# Análise do impacto do uso de Mixers no Clustering H1

**Maria Rita Vieira Souza**[1], **Ivan da Silva Sendin**[1]

[1]Faculdade de Computação – Universidade Federal de Uberlândia (UFU)
Av. João Naves de Ávila, n° 2121, CEP 38.400-902 – Uberlândia – MG – Brasil

{mariarvsouza,sendin}@ufu.br

***Resumo.*** *A análise forense do Bitcoin tem como objetivo a detecção de crimes e a identificação dos criminosos usando as informações presentes na Blockchain. Para isso, um método amplamente empregado é o clustering baseado na H1, que auxilia na identificação dos responsáveis pelos endereços publicamente registrados na rede. Contudo, a aplicação de mixers, ferramentas usadas no processo de lavagem de dinheiro para mascarar o rastro financeiro, invalida a premissa dessa heurística e gera clusters incorretos de entidades. Dessa forma, este trabalho visa analisar e mensurar o impacto do uso de mixers nos resultados obtidos pela H1 e, consequentemente, na precisão dessas investigações.*

***Abstract.*** *Bitcoin forensics aims to detect crimes and identify criminals using information present on the Blockchain. For this purpose, a widely employed method is clustering based on the H1 heuristic, which helps identify those responsible for the addresses publicly registered on the network. However, the application of mixers, tools used in money laundering to mask financial trails, invalidates the premise of this heuristic and generates incorrect clusters of entities. Therefore, this work aims to analyze and measure the impact of using mixers on the results obtained by the H1 heuristic and, consequently, on the accuracy of these investigations.*

## 1. Introdução

O Bitcoin é uma moeda digital descentralizada que utiliza a tecnologia *peer-to-peer* (P2P) para operar sem uma autoridade central, garantindo transparência, pseudoanonimato e acessibilidade [Nakamoto 2009]. Esse ambiente chama a atenção pelo seu potencial de criar um ecossistema financeiro digital globalizado e descentralizado, pois oferece custos reduzidos de transações e facilidade nos pagamentos internacionais [Patsakis et al. 2024]. Todavia, a ausência de uma autoridade central de controle, o uso avançado de criptografia, a facilidade de uso, a acessibilidade, a relativa anonimidade e a independência de fronteiras ou legislação [van Wegberg et al. 2018], conferem ao Bitcoin uma confiabilidade que, paradoxalmente, pode ser usada como aliada para atividades ilícitas, como lavagem de dinheiro, extorsão via *ransomware* e comércio de produtos ilícitos.

Nessas circunstâncias, uma etapa crítica das atividades criminosas é o *cashing out* [Patsakis et al. 2024], processo que é essencialmente a lavagem de dinheiro -visa eliminar o rastro deixado na *Blockchain* para encobrir a origem dos ativos e dificultar a rastreabilidade das operações. Contudo, esse aparente anonimato do Bitcoin, que contribuiu para sua popularização em atividades ilegais, é ilusório, pois essa moeda oferece, na realidade,

pseudoanonimato, já que, embora os endereços não possuam as identidades dos usuários explícita e propriamente ditas, as transações e seus dados estão registrados na *Blockchain*, o que permite a condução de análises para reconstruir as trajetórias criminosas, mesmo com o uso de técnicas avançadas para aumentar o anonimato [Sendin et al. 2024].

Nesse cenário, surgem os *mixers*, que são usados nessas tentativas de mascarar o caminho deixado na *Blockchain* e, simplificadamente, funcionam reunindo as moedas de vários usuários e, em seguida, redistribuindo-as de uma forma que quebra o vínculo entre os endereços originais e os de destino [Schnoering and Vazirgiannis 2023, Patsakis et al. 2024]. Tendo isso em vista, o presente trabalho foca no impacto dessas ferramentas sobre a Heurística de Múltiplas Entradas (H1), comumente usada no processo de *clustering* de endereços. O objetivo é demonstrar e mensurar como o uso de *mixers* como o Wasabi e o Joinmarket invalidam essa premissa, provocando fusões drásticas de entidades e, consequentemente, comprometendo a integridade das investigações na *Blockchain*.

## 2. Fundamentação teórica

### 2.1. O ecossistema do Bitcoin

Como o Bitcoin opera sem uma autoridade central, a gestão das transações e a emissão de novos ativos é realizada coletivamente pela rede, evitando um único ponto de falha, e todas as transações são registradas publicamente na *Blockchain*, características que tornam o Bitcoin uma alternativa robusta e confiável [Nakamoto 2009]. Para manter esse sistema, os Bitcoins são criados através da mineração, um processo competitivo de alto custo computacional que produz o *proof-of-work*, essencial para o consenso na rede, e que é responsável por atualizar a *Blockchain*, trazendo novas moedas à cadeia [Antonopoulos 2014].

Nesse cenário, usuários de Bitcoin possuem endereços que são essencialmente chaves públicas, que lhes permitem provar a posse de moedas na rede [Antonopoulos 2014]. O controle efetivo desses endereços manifesta-se na gestão dos UTXOs (*Unspent Transaction Outputs*), que são os saldos não gastos de transações anteriores e servem como entradas para novas transações e, a fim de transferir determinado valor para novos destinatários, o usuário deve criar uma transação e assiná-la com a chave privada correspondente àquele endereço de Bitcoins de origem. Note que, embora esses UTXOs sejam vinculados a endereços individuais, na prática, múltiplos endereços podem ser geridos por uma única entidade controladora, até mesmo um usuário individual.

### 2.2. Mixers

Os *mixers* são serviços que recebem e misturam Bitcoins de múltiplos usuários para quebrar o vínculo entre os endereços de origem e de destino, bem como dificultar o rastreamento de recursos ilícitos. Eles são especialmente desafiadores de analisar, uma vez que operam como ”caixas-pretas”e, além dessas camadas de abstração que ocultam o fluxo dos fundos, seus proprietários muitas vezes não estão dispostos a cooperar com as autoridades competentes [Zola et al. 2025], tornando o rastreamento dos fluxos na *Blockchain* excepcionalmente difícil.

Nesse contexto, o método do *CoinJoin*, implementado nos *mixers* presentes neste trabalho, envolve uma colaboração na qual os indivíduos combinam as entradas de suas transações em uma única e grande transação. De forma simplificada, $x$ pessoas se unem

para fazer uma transação com $x$ UTXOs de valores iguais e criam $x$ saídas, porém embaralhando sua ordem, de forma que não é possível identificar qual usuário está relacionado a qual saída [Sendin et al. 2024]. Esse processo, além de ofuscar o rastro dos ativos digitais, também cria inúmeros vínculos na *Blockchain* entre participantes que não têm uma conexão real, o que confunde muitas heurísticas de análises existentes, como a heurística das entradas múltiplas, tratada na Seção 2.4, a qual assume que todos os endereços de entrada em uma transação são controlados pela mesma entidade [Schnoering and Vazirgiannis 2023].

### 2.2.1. JoinMarket

O JoinMarket é um *mixer* que permite aos usuários, denominados *takers*, coordenarem rodadas *CoinJoin*, baseando-se em ofertas fornecidas pelos *makers*, participantes passivos que definem as denominações em que estão dispostos a participar, uma taxa e a contribuição para a taxa de rede. Dessa forma, o *taker* seleciona essas ofertas e se responsabiliza por construir a transação, incluindo os TXOs (*Transaction Outputs*) de todos os *makers* que concordaram. No fim, cada participante recebe uma saída *post-mix* na denominação definida e, potencialmente, um troco [Schnoering and Vazirgiannis 2023].

### 2.2.2. Wasabi

O Wasabi é um *mixer* de carteira Bitcoin que, inicialmente nas versões 1.0 e 1.1, baseou-se no protocolo ZeroLink, uma implementação do Chaumian CoinJoin, permitindo realizar um *round* sem a necessidade de confiar no coordenador. O Wasabi 1.0 utilizava uma denominação única próxima de 0.1 BTC, enquanto a versão 1.1 introduziu níveis de mistura. Além disso, com o objetivo de minimizar ou eliminar o troco, otimizando a privacidade, foi criado também o Wasabi 2.0, versão que implementou o protocolo WabiSabi [Ficsór et al. 2021], permitindo valores variáveis e um conjunto de denominações fixas. Assim, a versão mais recente permite que uma denominação seja escolhida várias vezes por um mesmo participante [Schnoering and Vazirgiannis 2023].

## 2.3. Clustering

Uma transação é normalmente composta de um ou mais UTXOs que são controlados por uma entidade que tem participação nas transações que envolvem esses endereços, então elas não são definidas como uma propriedade da conta. Por exemplo, no caso de um serviço de carteira que possui conhecimento das chaves privadas dos endereços de seus clientes, tal serviço é considerado o controlador desses endereços, embora os fundos pertençam a vários usuários distintos [Meiklejohn et al. 2013].

Nesse contexto, o *clustering* surge como processo para organizar os endereços do ecossistema do Bitcoin em subconjuntos distintos e mutuamente exclusivos, os *clusters*, cada qual denota uma entidade final, ou seja, eles representam um controlador/usuário único. Esse processo parte de um estado no qual cada endereço forma um grupo individual e faz fusões entre *clusters* para montar as entidades finais, fazendo uso de heurísticas fundamentadas nos comportamentos dessas entidades [Schnoering et al. 2024].

### 2.4. Heurística H1

A Heurística de Múltiplas Entradas é uma das principais ferramentas de análise da *Blockchain*, e, justamente devido à sua importância, é identificada como H1. A H1 é usada no processo de *clustering* de transações na tentativa de identificar as entidades que controlam os endereços presentes na *Blockchain*, e o seu mecanismo de funcionamento considera que, se uma transação possui duas ou mais chaves públicas como entrada, elas são controladas pelo mesmo usuário, já que o remetente da transação precisa conhecer a chave privada de assinatura pertencente a cada chave pública de entrada. Assim, se uma $tx1$ tem ao menos um endereço em comum com uma $tx2$ e essa $tx2$ tem ao menos um endereço em comum com uma $tx3$, os endereços de entrada de $tx1, tx2$ e $tx3$ pertencem à mesma entidade, ou seja, os efeitos dessa heurística são transitivos e se estendem além das entradas de uma determinada transação [Sendin et al. 2024]. Exemplos de uso da H1 podem ser encontrados em [Meiklejohn et al. 2013, Harrigan and Fretter 2016]

Essa heurística, no entanto, provoca falsos positivos e é invalidada quando utilizada no contexto de transações *CoinJoin*, já que esse tipo de transação une os endereços de diferentes indivíduos para a mixagem, com o objetivo de impossibilitar a ligação de cada usuário com seus fundos. Sob condições normais, o comportamento típico de um agrupamento usando a H1 é incremental, mas o uso dos *mixers*, combinado ao caráter unificador da H1, faz com que o *clustering* dessas transações resulte em raras fusões drásticas no ecossistema [Harrigan and Fretter 2016] e integre muitos usuários em *superclusters,* o que implica em uma análise equivocada no processo de *clustering*, pois esses grupos passam a englobar endereços de diversas entidades distintas sob o que deveria ser a identidade de um único usuário.

## 3. Trabalhos relacionados

Diante dos desafios impostos pelos *mixers* à rastreabilidade de fundos na *Blockchain*, a comunidade científica direcionou esforços à compreensão e identificação dessas ferramentas. O JoinMarket, criado por Chris Belcher em 2015, foi mapeado em trabalhos como [Möser and Böhme 2017], que conduziu o primeiro estudo empírico em grande escala sobre esse serviço, enquanto o Wasabi, lançado oficialmente em 2018 com o protocolo ZeroLink e aprimorado para o Wasabi 2.0 com o protocolo WabiSabi [Ficsór et al. 2021] em 2022, foi abordado em trabalhos como [Stockinger et al. 2021] e [Stütz et al. 2023], os quais focaram no rastreio do volume financeiro que flui dos *mixers* e mapeamento do comportamento dos usuários. Esse rastreamento do Wasabi foi aprimorado, por fim, em [Schnoering and Vazirgiannis 2023], que estabelece heurísticas de detecção atualizadas para JoinMarket e Wasabi 2.0, fornecendo uma base metodológica direta para a identificação de *mixers* nesse trabalho.

Já a Heurística de Múltiplas Entradas teve sua ideia mencionada inicialmente no *white paper* do Bitcoin [Nakamoto 2009] e desenvolvida nos trabalhos [Androulaki et al. 2013] e [Meiklejohn et al. 2013]. Também, ela foi formalizada em [Schnoering et al. 2024], que citou esse impacto das transações *CoinJoin* e retirou-as do seu processo de *clustering*. Além disso, a H1 é amplamente utilizada nas análises da *Blockchain*: [Gong et al. 2022] quantificou sua precisão por meio de uma simulação da rede, [Harrigan and Fretter 2016] analisou as razões práticas que a tornam tão eficaz (mencionando o efeito dos *mixers*) e [Möser and Narayanan 2022] ignorou essas ferra-

mentas de mixagem intencionalmente no seu processo de *clustering*. Como visto, esses trabalhos reconheceram o impacto desses serviços na H1, mas não buscaram mensurá-lo.

## 4. Metodologia

O presente estudo propõe uma análise que visa mensurar o impacto dos *mixer*s na integridade da H1, umas das heurísticas utilizadas no processo de *clustering*. Com isso em vista, a abordagem tomada pode ser dividida em duas seções principais, a elaboração de uma estratégia para identificação das transações de *mixer*, e a realização do *clustering* com duas premissas diferentes: a primeira sendo aplicar o *clustering* independentemente de a transação ser *CoinJoin* ou não, o que permite que os *super-clusters* se formem, e a segunda evitar o agrupamento das transações *CoinJoin*. Para este trabalho, foram selecionadas as transações dos três primeiros meses de 2025, sobre as quais foram aplicas as heurísticas de identificação dos *mixers* e, sobre as transações com pelo menos dois inputs, o processo de *clustering* foi feito, já que a heurística H1 não tem efeito em transações com um ou menos endereços de entrada. Esse recorte de tempo é suficiente para a observação do fenômeno descrito, mas ainda garante a viabilidade da execução dos algoritmos dentro de um ambiente computacional com recursos limitados.

### 4.1. Detecção de transações de mixer

Para a detecção das transações de *mixers*, adotamos heurísticas baseadas em um estudo de suas características e na análise técnica presente em [Schnoering and Vazirgiannis 2023]. Como a ausência de um conjunto de dados público e verificado de transações *CoinJoin* dificulta a análise quantitativa direta da eficácia do método, a escolha das heurísticas de [Schnoering and Vazirgiannis 2023] fundamenta-se em sua construção técnica, feita a partir do estudo do código-fonte *open source* de cada protocolo, e na demonstração de sua consistência por meio do alinhamento entre os picos de volume das transações e eventos reais *off-chain*.

Além disso, essas heurísticas são amplamente aplicadas na literatura recente, sendo empregadas para a extração de transações em [Svenda et al. 2026], como base para o agrupamento de endereços em [Schnoering et al. 2024] e na etapa de limpeza dos dados na estruturação dos grafos de transações em [Schnoering and Vazirgiannis 2024]. Ainda, esse método também serviu como base para [Ziegler et al. 2025], onde foi introduzida uma regra complementar para eliminar falsos positivos em transações anteriores ao lançamento do Wasabi 2.0, ocorrido oficialmente em 2022.

Dessa forma, foram definidas as variáveis operacionais na Tabela 1. Note que os scripts de entrada/saída representam conjuntos de assinaturas criptográficas usadas para desbloquer os fundos dos UTXOs, ou seja, a contagem desses scripts distintos é utilizada para estimar o número de usuários independentes que colaboram em uma transação. Ainda, com base nessas definições, foram adotadas as heurísticas para identificação de transações de JoinMarket e Wasabi apresentadas na Tabela 2.

| Símbolo | Definição |
|---|---|
| $\|\Delta_{in}\|$ | Número total de entradas na transação. |
| $\|\Delta_{out}\|$ | Número total de saídas na transação. |
| $n$ | Número estimado de participantes. |
| $n_{scripts,in}$ | Número de *scripts* de entrada distintos. |
| $n_{scripts,out}$ | Número de *scripts* de saída distintos. |
| $n_{change}$ | Número de saídas de troco (*change outputs*). |
| $n_{post-mix}$ | Número de saídas de valor padronizado pós-mistura. |

**Tabela 1. Definição das variáveis utilizadas nas heurísticas**

| Mixer | Heurísticas de Detecção |
|---|---|
| **JoinMarket** | **1.** O número de participantes deve ser maior ou igual à metade do número de saídas: $n \geq \frac{\|\Delta_{out}\|}{2}$. |
| | **2.** O número de participantes deve respeitar o intervalo entre 3 e o total de scripts de entrada distintos: $3 \leq n \leq n_{scripts,in}$. |
| **Wasabi** | **1.** Utilização de endereços P2WPKH nativos (prefixo "bc1"), baseados no *Segregated Witness* (SegWit) [Todd et al. 2015], alteração no protocolo do Bitcoin que separa os dados de assinatura do corpo da transação. |
| | **2.** Todas as saídas protegidas por scripts distintos: $\|\Delta_{out}\| = n_{scripts,out}$. |
| | **3.** Emprego de denominações fixas e $n_{change} \leq n \leq n_{post-mix}$. O código verifica se a contagem de qualquer valor de saída (exceto o troco) é pelo menos 2 e se $n_{change} \leq n$. |
| | **4.** O valor de todas as saídas deve ser superior a zero, respeitando o limite mínimo estipulado pelo protocolo. |
| | **5.** O número de entradas deve ser maior ou igual ao de participantes. |

**Tabela 2. Heurísticas de detecção de transações para JoinMarket e Wasabi**

### 4.2. Clustering

A fim de isolar a influência dos *mixers*, o agrupamento foi executado em duas etapas distintas sobre o mesmo conjunto de dados, utilizando um algoritmo de união de conjuntos disjuntos para a aplicação da H1 [Sendin et al. 2024]. O método baseia-se nas seguintes variáveis operacionais: $TX$ representa o conjunto de transações com pelo menos duas entradas, $tx.inputs$ é o conjunto de endereços de entrada de $tx$, $Clusters$ a partição de entidades formadas, $enderecos$ o conjunto acumulado de endereços correlacionados e $M(tx)$ um predicado booleano que indica se a transação $tx$ provém de um *mixer*. O procedimento está definido nos Algoritmos 1 e 2, conforme os cenários:

**Cenário 1** implementado pelo Algoritmo 1, aplica a heurística H1 a todas as transações dentro da janela de tempo, com o objetivo de simular uma análise convencional que ignora a existência dos *mixers*, permitindo a formação dos *super-clusters*;

**Cenário 2** implementado pelo Algoritmo 2, trata as transações classificadas como *CoinJoin* como exceções à regra e não as agrupa, evitando o colapso de múltiplas entidades independentes em um único grupo.

A aplicação desse método resultou na construção de dois grafos de entidades distintos sobre a mesma base de dados. Neles, cada nó é um conjunto de endereços e representa um *cluster* consolidado, isto é, uma entidade, enquanto cada aresta representa a existência de pelo menos uma transferência de valor entre os dois nós que liga.

**Algoritmo 1** *Clustering* H1 com *mixers*

**Input:** Conjunto de transações $TX$
$Clusters \leftarrow \emptyset$
**for** $tx \in TX$ **do**
  $enderecos \leftarrow tx.inputs$
  **for** $c \in Clusters$ **do**
    **if** $enderecos \cap c \neq \emptyset$ **then**
      $enderecos \leftarrow enderecos \cup c$
      Remove $c$ de $Clusters$
    **end if**
  **end for**
  Insere $enderecos$ em $Clusters$
**end for**
**return** $Clusters$

**Algoritmo 2** *Clustering* H1 sem *mixers*

**Input:** Conjunto $TX$, Predicado $\mathcal{M}(tx)$
$Clusters \leftarrow \emptyset$
**for** $tx \in TX$ **do**
  **if** $\mathcal{M}(tx)$ **then continue**
  $enderecos \leftarrow tx.inputs$
  **for** $c \in Clusters$ **do**
    **if** $enderecos \cap c \neq \emptyset$ **then**
      $enderecos \leftarrow enderecos \cup c$
      Remove $c$ de $Clusters$
    **end if**
  **end for**
  Insere $enderecos$ em $Clusters$
**end for**
**return** $Clusters$

## 5. Resultados

### 5.1. Detecção de transações de mixer

Após a aplicação das heurísticas de detecção de Wasabi e Joinmarket, foram coletadas um total de 34.955.822 transações para o primeiro trimestre de 2025, e, entre elas, foram extraídas no total 4.251 transações de JoinMarket e 10.634 transações de Wasabi, conforme detalhado na Tabela 3. Além disso, a partir desses dados, foi feita uma análise sobre as ocorrências de cada *mixer* por dia, como mostrado na Figura 1, o que resultou em uma média de aproximadamente 118,16 transações diárias de Wasabi e 47,23 de JoinMarket.

| Transações / Mês | JoinMarket | Wasabi | Transações 1 ou menos inputs | Total |
|---|---|---|---|---|
| Janeiro | 2.007 | 3.753 | 9.116.951 | 11.559.973 |
| Fevereiro | 1.084 | 2.716 | 9.412.745 | 11.369.846 |
| Março | 1.160 | 4.165 | 10.157.474 | 12.026.003 |
| **Total** | 4.251 | 10.634 | 28.687.170 | 34.955.822 |

**Tabela 3. Quantidade de transações por mês para o primeiro trimestre de 2025**

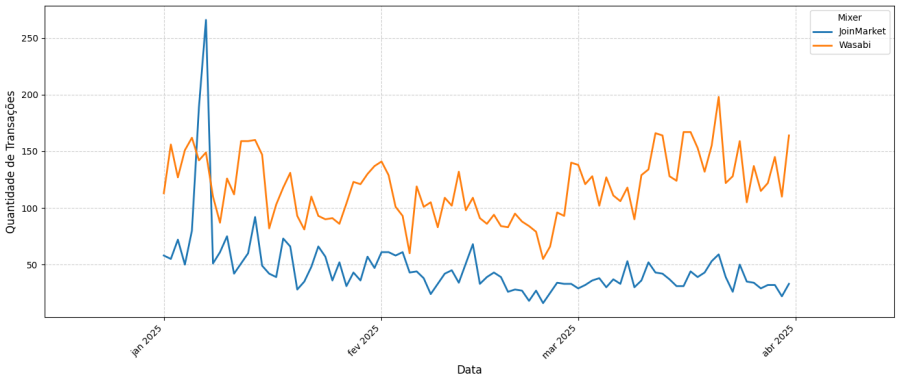
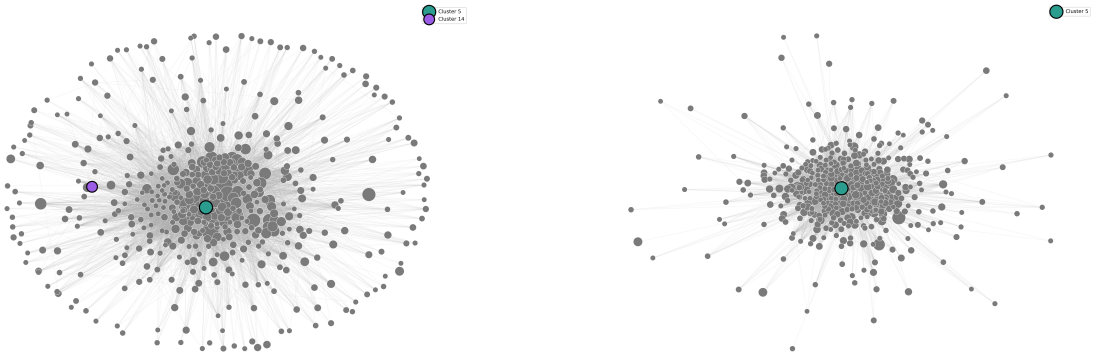



**Figura 1. Quantidade de transações diárias por mixer**

### 5.2. Clustering

Nesta Seção, são apresentados os resultados obtidos pela aplicação da H1 sobre os dados coletados nos dois cenários descritos na Seção 4.2. Após a remoção das transações com um ou menos inputs, o conjunto restante engloba 76.059.223 inputs no total (média de 11.49 por transação). E, conforme mostrado na Seção 5.1, dentre o total analisado, 10.634 transações eram de Wasabi e 4.251 eram de Joinmarket, o que é um volume pequeno, mas suficiente para causar um impacto na topologia dos *clusters*, ilustrada na Figura 2.



(a) Cenário com mixers (b) Cenário sem mixers

**Figura 2. Comparação da topologia dos 500 maiores clusters nos dois cenários**

O processo de formação dos *super-clusters* estudado no presente trabalho fica evidente tanto ao analisar visualmente a topologia dos *clusters* na Figura 2 anterior, quanto ao observar os dados na Tabela 4, pois, ao evitar agrupar as transações de *mixer*, ocorreu um salto na quantidade de *clusters* e arestas (transações que ligam os grupos), revelando que centenas de milhares de entidades haviam sido indevidamente agrupadas.

| **Métrica** | **Clusters com Mixers** | **Clusters sem Mixers** |
|---|---|---|
| Número de clusters | 5.485.809 | 6.246.669 |
| Número de arestas | 10.641.683 | 151.868.038 |
| Média de transações por cluster | 1,21 | 1,06 |
| Máximo de transações em um cluster | 1.396.779 | 1.396.490 |
| Média do tamanho dos clusters | 4,53 | 3,98 |
| Tamanho máximo de um cluster | 913.340 | 913.340 |
| Número de clusters de tamanho 1 | 3.438.736 | 4.210.676 |
| Número de clusters de tamanho $> 100$ | 11.571 | 9.833 |
| Clusters com envolvimento Wasabi | 9.391 | 10.284 |
| Clusters com envolvimento Joinmarket | 2.067 | 2.361 |

**Tabela 4. Comparação das métricas dos clusters entre os dois cenários**

Além disso, no histograma da Figura 3 de distribuição do tamanho dos *clusters* montados, é possível observar que, embora as distribuições sejam semelhantes, a exclusão dos mixers implicou em uma quantidade maior de *clusters* de tamanhos menores, enquanto diminuiu o número de grupos gigantes. Ou seja, excluir os *mixers* do processo de *clustering* fragmentou os *super-clusters* que tinham sido formados no Cenário 1.

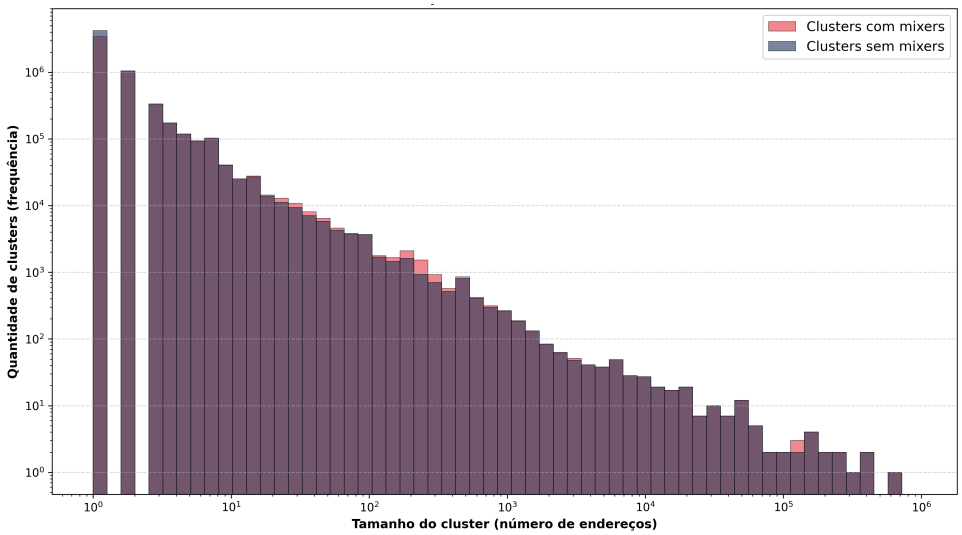



**Figura 3. Distribuição do tamanho dos clusters nos dois cenários**

Para investigar esse processo, coletamos os dados dos 5 maiores *clusters* formados sob ambas as premissas, representados na Tabela 5. Note que as métricas ”Interações com Wasabi”e ”Interações com Joinmarket”contabilizam o número de entidades distintas que atuaram como remetentes em transações de *mixer*. Dentre esse grupo, o *Cluster* 5 ilustra bem o efeito estudado, já que inicialmente agrupava 289.993 endereços, tendo tido 237 interações com Wasabi e 1.777 com Joinmarket, e, após a remoção das transações *CoinJoin*, se separou de 863 nós que haviam sido erroneamente fundidos a ele.

| Cluster | Métrica | Com mixers | Sem mixers |
|---|---|---|---|
| **1** | Tamanho | 913.340 | 913.340 |
| | Total de transações | 11.038 | 11.038 |
| | Interações com Wasabi | 0 | 0 |
| | Interações com JoinMarket | 0 | 0 |
| **2** | Tamanho | 576.763 | 576.757 |
| | Total de transações | 9.630 | 9.628 |
| | Interações com Wasabi | 0 | 0 |
| | Interações com JoinMarket | 6 | 4 |
| **3** | Tamanho | 433.914 | 433.914 |
| | Total de transações | 18.236 | 18.236 |
| | Interações com Wasabi | 0 | 0 |
| | Interações com JoinMarket | 0 | 0 |
| **4** | Tamanho | 387.088 | 387.088 |
| | Total de transações | 41.414 | 41.414 |
| | Interações com Wasabi | 0 | 0 |
| | Interações com JoinMarket | 0 | 0 |
| **5** | Tamanho | 289.993 | 289.130 |
| | Total de transações | 1.396.779 | 1.396.490 |
| | Interações com Wasabi | 237 | 220 |
| | Interações com JoinMarket | 1.777 | 1.722 |

**Tabela 5. Comparação de métricas dos 5 maiores clusters nos dois cenários**

Além disso, um impacto mais agressivo do efeito estudado foi evidenciado no

*Cluster* 14 do cenário de *clustering* com *mixers*, cujos dados são apresentados na Tabela 6. Nessa etapa, ele englobava 131.843 endereços, com 565 interações com Wasabi, mas, ao executar o Cenário 2, esse agrupamento colapsou e ele desapareceu do ranking de maiores *clusters* (mesmo quando observando os 20 maiores), mostrando que esse grupo imenso tinha sido formado pelos falsos positivos causados pelo efeitos das ferramentas de *mixagem* na H1.

| **Cluster 14** | |
|---|---|
| Tamanho | 131.843 |
| Total de transações | 593 |
| Interações com Wasabi | 565 |
| Interações com JoinMarket | 0 |

**Tabela 6. Dados do Cluster 14 no cenário de clustering com mixers (Cenário 1)**

## 6. Conclusões

O ecossistema das criptomoedas é um ambiente complexo, cujo pseudoanonimato atrai agentes que buscam acobertar atividades ilícitas através do *cashing out* por meio do uso dos *mixers*, processo que fica evidente na *Blockchain*. Nesse cenário, a Heurística de Múltiplas Entradas (H1), que é primordial na análise forense para auxiliar na identificação dos participantes de atividades ilegais, é comprometida pela presença de transações oriundas de *mixers*, que causam a formação de *super-clusters* que não refletem as entidades reais da rede. Este trabalho expôs empiricamente esse efeito em uma amostra de transações coletadas no intervalo de tempo entre janeiro e março de 2025, demonstrando que remover as transações de *mixers* do processo de *clustering* causa a fragmentação desses grupos gigantes, como demonstrado pelos *Clusters* 5 e 14 na Seção 5.2.

Trabalhos futuros poderiam envolver a ampliação da janela temporal do estudo como forma de demonstrar o impacto contínuo dessas ferramentas, a inclusão de uma diversidade maior de serviços *mixer*, tanto isolados como em conjunto, e a mensuração da eficácia da análise. Além disso, a análise aprofundada das características estruturais dos *clusters* que interagem ativamente com os *mixers* abre uma oportunidade para o desenvolvimento de novas técnicas para detecção de *mixers*, ainda não identificadas na literatura.

## Agradecimentos

O presente trabalho foi realizado com o apoio do Programa de Educação Tutorial (PET), do grupo PET Computação, financiado pela Secretaria de Educação Superior do Ministério da Educação (SESu/MEC) e pelo Fundo Nacional de Desenvolvimento da Educação (FNDE).

## Referências

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., and Capkun, S. (2013). Evaluating user privacy in bitcoin. In Sadeghi, A.-R., editor, *Financial Cryptography and Data Security*, pages 34–51, Berlin, Heidelberg. Springer Berlin Heidelberg.

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Crypto-Currencies*. O'Reilly Media, Inc., 1st edition.

Ficsór, , Seres, I., Kogman, Y., and Ontivero, L. (2021). Wabisabi: Centrally coordinated coinjoins with variable amounts. *Cryptoeconomic Systems*.

Gong, Y., Chow, K.-P., Ting, H.-F., and Yiu, S.-M. (2022). Analyzing the error rates of bitcoin clustering heuristics. In *IFIP International Conference on Digital Forensics*, pages 187–205. Springer.

Harrigan, M. and Fretter, C. (2016). The unreasonable effectiveness of address clustering. In *2016 Intl IEEE Conferences on Ubiquitous Intelligence amp; Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, page 368–373. IEEE.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 127–140, New York, NY, USA. ACM.

Möser, M. and Narayanan, A. (2022). Resurrecting address clustering in bitcoin. In Eyal, I. and Garay, J., editors, *Financial Cryptography and Data Security*, pages 386–403, Cham. Springer International Publishing.

Möser, M. and Böhme, R. (2017). The price of anonymity: Empirical evidence from a market for bitcoin anonymization. *Journal of Cybersecurity*, 3.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system.

Patsakis, C., Politou, E., Alepis, E., and Hernandez-Castro, J. (2024). Cashing out crypto: state of practice in ransom payments. *International Journal of Information Security*, 23:699–712.

Schnoering, H., Porthaux, P., and Vazirgiannis, M. (2024). Assessing the efficacy of heuristic-based address clustering for bitcoin. *ArXiv*, abs/2403.00523.

Schnoering, H. and Vazirgiannis, M. (2023). Heuristics for detecting coinjoin transactions on the bitcoin blockchain. *ArXiv*, abs/2311.12491.

Schnoering, H. and Vazirgiannis, M. (2024). Bitcoin research with a transaction graph dataset.

Sendin, I. d. S., Miani, R. S., and Ribeiro, P. H. R. (2024). *Análise Forense aplicada ao Bitcoin*, chapter 4, pages 132–179. Minicursos do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais.

Stockinger, J., Haslhofer, B., Moreno-Sanchez, P., and Maffei, M. (2021). Pinpointing and measuring wasabi and samourai coinjoins in the bitcoin ecosystem. *ArXiv*, abs/2109.10229.

Stütz, R., Stockinger, J., Moreno-Sanchez, P., Haslhofer, B., and Maffei, M. (2023). Adoption and actual privacy of decentralized coinjoin implementations in bitcoin. In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, AFT '22, page 254–267, New York, NY, USA. Association for Computing Machinery.

Svenda, P., Gavenda, J., Mavroudis, V., and Hicks, C. (2026). Coinjoin ecosystem insights for wasabi 1.x, wasabi 2.x and whirlpool coordinator-based privacy mixers. *Proceedings on Privacy Enhancing Technologies*, 2026:557–592.

Todd, P., Wuille, P., and Johnson, J. (2015). Bip 141: Segregated witness (consensus layer). `https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki`.

van Wegberg, R., Oerlemans, J. J., and van Deventer, O. (2018). Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25:419–435.

Ziegler, M. H., Nowostawski, M., and Katt, B. (2025). A similarity measure for linking coinjoin output spenders. *Journal of Cybersecurity and Privacy*, 5(4).

Zola, F., Medina, J. A., Venturi, A., and Orduna, R. (2025). Topological analysis of mixer activities in the bitcoin network. *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–5.