Vol.2021-DPS-186 No.45
Vol.2021-CSEC-92 No.45
2021/3/16

不正な暗号資産のマネーフロー分析を目的とした取引タイミングに着目した可視化手法の提案

森 博志[1]　熊谷 裕志[1]　インミン パパ[1]　高田 雄太[1]　鈴木 将吾[1]　神薗 雅紀[1]

概要：Bitcoin や Ethereum といった暗号資産は，その性質上，法定通貨と比べると匿名性が高いため，犯罪への悪用が問題になっている．例えば，ランサムウェアの身代金の送金手段や，ダークウェブ上の違法な商品売買やサービスの決済手段として悪用されている事例が報告されている．違法な取引で得た収益は，追跡や分析を妨害するために複数の暗号資産アドレスを経由した後，最終的に特定のアドレスに集約されることが知られている．このようなマネーフローを分析するために，暗号資産トランザクションを可視化する手法が提案されているが，アドレスやクラスタリングされたアドレス間のマネーフローを二次元グラフで表現することが多く，その他の情報については十分に可視化されていない．そこで本稿では，トランザクションのタイミングを加味した三次元グラフによりトランザクションとアドレスの関係を可視化する手法を提案する．そして複数のアドレスを経由することにより追跡を困難にしているトランザクションについて，提案手法により効率的にアドレス管理者の同一性を特定することができる事例を示す．

Visualizing Method for Clustering Illicit Cryptocurrency by Transaction Time

Mori Hiroshi[1]　Kumagai Hiroshi[1]　Yin Minn Pa Pa[1]　Takata Yuta[1]　Suzuki Shogo[1]
Kamizono Masaki[1]

1. はじめに

Bitcoin や Ethereum といった暗号資産は，銀行口座に相当する暗号資産アドレス (以降，単にアドレスと記載する) を用いて通貨の取引 (以降，トランザクションと呼ぶ) を行う．暗号資産の利用者は任意のタイミングで無制限にアドレスを生成できるため，法定通貨よりも利用者や暗号資産を用いたトランザクションの匿名性が高い．そのため，犯罪者やテロ組織による悪用が問題となっている．例えば，ランサムウェアによる身代金の送金手段や，ダークウェブ上の違法な商品売買やサービスの決済手段として悪用されている事例が報告されている [1], [2], [3]．違法な取引で得た収益は，追跡や分析を妨害するために複数のアドレスを経由した後，最終的に特定のアドレスに集約されることが知られている [4], [5]．このようなマネーフローを分析するために，トランザクションを可視化する手法が提案されている．しかしながら，既存の可視化手法では，アドレスやクラスタリングされたアドレス間のマネーフローの関係性を二次元グラフで可視化した手法が多く，それ以外の情報は十分に可視化されていない．前述の通り，複数のアドレスにマネーフローを分散させるとそれらのアドレスの管理者の追跡が難しくなる．一方で，複数のアドレスを使い分けていてもアドレスの管理者が同じ場合，同時刻や近い時刻帯でトランザクションをすることが考えられる．そのため，トランザクションのタイミングを可視化することでアドレス管理者の同一性が特定できる可能性がある．そこで本稿では，トランザクションのタイミングを加味した三次元グラフにより，トランザクションとアドレスの関係を可視化する手法を提案する．複数のアドレスを経由することによりマネーフローの追跡を困難にしている Bitcoin トランザクションについて，提案手法により効率的にアドレス管理者の同一性を特定できる事例を示す．

[1] デロイト トーマツ サイバー合同会社
Deloitte Tohmatsu Cyber LLC

本稿の構成は以下の通りである．まず，2 章で研究対象である暗号資産についてその概要を述べる．次に，3 章で暗号資産のマネーフロー分析に関する既存研究について述べる．4 章では提案手法について述べ，5 章では提案手法を実装したシステムについて述べる．そして，6 章で提案手法を実装したシステムによる解析事例を挙げ，7 章で考察を行い，最後に 8 章でまとめとする．

2. 暗号資産

暗号資産とは，資金決定に関する法律 [6] で以下の性質をもつ資産と定義されている．

(1) 不特定の者に対して，代金の支払い等に使用でき，かつ，法定通貨（日本円や米国ドル等）と相互に交換できる．
(2) 電子的に記録され，移転できる．
(3) 法定通貨または法定通貨建ての資産 (プリペイドカード等) ではない．

暗号資産の例として，Bitcoin や Ethereum などが挙げられる． これらの暗号資産では，英数字からなるアドレスを用いて通貨の送金や着金を行う．暗号資産の利用者は，口座情報に相当するアドレスを任意のタイミングで無制限に生成できる．暗号資産はその種類により異なる点もあるが，自由に生成したアドレスを用いて個人間決済できる点や，後述のブロックチェーンによりデータが分散管理されている点等から，法定通貨と比べて匿名性が高い．一方で，この匿名性の高さは，ランサムウェアや脅迫メールにおける身代金の送金に悪用されたり，ダークウェブ上においてドラッグや武器，盗取されたクレジットカード情報など様々な違法な商品やサービスの決済に悪用されたりしていることが報告されている [1], [2], [3].

2.1 Bitcoin

暗号資産の中でも Bitcoin は利用者が多く，不正な活動にも頻繁に悪用されていることが知られている．Bitcoin は，ナカモトサトシという人物が書いたとされる論文 [7] で提案された暗号資産である．2009 年に最初のトランザクションが記録されて以降，2021 年 2 月 16 日現在に至るまで大きな不具合も無く運用されている．その時価総額は年々増加し，現時点で 90 兆円を超えている [8]．本研究では，高いシェアを誇る Bitcoin を分析対象とする．

2.1.1 ブロックチェーン

ブロックチェーンは，鎖状に連結したブロックと呼ばれるデータで構成されている．各ブロックは，前のブロックのハッシュ値を格納しており，ブロックが連結したタイミングの時系列に連結している．したがって，もしあるブロックを改変したとしても，その後のブロックに記録されているハッシュ値も異なってしまうため，ブロックチェーンのデータ改ざんは困難である．暗号資産では，利用者によるハッシュ値の計算に基づき承認されたトランザクションが，ブロックチェーン上のブロックとして管理されている．すなわち，ブロックチェーンの仕組みにより，暗号資産における過去のトランザクションの改変は困難になるため，取引の整合性が担保される．また，ブロックチェーンは，P2P により複数のノードで管理されているため，ロバスト性にも優れている．

2.1.2 Bitcoin の匿名性

Bitcoin のブロックチェーンは公開情報であり，誰でも閲覧可能である．すなわち，どのトランザクションにおいて，どのアドレスからどのアドレスへ，どれだけの Bitcoin を送金したのかを調べることが可能である．しかし，Bitcoin アドレスは個人が無制限に生成できるため，Bitcoin 利用者は自身が生成した複数のアドレスを経由して送金することにより，トランザクションの匿名性を高めることができる．加えて，ミキシングと呼ばれる手法を用いることによりマネーフローを複雑化させることも可能である．ミキシングは，一つのトランザクションに管理者が異なるアドレスを複数参加させることで取引を複雑化し，さらにその複雑化した取引を繰り返すことにより，匿名性をより高める手法である．Bitcoin では複数のミキシングサービスが存在することが報告されている [9].

前述したとおり，Bitcoin の匿名性の高さは，一般の利用者に限らず不正な利用者にとっても優位に働き，マネーロンダリングや不正送金に悪用されている．しかし，分析を妨害するために複数のアドレスにマネーフローを分散させたとしても，それらのアドレスの管理者が同じ場合，トランザクションのタイミングが同じであったり近い時間帯になることが考えられる．そのため，アドレスごとのトランザクションのタイミングを比べることでそれらのアドレスの管理者の同一性を特定できる可能性がある．そこで我々は，トランザクションのタイミングに着目し，XY 平面に加えて，時間を表す Z 軸を加えた三次元グラフを用いてトランザクションを可視化する手法を提案する．上記のような不正なマネーフローの特徴を捉えるような分析を通じてアドレス管理者の同一性を推測することにより，不正な利用者の特定や不正対策に貢献できると考える．

3. 関連研究

3.1 ブロックチェーンの分析

文献 [10] では，Bitcoin などのブロックチェーンを利用した暗号資産を効率的に分析するためのフレームワーク BlockSci を提案しており，オープンソースのソフトウェアとして公開している [11]．このフレームワークは，ブロックチェーンをパースし，トランザクションやアドレスを効率よく分析できるように独自のデータベースを生成する．また，後述するクラスタリング機能やミキシングされたトランザクションを検知する機能も持つ．本研究では提案手

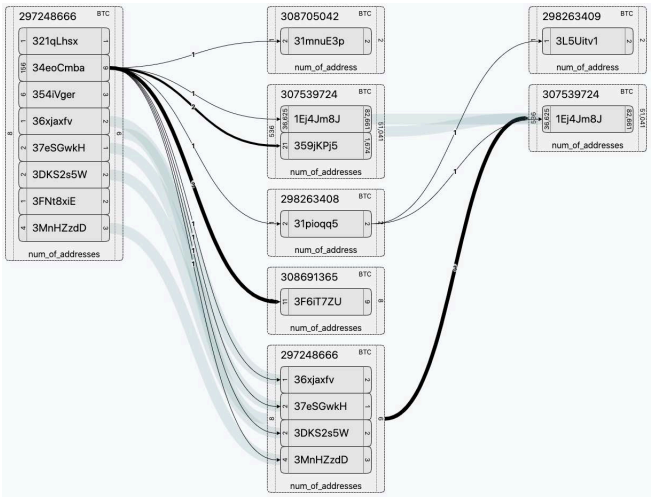

図 1 GraphSense による可視化例

法の実装に当該フレームワークを利用している．

3.2 アドレスのクラスタリングとタグ付け

トランザクションの特徴から，アドレスをクラスタリングする手法が提案されている．例えば，文献 [12], [13], [14] では，「同一トランザクションに参加する送金元アドレスの管理者は同一である」という推測により，アドレスをクラスタリングしている．また，上述した BlockSci は，上記手法によるクラスタリング機能に加えて，アドレスを管理するウォレットソフトウェアの実装に見られる特徴に基づき，アドレスをクラスタリングする機能も提供している．

不正なマネーフローの分析において，アドレスのクラスタリングは，アドレスの管理者または管理組織の同一性を推測する手段の一つとして活用できる．例えば，複数のアドレスが含まれるクラスタにおいて，そのうち一つのアドレスが不正行為に利用されていたことが判明した場合に，そのクラスタやクラスタに含まれるすべてのアドレスに “不正行為関与の疑い” のタグ付けをすることができる．しかしながら，既存のクラスタリング手法は，トランザクションの性質に基づく分類であり，必ずしもアドレス管理者の同一性を分析することが目的ではないため，一概に上記のようなタグ付けができる訳ではない．例えば，ミキシングにより同一トランザクションにおいて複数の管理者のアドレスが混合した場合に，これらのアドレスはアドレス管理者の同一性という観点では正しくクラスタリングできない問題がある．一方で我々は，トランザクションがブロックチェーンに取り込まれるタイミングに着目しており，不正なマネーフローの特徴に基づく分析手法を提案している．提案手法は，上記クラスタリング手法を補完し，不正なマネーフローの分析効率化に貢献できると考える．

3.3 トランザクションの可視化

暗号資産を可視化する手法はこれまでに多数提案されている．文献 [15] は，インターネット上に公開されている暗号資産可視化システムや，暗号資産の可視化に関連する論文について合計 76 件を調査し，用途や粒度の観点で可視化手法を分類している．上記文献や著者らが独自に調査した可視化手法の中で，提案手法と関連性が高い既存研究について以下に述べる．

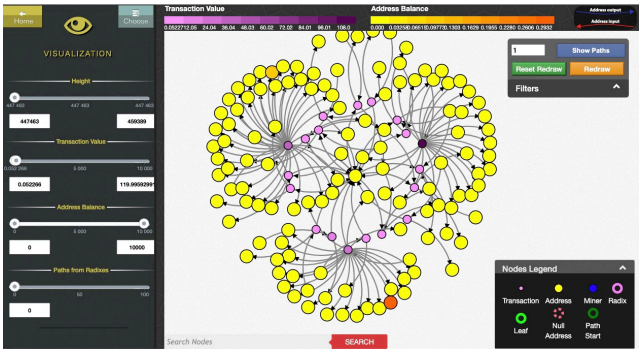

図 2 BlockChainVis による可視化例

GraphSense [16] は，Bitcoin や Bitcoin Cash，Litecoin などの暗号資産の分析プラットフォームでありアドレスや上述のクラスタリング手法によるクラスタの関係を可視化する．図 1 は GraphSense によりいくつかのアドレスを可視化した画面である．GraphSense ではアドレスを小さい長方形，クラスタはアドレスを包含する大きな長方形として描画される．

BlockChainVis [17] は，Bitcoin を分析するための可視化システムであり，実装されている多数のフィルターにより複雑なアドレスの関係をシンプルな関係に描画できる．図 2 は BlockChainVis による可視化画面である．画面左側のビューを操作することでトランザクション時間やアドレスの Bitcoin 残高などについて表示するノードをフィルタすることができる．

上記の既存研究以外にも，最新のトランザクションを描画する可視化システム [18] や，高解像度ディスプレイを複数利用することで一般的なディスプレイの解像度では描画しきれない大量の Bitcoin トランザクションを一度に描画する手法 [19] などが提案されている．本研究では，これらの既存研究と同様にトランザクションをインタラクティブなグラフとして描画するが，そのグラフをトランザクションのタイミングを加味した三次元グラフとして描画するという点で異なる．トランザクションのタイミングを加味した可視化手法は，著者らが知る限りでは提案されていない．

4. 提案手法

提案手法は，はじめに解析したい Bitcoin アドレスを指定し，そのアドレスを起点として関連するアドレスとトランザクションに関する情報を可視化することで解析を補助する．

4.1 アドレスとトランザクションの三次元グラフ

解析者が解析対象のアドレスを入力すると，入力したアドレスとそのアドレスが直接関係するトランザクションを三次元グラフとして描画する．その際，アドレスは球として，トランザクションを立方体として描画する．また，トランザクションに直接関係するアドレスは直線で接続する．

直線の色はトランザクションにおけるアドレスの役割を表しており，図 3 の場合，赤い線で接続されているアドレス A は送金元アドレス，緑色の線で接続されているアドレス B は送金先アドレスであることを示している．また，黄色の線で接続されているアドレス C は当該トランザクションにおいて，送金元かつ送金先のアドレスであることを示している．また，扱う金額が大きくなるほどオブジェクトを大きく描画する．なお実際は，提案手法ではトランザクションを三次元グラフで可視化するが，便宜上ここでは簡略化して二次元グラフで図示している．

三次元空間におけるアドレスとトランザクションのレイアウトは二つの手法を適用して決定する．まず，アドレスとトランザクションをノードとした力学モデルのグラフレイアウトアルゴリズムを用いて，XY 平面のレイアウトを決定する．次に，トランザクションがブロックチェーンに組み込まれた時間を基準に，トランザクションが時系列に並ぶよう Z 軸座標を決定する．この時，アドレスの Z 軸座標は，描画されているトランザクションのうち直接関連するトランザクションの Z 軸座標の中央値としている．

図 4 は，以上の手法により可視化した画面の例である．なお図中の X,Y,Z 座標軸は便宜上表示しているものであり実際には表示されない．図中 A は，解析者が解析の起点となるアドレスを入力するフィールドである．フィールドにアドレスを入力すると，図中 B のように三次元空間にアドレスとトランザクションを表す 3D オブジェクトが描画される．描画されたオブジェクトはクリックして選択でき，選択されたオブジェクトには C のようにオレンジ色のアウトラインが表示される．オブジェクトを選択するとそのオブジェクトに関する情報が E に表示される．

4.2 オブジェクトの選択と展開

オブジェクトを選択した状態で F の展開ボタンを押すと，当該オブジェクトが直接関係するトランザクションまたはアドレスが追加で描画される．展開されたオブジェクトを選択して更に展開することも可能であり，解析者は対象のアドレスやトランザクションを次々と展開していき，アドレスとトランザクションの関係を解析することができる．

また，B において球で描画されているアドレスのオブジェクトを選択した場合，D のように画面上部に棒グラフが表示される．当該グラフでは選択されたアドレスが直接関与するトランザクションについて，そのアドレスの送金額や着金額が表示される．

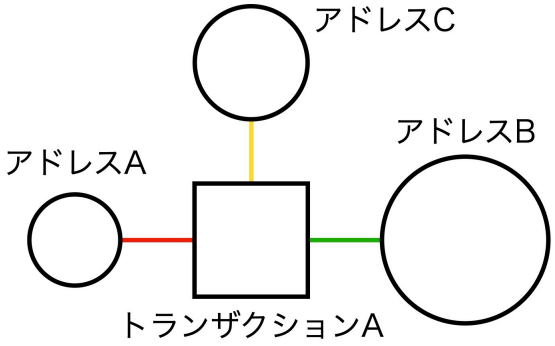

図 3 提案手法により描画するノードの関係

5. 提案手法の実装

本研究では，提案手法をインタラクティブな可視化ユーザインタフェースを提供するクライアント（以下，可視化クライアント）と，指定されたアドレスについて Bitcoin のブロックチェーンをパースし，当該アドレスに関連するトランザクション情報を提供する分析サーバ（以下，分析サーバ）からなるシステムとして実装した．クライアントとサーバは，HTTP 通信により必要な情報を送受信する．

5.1 可視化クライアント

可視化クライアントは，Unity [20] を用いて実装した．可視化クライアントでは，アドレスとトランザクションの 3D 描画やそれらのオブジェクトのレイアウト決定処理などを行う．また，4.2 節で述べた手順により，解析者が特定のアドレスに関係するトランザクションについて追加の描画を要求した場合，可視化クライアントは分析サーバに指定されたアドレスに関するトランザクション情報を HTTP 通信でリクエストすることにより，描画に必要な情報を取得する．なお，Bitcoin 取引所やミキシングのように，関係するトランザクションやアドレスの数が大量になる場合は，オブジェクトの描画数を制限している．

5.2 分析サーバ

Bitcoin のブロックチェーン情報のデータサイズは 260GB を超えており，この中から特定のアドレスに関するトランザクション情報を取得する処理には時間を要する．そこで，BlockSci [11] を用いて事前にブロックチェーンのパース処理を行い，当該フレームワークが提供する API を利用することで可視化クライアントが必要とするトランザクション情報を取得する．分析サーバでは Django [21] を実行し，可視化クライアントと HTTP 通信を行う．

6. 提案手法による分析事例

本章では提案手法を実装した可視化システムにより二つのランサムウェアが身代金の送金先アドレスとして表示す

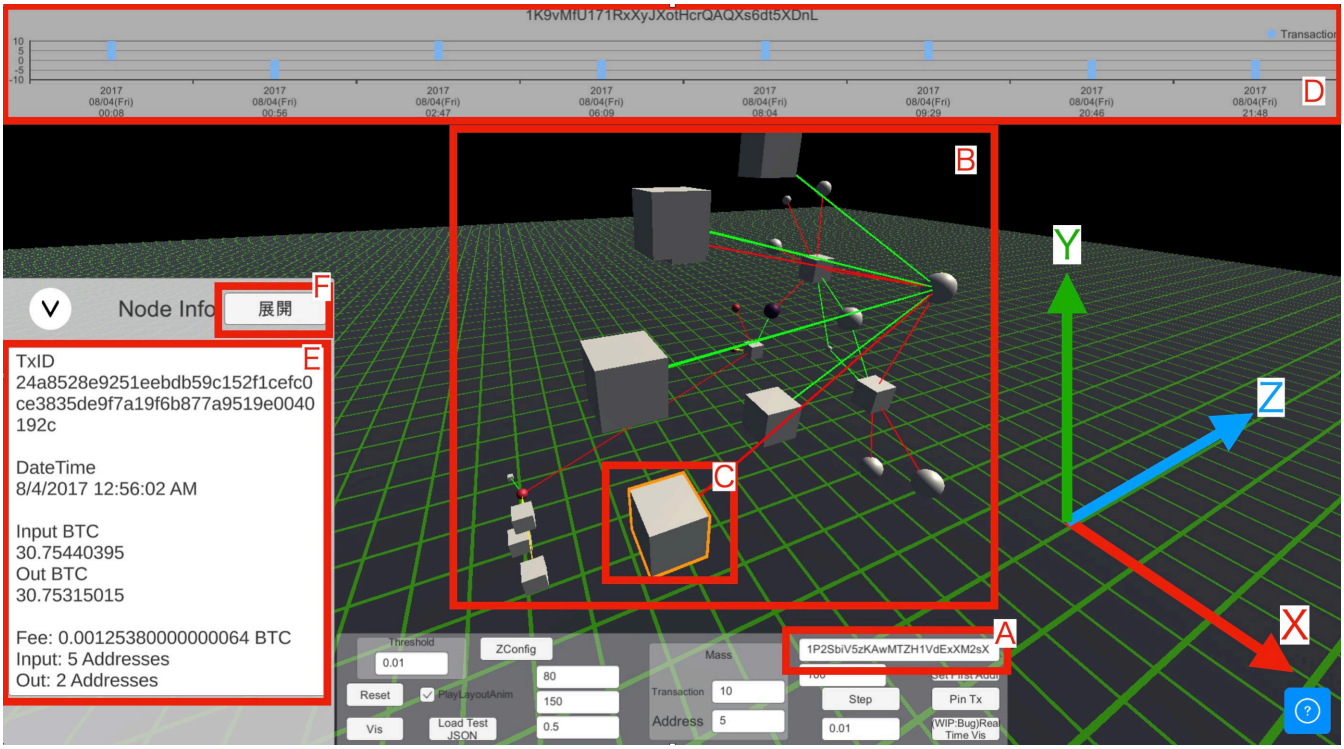

図 4 提案手法による可視化例

る Bitcoin アドレスを分析した結果を述べる．なお，提案手法による可視化では視点を自由に変更することができるが，本章で説明する可視化結果の図については，左側が時間的に古く，右脇に行くほど新しい時間のトランザクションが表示されるように視点の向きを調整している．

6.1 事例 1: WannaCry

WannaCry は McAfee 社のセキュリティレポート [1] によると，2015 年 5 月に複数の組織での感染が確認されており，身代金の送金手段として以下のビットコインアドレスのうちいずれかを表示する．

- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

図 5 は，上記アドレスのうち 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw を可視化した画面である．画面左側には，ランサムウェアのアドレスに対して多数の送金トランザクションがあり，画面右側には，ランサムウェアのアドレスから別のアドレスに送金していることが分かる．

トランザクションのタイミングに注目するために，可視化画面を俯瞰視点 (時間の Z 軸を横軸にした視点) に変更すると図 6 のようになる．なお，図中の日時情報は，4.1 節で述べた機能により調べた結果を記入している．図 6 を見ると 2017 年の 5 月中旬から頻繁に Bitcoin を受け取っており，約 3 ヶ月後の 8 月 3 日に二回に分けて送金していることが分かる．

図 7 は，残り二つのアドレスについて俯瞰視点で可視化した画面である．どちらの可視化結果も図 6 と類似していることから，同様のタイミングで取引されていることが容易に分かる．また，4.1 節で述べた機能により詳細を確認すると，画面右側に描画されている送金のタイミングは，3 アドレスとも同じ日の 2017 年 8 月 3 日または同日の一時間以内での送金であることが分かる．これらのランサムウェアで使用された 3 アドレスの送金先アドレスはすべて異なるものの，被害者からランサムウェアのアドレスへの送金が開始されたタイミングが近いことや，別のアドレスへの送金タイミングがほとんど合致していることから，これらの異なるアドレスの管理者は同一であると推測することができる．

6.2 事例 2: CryptoWall

CryptoWall は SecureWorks 社のセキュリティレポート [2] によると，少なくとも 2013 年 11 月ごろにその存在が確認されている．当該レポートでは CryptoWall が表示する Bitcoin アドレス 34 個を特定し，これらのアドレスへの着金総額は約 939BTC であったと報告されている．

本節では，以下に示す 5 個のアドレスについて提案手法により可視化した結果を示す．アドレスは上記レポートにより報告されている 34 個のアドレスのうち，着金額が多い上位 5 アドレスを用いた．

- 1CeA899xpo3Fe6DQwZwEkd6vQfRHoLuCJD
- 1M8oK3D2G8ipTy7sCxiatrHC35CpAgmrrw
- 1ApF4XayPo7Mtpe326o3xMnSgrkZo7TCWD

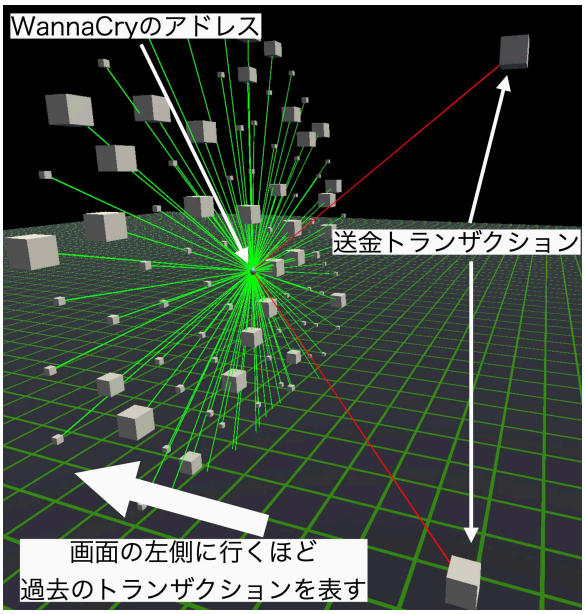

図 5　12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw の可視化画面

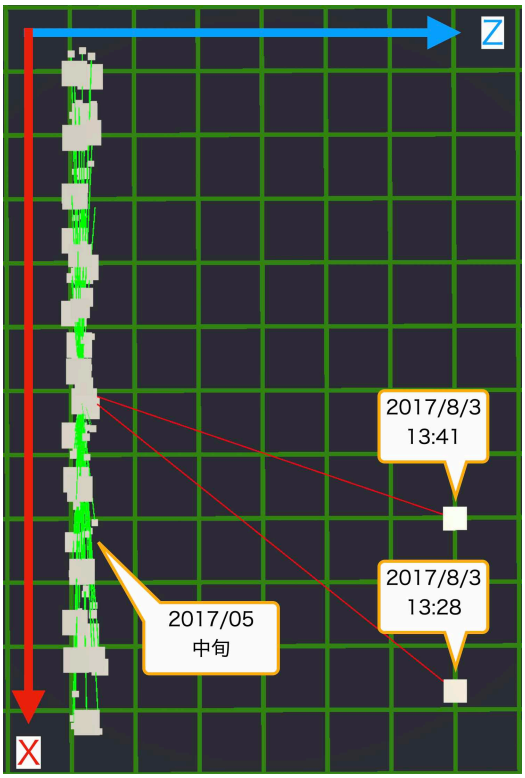

図 6　12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
の可視化画面（俯瞰視点）

- 1HYDwtwtotSedCDCHDcgbRks2a7yPcicwd
- 1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1

図 8 および図 9 に 1CeA... の可視化結果を，図 10 および図 11 に 1EmLL... の可視化結果をそれぞれ示す．なお，残りの 3 アドレスについては可視化結果が 1CeA... の可視化結果（図 8 および図 9）と類似していたため，紙面の都合上省略する．

可視化結果を見ると，いずれのアドレスにおいても，送金を示す赤色または黄色の線で 4 個以上のトランザクションオブジェクトと接続されていることから，送金を 4 回以上行っていることが分かる．また，俯瞰視点からトランザクションオブジェクトを可視化すると（図 9 および図 11），送金しているタイミングはバラバラであることが分かる．以上のことから前節の事例と異なり，被害者からの着金後に間をおいて一括で送金していないことが分かる．

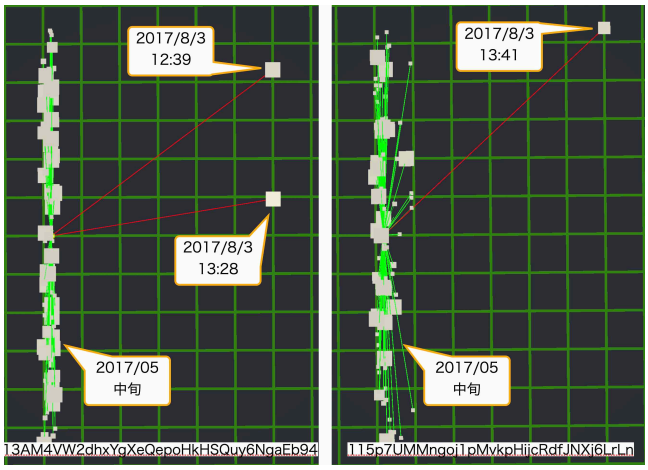

図 7　左が 13AM...，右が 115p...
の可視化画面（俯瞰視点）

次に，1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1（図 10 および図 11）と他のアドレスの可視化結果を比べると，当該アドレスのみ黄色の線でトランザクションと接続されていることが分かる．これにより当該アドレスが送金時に一部の Bitcon を自身のアドレスに送金していることが分かる．そのため，当該アドレスは他アドレスと運用方針に違いがあると推測できる．

最後に，残りの 4 アドレスについて，送金タイミングからアドレス管理者の同一性を確認するために，送金トランザクションの時間を調査した．しかし，4 アドレスはそれぞれ異なる時期に使われており，4 アドレスについて共通する期間内でのトランザクションは存在しなかった．そのため，これら 4 アドレス間で送金タイミングが合致しているトランザクションは存在せず，トランザクションのタイミングにより管理者の同一性の有無を確認することはできなかった．

7. 考察

6.1 節事例 1 のように，提案手法で Bitcoin トランザクションを可視化することにより，送金のタイミングがほぼ同時であることを確認することで送金先の異なるアドレスの管理者が同一人物であることを推測できる場合がある．

このような場合について，提案手法による可視化がアドレスの管理者の推測に有効である．

一方で，6.2 節事例 2 のように時期によって攻撃に用いるアドレスを使い分けられた場合や，被害者から Bitcoin

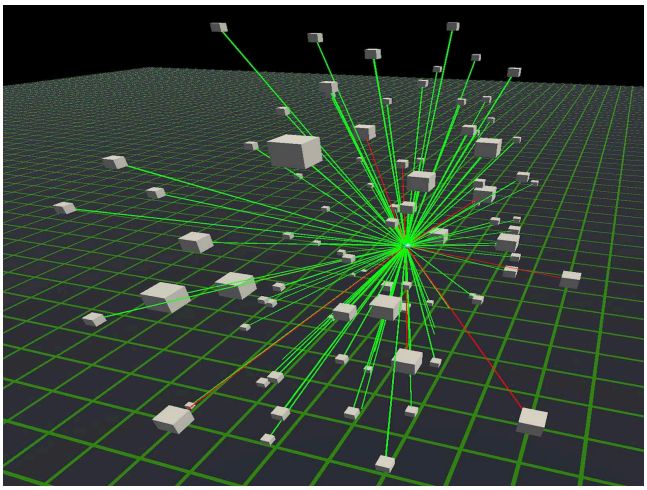

図 8 1CeA899xpo3Fe6DQwZwEkd6vQfRHoLuCJD の可視化画面

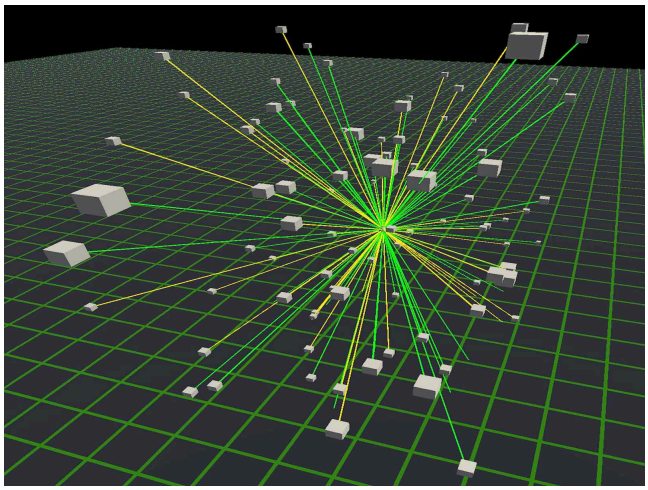

図 10 1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1 の可視化画面

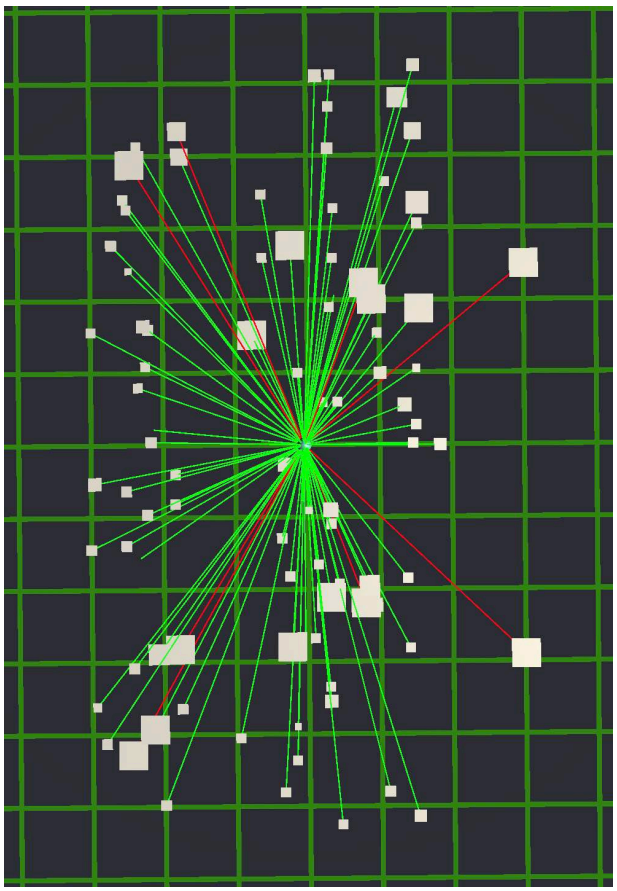

図 9 1CeA899xpo3Fe6DQwZwEkd6vQfRHoLuCJD の可視化画面（俯瞰視点）

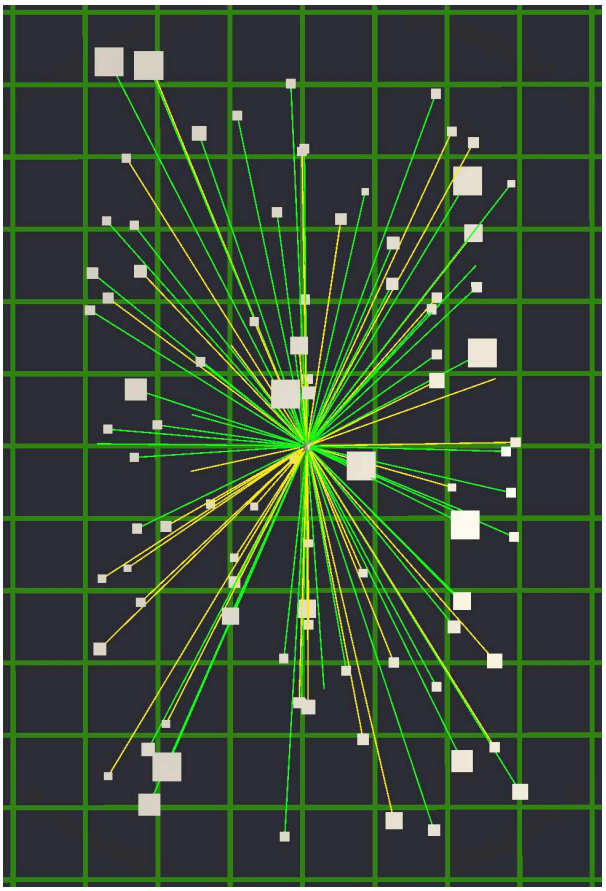

図 11 1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1 の可視化画面（俯瞰視点）

を受け取る度に Bitcoin を別のアドレスに送金する場合は，提案手法による可視化ではアドレス管理者の同一性の推測が困難である．そのため，提案手法を単独で適用するのではなく既存のクラスタリング手法などと組み合わせて解析することが有効であると考えられる．

8. まとめと今後の課題

本稿では，トランザクションのタイミングに着目した可視化手法について提案し，提案手法により複数のアドレスの管理者が同一であることを推測できる事例を示した．

暗号資産の中でも Bitcoin を対象にトランザクションとアドレスの関係を可視化したが，暗号資産の不正な利用は Bitcoin 以外でも行われているため，Bitcoin 以外の暗号資産への手法の適用が課題である．また，暗号資産取引所のように 1 つのアドレスが大量のトランザクションで利用される場合や，ミキシングのような 1 つのトランザクション

に大量のアドレスを含む場合は，描画するオブジェクト数が膨大になるため，これらのアドレスとトランザクションの関係を単純に可視化することは困難である．そのため，必要に応じて適切なクラスタリングを適用することで描画ノード数を減らす手法の提案も課題である．

参考文献

[1] Raj Samani, C. B.: 拡大する WannaCry ランサムウェアの分析，McAfee（オンライン），入手先 ⟨https://blogs.mcafee.jp/wannacry-f851⟩（参照 2020-02-10）.
[2] Dell SecureWorks Counter Threat Unit Threat Intelligence: CryptoWall Ransomware Threat Analysis, SecureWorks, Inc. (online), available from ⟨https://www.secureworks.com/research/cryptowall-ransomware⟩ (accessed 2020-02-16).
[3] 中沢　潔：ダークウェブに関する現状，JETRO, IPA（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000080167.pdf⟩（参照 2020-02-10）.
[4] Paquet-Clouston, M., Haslhofer, B. and Dupont, B.: Ransomware Payments in the Bitcoin Ecosystem, *Workshop on the Economics of Information Security (WEIS)* (2018).
[5] Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Mcroberts, K., Bursztein, E., Levin, J., Levchenko, K., Snoeren, A. C. and Mccoy, D.: Tracking Ransomware End-to-end, *IEEE Symposium on Security and Privacy (S&P)* (2018).
[6] 日本銀行：暗号資産（仮想通貨）とは何ですか？，日本銀行（オンライン），入手先 ⟨https://www.boj.or.jp/announcements/education/oshiete/money/c27.htm/⟩（参照 2020-02-10）.
[7] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, Technical report (2008).
[8] : CoinMarketCap, - (online), available from ⟨https://coinmarketcap.com/⟩ (accessed 2020-02-16).
[9] 廣澤龍典，上原哲太郎：ビットコインのミキシングにおける資金移動の分析，研究報告コンピュータセキュリティ (CSEC)， Vol. 2018, No. 9, pp. 1–8 (2018).
[10] Kalodner, H., Möser, M., Lee, K., Goldfeder, S., Plattner, M., Chator, A. and Narayanan, A.: BlockSci: Design and applications of a blockchain analysis platform, *USENIX Security Symposium*, pp. 2721–2738 (2020).
[11] Kalodner, H., Möser, M., Lee, K., Goldfeder, S., Plattner, M., Chator, A. and Narayanan, A.: BlockSci, Princeton University (online), available from ⟨https://github.com/citp/BlockSci⟩ (accessed 2020-02-16).
[12] Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T. and Capkun, S.: Evaluating user privacy in bitcoin, *International Conference on Financial Cryptography and Data Security*, pp. 34–51 (2013).
[13] Reid, F. and Harrigan, M.: An Analysis of Anonymity in the Bitcoin System, *Security and Privacy in Social Networks*, Springer, pp. 197–223 (2013).
[14] Ron, D. and Shamir, A.: Quantitative Analysis of the Full Bitcoin Transaction Graph, *International Conference on Financial Cryptography and Data Security*, pp. 6–24 (2013).
[15] Tovanich, N., Heulot, N., Fekete, J.-D. and Isenberg, P.: Visualization of blockchain data: a systematic review, *IEEE Transactions on Visualization and Computer Graphics* (2019).
[16] Haslhofer, B., Karl, R. and Filtz, E.: O Bitcoin Where Art Thou? Insight into Large-Scale Transaction Graphs., *SEMANTiCS (Posters, Demos)* (2016).
[17] Bistarelli, S. and Santini, F.: Go with the-bitcoin-flow, with visual analytics, *International Conference on Availability, Reliability and Security*, pp. 1–6 (2017).
[18] : DailyBlockchain, - (online), available from ⟨https://dailyblockchain.github.io/⟩ (accessed 2020-02-10).
[19] McGinn, D., Birch, D., Akroyd, D., Molina-Solana, M., Guo, Y. and Knottenbelt, W. J.: Visualizing dynamic bitcoin transaction patterns, *Big Data*, Vol. 4, No. 2, pp. 109–119 (2016).
[20] Unity Technologies: Unity Real-Time Development Platform, , available from ⟨https://unity.com/⟩ (accessed 2020-02-10).
[21] Django Software Foundation: The web framework for perfectionists with deadlines, , available from ⟨https://www.djangoproject.com/⟩ (accessed 2020-02-10).