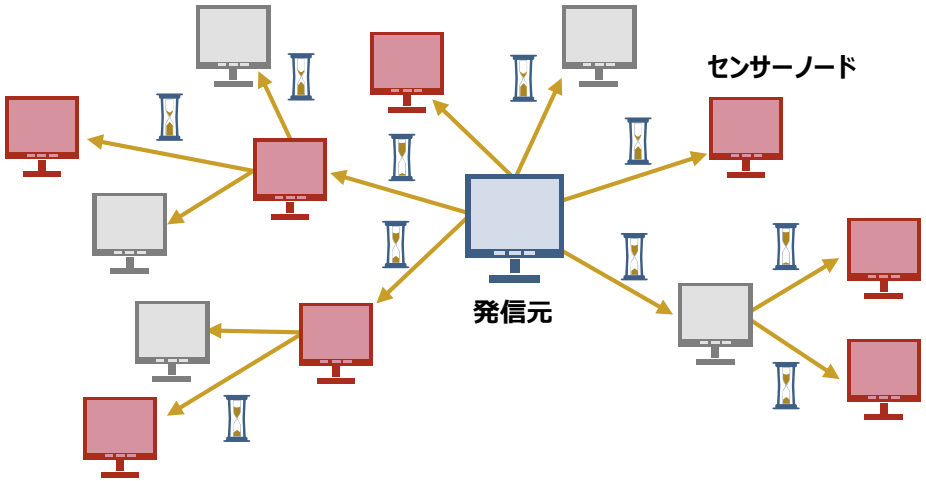
上図を例にすると、複数のショッピングサイトにバナー広告等を掲載することで、それぞれのサイトの閲覧者の商品購入に関する情報（各サイトのアカウント情報と各商品の送金元アドレス）を紐付けることができる。

3.2.2 ブロックチェーンの再識別技術

トランザクションの発信元の特定には、P2Pネットワーク上で十分な数のセンサーノードを用意して推測する手法が提案されている。実際に、仮想通貨モナコインにおいて、200個以上のセンサーノードを用いて実施された事例がある。

トランザクションの発信元の再識別イメージ

地震の震源地推定と同様に、センサーノードの結果から発信元を推測する。ここで、発信元と直接つながる確率を高めるため、十分な数のセンサーノード（下図の赤いノード）が必要。ただし、発信元を特定できたとしても、匿名通信により、本来の発信元IPアドレスとは異なる可能性がある。



事例は以下の資料に基づく; 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://www.japan-d2.com/news-detail/2018/11/5, 2018/12/12

3.3 P2Pレイヤー/インターネットレイヤー

3.3.1 P2Pレイヤー/インターネットレイヤーの匿名化技術
3.3.2 P2Pレイヤー/インターネットレイヤーの再識別技術

3.3.1 P2Pレイヤー/インターネットレイヤーの匿名化技術

3.3.1.1 匿名通信技術の概要
3.3.1.2 匿名通信技術の分類
3.3.1.3 主要な匿名通信技術
3.3.1.4 匿名通信の課題と方向性

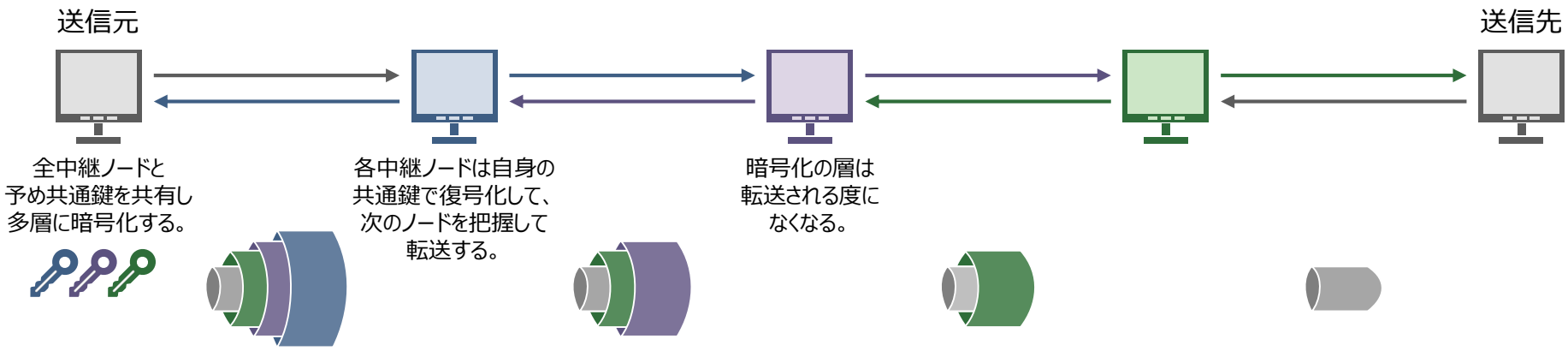
3.3.1.1 匿名通信技術の概要 – 匿名化の考え方

インターネット上の通信の匿名化対象としては、通信内容、およびIPパケットの伝送経路の二つが挙げられる。

- 通信内容は、送信元と送信先のみが把握できれば良い。そのため、匿名化にあたっては暗号化等が用いられる（一般的なSSL通信などと同様）。
- 伝送経路は、送信元・送信先IPアドレスがIPパケットに記録され、この情報にしたがって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。

通信内容および全体の伝送経路の匿名化の例

IPパケットを多層に暗号化しておき、伝送系路上の中継ノードには次のノードへの情報のみを開示することで、元々の送信元のIPアドレスおよび通信内容を中継ノード含めた第三者から隠蔽する（オニオンルーティング）。



3.3.1.1 匿名通信技術の概要 – 匿名通信技術を悪用した事件

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報共有を目的として開発された一方で、違法な物品売買や犯罪に使用されるケースも多い。

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	内容
パソコン遠隔操作事件	• 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アドレスに基づいて捜査した結果、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。
年金情報流出事件	• 2015年5月、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、犯人の特定が困難であったため、容疑者不詳のまま書類送検された。
学校爆破予告事件	• 2017年1月、専門学校に対する爆破予告のメールが複数回送信され、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。
児童ポルノ公開事件	• 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。

3.3.1.2 匿名通信技術の分類－分類の軸

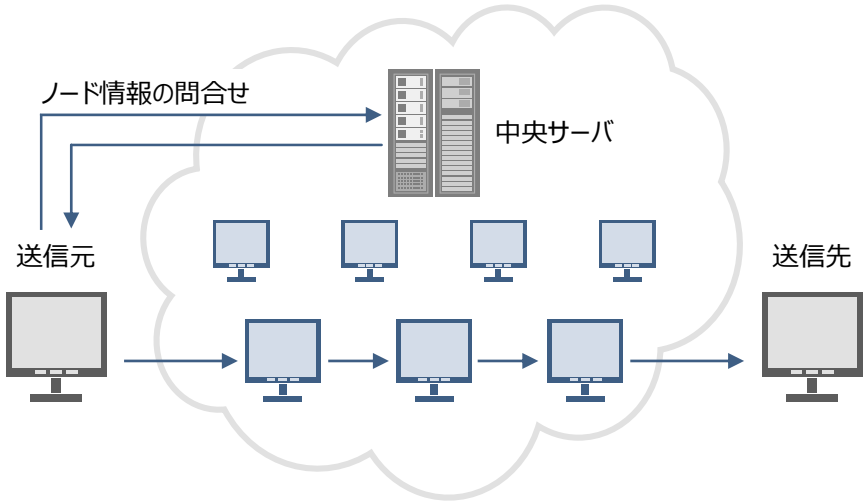
本調査研究では、技術的な視点と当局の視点を考慮し、ルーティングという軸で整理した。

- ルーティングは伝送経路の決定方法を指し、匿名性の強度や通信性能（技術面）、制度対象先の特定（制度面）に関わる。大きく、ソースルーティング方式とホップバイホップ方式に分かれる。

ソースルーティング方式のイメージ

送信元が全体の伝送経路、すなわち、送信先までの中継ノードやその順序（ルート）を決定する。
そのため、送信元は全ての中継ノードを予め把握しておく必要があり、ノード情報を集中して管理する主体が必要となるため、規制対象先が存在することになる。

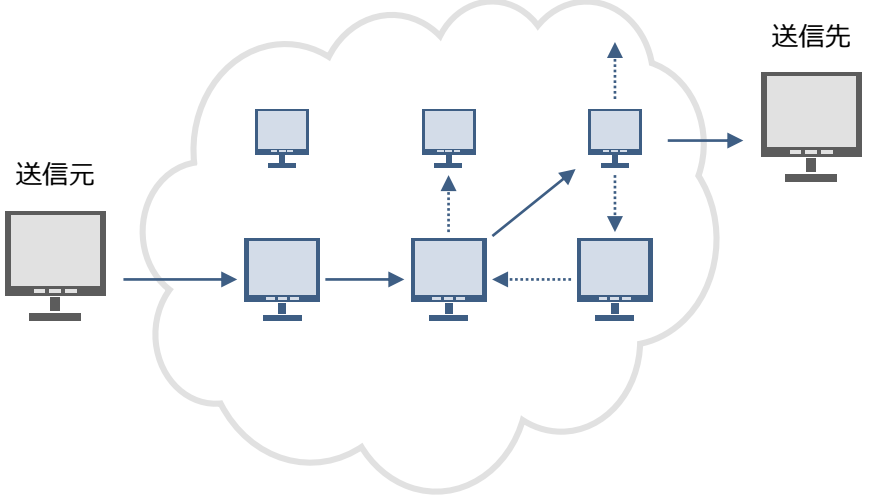
伝送経路は事前に確定



ホップバイホップ方式のイメージ

送信元は全体の伝送経路は決定せず、各中継ノードにIPパケットが到達した時点で、各中継ノードが次の転送先を決定する。
ノード情報を集中して管理する主体が存在しないため、規制対象先は曖昧となる。

伝送経路は事前には未定
（試行を繰り返しながら転送される）



3.3.1.2 匿名通信技術の分類－一覧表

以降の項で各プロジェクトについて記載する。

匿名通信技術の一覧表

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。

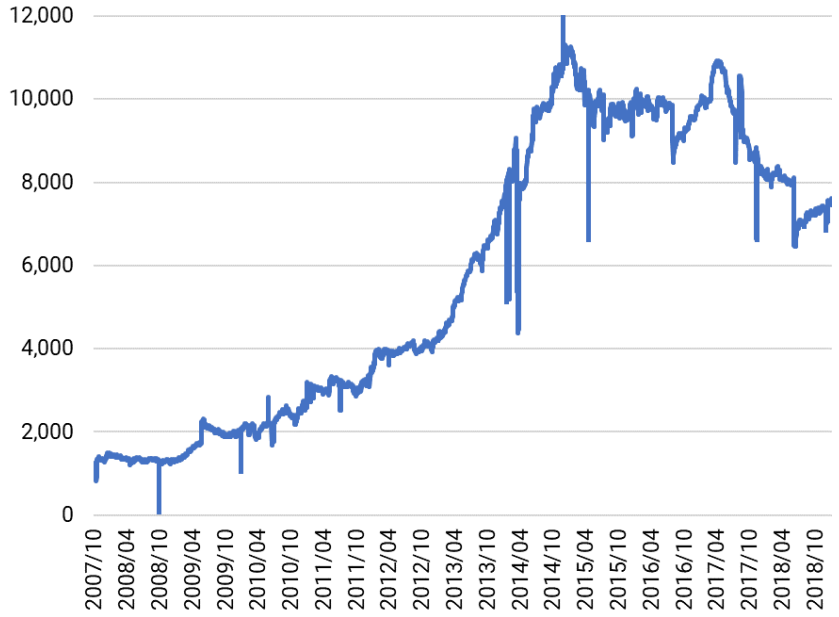
3.3.1.3 主要な匿名通信技術－Tor（The Onion Router）

最も著名な匿名通信ツールであり、Webブラウジング等の利用を念頭に、通信遅延を抑えた匿名通信の実現を図っている。

スマートフォンなどからも容易に利用でき、足元のユーザ数は約200万超、中継ノード数は約7,500前後と見積もられている（うち、出口ノードは約1,150）。

Torユーザ数の推移

Tor中継ノード数の推移



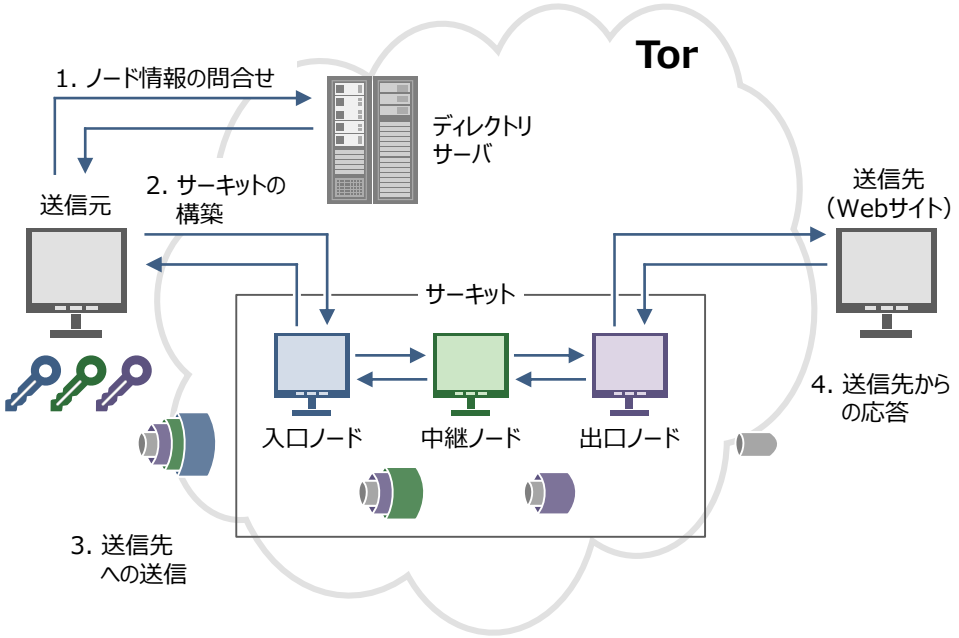
（左・右）The Tor Project, The Tor Project, Inc., "Tor Metrics", https://metrics.torproject.org/, 2019/2/4より三菱総研作成
なお、2013年央のユーザ数急増はボットネットによるとの指摘がなされている。Hopper, N., University of Minnesota, "Challenges in protecting Tor hidden services from botnet abuse", https://www-users.cs.umn.edu/~hoppernj/fc14-botnet.pdf, 2019/2/18

3.3.1.3 主要な匿名通信技術－Tor－通常のWebサイトとの間

送信元からの通信を、複数のノード（入口ノード・中継ノード・出口ノードの三種類）を経由させ、各ノードは自身の前後のノードしか分からないようにすることで「全体の伝送経路」の隠蔽を行う。通信内容の隠蔽にはSSLなど別途の対応が必要。

※ 送信先のIPアドレスは公開されているという前提。

Torの処理フロー



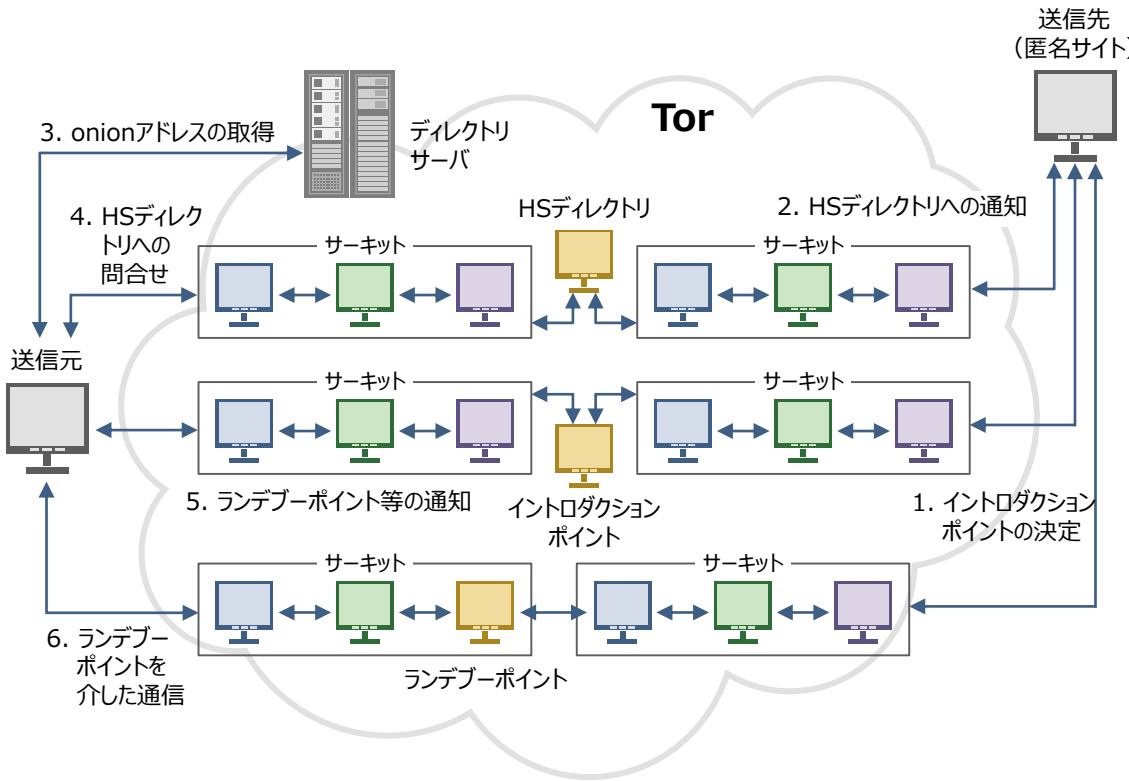
1. 送信元は、全てのノード情報を管理しているディレクトリサーバ（現時点で計10個）から中継ノードに関する情報（IPアドレスや公開鍵等）を取得する。
2. 送信元は、利用するノードを決定し、それらとの間に双方向の通信経路（サーキット）を構築する。具体的には、ディフィー・ヘルマン鍵共有により、お互いに自身の秘密鍵と相手の公開鍵を組合せて共通鍵を作成する。匿名性を高めるよう、サーキットは10分毎に再構築される。
3. 送信元は入口ノードへデータを送信する。入口ノードは受け取ったデータを、送信元との共通鍵で復号化し、次の中継ノードへ転送する。転送が繰り返され、最終的に出口ノードから送信先へデータが転送される。
4. 送信先は応答データを出口ノードに送信する。同じサーキットを経由して送信元へ応答データが転送され、転送の度に共通鍵で暗号化される。

SSL/TLSなどで通信内容を暗号化しない場合、出口ノードは通信内容を把握可能である点に留意が必要である。

3.3.1.3 主要な匿名通信技術－Tor－秘匿サイトとの間

送信元に加え、送信先のIPアドレスも隠蔽する仕組み（秘匿サービス）がTorにはあり、これを利用したサイトは一般にダークウェブと呼ばれる。サーバアドレスの指定には、独自のURL（http://***.onion）が用いられる

Tor秘匿サービスの処理フロー



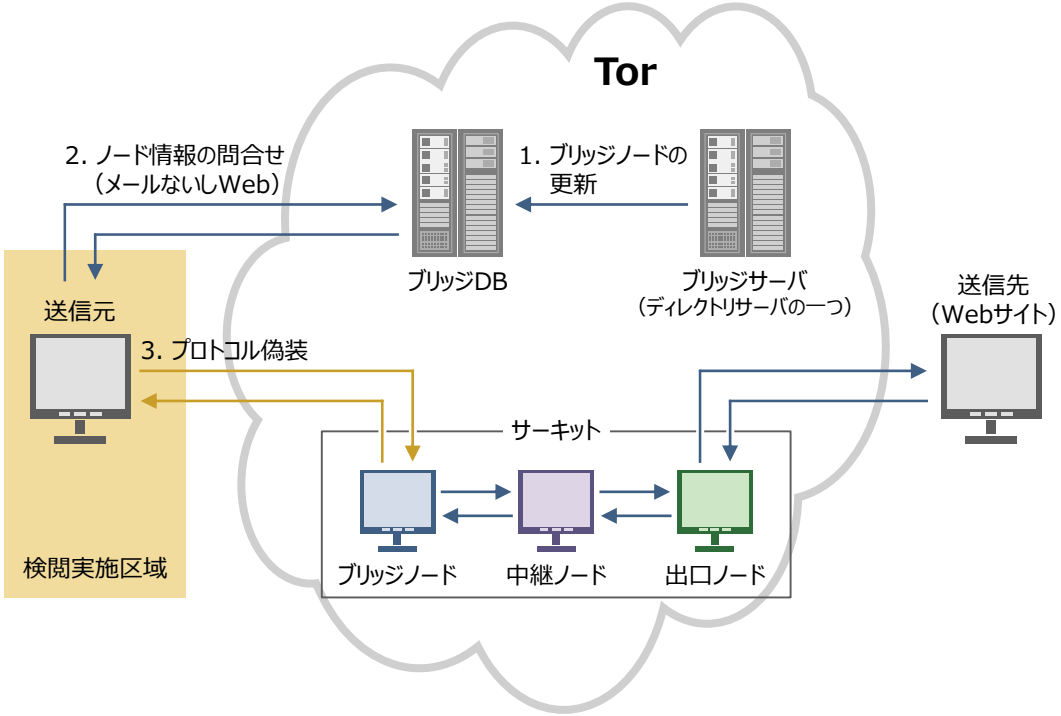
1. ダークウェブ上の匿名サイトは自身の窓口となるノード（イントロダクションポイント）を3つ選び通知する。ここで、以降も含めて、通信は全てサーキットを介して行われる。
2. 匿名サイトはイントロダクションポイントをまとめた情報（HS descriptor）を6つのノード（HSディレクトリ）に通知する。
3. 匿名サイトの公開鍵のハッシュ値の前半半分をBase32形式に変換したものがonionアドレスとなり、SNSやブログ等を介して送信元に伝えられる。
4. 送信元はディレクトリサーバからHSディレクトリの一覧を得て、onionアドレスに対応するHSディレクトリからHS descriptorを取得する。
5. 送信元はランダムにランデブーポイントを決定し、イントロダクションポイントを介して、ランデブーポイント等を匿名サイトに通知する。
6. 送信元と匿名サイトはランデブーポイントを介して通信を行う。

6.において、送信元・匿名サイトともにサーキットを用いることで、自身のIPアドレスを隠蔽して通信が行える。また6.の全ての経路上でデータは暗号化されている。

3.3.1.3 主要な匿名通信技術－Tor－プロトコル偽装による検閲耐性

政府等によるIP制限がある場合は、IPアドレスが非公開のブリッジノードを介して接続することができる（入口・中継・出口ノードはIPアドレスが公開されているため、IP制限の対象となる可能性）。ここで、送信元からブリッジノードまでの接続を、通常の通信のように見せかけるプロトコル偽装を行うことで、パケット内容の検査を行うディープ・パケット・インスペクションが実施されても、検知されないようにしている。

Torブリッジモードの処理フロー



1. 入口ノードの代わりにブリッジノードが使われる。ブリッジノードは自分自身の情報を暗号化してブリッジサーバへ送り、ブリッジサーバは集めたブリッジノードの情報を定期的にブリッジDBに格納する。

2. 送信元は、HTTPSのWebサイトないしメールでブリッジDBにブリッジノードを問合せ、3つほどを取得する（ブリッジノードを全て把握されないように、一度に僅かしか取得できない）。

3. 送信元は、プロトコル偽装して、ブリッジノードへ接続する。プロトコルの偽装方法は、通常のTLS接続やランダムノイズのように振る舞うなど数パターンあり、検閲体制に応じて変更することができる。通常の接続と見分けがつかないため、検閲側はTorの接続と認識することが難しい。

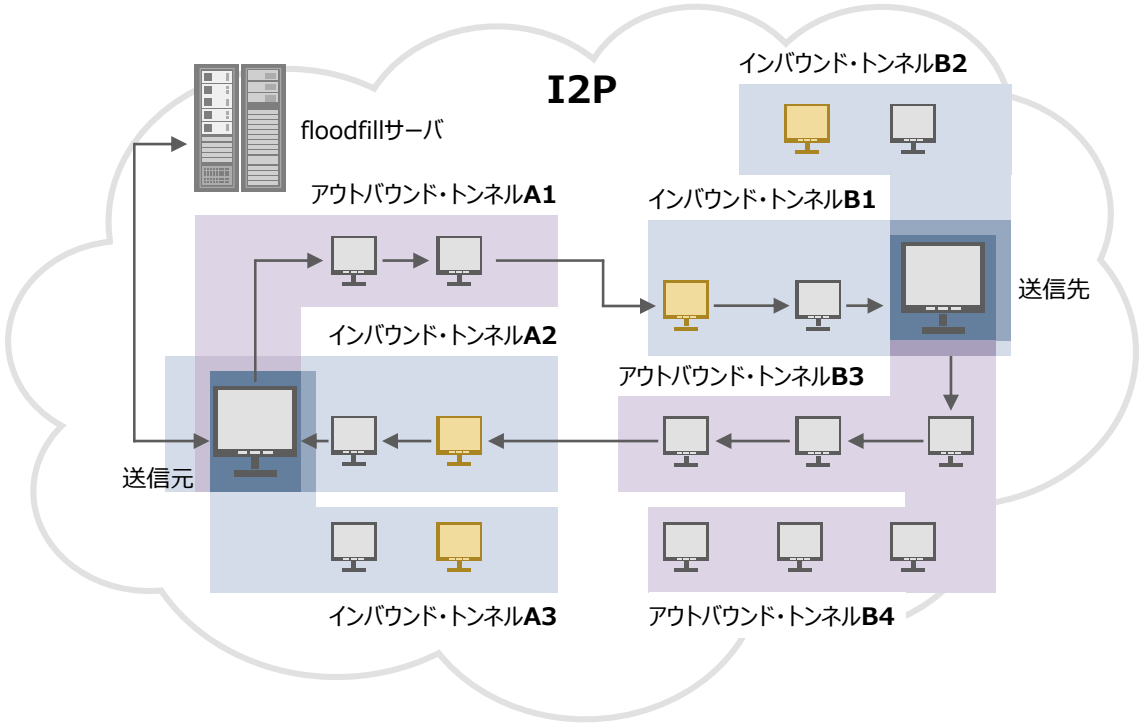
4. ブリッジノード以降は、通常のTorの接続と同様に、サーキットを介して送信先とやり取りする。

送信元とTorの入り口となるブリッジノードの間はプロトコル偽装されてやり取りする点がポイントとなる。しかし、ブリッジノードのIPアドレスが露呈される脆弱性なども指摘されており、学術的な意味での安全性の検証はまだ途上と考えられる。

3.3.1.3 主要な匿名通信技術－I2P（Invisible Internet Project）

独自のネットワーク内で閉じた匿名通信の実現を図っており、通常のWebサイトのブラウジング用途では通信遅延が大きい。ノード情報が分散して管理される、一方向で通信される、中継ノードの種別がない、複数のメッセージがまとめて暗号化されるなどの違いが存在するが、基本的にはTor類似と整理される。

I2Pの処理フロー



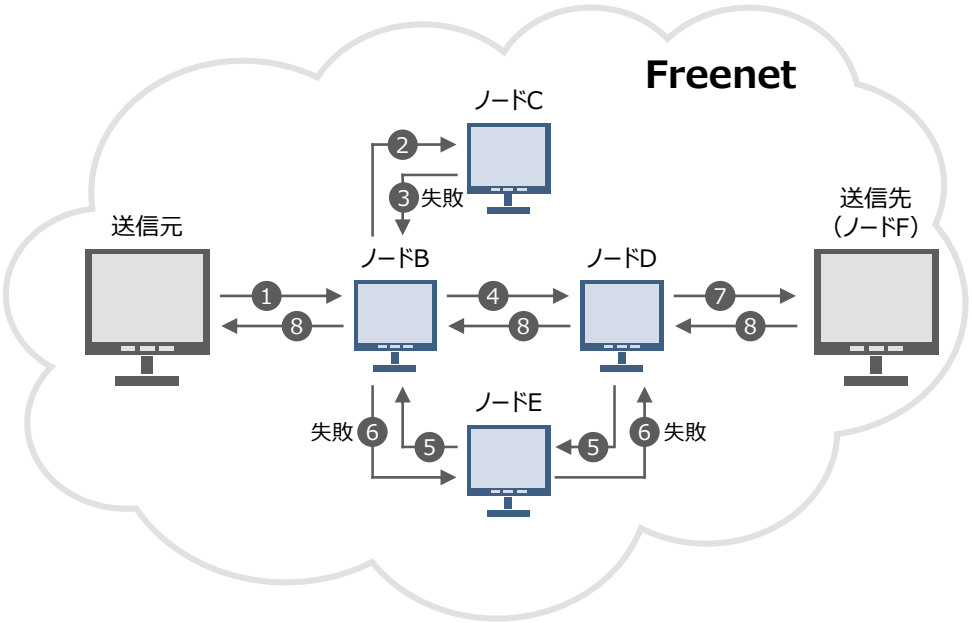
1. 送信元、送信先ともに、送受信用の通信路（トンネル）を複数用意する。トンネル構築にあたっては、Torと同様に、各中継ノードや送信先との間で共通鍵を作成する。匿名性を高めるよう、トンネルは10分毎に再構築される。
2. 送信元は、全てのノード情報を分散して管理しているfloodfillサーバから、送信先のインバウンド・トンネル（図のB1）のゲートウェイ情報（図の黄色ノード）を取得する。
3. 送信先は自身のアウトバウンド・トンネル（図のA1）を通して、送信先のインバウンド・トンネル（図のB1）のゲートウェイ（図の黄ノード）に送信する。ゲートウェイは終端となる送信先までデータを転送する。
4. 送信先は応答メッセージを自身のアウトバウンド・トンネル（図のB3）を通して、送信元のインバウンド・トンネル（図のA2）のゲートウェイ（図の黄色ノード）に送信し、データは送信元まで転送される。

ここで、全ての経路上でデータは暗号化されている。

3.3.1.3 主要な匿名通信技術－Freenet

独自のネットワーク内で閉じた匿名情報共有（匿名でのファイル共有や掲示板など）の実現を図っている。ノード情報の管理主体が存在しないホップバイホップ形式であるため、通信遅延は大きい。また、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ため、元の発信者がオフラインとなっても、当該データはFreenet上に残る。

Freenetの処理フロー



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。

ノード数の増加とともに通信遅延（すなわち、経由するノード数）は指数関数的に増加すると見積もられているが、実際のネットワークでは十分に確認されていない。

3.3.1.4 匿名通信の課題と方向性 – 匿名性について

現在までに匿名通信に関するプロトコルレベルでの致命的な脆弱性は報告されていないが、今後は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重要な課題になっていくと考えられる。

匿名通信の課題と方向性

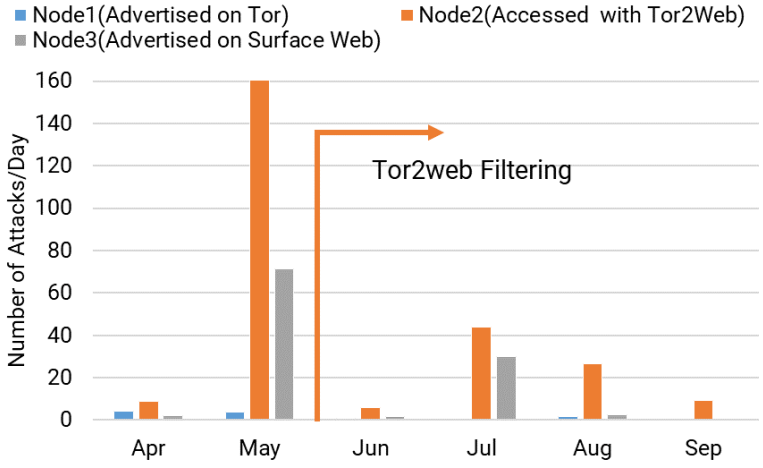
課題	内容
他アプリケーションと組み合わせることによる脆弱性	• 特にTorはプロキシサーバとして機能し他のアプリケーションと併用することが容易であるが、例えばビットコインとTorを併用する場合に、匿名性を大幅に低下させる攻撃手法などが提案されている。 • アプリケーションを組み合わせて使用することで、単体では生じなかった新たな脆弱性や技術的課題が生じる危険性がある。
匿名セットのサイズと質のトレードオフ	• 匿名化には、偽装するための他者（匿名セット）を十分な数確保することが望ましい。 • その一方で、利用者が増えると、通信性能の低下や、初心者の脆弱な設定による匿名性の低下等が生じ得る。
単一信頼点・単一障害点の存在	• 例えば、TorやI2Pなどではノード情報を管理する主体（ディレクトリサーバ等）が存在し、これが正しく応答するという信頼を置いている。中継ノードにも、転送を正しく行うという信頼を置いている。 • そのため、こうした単一信頼点は匿名通信を妨害する攻撃のターゲットとなり得る。例えばTorではディレクトリサーバの過半数を管理下に置き、不正なノード情報を送信元に返すことで、Torを用いた通信を妨害することが可能になると指摘されている。
その他の脆弱性	• 例えば、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、データの伝送経路や送信者と受信者のつながりを特定する方法（タイミング攻撃）などが提案されている。この点については匿名通信側で特に改善が取り組まれている。

3.3.1.4 匿名通信の課題と方向性 – 裾野の拡大について

匿名通信ツールが容易に利用可能になりつつある一方で、ダークウェブ利用者へのフィッシング詐欺やダークウェブ内での抗争も激化しつつあり、今後もこの傾向は続くことが考えられる。

ダークウェブサイトへの攻撃

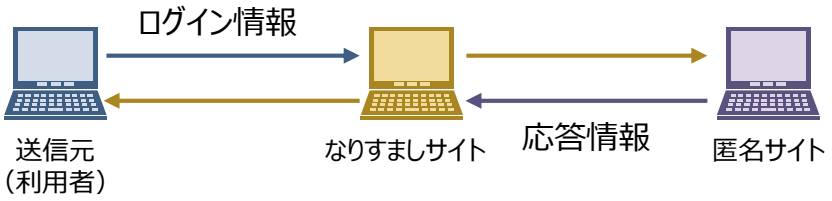
ダークウェブのダミーサイト（マーケットプレイスやブログサイト）に対する攻撃は最大で170回/日に上った。通常のブラウザでもダークウェブへの接続が可能となるTor2web経由で攻撃する場合が多かったが、それらをフィルタリングした後も、サイト改竄等の攻撃は続いた。
こうしたことから、サイバー攻撃者はライバル組織のサイトを相当な労力をかけて手動で探索しては攻撃・妨害していると考えられる。



ダークウェブ利用者を対象としたフィッシング詐欺

例えば Tor はスマートフォンからも容易にアクセス可能。

匿名サイトは、自身の身元を明かしたくないため、一般にルート認証局から証明書を得ることなどはしない。すなわち、利用者は匿名サイトの真正性を判断できないため、フィッシング詐欺に気づくのが困難となる。



（左）Catakoglu, O., et al, madlab.it, "Attacks Landscape in the Dark Side of the Web", http://www.madlab.it/papers/sac17_darknets.pdf, 2019/1/30より三菱総研作成
（右上） Guardian Project, guardianproject.info, "Orbot: Tor for Android", https://guardianproject.info/wp-content/uploads/2010/02/featuregraphic.png, 2018/12/14

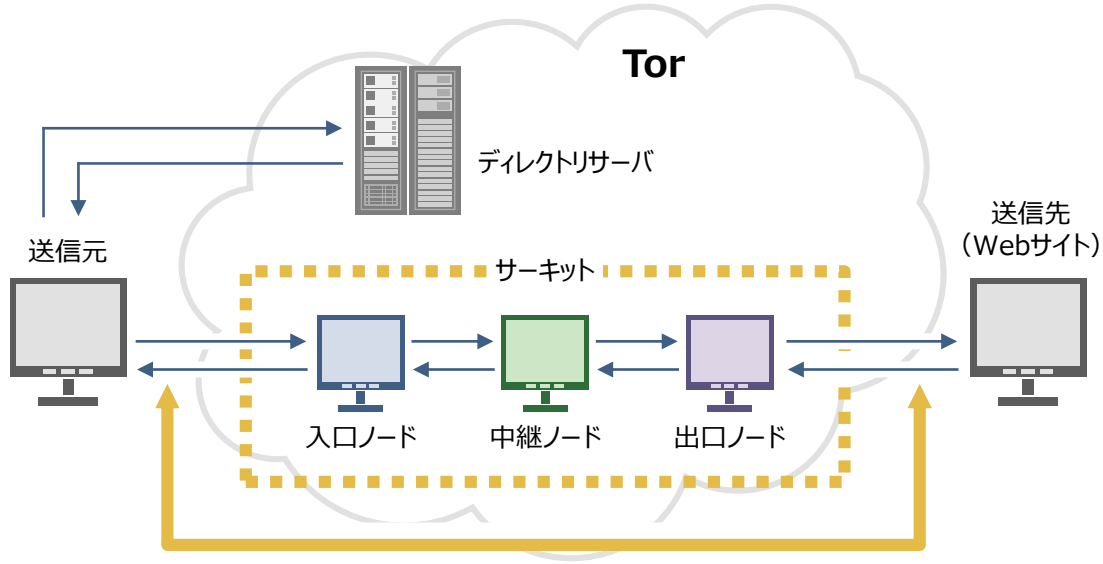
3.3.2 P2Pレイヤー/インターネットレイヤーの再識別技術

3.3.2 P2Pレイヤー/インターネットレイヤーの再識別技術

全体の伝送経路の特定には、ネットワークのトラフィックパターン分析や、用意した中継ノード・出口ノードから情報収集して推測する手法が提案されている。ただし、いずれもあくまで確率的な推測に留まる。

匿名通信上の伝送経路の再識別イメージ

特にTorの場合、通信遅延を小さくするため、送信元のデータのタイミングと、送信先のデータのタイミングは近い可能性が高い。そのため、候補となる経路上のトラフィックパターンの類似度等から推測することが可能とされる。



トラフィックパターンの類似度による推測

3.4 実世界レイヤー

3.4.1 実世界レイヤーの匿名化技術
3.4.2 実世界レイヤーの再識別技術

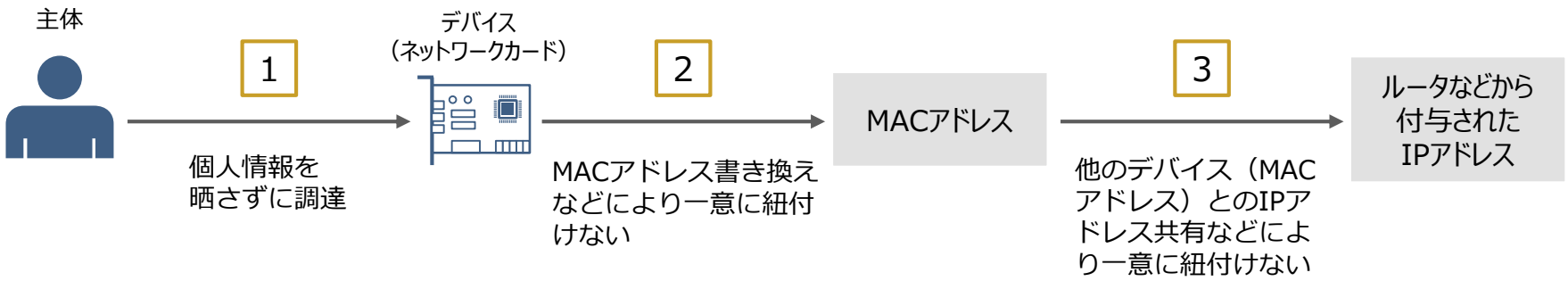
3.4.1 実世界レイヤーの匿名化技術

3.4.1 実世界レイヤーの匿名化技術－匿名化の考え方

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（ネットワークカード）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。

- 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、MACアドレスを書き換えるなど、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、他とIPアドレスを共有するなど、 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。

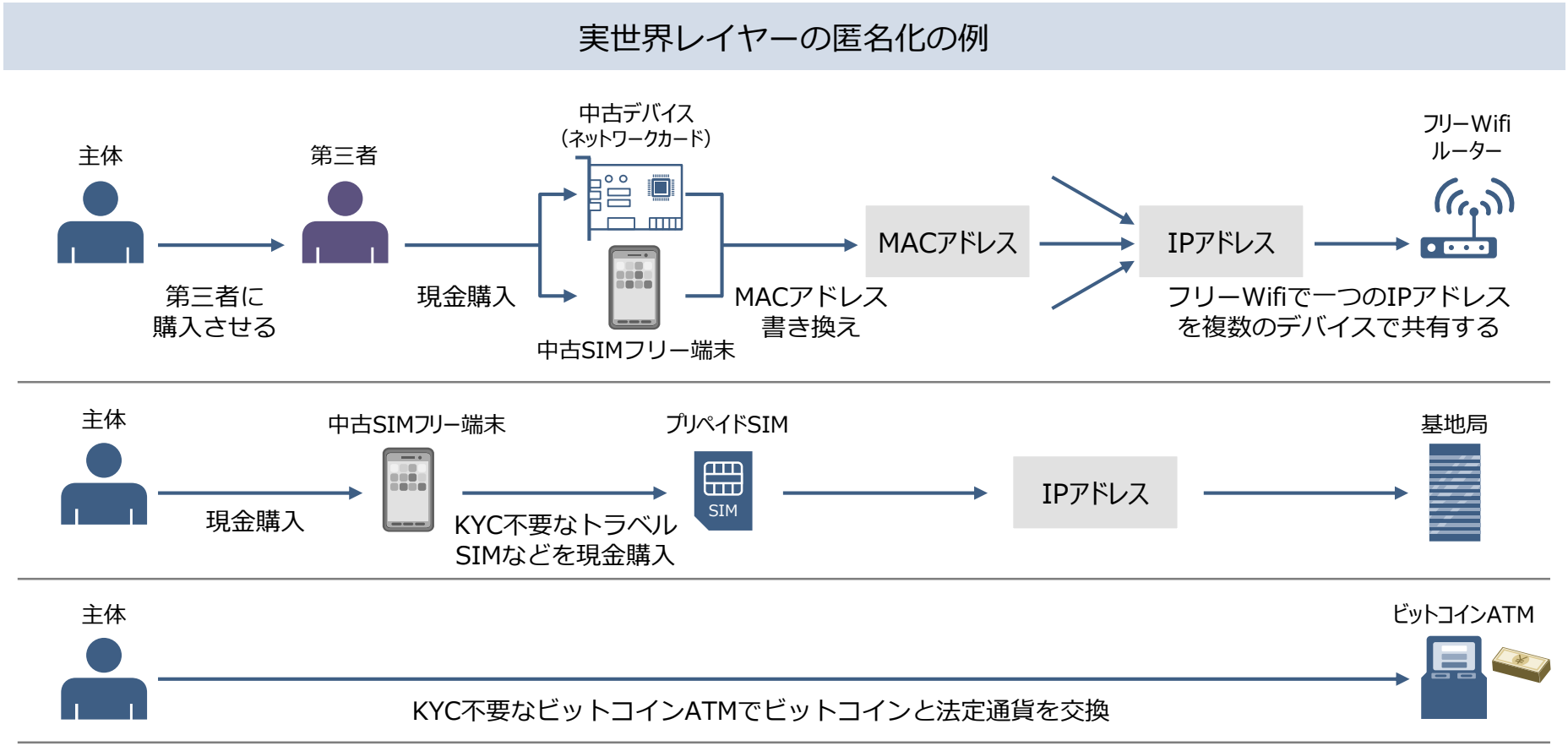
実世界レイヤーにおける匿名化のポイント



※ 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。

3.4.1 実世界レイヤーの匿名化技術

端末調達は中古端末購入（デバイス受取は第三者に依頼）や窃盗で行い、MACアドレスを書き換えた後に、（1）フリーWifiで接続する方法、（2）KYC情報なしに利用可能なプリペイドSIMを利用する方法、（3）KYC確認を行わないビットコインATMを利用する方法などが考えられる。



3.4.2 実世界レイヤーの再識別技術

3.4.2 実世界レイヤーの再識別技術

大きく（1）IPアドレスからログデータを用いて特定していく方法と（2）IPアドレスからレジストリデータを用いて主体を特定する方法がある。どちらもログ情報・購買履歴やレジストリデータ等のデータの質と量に大きく依存するが、一定期間後に廃棄される場合やレジストリデータの精度が悪い場合も多く、困難が見込まれる。

実世界レイヤーの再識別の例

1 ログデータから特定する方法

犯行時刻と近い時期のログが必要だが、一定期間後に廃棄されている可能性がある。

2 レジストリデータから特定する方法

レジストリの登録データに抜け漏れがある場合や更新されていない場合がある。

4 実証実験

4.1 実証実験シナリオの一覧
4.2 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
4.3 ミキシングサービスを用いたクリプトロンダリング
4.4 リスクスコアリングツールによる評価

本章の要旨

- 本実証実験では、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クリプトロンダリング、（2）ミキシングサービスを用いたクリプトロンダリング、（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。
- （1）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。
- （2）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。また、ミキシングサービス事業者は、相当程度の規模の暗号資産を扱っている可能性があることが分かった。
- （3）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。

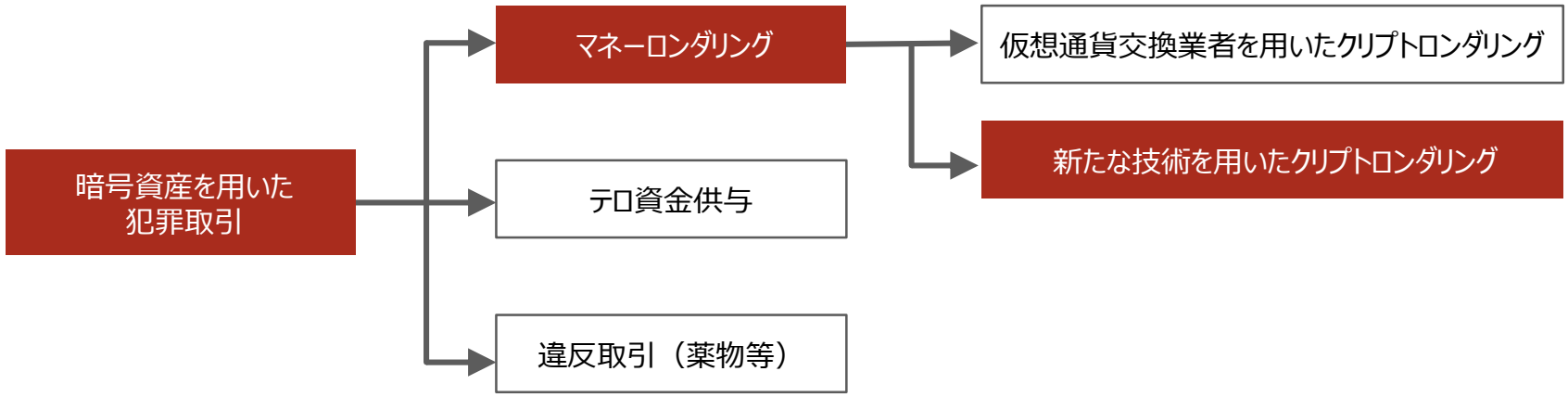
4.1 実証実験シナリオの一覧

本実証実験の目的は、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である。

現在までに我が国の犯罪取引の大半を占めるマネーロンダリングを検討対象とし、具体的には、犯罪収益として得た暗号資産を資金洗浄する場合を考えた。

実証実験の対象の考え方

暗号資産の犯罪取引としては、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と考えられるが、本調査実験では我が国の犯罪取引の大半を占めるマネーロンダリングを検討対象とした。



4.1 実証実験シナリオの一覧

専門家等の意見を踏まえ、以下の実証実験を行った。

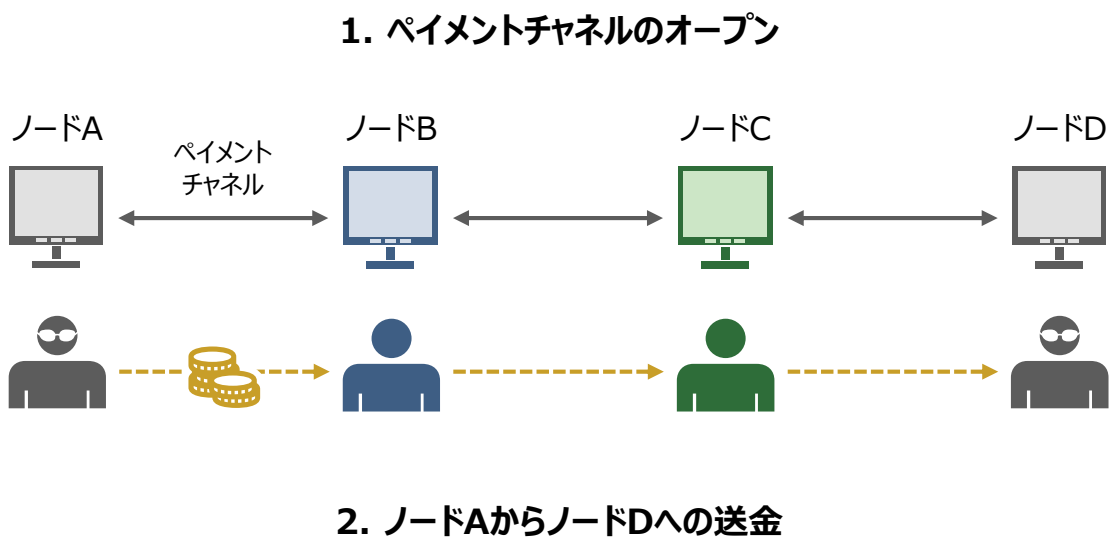
実証実験シナリオの一覧

No	名称	実験内容	検証内容
1	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	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。	• ブロックチェーン上のデータに基づく追跡の度合い → 追跡は困難 • ネットワーク上のパケットデータに基づく追跡の度合い → 追跡は困難
2	ミキシングサービスを用いたクリプトロンダリング	一般に利用可能なミキシングサービスを用いて送金する。	• 利便性の度合い → 使い方は平易で容易に利用可能 • ブロックチェーン上のデータに基づく追跡の度合い → 追跡は困難（ミキシングサービスが使われたことを特定することも困難と推測される）
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、実際のビットコインのアドレスを評価する。	• リスクの妥当性の度合い → リスク評価の結果は必ずしも適切でない • ミキシングサービス利用有無の特定の度合い → ミキシングサービスが使われたことを特定できないツールが大半を占めた

4.2 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 – 概要

本実験では、ビットコインのネットワーク（テストネット）を用いて、犯罪収益と見立てたビットコインを、ライトニングネットワーク上の2台のノードを経由して移転した。なお、ライトニングネットワークは4種類を用いた。追跡可能性の評価にあたっては、（1）ブロックチェーン上のデータから移転経路が分かるか、（2）ネットワーク上のパケットデータから移転経路が分かるかの二点を評価した。

ライトニングネットワークを用いた中継送金のイメージ



取引所などから窃取されたビットコインが、ノードAの保有するアドレスに既に移転されているとする。そして、犯行者はライトニングネットワークを用いて、中継ノードBおよびCを経由して、自身の保有する別のノード（ノードD）のアドレスへ送金する場合を考える。

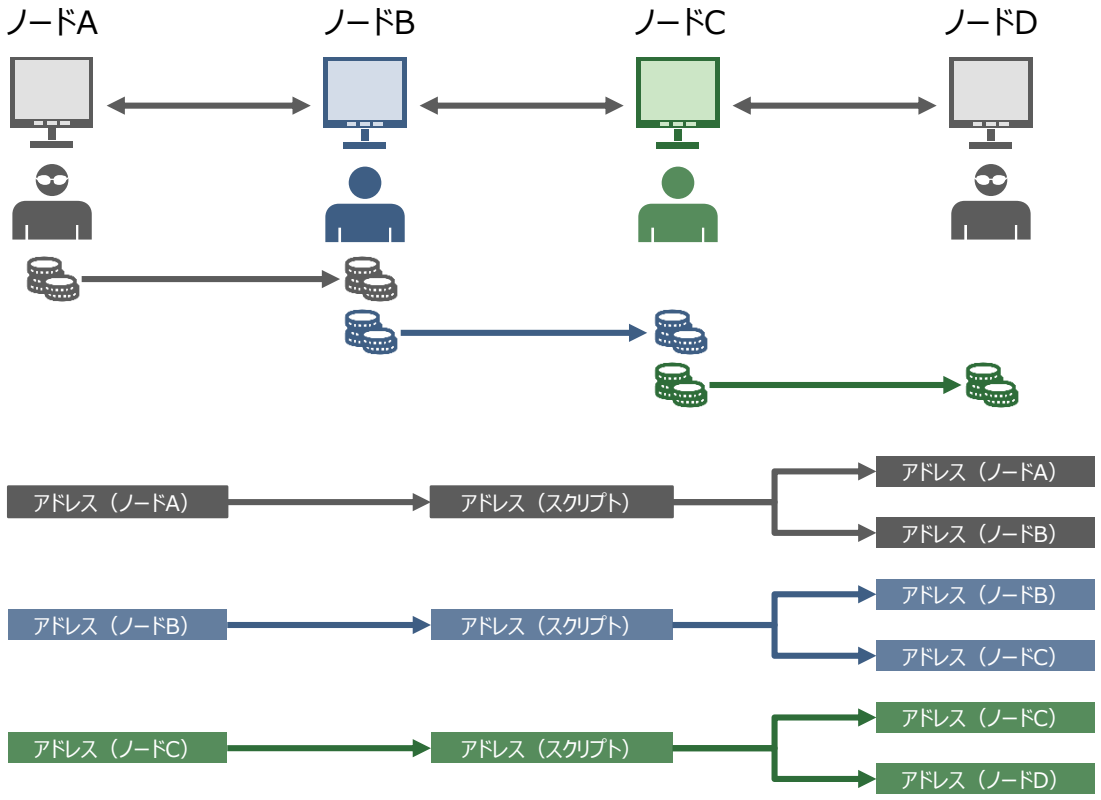
1. 犯行者はノードA・B間、ノードC・D間のペイメントチャネルを開く（ノードB・C間のペイメントチャネルは既に開かれているとする）。
2. 犯行者はノードA→B→C→Dという移転経路を決定した上で、ノードAからビットコインを送金する。

※ライトニングネットワーク基盤として、c-lightning、LND、eclair、ptarmiganの4種類を用いた。

4.2 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－ブロックチェーン上のデータ

中継送金には異なるビットコインが使われるため、第三者がブロックチェーン上のデータから全体の移転経路を把握することはできない。

ブロックチェーン上のデータから把握できる移転経路
（上：中継送金の仕組み、下：ブロックチェーン上のデータのイメージ）



ライトニングネットワークを用いた中継送金は、中継ノードにビットコインを送金し、代わりに当該ノードが同額のビットコインを次のノードへ送金するという形で行われる。

そのため、ノードAが送金したビットコインと、ノードDが受け取ったビットコインの関係は第三者からは分からないことになる。

ブロックチェーンデータからは、ノードAのビットコイン（左上）は、最終的に2つのアドレスに分割されたこと（右上）しか分からない。

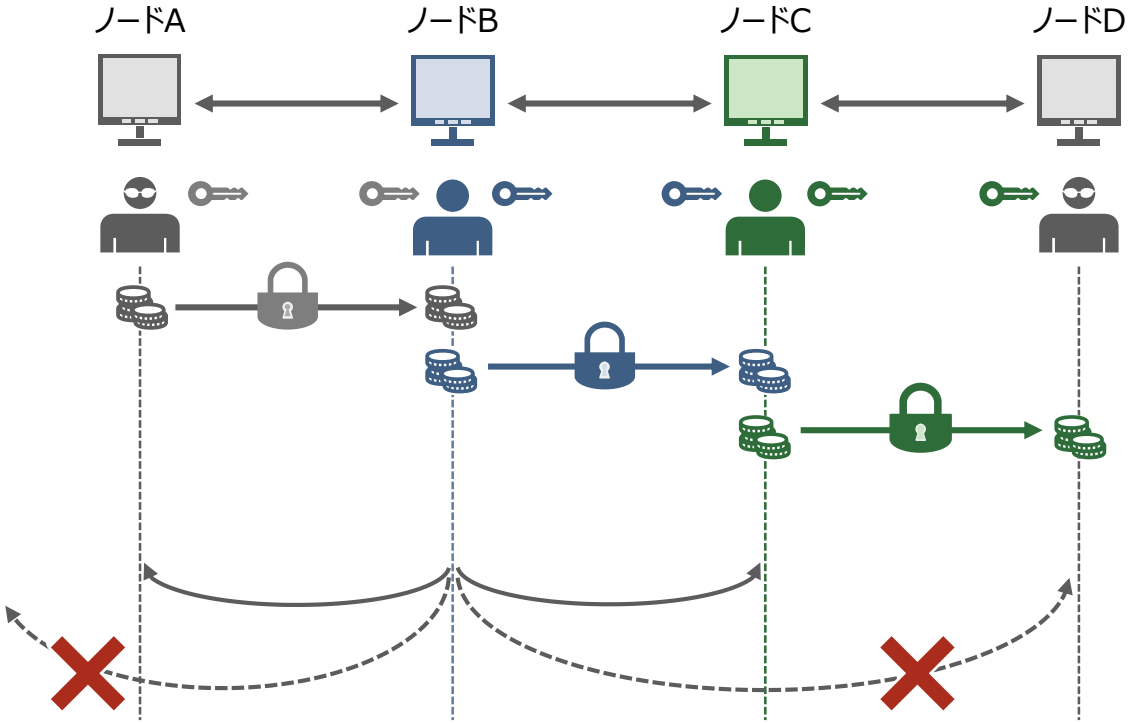
また、ノードAからの経路（黒）、ノードBからの経路（緑）、ノードCからの経路（茶）は、必ずしも時系列順に記録されない。

※本稿執筆時点の仕様では、取引当事者の片方のみがデポジットを行う。

4.2 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 – ネットワーク上のパケットデータ

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、第三者がその取引内容を把握することはできない。また、送金人以外は全体の経路を把握することはできない。

ネットワーク上のIPパケットから把握できる移転経路



ライトニングネットワークを用いた中継送金では、移転経路上のIPパケットは暗号化されており、当事者しか内容が分からない。

また、中継ノードは前後のノードしか分からないため、中継ノードBからみて、ノードDは分からず、またノードAは送金人のノードから中継ノードかは分からない。

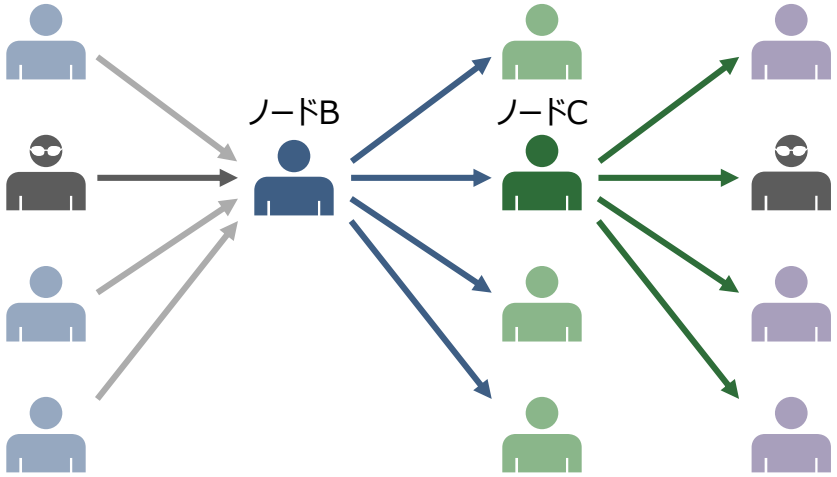
そのため、送金人以外は、送金元（ノードA）と送金先（ノードD）を含む、全体の経路を知ることはできない。

4.2 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 – 更なる匿名性の向上

犯行者は、経路長を長くすることや、ハブとなる中継ノードを経由することで、移転経路の匿名性を高めることができる。また、自身が中継ノードになって資金洗浄を図ることもできる。今後、スクリプトレススクリプトやMulti-Hop Locksが実用化されると、匿名性はさらに高まると考えられる。

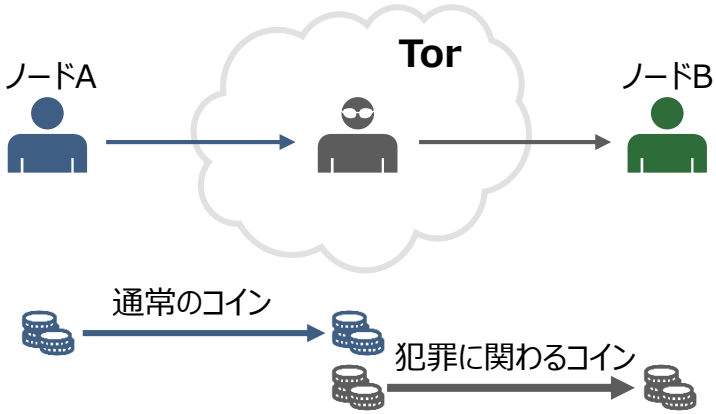
ハブとなる中継ノードを経由するイメージ

犯行者は、ハブとなる中継ノード（下図のノードBやノードC）を経由することで、自らの移転経路が特定される確率を下げることができる。経路長を長くすることでも、自らの移転経路が特定される確率を下げることができる。



自身が中継ノードとなるイメージ

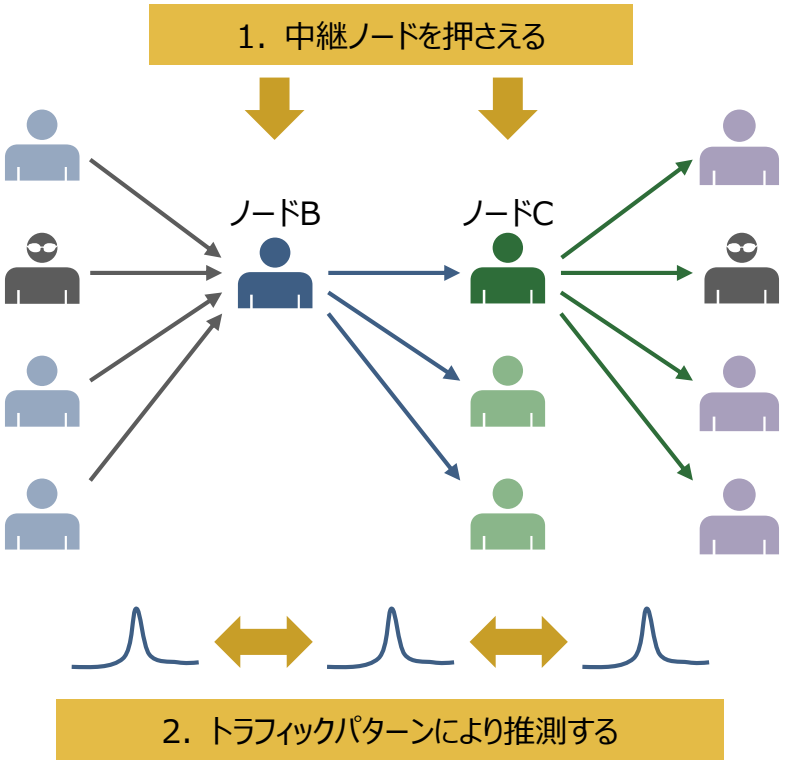
犯行者は中継ノードになることもできる。下図の場合、自身の犯罪収益をノードBへ送金し、代わりに同額の通常のコインをノードAから受けることで、資金洗浄を図ることができる。
ただし（1）送金元（ノードA）が通常のコインを保持している必要がある、（2）犯行者は自身の身元を隠すためTor秘匿サービスなどを併用することが望ましい、（3）犯行者はハブとなることが望ましい、など、実利用にあたってのハードルは複数存在する。



4.2 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 – 再識別

再識別にあたっては、全ての中継ノードを押さえることなどが考えられるが、ライトニングネットワークを用いた中継送金は匿名性が極めて高いため、中継ノードに対する規制上の位置付けは今後明確化されていく必要があると考えられる。

ライトニングネットワークの中継送金に対する再識別のイメージ



全ての中継ノードの取引データを確認して全体の移転経路を把握する場合、中継ノードが取引データやその復号鍵を廃棄していると移転経路を把握することができない。

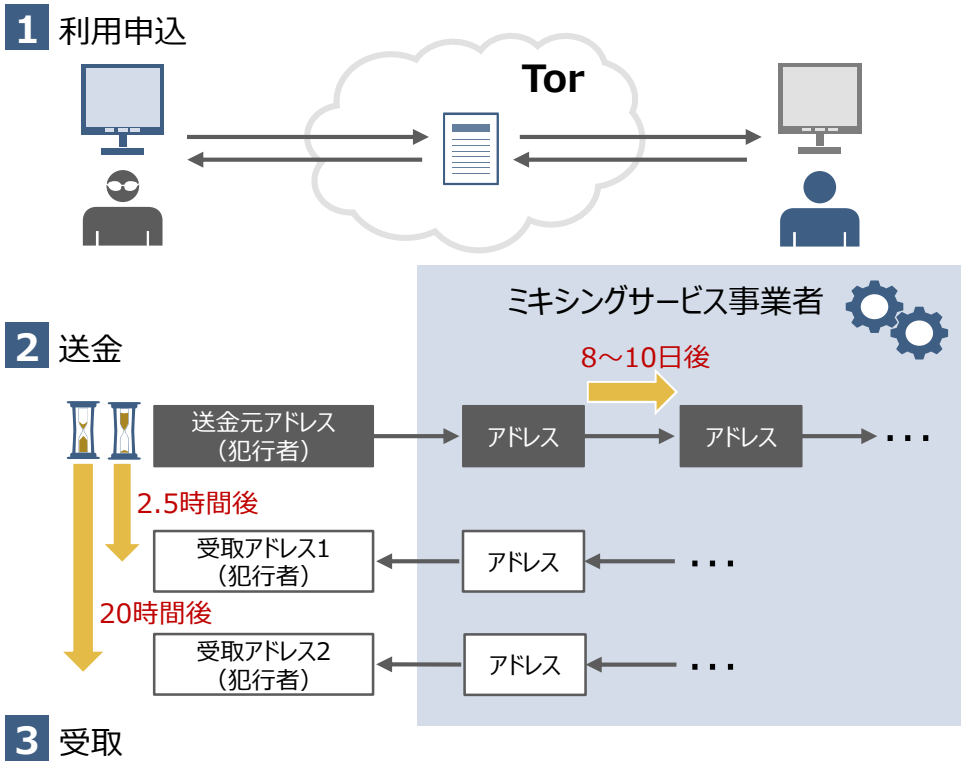
そのため、中継ノードの運営主体が資金移動業者（Money Transmitter）など規制監督上の対象に該当するかについて、今後明確化されるのが望ましいと考えられる。

※なお、中継ノードの経済的インセンティブを考えると、その普及の速度は予測が難しい。例えば、中継ノードは、相手毎にデポジットが必要となり（初期コスト）、デポジットしたコインを他へ転用することもできない（機会コスト）。中継送金毎の手数料が収入の場合、こうしたコストを賄いきれない可能性がある。

4.3 ミキシングサービスを用いたクリプトロンダリング – 概要

本実験では、一般に利用可能な２つのビットコインのミキシングサービスを用いて、資金洗浄がどのように行われるかを確認した。使い方は平易で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極めて困難であることが分かった。

ミキシングサービスの利用イメージ



犯行者がミキシングサービスを用いて資金洗浄を行う場合を考える。

1. 犯行者は、ダークウェブ上のミキシングサービス事業者のホームページから、利用申込を行う。受取先のアドレスや受取時刻を設定すると、ミキシングサービス事業者のアドレスが表示される。
2. 犯行者がミキシングサービス事業者のアドレスへ送金する。
3. 指定時間後に全く別なアドレスから返金が行われる。

送金元のビットコインとは異なる経路からビットコインを受け取るため、送金したビットコインと受け取ったビットコインの関係は第三者からは分からないことになる。

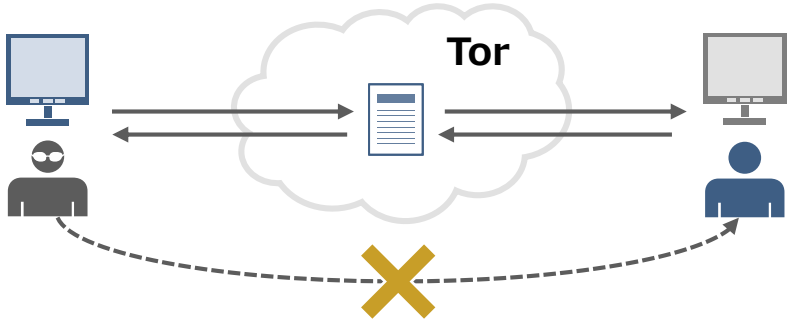
また、受取アドレスは複数指定可能であり、各々時間差も指定できるため、第三者がそれら受取アドレス群を紐付けることは困難と考えられる。

ビットコインのアドレスは無限に作成できるため、こうしたミキシングサービス事業者のアドレスを特定したり、ミキシングサービスが行われたことを特定するのも一般には困難と考えられる。

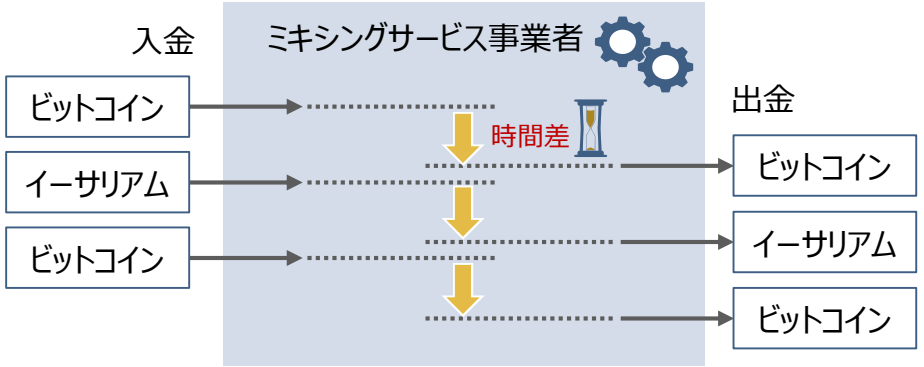
4.3 ミキシングサービスを用いたクリプトロンダリング – 他の論点

ダークウェブ等が用いられているため、ミキシングサービス事業者の所在地の特定は困難であると考えられる。なお、ミキシングサービス事業者の手数料収入は1-3%程度であるが、それ以外のビジネスなども行える可能性があると考えられる。

ミキシングサービスの特徴



ミキシングサービス事業者がTorの秘匿サービスなどを用いている場合、その所在地や運営主体を把握することは困難である。



ミキシングサービス事業者は相当程度の規模の暗号資産を動かしていると推測される。入出金の間の時間差から生じる残高などを運用している可能性が考えられる。

また、ビットコインやイーサリアムなど複数の暗号資産を扱う場合は、それらの資産変換などを行うこともできる。

こうしたことから、ミキシングサービス事業者は手数料以外のビジネスも行える可能性があると考えられる。

4.4 リスクスコアリングツールによる評価

本実験では、現在利用可能な複数のリスクスコアリングツールを用いて、実際のビットコインのアドレスのリスクを評価した。総じて、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。また、ミキシングサービスが使われたことを特定できないツールが大半を占めた。

リスクスコアリングによる評価のイメージ

No	Bitcoin Address	Risk Score			
		A	B	C	D
1	1F**********	■	■	■	■
2	3H**********		■	■	■
3	16**********		■	■	■
4	1N**********	■		■	■
5	14**********			■	■
6	bc**********		■	■	■
7	17**********			■	■
8	3D**********			■	■
9	34**********			■	■

実際にミキシングサービスを用いたアドレスや取引所のアドレスなどについて、複数のツールでリスク評価を行ったが、その評価は分かれた。

- 全般にリスクを低く評価しすぎるものが多かった。
- ミキシングサービスが使われていることを特定できたツールは限られていた。
- 犯罪に関連するアドレスからコインが移転された子アドレス・孫アドレスのリスクの評価は分かれた。アドレス間の関係を考慮しないと見受けられるツールも存在した。
- 取引件数が極めて多い取引所などのアドレスは、たとえ犯罪収益に関わる取引がその中にあったとしても、全体としてはリスクが薄まって評価された。犯行者は、このようなアドレスを経由することで、リスクを低く見せかけることが可能になると考えられる。

5 当局としての対応策

5.1 理論的考察及び実証実験を通じて把握された課題

5.2 課題への対応策

本章の要旨

- 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ない。その意味で極めて匿名性の高いクリプトロンダリングは既に可能であり、その技術的・心理的なハードルは低い。各種匿名化技術の進展は急速であり、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。
- 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、現時点では以下の方針が考えられる。
  - 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。
  - 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。

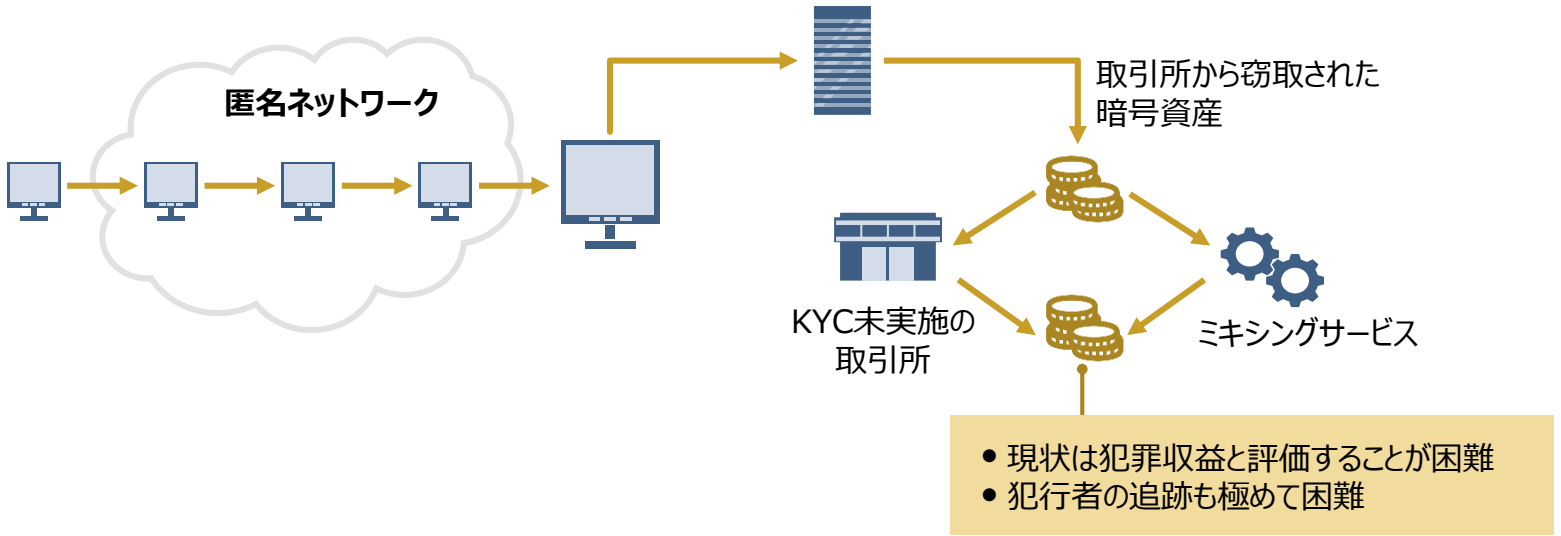
5.1 理論的考察及び実証実験を通じて把握された課題

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ない。その意味で極めて匿名性の高いクリプトロンダリングは既に可能であり、その技術的・心理的なハードルは低い。そのため、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。

- 現状は、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。
- 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。

事後的な再識別の技術的限界

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。



5.1 理論的考察及び実証実験を通じて把握された課題

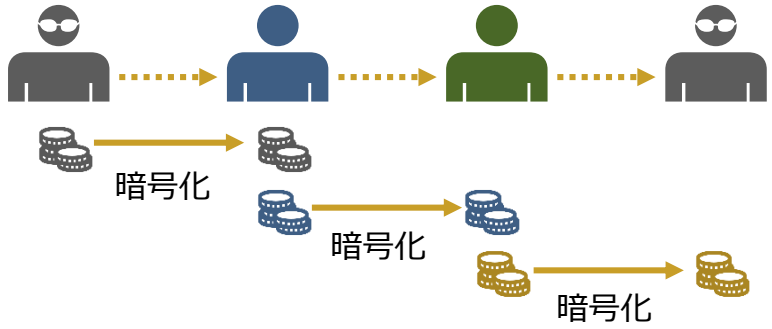
匿名化技術は、一部の暗号資産（モネロ、ジーキャッシュ等）だけでなく、ビットコインにおいても積極的に開発が進められている。そのため、匿名通貨等を規制するだけでは不十分となる懸念がある。

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。

ライトニングネットワークを用いた資金洗浄

例えば、ライトニングネットワークを用いた中継送金が行われると、ブロックチェーン上およびネットワークトラフィック上の情報からでは追跡できない。

ライトニングネットワークの中継送金

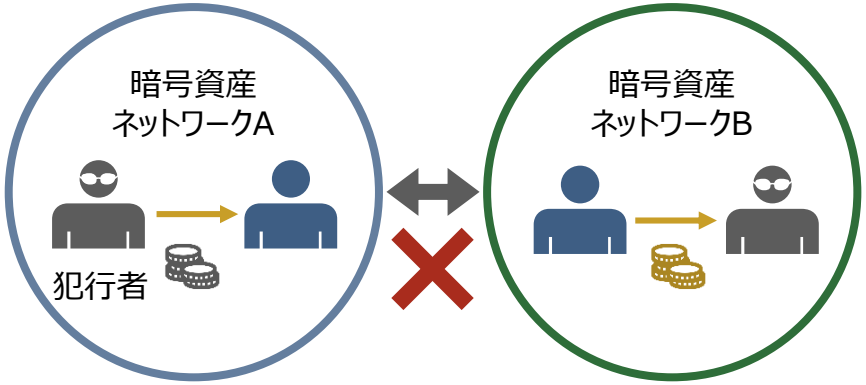


第三者が資産の流れを追うことは困難

新たな暗号資産交換手段による資金洗浄

DEXやアトミック・クロスチェーン・スワップなど、従来の取引所を介さずに暗号資産の交換を行う手段も実用化へ向けた取組が進んでいる。

アトミック・クロスチェーン・スワップ



第三者が二つの取引を紐付けることは困難

5.2 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。

暗号資産経済圏の代表的な特徴

暗号資産経済圏

グローバル性

一国の管轄権の及ばない海外を含めてやり取りされる。そのため、規制の適用やそのエンフォースメントを図れない懸念。

自律分散性

単一の管理主体は存在しない。サービスは、事業者、個人や主体が介在しないプログラムにより提供され、各々は自身の利得最大化に向けて行動する。そのため、明確な規制対象先が存在せず、また規制のエンフォースメントを徹底できない懸念。

開放性

技術開発やサービス提供にあたって参入障壁がない。そのため、種々のサービス提供主体が生じることで、規制対象先が膨大になる懸念やそれらが表に現れない懸念。

高可用性・改竄耐性

ネットワークを止めることや台帳を事後に変更できない。そのため、サービスを停止させる、プログラムを事後に修正するなどのエンフォースメントを図れない懸念。

トラストレス・仲介者排除

取引仲介者を排除して、取引当事者同士のみでやり取りを可能とする。そのため、取引の内容や存在を当局が検知できなくなる懸念。

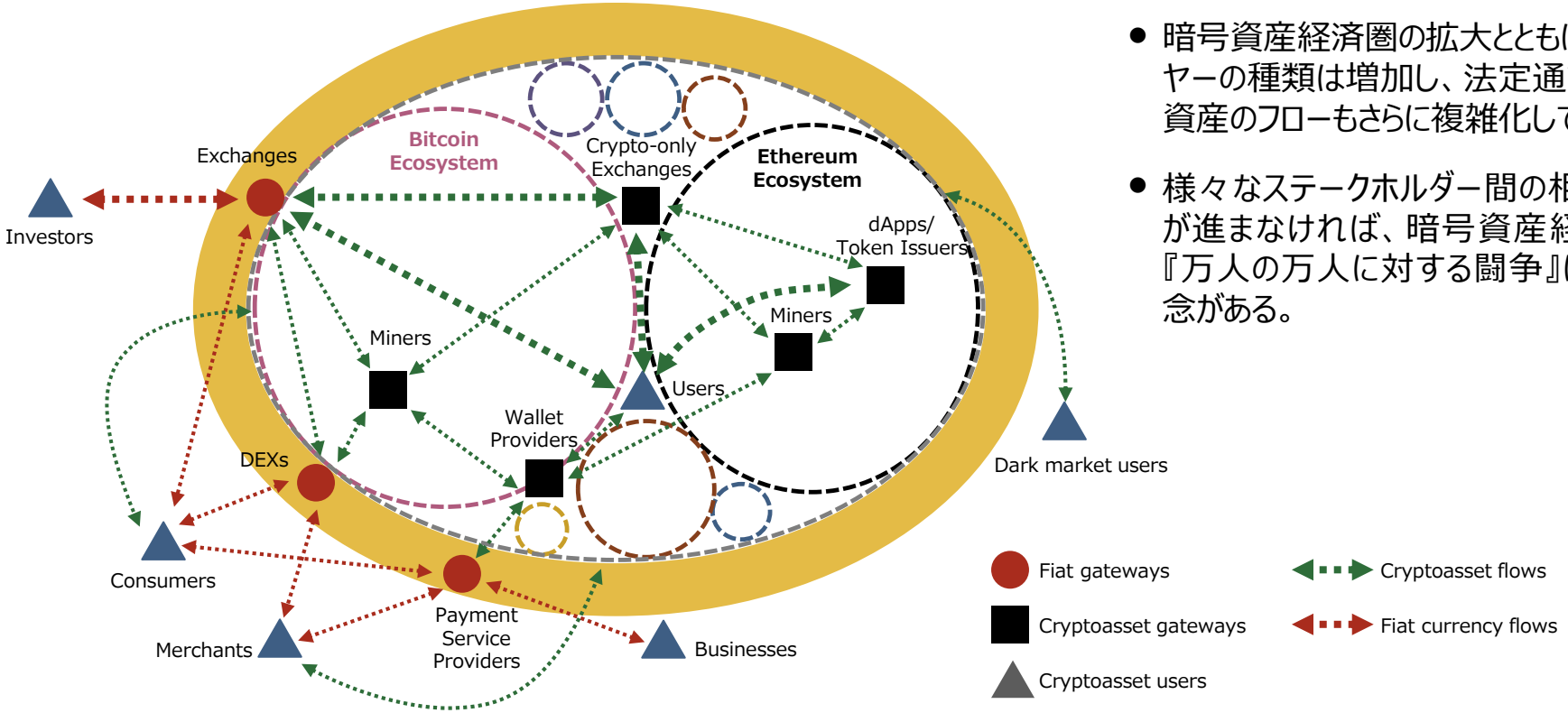
技術志向性

新たなサービスが技術進展と密接に関連している。そのため、規制やエンフォースメントをアップデートしていくのが困難になる懸念。

5.2 課題への対応策

前項までの内容を踏まえ、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今後議論を深めていく必要があると考えられる。

暗号資産経済圏内外の資産移転のイメージ



- 暗号資産経済圏の拡大とともに、プレーヤーの種類は増加し、法定通貨・暗号資産のフローもさらに複雑化していく。
- 様々なステークホルダー間の相互理解が進まなければ、暗号資産経済圏は『万人の万人に対する闘争』に陥る懸念がある。

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を参考に三菱総研作成

5.2 課題への対応策－基本的な考え方

極めて進展が早い分野であることに加え、法令等の実効性確保が技術的に難しい部分も存在するため、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と考えられる。

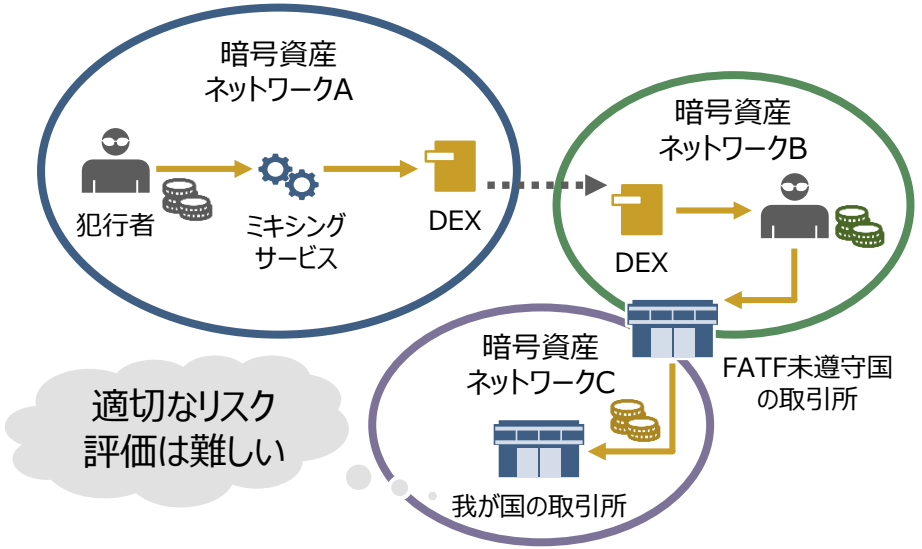
法令等での対応が難しい例（対象先）

AML/CFTで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、暗号資産経済圏の特性上、以下の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。

- 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）

法令等での対応が難しい例（実効性）

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法令対応を徹底させることは難しい。
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。



5.2 課題への対応策－基本的な考え方

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。