Vol.2021-DPS-186 No.42
Vol.2021-CSEC-92 No.42
2021/3/16

オーバレイネットワーク情報を活用した暗号通貨追跡手法の研究

髙橋　智士[†1]　大塚　玲[†1]

概要：Bitcoin を筆頭に暗号通貨経済圏が拡大していくのに伴い、暗号通貨関連の犯罪が年々増加している。暗号通貨の取引のデータ等を用いて取引当事者を絞り込むための手法が数多く研究されているが、これら手法はある一つの特定の暗号通貨に限られてしまっている．しかしながら、近年の暗号通貨の種類急増に伴い，暗号通貨間での取引の需要も増加してきており，異種暗号通貨の交換を容易に行える Web プラットフォームが複数確認されている．そのため，単一の暗号通貨の追跡だけでなくブロックチェーンを跨ぐような暗号通貨間の交換について追跡する手法も重要となってきている．本研究では，Bitcoin のオーバレイネットワーク上で流れるトランザクション等のデータを活用して、該当プラットフォームで交換された通貨を追跡する手法を提案する．

キーワード：ブロックチェーン，暗号通貨，オーバレイネットワーク, Bitcoin

Traceability analysis of cryptocurrency in the overlay network layer

Satoshi Takahashi[†1]　Akira Otsuka[†1]

Abstract: With the expansion of the cryptocurrency economy, especially Bitcoin, the number of cryptocurrency-related crimes has been increasing every year. There are many researches on methods that can narrow down the number of parties involved in a transaction to some extent by using the data of transactions of cryptographic assets (transactions). However, considering the recent surge of cryptocurrencies other than Bitcoin, it is important to track not only shingle cryptocurrency but also the exchange of currencies between different cryptocurrencies. In this research, we propose a method to track currencies exchanged on the relevant platform by utilizing data such as transactions flowing on the Bitcoin overlay network.

Keywords: Blockchain, Cryptocurrency, Overray Network, Bitcoin

1. はじめに

近年，Bitcoin を始めとする暗号通貨が経済圏を拡大していくに伴い，暗号通貨関連の犯罪が増加している．米国 ChipherTrace 社のレポート [1] によると，暗号通貨取引所等の詐欺や盗難といったサイバー犯罪被害額は，2019 年第 3 四半期までに，2018 年の約 2.5 倍 (44.4 億ドル) に増加している．また，警察庁が公開している「令和元年版警察白書」[2] によると，犯罪収益や資金洗浄の疑いがあると暗号通貨交換事業者から届け出された件数が 7,096 件と前年比 10 倍以上となっており，海外だけでなく日本国内でも暗号通貨が犯罪に使用されるケースが増加していると言える．

暗号資産にかかる取引の流れはブロックチェーン上に保存されており，それを参照することで追跡可能であるが，特定の取引に関与しているユーザの属性（氏名，住所，電話番号，メールアドレス等のユーザの特定や絞込みにつながる情報）はブロックチェーン上には保存されておらず取引当事者を特定するのは困難とされている．しかしながら，近年この匿名性を破る研究が進められており，Bitcoin においては以下のような手法が既に提案されている．[3]

[†1] 情報セキュリティ大学院大学
Institute of Information Security.

Vol.2021-DPS-186 No.42
Vol.2021-CSEC-92 No.42
2021/3/16

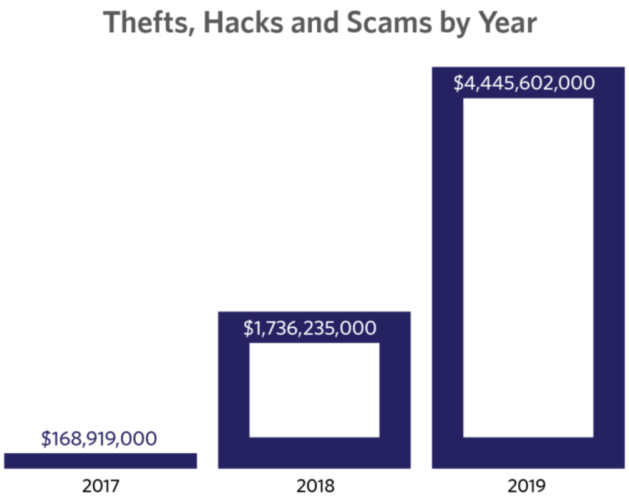

図 1　暗号通貨関連犯罪の被害額 (Source:[1] p.17 Figure 7)

- ブロックチェーンの分析とクラスタリング
  - トランザクションの入力と出力の分析
  - 行動分析
- Bitcoin P2P Network の分析

これらの手法は Bitcoin のブロックチェーンや P2P Network 上の情報を活用するものであり，現金化や別の暗号通貨へ交換されてしまうと追跡不可能となってしまう．

一方で，暗号通貨の種類は Bitcoin 以外にも多数存在しており，現時点でも 3,000 種類を超えている。また，英国 CryptoCompare のレポート [4] によると，70 以上の取引所のデータを用いた調査で，2018 年 10 月〜11 月の一ヶ月間の暗号通貨同士の取引額は現物取引全体の約 2/3 を占めたとされている．

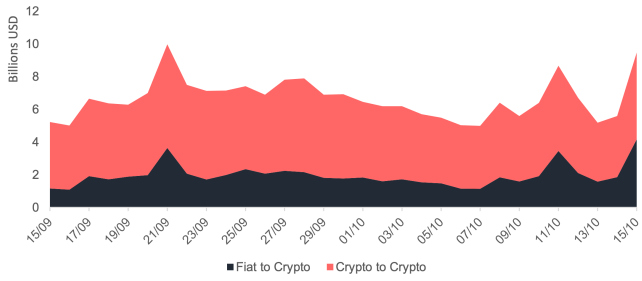

図 2　現物取引における暗号通貨取引額の内訳
(Souce:[4] p.11 Figure 5)

そのため，現在暗号通貨を追跡するにあたっては，単一の暗号通貨内での追跡だけでなく，異なる種類の暗号通貨間の取引も識別し追跡を行う手法も必要となってきている．

以降本稿では，2 章で先行研究を紹介し，3 章で本研究の位置づけを説明し，4 章で実験内容とその結果，5 章で考察，6 章でまとめについて述べる．

2. 先行研究の紹介

Yousaf ら [5] は，異種暗号通貨間の取引プラットフォームに注目し，その使用方法及び追跡方法について調査している．

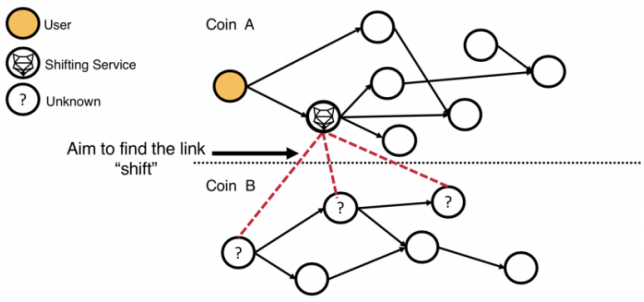

図 3　先行研究の概要 (Source:[6])

従来，違法に入手した暗号通貨を現金化しようとする犯罪者は取引所を使用する必要があったが，近年，暗号通貨取引所では厳格な顧客確認やマネーロンダリング防止のポリシーを実装しており，犯罪者にとっては身元が明らかとなってしまうリスクが存在している．その代替手段としてここ数年内に ShapeShift や Changelly 等の顧客情報確認が不要な暗号通貨取引プラットフォームが誕生している．(ShapeShift では 2018 年 10 月までアカウント確認は不要であった)

2.1 取引プラットフォームの使用方法

ShapeShift や Changelly といった取引プラットフォームのほとんどは Web ブラウザから操作出来るのに加えて，API も備えている．これらプラットフォームの主な使用方法及び流れは以下の通りである．

(1) 入金暗号通貨，出金暗号通貨を選択
(2) 出金先の宛先アドレスを入力
(3) サービス側（プラットフォーム）が以下を提示
  - 取引レート
  - 入金用宛先アドレス
  - ブロックチェーン上の手数料
(4) 入金用宛先アドレスへ送金
(5) サービス側が出金先のアドレスへ送金

この論文内では，上記（4）のプラットフォームへの入金を Phase1，（5）のプラットフォームからの出金を Phase2 としてそれぞれ追跡の手法を検討している．

2.2 Phase1 の追跡

Shapeshift の API では直近の取引履歴を取得することが可能であるが，参照可能な情報は入金暗号通貨と出金暗号通貨の種別と取引日時，入金金額に限られている．そこで論文内では上記情報をもとに，ブロックチェーン上で

- API で取得した日時にある程度近い日時のトランザクション
- 金額が同一

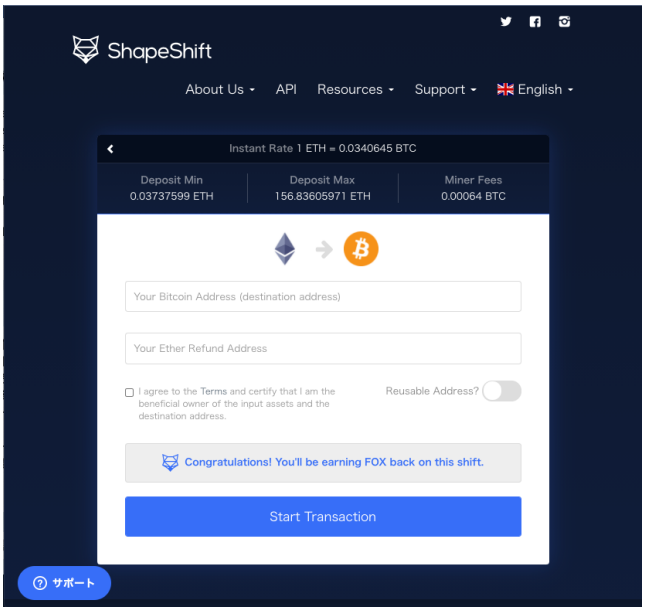

図 4　ShapeShift の取引画面
(Source:https://classic.shapeshift.com)

であるトランザクションを探すもとのして，Shapashift の API で取得したトランザクションの発生時間を t とし，その t に一番近く承認されたブロックを b (その高さを h) としたとき，探すべきトランザクションを含むブロックの範囲は，$[h-\delta_b, h-\delta_a]$ であるとしてその手法を提案している．(δ_a, δ_b は入力暗号通貨の固有パラメータ)

そして，精度を上げるためや候補を絞り込むために ShapeShift の API にて検証する方法も併せて提案している．

ShapeShift の API の機能の 1 つには，アドレスをパラメータとして渡すことで，そのアドレスが ShapeShift の取引に使用されたアドレスであるかどうか，どの取引に使用されたものか回答してくれる機能がある．これを利用し，前記で探しだしたトランザクションの出金先アドレスについて全て照会を行い，検証を行うことによって精度を大幅に向上させることが出来る．

また，検証が成功した場合は，その ShapeShift の取引の出金暗号通貨の種別と出金取引のトランザクション ID も取得出来るため，Phase2 の追跡も兼ねることが可能である．

```
$ curl -s --location --request GET 'shapeshift.io/txstat/0xebe15a6ce46ebe819f4131bbef66160c83563d0e' | jq .
{
  "status": "complete",
  "address": "0xebe15a6ce46ebe819f4131bbef66160c83563d0e",
  "withdraw": "3H4DZQeGMwCr5RpM62kU5UV8dA9TLam3wW",
  "incomingCoin": 0.035,
  "incomingType": "ETH",
  "outgoingCoin": "0.00064793",
  "outgoingType": "BTC",
  "transaction": "a3af974b7113aba3803bbff9e9cc15b46277b37f874db899d4a6152566ea7501",
  "transactionURL": "https://blockchain.info/tx/a3af974b7113aba3803bbff9e9cc15b46277b37f874db899d4a6152566ea7501"
}
```
出金トランザクションID

図 5　ShapeShift API による検証

2.3　Phase2 の追跡

前記 2.1 で記載した ShapeShift の API にて検証作業により，出力取引のトランザクション ID が判明するため，Phase2 の追跡も可能である．

しかし，API のこの機能が半永久的に使用できる保証はないため，別の手法にも言及している．その方法とは，Phase1 と同様に日時や金額が近いトランザクションをブロックチェーン上から探し出すというものである．しかし，探し出す金額は 入金額×取引レート－手数料となり，取引レートは変動するため、ある程度の範囲を見込む必要がある．それにより，候補として抽出されるトランザクションの数は多数となってしまい、結果として誤検知が多数となってしまう．

2.4　課題

前記の通り，紹介した先行研究の提案手法は ShapeShift の API を前提としており，API が廃止されると適用不可となってしまう．また，Changelly 等他の取引プラットフォームで実装されている API では、基本的には自身が行った取引情報の参照程度しか出来ず，提案手法で利用したような ShapeShift の API と同等の機能は提供されていない．

そのため，先行研究の提案手法は適用箇所は限定的となってしまっている．

3.　提案手法

3.1　本研究の目的

本研究では，先に紹介した先行研究の課題である ShapeShift の API を使用しない異種暗号通貨間の取引の追跡を目的とする．ただし，近年暗号通貨の種類は数多く存在するため，一旦その中でも取引量の多い Bitcoin を追跡の対象とする．追跡に使用する情報は先行研究でも使用したブロックチェーン上の情報に加えて，Bitcoin の P2P Network といったオーバーレイネットワークの情報を活用して異種暗号通貨間の取引プラットフォームによる取引の繋がりを見つけ出す．

3.2　提案手法

Bitcoin の P2P Network において，トランザクションのデータは基本的に送金者によって作成されてネットワーク内にブロードキャストされる．そのため，ShapeShift や Changelly といった取引プラットフォームからの送金（先行研究における Phase2）トランザクションは，取引プラットフォームからブロードキャストされていると考えられる．そのため，Phase2 のトランザクションを探索する際に，そのトランザクションのデータが含まれるパケットの送信元 IP アドレスを識別することによって，取引プラットフォームからの出金であると推定することが可能である．

つまり，先行研究がブロックチェーン上のデータから Phase2 のトランザクションを探索するための検索条件として挙げていた

- 日時
- 金額

に加えて，該当する取引プラットフォームの IP アドレスも条件として加えることで、識別精度の向上が見込めると考えられる．

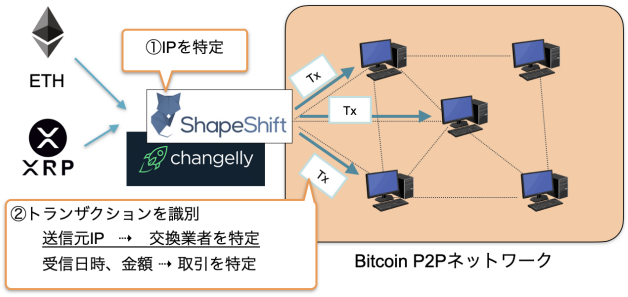

図 6　提案手法概要

尚，本手法を実現するためにはまず事前処理として，上記の通り取引プラットフォームの IP アドレスの特定が必要となる．また，取引プラットプォームの IP を特定する上で P2P Network 上でのデータの伝播の様子を確認する必要があるため，基本的に P2P Network 内の全ノードとの接続が必要となる．

3.3　IP アドレスの特定

前述の通り，Bitcoin の P2P Network において，トランザクションのデータは基本的に送金者によって作成されネットワーク内にブロードキャストされる．それを受信した個々のノードはそれぞれ自身の接続先にそのトランザクションのデータを伝播させる．そのため，その伝播の仕方を観察すればトランザクションの作成者を絞り込むことは可能である．

Koshy ら [7] は，P2P ネットワークにおける通信経路やその中継パターン（リレー・パターン）を手掛かりに，取引のアドレスとそれに対応するユーザの端末（ウォレット等）の IP 庵治レスを関連付ける手法を提案している．具体的には，トランザクションがリレーされる状況を観察し，観察者に一番最初にトランザクションを送信してきた IP がトランザクションの発生元であるという前提で，そのトランザクションの Input となる Bitcoin アドレスと IP アドレスを関連付けようとした．しかし，約 550 万件の取引データを収集・分析し観察した結果，観察したトランザクションの大部分を占める (約 91.4%) プロトコル上正常な中継パターン（複数の IP がそれぞれ 1 回だけ中継するパターン）での IP アドレス・Bitcoin アドレスの関連付けにはあまり効果がなかったとしている．

これは，Koshy らの提案手法には Bitcoin でのフラッディング方式についての考慮が不足していたものと考えられる．Bitcoin のフラッディング方式は 2014 年当時「Trickle」と呼ばれるもので，データ転送先を 200ms 毎にランダムに選択する方式であり，その選択した順番によっては観測者はトランザクション作成者と直接接続を行っていた場合でも，他ノードが一番最初にトランザクションを送信してくる場合がある．

Fanti ら [8] は，Bitcoin P2P Network を d-正則木としてモデル化し，この「Trickle」と 2015 年に新しく採用された「Diffusion」それぞれのフラッディング方式について双方の匿名性レベルについて評価を行っている．

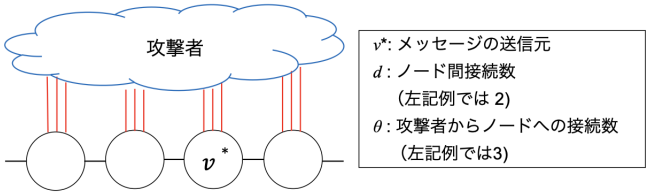

図 7　検討モデル ([8] Figure 1 を元に作成)

その中で First-timestamp estimator という手法について提案しているが，この手法は Koshy らの手法とベースは同じであるが，Bitcoin の各ノードに対する接続数を増やすことで IP アドレスの検出率を向上できるとし，その検出率は $\frac{\theta}{d-2}\log(\frac{d+\theta-2}{\theta})$ であるとしている[*1]．

本研究では，この First-timestamp estimator の手法にて IP アドレスの特定を目指すが，この手法を行うためには Bitcoin P2P Network 上の全ノードそれぞれに対して複数接続を行う必要がある．そこで，「Bitnodes」という Bitcoin P2P Network 内の到達可能なノードの IP 等の情報を収集&接続を行うツールを使用し全ノードへの接続を試みる．

3.4　Bitnodes

3.4.1　概要

Bitnodes は Bitcoin P2P Network 内の到達可能な全てのノードを見つけ，Network のサイズを推測するために開発されたクローラツールで，Github に Python ベースのソースコードが公開されている [10]．

本ツールで取得されたデータは Web サイト Bitnodes.io (`https://bitnodes.io`) で参照出来ると共に，

- Network Snapshot
- 24-hour Charts
- Live Map
- Network Map

[*1] 本理論式の導出過程は，同筆者の別論文 [9] の Appendix B.4 に記載されている

- Leaderboard

などをグラフィカルに閲覧することも可能となっている．

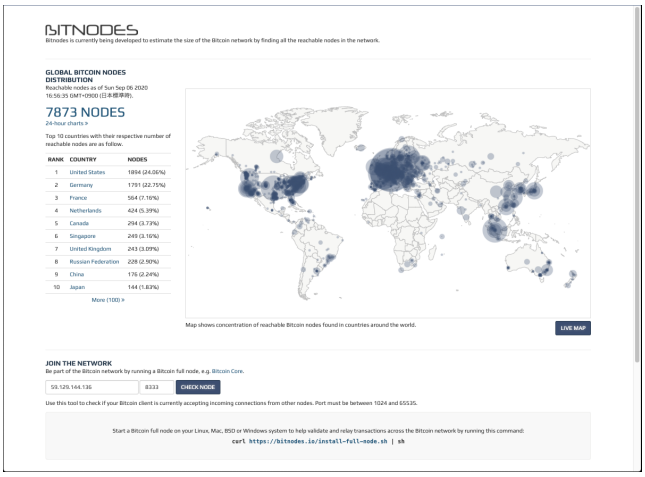

図 8 Bitnodes.io の Web サイト (Source:`https://bitnodes.io`)

Bitnodes は，Bitcoin のプロトコル [11][12] 上定められている「GETADDR」メッセージを接続先のノードに対して送信する．プロトコル上「GETADDR」メッセージを受信したノードは，「ADDR」メッセージにて自身の持つ最大 2500 個のノード情報（IP，ポート等）を「GETADDR」メッセージ送信者に送信する仕様となっている．

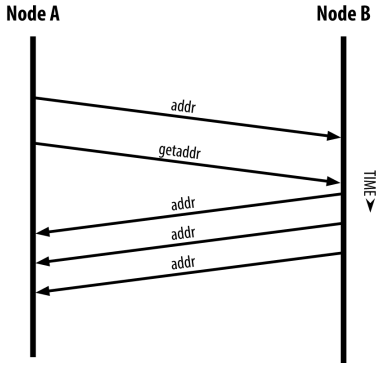

図 9 GETADDR メッセージと ADDR メッセージ
(Source:[12] Figure 4)

Bitnodes はこの受信した IP，ポート番号に対して接続と「GETADDR」メッセージの送信を再帰的に繰り返し，ネットワーク内の到達可能な全てのノードを見つける仕組みとなっている．

また，ノード情報の収集だけではなく，接続されたノードから受信した「INV」メッセージについても，

- トランザクション ID（ハッシュ値）
- 送信ノード情報（IP アドレス，ポート番号）
- タイムスタンプ

を保存する仕様にもなっている．

「INV」メッセージとは，Bitcoin P2P プロトコル上，トランザクションのデータを送信する前の送信可否を問うためのメッセージで，ネットワークの負荷を減らす目的でトランザクションのハッシュ値と共に送信される．「INV」メッセージを受け取ったノードは，そのトランザクションのデータが手元になければ，送信元に「GETDATA」メッセージを送信しそのトランザクションのデータを送信するよう促す．逆に既にそのトランザクションデータがあればそのまま，「INV」メッセージを無視するだけで構わない．

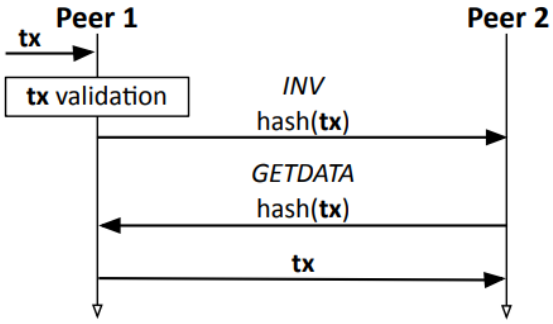

図 10 INV メッセージと TX メッセージ
(Source:[13] Figure 3)

Bitnodes はこの「INV」メッセージについて前述の情報をデータベースに保存するため，特定のトランザクションについてのネットワーク上の伝播状況を知ることが可能となっている．

3.4.2 改良点

前記 IP 特定手法では，1 つの Bitcoin ノードに対して複数接続が必要となる．しかし，Bitnodes は Bitcoin P2P Network 用 IP アドレスのクローラであるため，ノードへの接続は基本的に 1 ノードあたり 1 本となる．そのため，以下のような機能を持つ Python モジュールを別途作成した．

- 既存接続の読み取り
- 接続（version/varack メッセージによるハンドシェイク）
- 接続維持（ping や addr メッセージによる KeepAlive）
- 最大接続数の定義（設定ファイルの読み込み）

作成したモジュール「multi.py」の位置付けと構築システム構成は下図の通り．

3.5 研究の流れ

本研究では，事前準備と予備実験，本実験の三段階に分けて進めていく．具体的には，事前準備では，前述の Bitnodes 環境の構築を行う．予備実験では，IP 特定手法の有効性を取引プラットフォームを使用しない状態で Testnet 及び Mainnet 両方で検証する．具体的には，Bitcoin の Testnet で作成モジュールの動作確認及び手法の有効性を確認し，Mainnet で接続数の妥当性を検証する．そして，本実験では取引プラットフォームの IP 特定の実験と取引プラット

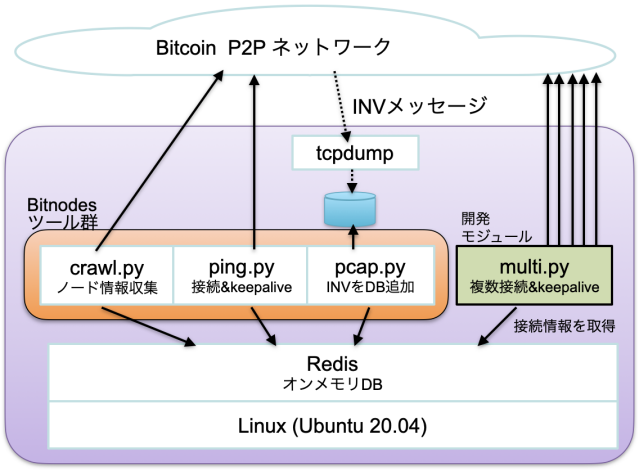

図 11　システム構成及び作成モジュールの位置付け

フォームにて交換された暗号通貨交換を識別し追跡できるか実験を行う．識別対象の取引は，「Etherscan.io」等で ShapeShift と既に識別されているアドレスに入金されたものを対象とし，交換後 BTC へ出金されたトランザクションを追跡出来るか確認する．なお，本実験における評価方法としては，先行研究の ShapeShift API を使用した追跡手法を用いる予定としている．そのため，本研究内の実験で使用する取引プラットフォームは全て ShapeShift とする．

4. 実験

4.1 予備実験 (Testnet)

ここでは，ShapeShift を使用せずにトランザクションのデータを発信するノード (以降，TX 発信ノードと記載) を Testnet 上に用意し実験を実施した．実験の内容としては，Bitnodes 稼働ノード（以降，検証機と記載）から Testnet 内のノードに複数接続を行った状態で，TX 発信ノードより TX を発信した際に，検証機で TX 発信ノードの IP アドレスを特定できるか（TX データを一番最初に送信してきた IP アドレスは TX 発信ノードのものであるか）を確認した．検証機から各 Bitcoin ノードへの接続数を変動させて，各接続数毎に 10 ずつ取引を行った結果が下表の通り．（理論値は，Fanti ら [8] が定義した $\frac{\theta}{d-2}\log(\frac{d+\theta-2}{\theta})$ にて算出）

表 1　Testnet での IP アドレス検出率

接続数 θ	最速の INV 送信元が TX 発信ノード	検出率	理論値
1	2 回	0.2	0.27
5	3 回	0.3	0.59
10	3 回	0.3	0.73
12	5 回	0.5	0.76
20	7 回	0.7	0.84
30	7 回	0.7	0.88

表を見て分かる通り，接続数を増やすと IP アドレスの検出率が向上していることことが確認できた．

4.2 予備実験 (Mainnet)

上記実験の内容を Mainnet にて実施した結果は下表の通り．

表 2　Mainnet での IP アドレス検出率

接続数 θ	最速の INV 送信元が TX 発信ノード	検出率	理論値
20	4 回	0.4	0.57
30(25)	4 回	0.4	0.50

接続数 θ が「30(25)」となっている箇所は，最大接続数を「30」と設定していてが HW リソースの限界等により，25 までしか接続が確立できなかったものである．Mainnet 環境では Bitcoin ノード数が多く，TX 発信ノードと他 Bitcoin ノード間の接続数も Testnet より多かったため，実測値及び理論値ともに Testnet での予備実験より低い値となった．

4.3 本実験 (ShapeShift の IP アドレス特定)

ここでは，実際に ShapeShift にて Ethereum から Bitcoin への交換取引を行い，Bitcoin として送金されるトランザクションを一番最初に送信してきた IP アドレスとを ShapeShift のものである特定する実験を実施した．計 10 回取引を実施したところ，ある特定の IP アドレスが 2 回の取引で一番最初に送信してきた IP となった．（本 IP アドレスは ShapeShift の IP アドレスであると断定は出来ないため，本稿では実アドレスは記載せずに，以降は IP:X と記載する．）

4.4 本実験 (交換通貨の特定可否)

前実験で得られた ShapeShift の IP と推測される「IP:X」とトランザクションの情報から，第三者の ShapeShift での取引で送金された Bitcoin を特定できるかどうかを実験した．前実験での ShapeShift との取引結果及び Etherscan.io にて ShapeShift のメインアドレスは以下と特定している．

0x70faa28A6B8d6829a4b1E649d26eC9a2a39ba413

そのため，このアドレスに送金するトランザクションがあれば，ShapeShift 上で Ethereum から何らかの暗号通貨への交換取引が行われたものと推定できる．したがって，このメインアドレスに送金したトランザクションの日時・金額を取得し，Bitcoin のトランザクションの中で以下条件 3 点に適合するものが ShapeShift で交換された Bitcoin であると特定することが可能となる．

- ETH 送金トランザクションの直後
- 金額が近似（ETH 金額 × 交換レート- 手数料）
- ShapeShift の IP と思料される「IP:X」から一番最初

に受信したトランザクション

この実験の結果は以下のとおり．

- データ収集期間： 2/10 0:00〜 2/10 23:59
- ShapeShift への入金数： 23 件
- 条件 3 点に該当する TX 数： 0 件

尚，本実験のデータ収集期間中，検証機と ShapeShift の IP アドレス思料される「IP:X」間の接続は HW リソースの限界により，1〜2 本程度であった．

5. 考察

Testnet での予備実験結果で接続数を増やすと IP アドレス検出率が向上することから，IP アドレス特定手法の有効性を確認することができた．また，Mainnet では Bitcoin ノード全体数が Testnet より多いため，高い検出率を得るためには，十分な接続数が必要であることがわかった．また，2 つの実験を通して検出率の実測値が理論値より 0.1〜0.3 低い値となっていた．現状この原因は不明であるが，先行研究では Bitcoin ネットワークを d-正則木としてモデル化しており，実際の接続状況は閉路があったり等さらに複雑である可能性がある．

本実験での IP アドレス特定の結果については，検出率：0.2 と Mainnet での予備実験時 (0.4) と比べかなり低い値となっている．交換した通貨の特定実験も上手くいかなかったことから，検出した「IP:X」が誤りだった可能性もある．

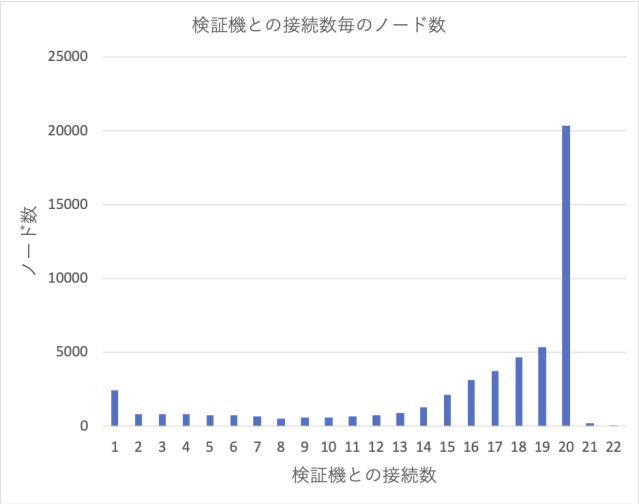

図 12 IP 特定実験時の検証機の接続数

上図は，IP 特定実験時の検証機の接続数をグラフ化したものである．最大接続数を「20」と設定していたため，接続数：20 のノード数が多数 (20,360) ではあるものの，接続数：1〜19 のノードは合計 31,438 となっており全体の半数以上となっている．そのため，検証機と ShapeShift のノード間で十分な接続数を確保できていなかった可能性が十分あり，それが原因で検出率が低い，または検出した IP：X が誤りであったものと考えられる．

この問題は検証機からの接続数を増やすことで改善する可能であるが，接続数を増やす上で以下課題が存在する．

CPU リソースの枯渇

Mainnet は Testnet に比べて圧倒的にノード数が多く、その全てに接続を行って KeepAlive を続けるため、CPU の消費量が膨大になる。そのため、最大接続数を 30 に設定した際には、CPU 使用率が 100%となり、そのせいか TX 発生ノードとの接続数は 25 を超えることはなかった。

ポート番号不足

現在、Bitcoin P2P Network 上で接続可能なノード数は約 8,500〜23,000 台であるとされている [14]。 23,000 台は約 1 ヶ月連続的に観測した結果であって、最初の 1 日で観測出来たのは 8,500 台であるため、Bitnodes で同時に接続が必要なのは約 8,500 程度と推測出来る。 RFC 60561[15] では、エフェメラルポートは 1024〜65535 までの範囲を使用するよう提言されており、Linux で使用可能なポート番号の最大は RFC と同じ 65535 であるため、Linux では最大約 64,000 のポートが利用可能であると言える。そのため、8,500 台に最大限で接続しようとすると、1 台あたりの接続数は 7 本程度になってしまう。

この課題は，スケールアップではなくスケールアウトで接続処理を分散することで解決することが可能である．Bitcoin 公式クライアントである Bitcoin Core の最大接続数のデフォルト値は 125 であるため，目標接続数をその半分の 60 程度とし，本研究で作成したモジュールの稼働実績を考慮すると，接続専用サーバの台数を約 100 台程度用意することで十分な接続数を確保可能なシステムを構成可能となる．

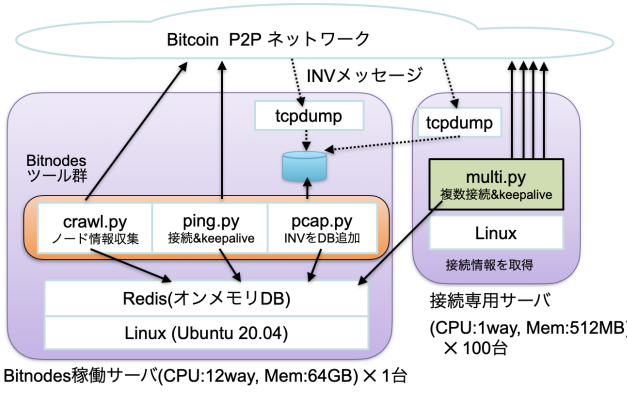

図 13 IP 特定実験時の検証機の接続数

6. まとめ

本稿では，異種暗号通貨間の取引の追跡手法について先行研究を紹介し，その課題及び本研究の目的・位置付けを明らかにし，オーバレイネットワークの情報を活用する新

しい手法を検討したものの，実験結果上では追跡可能な状況まで至ることは出来なかった．しかしながら，本手法の鍵となる IP アドレス特定についてはその有効性を Testnet 上で確認でき，Mainnet でその手法を適用する際にはより多くの接続数が必要になることが判明した．また，より多くの接続数を実現するためには十分な HW リソースが必要でありそれを実現するシステム構成案を最後に示したが，多数のサーバ数が必要となってしまい費用対効果は低く，もっと効率の良い手法の検討が必要である．加えて，本手法は FW や NAT 環境，Tor 等のこちらから接続不可な環境には対応していない等様々な課題や制約が残されているため，こちらも今後更なる検討が必要となる．

参考文献

[1] CipherTrace, Inc.. Cryptocurrency Anti-Money Laundering Report, 2019 Q3. https://ciphertrace.com/wp-content/uploads/2019/12/CipherTrace-Cryptocurrency-Anti-Money-Launder\ing-Report-2019-Q3-2.pdf
[2] 警察庁. 令和元年版　警察白書. https://www.npa.go.jp/hakusyo/r01/index.html
[3] Nasser Alsalami, Bingsheng Zhang. SoK: A Systematic Study of Anonymity in Cryptocurrencies. in *2019 IEEE Conference on Dependable and Secure Computing (DSC)*, Nov 2019, pp. 1–9.
[4] CryptoCompare, Crypt Coin Comparison LTD. CCCAGG Exchange Review, November 2018. https://blog.bitmex.com/wp-content/uploads/2018/11/cryptocompare_exchange_review_october_2018.pdf
[5] Haaroon Yousaf, George Kappos, and Sarah Meiklejohn. Tracing transactions across cryptocurrency ledgers. in *28th USENIX Security Symposium (USENIX Security 19)*.
[6] Haaroon Yousaf. Tracing transactions across cryptocurrency ledgers. https://www.benthamsgaze.org/2019/08/15/tracing-transactions-across-cryptocurrency-ledgers/
[7] Philip Koshy, Diana Koshy, Patrick McDaniel. An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. in *Financial Cryptography and Data Security*. 2014.
[8] Giulia Fanti, Pramod Viswanath. Deanonymization in the Bitcoin P2P Network. in *Advances in Neural Information Processing Systems(NIPS)*, pages 1364–1373, 2017.
[9] Giulia Fanti and Pramod Viswanath. Anonymity properties of the bitcoin p2p network. *arXiv preprint arXiv:1703.08761*, 2017.
[10] GitHub - ayeowch/bitnodes. Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network. https://github.com/ayeowch/bitnodes
[11] Protocol documentation - Bitcoin Wiki. https://en.bitcoin.it/wiki/Protocol_documentation
[12] Mastering Bitcoin. https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch08.asciidoc
[13] Gleb Naumenko, Gregory Maxwell, Pieter Wuille, Alexandra Fedorova, Ivan Beschastnikh, Bandwidth-Efficient Transaction Relay in Bitcoin, *arXiv preprint arXiv:1905.10518*, 2019.
[14] Sehyun Park, Seongwon Im, Youhwan Seol, Jeongyeup Paek. Nodes in the Bitcoin Network: Comparative Measurement Study and Survey. *IEEE Access* 2019, 7, 57009–57022.
[15] Internet Engineering Task Farce(IETF). RFC 6056(Recommendations for Transport-Protocol Port Randomization). https://www.rfc-editor.org/rfc/rfc6056.txt