5ZH-06

Bitcoin資金洗浄サービスUniJoinについての調査

大杉　遼†　　吉浦　紀晃†
埼玉大学大学院理工学研究科数理電子情報専攻†

1. はじめに

近年では電子決済技術の向上に伴いキャッシュレス化が進んでいる．インターネット上にのみ流通する仮想通貨の１種である Bitcoin[1]は，口座としての役割を果たす Bitcoin アドレスの取得が容易であり，電子署名とブロックチェーンによる安全性を備えているため，広く用いられている．

一方で，Bitcoin はその匿名性の高さから，犯罪者によって悪用されるケースも少なくない．地下市場の不正な取引によって得た Bitcoin を現実の通貨に交換する方法の一つとして，取引所で交換する方法がある．取引所で現実の通貨に交換する際には，個人情報の提示が必要になるため，取引所での取引において Bitcoin アドレスと個人を結び付けることが可能である．そのため，犯罪者は自身の特定を防ぐための方法として資金洗浄サービスを利用することが考えられる．資金洗浄サービスは，利用者から受け取った Bitcoin を本来の送金元が分からないように別の Bitcoin アドレスへの払い戻しを行うサービスであるため，資金洗浄サービスを経由した Bitcoin の追跡は困難である．

2. 研究の目的

資金洗浄サービスはユーザの所持する Bitcoin の追跡を困難にするため,ユーザが不正な取引により入手したBitcoinを資金洗浄する可能性が考えられる．

そこで,本研究では実際に資金洗浄サービスUnijoin[2]を利用したデータを元に資金洗浄が行われたユーザの入金元アドレスから,返金先アドレス候補を取得する.その後,得られた候補に対し,条件付けをすることで絞り込むことを目的とする．

Investigation on UniJoin, the Bitcoin money laundering service
Ryo Osugi†, Noriaki Yoshiura†
Department of Information and Computer Sciences, Saitama University†

3. Unijoinについて

Unijoin は,分散型資金洗浄サイトの一つである.Unijoin では,CoinJoin[3]と呼ばれる洗浄方法を使用している.トランザクションには,複数の入力と出力を指定できる.一つのトランザクションに多数の入力と多数の出力を設定し,トランザクションを行う.こうした多対多のトランザクションを複数回繰り返すことで,Bitcoin の追跡を困難にしている．

実際にUnijoinに入金し,返金を受け取ったデータを元に観察を行った結果,Unijoin の内部構造について想定できることを示す．

入金用のBitcoinアドレスは,利用者から受け取った金額をそのまま洗浄用と思われる多対多のトランザクションに全額送金される形で入力として参加する.ユーザへの返金用の Bitcoin アドレスは,洗浄用と思われる多対多のトランザクションの出力のうちの一つのBitcoinアドレスから,返金を受け取る.この際,差額の埋め合わせとして,おつり用と思われる Bitcoin アドレスも返金の際のトランザクションに参加している.また,多対多の取引に参加する Bitcoin アドレスは,基本的に１度の受け取りのトランザクションと,一度の送金のトランザクションにしか参加しない．

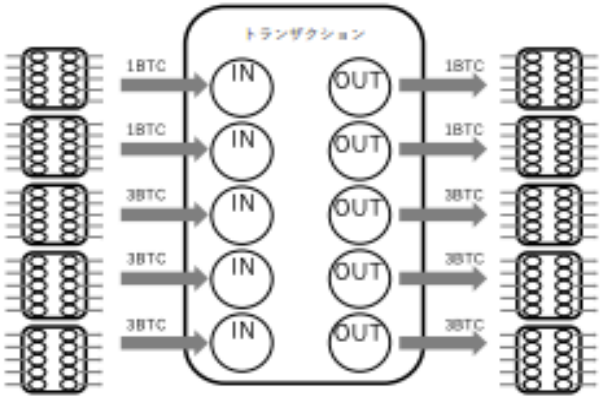

図 1:CoinJoin のモデル

Copyright ©2024 Information Processing Society of Japan.
All Rights Reserved.

4. 返金先アドレス候補群の取得

実際にUnijoinに入金し,返金を受け取ったデータを用いて,入金元 Bitcoin アドレスからのトランザクションを追跡し,返金先アドレス候補群を取得する.Unijoinの返金までの遅延時間は72時間である.返金までの多対多の洗浄用のトランザクションは何度も行われる.そのため,返金先アドレスの候補は膨大な数になってしまう.単純にトランザクションを追跡すると,返金を受け取った後の取引までも膨大に追跡しなければならない.

よって本研究では,一つのアドレスについて,3回以上のトランザクションに参加しているものに関しては,そのアドレスから派生するトランザクションは追跡をしないものとする.

5. 絞り込みの条件

取得した返金先アドレス候補は膨大であるため,Unijoin の保証しているパラメータを元に絞り込みを行う.

まず,Unijoin の利用には,取引手数料が入金額の1から3%の範囲で必要になる.この条件を元に,入金額から手数料を引いた範囲に収まるものが,返金先のアドレスが受け取る額になる.

また,洗浄用の多対多のトランザクションと返金用のトランザクションを区別するため,返金のトランザクションの送金先は,1つか2つの場合に限るものとする.

6. 実験

6.1 プログラム

全てのトランザクションを手作業で追跡することは困難であるため,作業を自動化するためのプログラムを作成した.

BlockStream.com[4]の API を利用し,トランザクションのデータを取得する.API のアクセスには制限があるため,API の利用回数を可能な限り減らすようにプログラムを設計する.

また,本実験では,返金までの時間を 5 時間と設定し,探索を行った.

6.2 結果

プログラムによる探索の結果,返金先アドレス候補として,3724個のアドレスを取得した.

この取得したアドレスに対して,洗浄用の多対多のトランザクションと返金用のトランザクションを区別するために,送金先の数による絞り込みを行った.その結果,3724 個のアドレスは 20 個に絞り込むことができた.さらに,取引手数料による絞り込みを行ったところ,1 個に絞り込むことができ,それは正しい返金先アドレスであった.

7. 考察

本実験では,資金洗浄サービスの一つである Unijoin の構造を利用し,追跡するトランザクションを制限して API の利用回数を出来る限り減らし,返金先アドレス候補を取得した.また,取得した返金先アドレス候補に条件付けを行うことで絞り込みをし,結果からその絞り込みは有効であることが示せた.しかし,本実験は返金までの時間を 5 時間と設定したため,実際にはより多くのアドレスが返金先アドレス候補として取得され,返金先アドレスをただ一つに絞り込めるとは限らないだろう.また,返金先アドレスの指定可能数は 1 から 8 個であり,本実験では返金先アドレスを 1 つと限定して行ったため,本実験で取得した返金先アドレスの候補に対して,Bitcoin の額の総和で入金先アドレスと複数の返金先アドレスを結びつける手法を検討する必要がある.

8. おわりに

本研究では Unijoin における返金先アドレス候補を取得し,取得したアドレスに対し絞り込みを行った.実験結果から,Unijoin における返金先アドレスの絞り込みは実験の手法で有効であることが示せた.

しかし,返金までの最大遅延時間時間までに設定した場合や,返金先のアドレスを複数に設定した場合について,検討や実験をする必要がある.

参考文献

[1] Satoshi Nakamoto: “Bitcoin: A Peer-to-Peer Electronic Cash System”,2008.

[2] Unijoin, available from <https://unijoin.io/>(accessed 2023-11-15).

[3] gmaxwell, Bitcoin Forum, “CoinJoin: Bitcoin privacy for the real world”,2018.

[4] blockstream.info,available from <https://blockstream.info/> (accessed 2023-11-15)

[5] 佐藤 大河, 吉浦 紀晃: “分散型 Bitcoin 資金洗浄サービスの出金先アドレスの検出と絞り込み”, 情報処理学会第84回全国大会 , 2022

Copyright ©2024 Information Processing Society of Japan.
All Rights Reserved.