2M-02

仮想通貨送金のモデル化と責任ある市場の創出

全珠美[1]　水野貴之[2]　Claudio J. Tessone[3]
総合研究大学院大学[1]　国立情報学研究所[2]　University of Zurich[3]

１．はじめに

仮想通貨の匿名性は利用者を仮想通貨市場に招く特徴でもあるが，仮想通貨を用いた違法行為がおこなわれる原因にもなる．仮想通貨を用いた違法行為は代表的にマネーロンダリング，ダークマーケットでの取引，ランサムウェア攻撃，ポンジ詐欺などがある．これらの違法行為は仮想通貨市場の健全性を脅威するため，各国の政府や仮想通貨関連企業は規制の強化と共に違法な取引やユーザーを検知する研究も活発におこなっている．

関連研究は匿名性を解消することが中心になる．一般的な匿名性を解消する研究[1,2]や詐欺やマネーロンダリングなど，特定の取引を追跡する研究[3,4,5]などがある．だが，実際の仮想通貨への規制は既存の金融市場の規制をそのまま適用しようとする傾向が強く，研究などで使われているデータを上手く活用していないと思われる．

本研究では，匿名性と分散処理など，仮想通貨の主な特徴を守りながら違法行為を防ぐ方法を提案する．中央の制御ではなく各ユーザー単位での制御による違法行為の防止が目的だ．違法行為の防止は違法行為をおこなうユーザー(違法なユーザー)への仮想通貨の流れを制御することによって実現しようとする．主なアイデアは 1）各ユーザーの近接ユーザーから違法なユーザーまでの最短経路長を把握，2）各ユーザーが最短経路長の長い近接ユーザーを選択して送金することによって，3）違法なユーザーまで流れる仮想通貨の総量を減らすことである．そのため，代表的な仮想通貨であるビットコインの取引データを利用し，ビットコインユーザーネットワークを分析する．そしてビットコインの流れをモデル化し，ユーザー単位の流れの制御で違法なユーザーまで流れるビットコインの総量を抑制することが出来るかを検証する．

２．データセット

2009 年から 2018 年までのビットコインの取引データセットを用いて分析をおこなう．データセットには各取引 ID と日時，ユーザーアドレスが含まれている．ビットコインの場合，同じユーザーが多数のアドレスを使うことができるため，アドレスをクラスタリングする．同じトランザクションに含まれるアドレス(multi-input)とトランザクション後のおつりを送るアドレス(change address)を同じユーザーのアドレスとする手法を利用し，ユーザー単位のデータにまとめる．本研究では違法なユーザーを区分するため，ラベル付きユーザーデータを収集する．違法なユーザーは関連研究[3]のデータ，仮想通貨関連コミュニティ[6]で収集したデータ，関連記事，違法行為報告サイト[7]などで公開されたデータを使う．本研究では SilkRoad (1,010)，HYIP とポンジ詐欺関連(22,916)，ギャンブルサイト関連(194,664)，ランサムウェア関連(130)ユーザーを違法なユーザーと定義する．また違法なユーザーと比較するため，一般ユーザーとして Exchange(8,584)，Service 関連 (433,462)ユーザーにもラベルを付けて分析に使う．

３．ビットコインユーザーネットワークの分析

一般ユーザーから違法なユーザーまでの最短経路長を計る前に，どれ位の時間単位で最短経路長のデータを更新するべきかを決めるため，ビットコイン取引ネットワークの時間変化を分析する必要がある．ユーザー間の送金関係をリンクとし，2009 年から 2018 年までのネットワークのリンクベクトルを作って，１年・６ヶ月・1 ヶ月の時間単位でコサイン類似度を計算する．その結果，月単位のコサイン類似度は平均 0.3 程度で，コサイン類似度が０に近い他の時間単位に比べ相関を持っていることが分かる．本研究では月単位でのデータ更新を想定する．そして一月前・後の相関に差があった 2017 年１月の取引データを用いてもっと詳しい分析を続く．

次はユーザーコミュニティの特徴を見る．2017 年１月の取引ネットワークを Infomap でコミュニティ検出する(重み付き方向付きネットワーク)．各コミュニティに含まれている一般ユーザーと違法なユーザーよる各コミュニティの構成を確認する．600 以上のユーザーがいるコミュニティ間の相関係数は 0.027(p-value=0.648)でユーザーの特徴によってコミュニティが分断されていることが分かる．またネットワークの時間相関に差がある二組のネットワークのユーザー構成を，ネットワークのリンクをランダムに組み合わせをし，F 値とカイ二乗検定で検証

Modeling cryptocurrency transfers and creating responsible markets
1.Joomi Jun ・The Graduate University for Advanced Studies, SOKENDAI
2.Takayuki Mizuno・National Institute of Informatics
3.Claudio J. Tessone ・University of Zurich

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.

する．コサイン類似度が高い(0.64)2016 年 12 月と 2017 年 1 月のコミュニティ，コサイン類似度が低い(0.28)2017 年 1 月と 2017 年 2 月のコミュニティのユーザー構成はあまり変わらない．

最短経路長を計算するネットワークは全ての送金関係のリンクではなく，各ユーザーが送金する上位二つのリンクに限定して，主な送金関係のみに注目する．主な送金関係ネットワークで 2017 年 1 月を基準に一ヶ月前後のネットワークとの中心性を算出すると，高い次数のユーザーでは，次数について強い時間相関が観測される．つまりコミュニティを連携しているハブは変わらないことが分かる．主な送金関係ネットワークで全てのユーザー(source)について，違法なユーザー(target)までの最短経路長を調査する．2017 年 1 月の場合，61.4%の繋がっているユーザーの平均最短経路長は 3.237 リンク，最長の最短経路長は 38 リンクである．

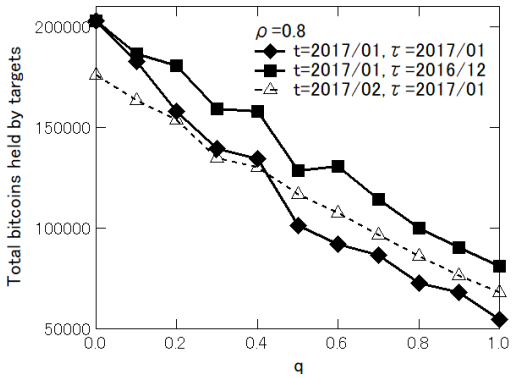
４．送金のモデル化と送金制御のシミュレーション

主な送金関係ネットワークでのビットコインの流れはページランクを応用してモデル化する．[式１]はビットコイン送金のモデルで，source から送金されたビットコインがネットワークで流れて，target に到着するビットコインの量を観測できる．V_tは時刻 t におけるノード(ユーザー)の Bitcoin の流動資産ベクトル，Aはノード i からノード j への送金行列，ρは貯蓄率でノードが保有する流動資産を貯蓄する割合，C^t は Source を起点のする送金ベクトルを表す．

$$V_{t+1} = (1-\rho)AV_t + C \quad [式１]$$

時期 t における最長の最短距離長からノード i の最短経距離長を引いた値を target への送金リスク r と設定して使用する．この送金モデルを用いて，時間 t におけるユーザー i の送金先を送金リスク r が低い方を選択して送金する時，target まで到達するビットコインの量が減少するのかをシミュレーションで調査する．またこの送金制御を導入するユーザーの導入率 q をおいて，導入率の変化による target へ送金されるビットコイン量の減少程度も調査する．シミュレーションは 2016 年 12 月，2017 年 1 月，2017 年２月の取引ネットワークを用いておこなう．

まず 2017 年 1 月の送金リスクを用いて同じ時期のネットワークで，導入率 q を調整しながらビットコインを流すと，q と比例して target に溜まるビットコインの量が減少する．30%のユーザーがこの制御を受け入れて送金すると target へ溜まるビットコインの量も 30%くらい減少する．その次は 2016 年 12 月の送金リスクを用いて 2017 年 1 月のネットワークに適用，そして 2017 年 1 月の送金リスクを用いて 2017 年 2 月のネットワークに適用してシミュレーションをおこなう．二つのシミュレーションでネットワークコサイン類似度が違う場合の効果も観察できる．コサイン類似度が違う場合も target への送金量の抑制効果の差はあまりなく，時間によるネットワークの変化があっても一ヶ月前の送金リスクデータを用いて十分に制御効果が得られることが分かる．



[図１]シミュレーション結果

５．まとめ

本研究ではビットコインのユーザーネットワークを用いて，一般ユーザーから違法なユーザーへ流れるビットコイン量を減らすことによってビットコインネットワークの健全性を確保する方法を提案する．そのため時期 t における各ユーザーから違法なユーザーまでの最短経路長を計算し，その距離が長い方を選んで送金するアイデアを実際のビットコインネットワークを用いてシミュレーションする．その結果，各ユーザーが違法なユーザーまでの最短経路長が長い方に送金することに参加することによってビットコインの流れを制御する効果が得られることが確認できる．即ち，中央制御ではなく，各ユーザーの参加により責任のあるビットコイン，仮想通貨市場の創出ができると期待する．

[参考文献]

[1] Yin, H.S., Langenheldt, K.C., Harlev, M.A., Mukkamala, R.R., Vatrapu, R.: Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. J. Manag. Inf. Syst. 36(1), 37-73 (2019)

[2] Lin, Y., Wu, P., Hsu, C., Tu, I., Liao, S.: An evaluation of bitcoin address classification based on transaction history summarization. In: IEEE International Conference on Blockchain and Cryptocurrency, 14-17, pp. 302-310 (2019)

[3] M. Bartoletti, B. Pes and S. Serusi, "Data Mining for Detecting Bitcoin Ponzi Schemes," 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 2018, pp. 75-84.

[4] Prado-Romero, M.A., Doerr, C., Gago-Alonso, A.: Discovering bitcoin mixing using anomaly detection. In: Mendoza, M., Velast´ın, S. (eds.) CIARP 2017. LNCS, vol.10657, pp. 534-541. Springer, Cham (2018).

[5] Ranshous, S., et al.: Exchange pattern mining in the bitcoin transaction directed hypergraph. In: Brenner, M., et al. (eds.) FC 2017. LNCS, vol. 10323, pp. 248-263.Springer, Cham (2017).

[6] https://bitcointalk.org

[7] https://www.bitcoinwhoswho.com/

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.