Um Estudo Sobre o Misterioso e Arriscado Mundo dos Misturadores de Criptomoedas

Rodolfo da Silva Costa[1], **Rostand Costa**[2]

[1]Centro de Informática (CI) – Universidade Federal da Paraíba (UFPB)
R. dos Escoteiros, s/n – Mangabeira, João Pessoa – PB – Brasil

[2]Laboratório de Aplicações de Vídeo Digital (LAVID) – Universidade Federal da Paraíba (UFPB)
R. dos Escoteiros, s/n – Mangabeira, João Pessoa – PB – Brasil

rodolfo.informatica@gmail.com, rostand@lavid.ufpb.br

Abstract. *The new paradigm that emerged with cryptocurrencies in the last decade allows higher transparency of the amounts involved in a specific digital financial asset and allows that all transactions executed can also be visualized. To ensure anonymity, a significant number of cryptocurrency users have tried to hide the origin of their digital assets. In order to cope with this demand, new specialized services, such as cryptocurrency mixers or tumblers, have emerged. In this paper, we present a study on how these services work and evaluate their dynamics and efficacy on unlinking the origin from the destination wallets. Preliminary results point to a high risk business model that moves enormous amounts of money and is debatable from an ethics point of view.*

Resumo. *O novo paradigma que emergiu com as criptomoedas na última década permite uma maior transparência nas grandezas envolvidas em um determinado ativo financeiro digital e possibilita que todas as transações realizadas possam ser visualizadas. Para garantir o anonimato, uma quantidade expressiva de usuários de criptomoedas tem buscado esconder a origem de seus ativos digitais. Para atender tal demanda, surgiram serviços especializados, chamados cryptocurrency mixers (ou tumblers). O objetivo deste trabalho é realizar um estudo acerca do funcionamento de tais serviços para avaliar a sua dinâmica de funcionamento e sua eficácia na desvinculação da carteira de origem com a carteira de destino. Os resultados preliminares apontam para um negócio de alto risco e que movimenta valores bilionários através de uma ética discutível.*

1. Introdução

Surge em 2008 uma nova proposta de moeda eletrônica que viria para revolucionar a forma como valores monetários podem ser transferidos. Com o artigo intitulado *Bitcoin: Um sistema ponto-a-ponto de dinheiro eletrônico*, [Nakamoto 2008] descreve um "sistema de pagamento eletrônico baseado em provas criptográficas ao invés da confiança mútua, permitindo quaisquer duas partes dispostas transacionarem diretamente entre si sem a necessidade da intermediação de uma terceira parte". Utilizando o sistema apresentado, torna-se possível realizar transações financeiras através da internet, sem a necessidade de um banco ou qualquer outro intermediador.

Nakamoto propôs um livro caixa público e compartilhado que viria a chamar-se *Blockchain*. Este é utilizado para registrar de forma pública todas as transações entre as partes, representadas por endereços de carteira. Nestas transações, é possível identificar quais moedas foram transferidas de uma conta para outra. Desta forma, protegendo o sistema contra adulteração de contas, gastos duplos ou criação de novos ativos.

Esse novo paradigma permite transparência nas grandezas envolvidas em um determinado ativo financeiro digital. Por concepção, a blockchain permite que qualquer um possa analisar todas as transações já realizadas no sistema, além de consultar o saldo que cada carteira contém e qualquer outra relação que possa existir entre os endereços de carteiras.

O fortalecimento e o surgimento destas novas moedas estavam ocorrendo para além do mercado financeiro tradicional, deixando governos sem a arrecadação de impostos. Mas o uso de exchanges, onde é possível trocar moedas convencionais por moedas digitais, permitiu aos países realizarem a cobrança de tais impostos. Uma das primeiras iniciativas norte americanas de taxação das criptomoedas ocorreu em novembro de 2017 [1], quando o governo "verificou que a quantidade das declarações no imposto de renda não se alinhava com a popularidade emergente das moedas digitais".

A Receita Federal Brasileira, em 31 de Outubro de 2018, anunciou que exigirá das corretoras declarações mensais de todas as operações de vendas de criptomoedas[2]. Outros países também estão iniciando processos no sentido de cercear o anonimato das blockchains, a China [3], onde órgãos reguladores da internet "propõem que todas as operações com a ferramenta (blockchain) realizadas no país sejam identificadas".

Para auxiliar nessa regulação, governos e empresas necessitam de ferramentas que forneçam condições de analisar as blockchains e identificar transações e indivíduos. Surge então um mercado de desenvolvimento dessas ferramentas capazes de colaborar não apenas com questões de fiscais mas também no combate ao crime. Por outro lado, na perspectiva de recuperar a característica de privacidade desejada na origem da Bitcoin, nasce um tipo de serviço de troca e embaralhamento de criptomoedas chamado de *cryptocurrency mixers* ou *cryptocurrency tumblers*.

Nesse cenário, encontramos um ambiente polarizado onde um grupo de instituições buscam identificar os usuários de criptomoedas e o outro grupo busca garantir a privacidade e o anonimato dos mesmos. Sendo assim, o objetivo desta pesquisa é realizar uma análise do funcionamento dos serviços de mixagem de Bitcoins que buscam anular as ferramentas de análise das blockchains. Os objetivos específicos desta primeira fase são avaliar a eficiência destes mecanismos para apagar os rastros de origem e movimentação das moedas, os possíveis riscos envolvidos no serviço e quais as motivações para uso dos mesmos.

Durante o desenvolvimento da pesquisa, foram executados experimentos usando

[1] "Coinbase ordered to give the IRS data on users trading more than $20,000". https://techcrunch.com/2017/11/29/coinbase-internal-revenue-service-taxation/.

[2] "Receita aperta fiscalização no uso de criptomoedas". https://economia.estadao.com.br/noticias/mercados,receita-aperta-fiscalizacao-no-uso-de-criptomoedas,70002575506.

[3] "Operações com blockchain deixarão de ser anônimas na china". https://meiobit.com/391950/china-blockchain-regulacao-fim-anonimato/.

quatro diferentes serviços de mixagem de Bitcoins, nos quais foram rastreados os caminhos que as moedas percorreram e suas transações dentro das reservas das mixers. Descobriu-se uma gigantesca quantidade de moedas circulando pelas carteiras destes serviços e alguns riscos inerentes a sua utilização. Apesar das evidências encontradas nesta investigação, o segmento milionário das misturadoras continua quase que completamente ignorado pela academia. Isso explica a existência de poucos artigos científicos sobre o tema.

O presente documento está estruturado de forma que na Seção 2 é apresentado o funcionamento básico dos *mixers* de criptomoedas. Na Seção 3, é detalhado como os experimentos foram realizados, enquanto que a análise e discussão dos resultados é feita na Seção 4. Na Seção 5 apontamos alguns trabalhos relacionados com a privacidade do Bitcoin, os quais foram utilizados como referencial nesta pesquisa. Finalmente, na Seção 6 são apresentadas as nossas considerações finais.

2. Mixers de Criptomoedas

Como discutido em [Böhme et al. 2015], cada Bitcoin individual pode ser facilmente rastreado através de todas as transações nas quais foi usado e, portanto, até o início de sua circulação. Todas as transações de Bitcoin são legíveis por todos em registros armazenados por estruturas de dados amplamente replicadas.

Os serviços de mistura e mescla de criptomoedas funcionam trocando as moedas enviadas de seus clientes por outras moedas que estejam em suas reservas, devolvendo-as, após uma série de operações de transferências coordenadas, em novos endereços de carteira de forma a não possuir relação com a carteira original (Figura 1). O objetivo é fazer com que não seja mais factível identificar o endereço de destino das criptomoedas a partir do endereço de origem. Os mixers, ao custo de uma pequena taxa, prometem garantir a privacidade do detentor de ativos através do embaralhamento da movimentação entre a carteira de origem e a carteira de destino.

Para promover o anonimato para as carteiras finais, os serviços misturadores fornecem ao cliente um endereço temporário de entrada para o qual devem ser enviadas as moedas que serão embaralhadas/trocadas. As interfaces de utilização dos sistemas permitem algumas personalizações de configuração, tais como:

- Dividir o destino das moedas em mais de uma carteira;
- Escolher o tempo de atraso entre o envio e o recebimento das novas moedas;
- Valor da tarifa a ser paga pelo serviço, que pode variar de 0,5% a 5%;

Após o envio das moedas para o endereço de entrada da misturadora, a entidade aguardará o tempo programado para iniciar as transações de devolução das novas moedas. Cada prestador desses serviço utiliza algoritmos próprios para evitar que as moedas sejam retornadas para os proprietários originais. São utilizadas então moedas da reserva da misturadora, as quais foram recebidas de outros clientes ou investidores do serviço.

2.1. Mixers em Operação

Em buscas rápidas na Internet é possível encontrar a oferta de uma série de serviços misturadores de criptomoedas que estão em funcionamento[4]. Cada um deles possui suas

[4]Neste trabalho foram testados e analisados os quatro serviços de mistura mais referenciados: *Bestmixer.io*, *Blender.io*, *Helix Light Grams*, *BTC Blender*.

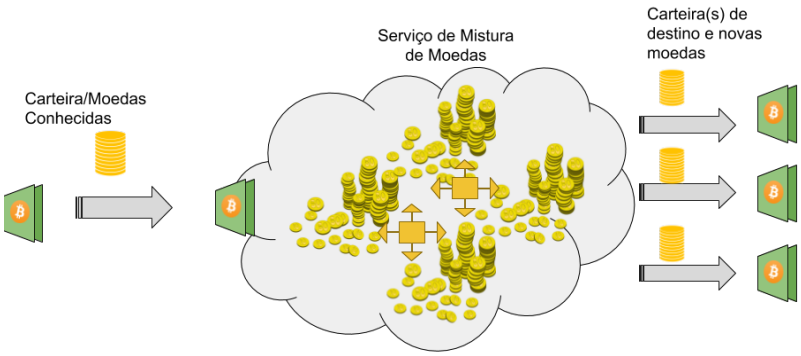

Figura 1. Serviço de Mistura de Moedas

características e particularidades envolvendo tarifas, tipos de moedas e algoritmos de embaralhamento. Muitos podem ser acessados através da Internet aberta, enquanto outros permitem acesso apenas na *deep web*, através da rede TOR, ou ambos.

Dentre as *mixers* pesquisadas, a **Bestmixer** destacou-se por trazer um novo nível de segurança para o segmento. O projeto foi apresentado no fórum Bitcointalk[5] em 16 de Março de 2018, prometendo o máximo de anonimidade para criptomoedas após a mixagem. Na ocasião, seus criadores afirmaram que a maioria dos serviços de mistura existentes anteriormente não garantiam o anonimato das transações e que seria possível identificar qual a carteira de saída a partir da transação de entrada. Eles haveriam disponibilizado para utilização uma ferramenta chamada *CAE-check*[6] ou *Coin Anonymisation Event-check* para comprovação pelos próprios clientes da ineficiência dos serviços.

É fato que após apontar as vulnerabilidades existentes nos mixers e entrar no mercado para fazer concorrência, a Bestmixer iniciou um novo ciclo de serviços mais eficientes em apagar rastros de moedas digitais. A equipe Bestmixer.io afirmou ter encontrado vulnerabilidade nos seguintes serviços existentes à época: Coinmixer.se, Bitmix.biz, Privcoin.io, Cryptomixer.io. Destes, apenas o Coinmixer foi descontinuado, os demais serviços continuam disponíveis após as falhas serem corrigidas.

3. Planejamento de Experimentos: Escopo e Dinâmica

Para este trabalho foram realizados experimentos utilizando mixers de criptomoedas com os objetivos de levantar dados, entender seu funcionamento e descobrir os possíveis riscos envolvidos. Na primeira etapa, realizou-se uma seleção de mixers, onde foram escolhidos 4 serviços, estes foram submetidos a testes de funcionalidades. Os dados resultantes dos testes, foram analisados na blockchain, e os relacionamentos entre as carteiras envolvidas foram rastreados; por fim, ocorreu a análise dos dados.

Durante a etapa de seleção dos serviços[7], foi utilizada uma lista contendo "9 me-

[5]https://bitcointalk.org/index.php?topic= 3140140.0

[6]Nós procuramos a ferramenta para estudos e testes mas a mesma foi removida do endereço web oficial (https://bestmixer.io/en/cae-check), bem como não pode ser encontrada via buscadores da internet. Quando questionados por e-mail sobre a ferramenta *CAE-check* em 27 de Novembro de 2018, os desenvolvedores responderam que "Quase todos os mixers com uma vulnerabilidade que encontramos, consertaram seus sistemas. Removemos essa funcionalidade do nosso site".

[7]Não foram encontrados textos acadêmicos que ranqueiam os serviços dos mixers.

lhores serviços misturadores de Bitcoin" como referência[8]. Apesar do título do texto mencionar nove serviços, o autor lista sete mixers como sendo os "melhores e mais populares": BestMixer, PrivCoin.io, Bitcoin Blender, CryptoMixer, Bitcoin Fog, Blender.io e MixTum.io e outros 3 serviços (Grams Helix, BTC Blender, Coinmixer) foram rotulados como sendo "não aprovados" e de "muito grande risco".

Os experimentos foram realizados com dois dos serviços considerados "melhores e mais populares"[8]: **Bestmixer** e **Blender.io**. Bem como, dois dos considerados de grande risco: **Helix Light Grams** e **BTC Blender**.

3.1. Realizando Transações de Mixagem

A configuração padrão para os testes possui os seguintes parâmetros: 0,001 Bitcoin é enviado para a mixer; as novas moedas são recebidas em 2 novos endereços de carteira; cada uma delas deveria receber um valor próximo a 50% do valor final; a taxa de serviço utilizada é a sugerida pela mixer, mas não superior a 2% do valor enviado; o tempo de atraso entre as confirmação do envio e o recebimento das novas moedas é de 2 horas para cada carteira de destino.

O serviço BTCBlender utilizou por padrão um valor randômico para a tarifa. No caso deste experimento, o valor foi 1%. Já a mixer Helix Light Grams não permitiu configuração da taxa de serviço, fixando o valor em 2,5%.

Os envios foram realizados no período entre 04 de outubro e 16 de novembro de 2018, sendo uma transferência para os serviços Helix Light Grams e BTC Blender e duas transferências para Bestmixer e Blender.io. O resumo pode ser encontrado na Tabela 1.

Tabela 1. Configurações dos experimentos e saldos pós mistura

Data	Mixer	Taxa	Valor Enviado	Total Recebido	Total Consumido	% Consumido
04/10/2018	Bestmixer	1,937%	0,001	0,00096951	0,00003049	3,05%
07/11/2018	Bestmixer	1,933%	0,001	0,00084593	0,00015407	15,41%
31/10/2018	Blender.io	1,35%	0,001	0,0007865	0,0002135	21,35%
16/11/2018	Blender.io	1,35%	0,001	0,0007865	0,0002135	21,35%
31/10/2018	BTCBlender	1%	0,001	0	0,001	100%
31/10/2018	Helix	2,5%	0,001	0	0,001	100%

A etapa seguinte ao processo de testes dos serviços é a análise da blockchain. Nesta etapa analisou-se os endereços das carteiras de entrada das mixers e seguiu-se o fluxo de transações a partir daquele endereço, em busca dos endereços que pertenceriam às reservas do serviço. O caminho inverso também foi rastreado buscando encontrar a origem das novas moedas recebidas.

3.2. Rastreando as Transações de Embaralhamento

O rastreio dos caminhos tomados pelas moedas após a entrada na rede das mixers, assim como o rastreio reverso, a partir da carteira de destino, foi realizada por dois scripts[9], desenvolvidos em Python, utilizando o módulo *blockexplorer* da *api-v1-client-python*[10].

[8]disponível em https://cryptalker.com/best-bitcoin-tumbler/

[9]Disponível para download em: http://bit.ly/mixersscript

[10]Disponível em https://github.com/blockchain/

Para a execução dos scripts são enviados como argumentos de entrada um endereço de carteira **E**, um limite de transações **T** a ser explorado por carteira encontrada, e a quantidade de níveis a ser explorado **N**.

Durante a execução dos scripts, as transações encontradas são varridas na blockchain de forma recursiva, iniciando pela carteira **E**, buscando até **T** transações posteriores, quando varrendo a partir da carteira de entrada da misturadora, e até **T** transações anteriores, quando varrendo a partir das carteiras finais que receberam as novas moedas.

Para cada teste realizado nas mixers, os scripts foram executados três vezes, alterando o argumento de endereço **E** em cada execução. Uma execução para a carteira de entrada da mixer, outras duas execuções com os endereços que enviaram as moedas para a carteira final do cliente.

O valor utilizado por padrão para o parâmetro **T** foi 10. Desta forma, as 10 últimas transações daquela carteira seriam varridas recursivamente até chegar ao nível **N** que, durante as análises, variou entre 8 e 13. Essa variação ocorreu com a finalidade de encontrar endereços pertencentes aos núcleos dos *pools*. A estratégia adotada para chegar ao núcleo foi aumentar gradativamente o valor de **N** até encontrar endereços de carteira que fossem comuns tanto na varredura de entrada, quanto na varredura inversa, de saída.

Os scripts realizam consultas aos endereços na Blockchain à uma velocidade média de 1,15 endereço por segundo. Durante as varreduras chegou-se a números de carteiras variando entre 1.000 e 18.000 endereços. Essa variação está diretamente ligada a quantidade de transações que cada carteira encontrada fez e quantas carteiras foram utilizadas em cada transação.

Como resultado, os scripts criam um registro em documento de texto com valores separados por vírgula (.csv). Nas varreduras de entrada, seu conteúdo é formado pelo **endereço** da carteira encontrada; o seu **nível** ou graus de distância até a carteira de origem do cliente; um campo chamado **para** que registra para quais outros endereços a carteira enviou moedas, a **quantidade de transações** já realizadas pela carteira, a quantidade de BTCs que a carteira já **recebeu**, a quantidade de BTC que a carteira já **enviou** e seu **saldo** atual. Enquanto que as varreduras reversas registram os dados referentes as carteiras que enviaram moedas até o destino.

Os arquivos gerados foram utilizados para análise do funcionamento dos algoritmos das mixers. Grafos foram criados e são apresentados na Seção 4, com o objetivo de facilitar a visualização dos caminhos percorridos pelas moedas quando enviadas para os serviços de mistura e identificar padrões. Sua renderização foi realizada com o software *Cytoscape*[11], uma plataforma de código aberto para visualização de redes complexas e integração com qualquer tipo de atributo de dados.

4. Resultados e Análise

Como dito em [Böhme et al. 2015] os protocolos de mistura geralmente não são públicos, portanto difíceis de terem sua eficiência avaliada. Neste trabalho foram realizados os experimentos com mixers e a análise da blockchain resultante da mixagem. Algumas informações relevantes foram levantadas acerca da dinâmica operacional e do nível de eficiência dos serviços em pauta.

[11] versão 3.7.0 disponível em https://cytoscape.org/

O endereço de entrada dos serviços, apresenta um padrão: o uso de uma carteira com um endereço novo e que não possua nenhuma transação registrada na blockchain. Tal carteira "inicial" terá duas transações após completadas todas as etapas de mistura; i) uma de recebimento do valor depositado pelo cliente e ii) uma de envio para uma (ou mais) carteira(s) seguinte(s), também de posse e escolha da mixer.

Ao consultar na blockchain a carteira de entrada fornecida pelo serviço Helix Light Grams <13jnQqaJ...>[12], imediatamente encontra-se uma diferença para todos os demais serviços: no momento do envio das moedas para o endereço de entrada, a carteira já possuía 23 transações de recebimento, nenhuma de saída.

Os serviços *Bestmixer* e *Blender.io* realizaram a entregas das novas moedas nos endereços previamente configurados. Quanto aos valores devolvidos, são variáveis e uma parcela bem superior à taxa de serviço cobrada na entrada é retirada até a saída. As mixers alertam sobre as taxas de transação inerentes da tecnologia mas não fornecem valores precisos. Na Tabela 1 encontra-se os valores de cada teste.

Em uma constatação inicial, o risco de não devolução das moedas submetidas para embaralhamento é real e foi concretizado durante os testes. Apesar de seguir todas as recomendações estabelecidas, como "Não enviar mais que 1 transação", "Não enviar menos que 0,0001btc" e "não enviar mais que 43btc" etc, o serviço *Helix Light Grams* não devolveu nenhuma quantia para as carteiras de destino. O mesmo ocorreu com o serviço *BTCBlender*. Não há garantias nem a quem reclamar em caso de perda. Em geral são serviços apócrifos e desviculados de qualquer entidade real, física ou jurídica. Apesar disso, o grande volume e o alto valor das transações de embaralhamento sugerem que tal risco tem sido negligenciado por algumas classes de clientes, como pode ser visto na Tabela 4, a qual relaciona um sumário do volume transacionado nas mixers avaliadas.

Para os serviços Bestmixer e Blender.io, os quais concluíram a entrega prometida das moedas submetidas, foi possível efetuar todo o processo de análise da blockchain descrito na seção anterior. Para ambos os casos é possível identificar comportamentos comuns de seus algoritmos. No que tange a eficiência, a partir dos endereços de entrada das moedas não é possível encontrar a carteira de destino fazendo uso dos mecanismo de rastreamento da blockchain. Atualmente, os serviços mantém as moedas de entrada paradas e só as movimentam após as novas moedas serem entregues às carteiras finais dos clientes, desta forma impedido a relação direta entre as moedas de entrada e as de saída. Para as transações testadas no serviço Bestmixer, o tempo de permanência das moedas na carteira de entrada foi, respectivamente, 24h30m e 2h40m enquanto a Blender.io manteve as moedas por 1 dia 21h e 2 dias 18h.

Outro meio de tentar encontrar a carteira de destino a partir do endereço de entrada foi explicado pelos desenvolvedores do Bestmixer [Bestmixer 2018]. Este método foi utilizado pela ferramenta CAE explorando uma falha no algoritmo das mixers em não aleatorizarem o tempo de entrega das novas moedas às carteiras de seus clientes.

Na prática, a ferramenta verificou que as mixers, ao identificarem as transações para a carteira de entrada, aguardavam o número mínimo de confirmações e utilizavam o horário da última confirmação como parâmetro base para buscas de transações com

[12]Por questões de sigilo, os endereços de carteiras serão exibidos truncados, com apenas 8 caracteres iniciais

Tabela 2. Horários de confirmação e entrega

	Bestmixer 04/10/2018	Bestmixer 08/11/2018	Blender.io 31/11 e 01/12	Blender.io 16/11/2018
Horário 3ª Confirmação	11:59:50	00:06:29	22:39:17	15:37:25
Recebimento Carteira 1	13:49:09	01:58:09	00:40:04	17:38:04
Recebimento Carteira 2	15:57:07	04:03:08	00:40:05	19:38:04

valores equivalentes na blockchain, repetindo este mesmo processo em intervalos exatos de uma hora. Desta forma, as novas buscas poderiam revelar o endereço da carteira de destino.

Foi observado nas análises que os serviços Bestmixer e Blender.io aguardam três confirmações da transação de entrada na blockchain para validarem o envio de moedas por parte do cliente. Analisando os horários das terceiras confirmações das transações e dos horários de criação das transações de pagamento, vindas das mixers testadas, é possível identificar que a Bestmixer utiliza uma variável aleatória de tempo para efetuar os pagamentos de cada uma das carteiras de destino, enquanto que a Blender.io demonstra ter a variável de tempo aleatório apenas para a primeira carteira. Os dados podem ser encontrados na Tabela 2.

4.1. Análise do Processo de Embaralhamento

O trabalho de rastrear o caminho percorrido pelas moedas, da entrada nas mixers até o núcleo das redes misturadas e da chegada nas novas carteiras até o núcleo, foi automatizado como descrito na Seção 3.2. A análise dos dados levantados apontam para valores elevados de Bitcoins sendo repassados através dessas redes, carteiras que participam da rede de mais de uma mixer e uma rede complexa de carteiras transacionando entre si.

Tabela 3. 07 carteiras que mais receberam moedas e possuem relações com Bestmixer (Valores em BTC)

#	Endereço	Total Recebido	Total Enviado	Saldo
1	<1NDyJtNT...>	3.677.916,1613	3.666.614,1191	11.302,0423
2	<1N52wHoV...>	1.962.513,6623	1.961.374,6008	1.139,0615
3	<1J37CY8h...>	1.613.947,2360	1.613.221,8376	725,3984
4	<1DEcTtkr...>	919.343,8349	919.177,5658	166,2690
5	<1NYAd6fA...>	399.610,7258	399.375,4699	235,2560
6	<14cQRmVi...>	319.483,1280	319.313,7818	169,3461
7	<32RQLBAM...>	285.918,4089	285.738,1449	180,264

Ao avançar por níveis dentro das reservas das mixers é possível identificar carteiras que aparecem com frequência em centenas de transações e que já movimentaram valores bilionários em criptomoedas. Nas Tabelas 3 e 4 encontram-se dados dos 07 endereços de carteiras identificadas no núcleo das transações de mistura que mais movimentaram criptomoedas.

Nas transações de teste realizadas na Bestmixer, a carteira encontrada com maior destaque em número e volume de transações foi a <1NDyJtNT...>. Esta carteira recebeu suas primeiras moedas em 08 de Agosto de 2017 e em pouco mais de um ano já

movimentou valores acima de 20 bilhões de dólares, assumindo a cotação da CoinMarketCap[13] em 18 de Novembro de 2018, cujo valor da Bitcoin era de $5.594,97. De acordo com esse ranking mostrado na Tabela 3, as 8 primeiras carteira também movimentaram valores bilionários e as demais atingem cifras milionárias.

Tabela 4. 07 carteiras que mais receberam moedas e possuem relações com o Blender.io (Valores em BTC)

#	Endereco	Total Recebido	Total Enviado	Saldo
1	<1Kr6QSyd...>	5.952.280,2888	5.951.392,8943	887,3945
2	<12cgpFdJ...>	4.572.637,4094	4.569.547,8559	3.089,5534
3	<1NDyJtNT...>	3.682.989,1028	3.673.724,1191	9.264,9837
4	<17A16Qma...>	3.065.897,8365	3.058.860,6970	7.037,1396
5	<14wXrm49...>	2.018.062,1586	2.018.062,1586	0,0167
6	<1MEe2meb...>	1.969.409,9391	1.969.409,9391	0,00
7	<1N52wHoV...>	1.963.032,4378	1.961.830,1066	1.202,3312

Na Tabela 4, encontra-se as carteiras que mais movimentaram moedas identificadas nas transações com a Blender.io e o montante transacionado pelas carteiras é ainda maior. O endereço <1Kr6QSyd...>teve sua primeira transação registrada em agosto de 2016 e em dois anos e um mês de existência já movimentou $33 bilhões de dólares americanos em criptomoedas, ainda considerando a cotação de 18 de Novembro.

Um fato observado durante a análise é a existência de uma mesma carteira encontrada no centro das redes de embaralhamento das duas mixers, o endereço <1NDyJtNT...>, uma das carteiras com alto volume e valor de transações. As possibilidades analisadas são que esse endereço pode pertencer a um investidor/apoiador em comum, a uma grande exchange ou a uma combinação dos dois.

Mais um endereço de carteira que faz relação com transações nas duas misturadoras é o <1BestMix...>. Esta carteira pertence ao pool da Bestmixer, e é usada para receber e efetuar transferências de valores menores que 1BTC, em sua maioria. Uma consulta na blockchain e encontra-se milhares de envios de valores iguais a 0,00000888 saindo desse "hub" para diferentes carteiras.

Considerando as informações apresentadas anteriormente, em conjunto com a informação de que o serviço Bestmixer fornece gratuitamente uma API (*Application Programming Interface*)[14] para interação com o seu mixer, e que o mesmo sugere "Crie seu próprio serviço embaralhador de Bitcoin de graça", é possível que o serviço Blender.io utilize a rede da Bestmixer.

4.2. Visualização Gráfica da Mixagem

Após o levantamento de dados da blockchain explicado na Seção 3.2, as transações mapeadas foram consolidadas e utilizadas para criação de grafos dirigidos acíclicos (DAG), buscando representar os caminhos que as criptomoedas podem percorrer ao entrar na rede de carteiras de uma mixer.

[13]disponível em https://coinmarketcap.com/historical/20181118/

[14]em: https://bestmixer.io/en/api

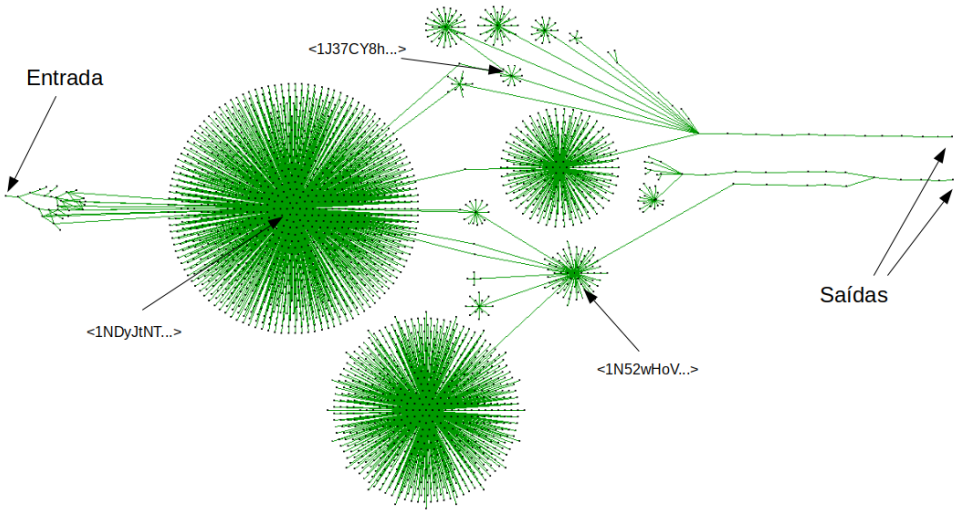

Figura 2. Grafo de Rastreamento da Bestmixer

Nos grafos apresentados nas Figuras 2 e 3, os vértices representam endereços de carteiras, enquanto as arestas representam transações entre elas. Os grafos foram organizados de maneira a representar a entrada na mixer no lado esquerdo e a saída, o recebimento das novas moedas, no lado direito.

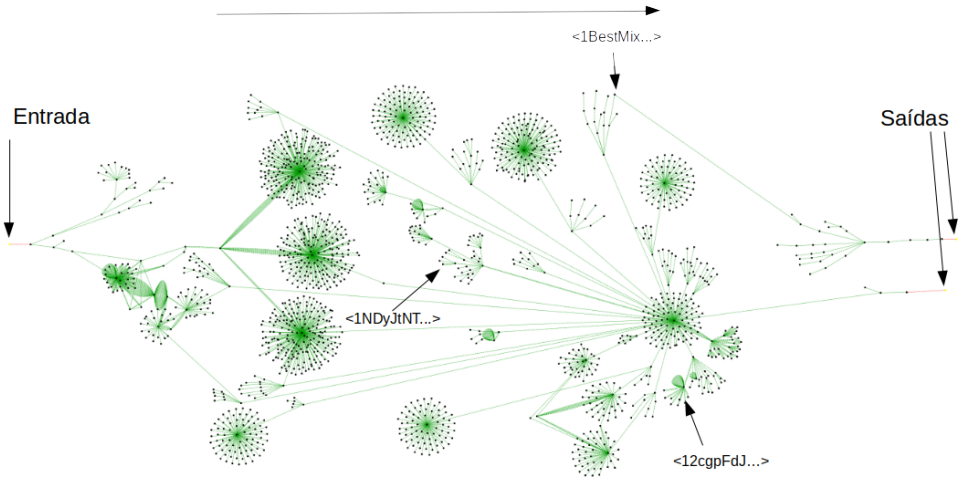

Figura 3. Grafo de Rastreamento da Blender.io

Na Figura 2, está representado o rastreamento realizado em uma das operações de mistura testadas com o serviço Bestmixer. Nela estão identificadas também três carteiras entre as que possuem maiores valores de movimentação de moedas durante o período de testes, conforme Tabela 3. Essas carteiras aparecem com frequência no rastreamento de ambas as transações realizadas com essa mixer. O endereço de carteira <1NDyJtNT...> foi encontrado nas duas operações de testes, 6 e 7 níveis após a entrada das moedas na mixer e, no rastreamento reverso, 12 níveis antes da carteira destino.

O comportamento padrão dos algoritmos durante a entrada é repassar moedas para

carteiras novas que não possuam muitas transações (normalmente 2), dividindo os valores da entrada até entregar a carteiras de destino ou chegar aos nós mais internos da rede de cada mixer, os quais possuem mais transações e mais moedas no saldo. Na saída foi possível identificar uma série de transferências sequenciais entre as carteiras, reduzindo gradativamente o valor das transferências até a chegada nos endereços finais.

A Figura 3, por sua vez, apresenta o grafo do rastreamento de uma operação com a mixer Blender.io. Para a geração desse grafo, foram rastreados e analisados 8 níveis a partir da carteira de entrada e, no rastreamento reverso, 9 níveis a partir da carteira de saída, para chegar a endereços de carteira que se relacionam e se interligam. Dois endereços chamam atenção ao serem localizados nessa representação por estarem presentes nos rastreamento das duas mixers, são as carteiras <1BestMix...> e <1NDyJtNT...>. Ao realizar uma comparação visual entre os grafos, analisando a complexidade de comunicações entre as carteiras apresentadas, a hipótese de adoção da API Bestmixer, por parte da Blender.io torna-se mais concreta.

4.3. Centralidade de Grau das Carteiras

Um padrão identificado nas redes de mistura aponta para carteiras com poucas transações em suas bordas enquanto, no núcleo, encontram-se algumas carteiras com elevado número de transações.

Para auxiliar na análise dos grafos, e identificar quais carteiras são influentes na rede, utilizou-se a ferramenta de medida de *Centralidade*. Como visto em [de Oriani e Paulillo et al. 2017] "existem três medidas de centralidade: i) centralidade de grau; ii) centralidade de proximidade; iii) centralidade de intermediação."

Tabela 5. Carteiras com maior centralidade de grau

Bestmixer					**Blender.io**				
#	Carteira	Entrada	Saída	Total	#	Carteira	Entrada	Saída	Total
1	<1NDyJtNT...>	24	6007	6031	1	<1BxVHak5...>	5	218	223
2	<1NyfNYAX...>	952	4	956	2	<1L26J8JG...>	219	1	220
3	<1AedYCVy...>	288	1	289	3	<3EN2aCf8...>	207	1	208
4	<14RcD35U...>	265	1	266	4	<38QyvVk8...>	205	1	206
5	<1KzemnJK...>	154	1	155	5	<3LZLpGi5...>	200	1	201
6	<1QCXuYkZ...>	153	1	154	6	<12ceuQRX...>	3	167	170

Na centralidade de grau, um ator (uma carteira Bitcoin, para este estudo) centraliza a relação com outros atores da rede. Esta medida consiste no número de ligações ou laços com os outros atores, simbolizando o quão influente é um ator em uma rede. De acordo com [Mascarenhas et al. 2018] O número de arestas incidentes a um nó *i* é denominado grau k_i. Em redes direcionadas, como as estudadas neste trabalho, considera-se para um nó *i* o grau de entrada k_i^{in} , de saída k_i^{out} ou total k_i.

Foram identificadas então as seis carteiras com maior centralidade de grau total de cada uma das redes, seus valores encontram-se na tabela 5.

Na rede Bestmix, a carteira com maior centralidade de grau total foi a <1NDyJtNT...> com 6031 interações. Esta carteira possui um elevado grau de saída quando comparado ao grau de entrada, sendo a carteira que registrou o maior número de

transferências de moedas durante a realização dos experimentos. No entanto, outros cinco endereços também apresentaram elevada centralidade de grau, porém com foco inverso à primeira. O grau de entrada dessas carteiras é muito superior ao de saída, o que indica que esses foram os endereços que mais receberam transferências durante os testes.

A rede Blender.io revelou um comportamento similar à rede Bestmix, quanto às carteiras mais influentes. Duas das carteiras com maior grau total, <1BxVHak5...> e <12ceuQRX...>, possuem elevado grau de saída e baixo grau de entrada, sendo esses endereços os que mais enviaram transferências para dentro da rede. As demais carteiras mais influentes, realizaram o papel inverso, com alto grau de entrada.

Ao analisar, na blockchain, os endereços de carteiras encontrados com alto grau de entrada, elucida-se que os mesmos funcionam como acumuladores, recebendo centenas de transferências de pequenos valores para formação de montantes elevados que serão redistribuídos em momento futuro.

5. Trabalhos Relacionados

A Bitcoin e a Blockchain são tecnologias que estão sendo pesquisadas, em diversas áreas, por toda a última década, a segurança é uma dessas áreas sendo exploradas. Em [Herrera-Joancomartí 2014] o autor discorre sobre os desafios da segurança da Bitcoin incluindo questões de privacidade e anonimato. É apresentada uma síntese sobre Análise de Blockchain e Análise de tráfego para identificação de transações. Como alternativa para a melhoria do anonimato na Bitcoin, o autor sugere a utilização de mixers disponíveis à época.

Em 2013, estudos acerca da utilização de misturadores de moedas surgem buscando entender seu funcionamento e suas possíveis falhas. [Moser et al. 2013] realizaram experimentos com duas das misturadoras de primeira geração: Bitcoin Fog e Bitlaundry, encontrando falhas na capacidade de anonimização da BitLaundry naquele ano através de rastreamento das transações na blockchain. Já em 2018 os próprios criadores da Bestmixer, mixer estudada neste trabalho, publicaram no fórum em [Bestmixer 2018], falhas das mixers existentes no período em que lançaram seu serviço.

Mais recente, em [van Wegberg et al. 2018], foi realizada uma pesquisa focada na lavagem de dinheiro utilizando Bitcoin. Os autores fizeram o levantamento financeiro e de usabilidade de cinco mixers e cinco exchanges, examinando dados de custos das transações desde as carteiras Bitcoin até os saques em dólares. Chegando a conclusão de que "é um conceito praticamente concebível e tem um alto grau de semelhança para ser integrado em esquemas atuais e futuros de lavagem de dinheiro".

Em [Khalilov and Levi 2018] é apresentado um survey sobre anonimato e privacidade em Bitcoins e outras criptomoedas. Os autores separam os trabalhos levantados durante o período de 03/01/09 até 01/01/17, em dois grandes grupos: por Resultados e por Métodos. Dentro da categoria Resultados, encontram-se os trabalhos que buscam fazer análises e ligações na blockchain a partir de endereços. Este é o grupo onde os autores encontraram mais trabalhos relacionados. Foram 27 pesquisas encontradas e outras 11 citadas. Dentre estes, outros trabalhos de estudo de mixers identificaram falhas nos serviços BitLaunder e Coinsplitter.

A respeito das análises de blockchain e grafos, em [Mascarenhas et al. 2018] há

um estudo sobre as transações na rede Ethereum. Nele é realizado uma análise da blockchain, onde são observadas as transações de carteiras pré-selecionadas realizadas entre os meses de maio e dezembro de 2017. O mapeamento dessas movimentações unidas aos cálculos dos graus dos nós avaliados, resultou em dados preliminares a respeito de padrões de comportamento na rede, visualmente representados em grafos

No sentido oposto ao de trazer anonimato para carteiras de criptomoedas, o trabalho de [Soares and Costa 2018] apresenta uma proposta de identificação de carteiras. Um serviço chamado *Address Name System* ou ANS. Nesta proposta apresenta-se dois módulos, um para registro de carteiras a ser utilizado "por parte do detentor de um endereço de carteira e de um certificado digital para registrar o mapeamento de endereço para entidade", e um módulo de consulta, correspondendo a um serviço que recebe parâmetros de entrada como um identificador de uma instância de DLT[15] e um endereço de carteira, e retorna ao usuário a identidade declarada, se houver uma.

6. Conclusões

Diante do novo paradigma financeiro pós surgimento da Bitcoin, que propôs uma nova forma de transferir valores entre usuários através da internet, utilizando criptografia e um livro caixa público, este trabalho realizou um estudo acerca do funcionamento de serviços de mistura ou embaralhamento de criptomoedas (*criptocurrency mixers* ou *tumblers*), complementaando e expandindo a pesquisa de [Moser et al. 2013], realizando a análise da nova geração de misturadores e seus algoritmos emergentes após o surgimento da Bestmix.io. Serviços estes que atraíram a atenção de muitos usuários que procuram anonimato e privacidade de suas carteiras com ativos digitais.

Foram executados testes com quatro serviços: Bestmixer, Blender.io, BTCBlender e Helix Light Grams, bem como o desenvolvimento de uma ferramenta própria de rastreamento das transações e carteiras envolvidas no embaralhamento das moedas digitais. Os resultados foram discutidos na Seção 4 e confirmam o risco de perca dos ativos envolvidos, pois duas (BTCBlender e Helix Light Grams) das quatro mixers testadas não devolveram nenhuma das moedas prometidas.

Ao analisar as duas mixers que concluíram a entrega das moedas, pode-se concluir que a mistura pode custar mais de 20% do valor de entrada enviado pelo cliente; nem todas as mixers entregam a segurança que prometem, a Blender.io pode conter uma falha conhecida e não garantir anonimidade de seus clientes; nem todas as mixers conseguem garantir o valor exato que será cobrado em todo o processo; a misturadora Bestmixer disponibiliza API para utilização de seus serviços e novas misturadoras estão utilizando sua infra-estrutura, como a Blender.io.

Isso posto, ao considerar os riscos de não recebimento das moedas, da possibilidade de falhas em garantir o anonimato, e de encargos totais que giram em torno de 20% do valor depositado, surgem alguns questionamentos como: A quem pode interessar um serviço com altos riscos e tarifas tão elevadas para conseguir anonimato? Apesar dos questionamentos, as mixers estão diariamente interagindo com diversos clientes, o que pode ser evidenciado pelas carteiras que movimentam os valores bilionários identificados.

[15] Sigla em inglês para Tecnologia Distribuída de Livro Razão, grupo de banco de dados o qual a Blockchain pertence.

A ética de tais serviços é claramente discutível pois, embora a primeira vista pareça resgatar o direito legítimo ao anonimato e sigilo financeiro, também favorece a execução de crimes. Como discutido em [van Wegberg et al. 2018] e [Böhme et al. 2015]“ a lavagem de dinheiro por Bitcoin pode evoluir para se tornar mais difícil de rastrear, particularmente quando os fundos são encaminhados através de misturadores”.

Como trabalho futuro destaca-se a necessidade de desenvolver uma nova ferramenta que possa identificar, a partir do endereço de entrada, em qual carteira serão depositadas as moedas de saída. Uma falha referente a falta de aleatoriedade no horário de entregas da moeda já havia sido explorada anteriormente por uma aplicação chamada *CAE-check* porém não é mais possível encontrar a aplicação, nem códigos-fonte, nem resultados de testes anteriores, e dados levantados levam a crer que ainda existam mixers vulneráveis.

Referências

Bestmixer (2018). Bestmixer.io the future of bitcoin mixing! technology is here. `https://bitcointalk.org/index.php?topic=3140140.msg33958885msg33958885`. [Acesso em: 10-10-2018].

Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2):213–38.

de Oriani e Paulillo, L., Garcia, L., and Neto, M. (2017). *Governanças de Redes: Economia, Política e Sociedade*. Elsevier Editora Ltda.

Herrera-Joancomartí, J. (2014). Research and challenges on bitcoin anonymity. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, pages 3–16. Springer.

Khalilov, M. C. K. and Levi, A. (2018). A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Communications Surveys & Tutorials*.

Mascarenhas, J. Z., Vieira, A. B., and Ziviani, A. (2018). Análise da rede de transações do ethereum. In *Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain-SBRC 2018)*, volume 1. SBC.

Moser, M., Bohme, R., and Breuker, D. (2013). An inquiry into money laundering tools in the bitcoin ecosystem. In *eCrime Researchers Summit (eCRS), 2013*, pages 1–14. IEEE.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Soares, M. and Costa, R. (2018). Auto identificação voluntária e verificável de participantes em aplicações baseadas em livros-razão distribuídos. In *Anais Estendidos do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 99–112, Porto Alegre, RS, Brasil. SBC.

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(2):419–435.