UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Um Modelo de Análise de Operações de Mixagem com Bitcoin em Serviços de Mistura Centralizada.

Rodolfo da Silva Costa

JOÃO PESSOA - PB

Abril - 2020

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Um Modelo de Análise de Operações de Mixagem com Bitcoin em Serviços de Mistura Centralizada.

Rodolfo da Silva Costa

Dissertação submetida ao Centro de Informática da Universidade Federal da Paraíba como parte dos requisitos necessários para obtenção do grau de Mestre em Informática.
Orientador: Prof. Dr. Rostand Costa

João Pessoa
2020

Catalogação na publicação
Seção de Catalogação e Classificação

C838m Costa, Rodolfo da Silva.
Um modelo de análise de operações de mixagem com bitcoin em serviços de mistura centralizada / Rodolfo da Silva Costa. – João Pessoa, 2020.
88 f. : il.

Orientação: Rostand Edson de Oliveira Costa.
Dissertação (Mestrado) – UFPB/CI.

1. *Bitcoin*. 2. Criptomoedas – Misturadores. 3. *Mixers*. 4. *Blockchain* – Análise. I. Costa, Rostand Edson de Oliveira. II. Título.

UFPB/BC CDU 336.74-021.131

Elaborado por RUSTON SAMMEVILLE ALEXANDRE MARQUES DA SILVA – CRB-0386

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Ata da Sessão Pública de Defesa de Dissertação de Mestrado de Rodolfo da Silva Costa, candidato ao título de Mestre em Informática na Área de Sistemas de Computação, realizada em 28 de julho de 2020.

Aos vinte e oito dias do mês de julho do ano de dois mil e vinte, às nove horas, por meio de videoconferência, reuniram-se os membros da Banca Examinadora constituída para julgar o trabalho do sr. Rodolfo da Silva Costa, vinculado a esta Universidade sob a matrícula nº 20181000804, candidato ao grau de Mestre em Informática, na área de "Sistemas de Computação", na linha de pesquisa "Computação Distribuída", do Programa de Pós-Graduação em Informática, da Universidade Federal da Paraíba. A comissão examinadora foi composta pelos professores: Rostand Edson Oliveira Costa (PPGI-UFPB) Orientador e Presidente da Banca, Guido Lemos de Souza Filho (PPGI-UFPB), Examinador Interno, Daniel Faustino L de Souza (UFERSA), Examinador Externo à Instituição, Denio Mariz Timoteo de Sousa (IFPB), Examinador Externo à Instituição. Dando início aos trabalhos, o Presidente da Banca cumprimentou os presentes, comunicou aos mesmos a finalidade da reunião e passou a palavra ao candidato para que o mesmo fizesse a exposição oral do trabalho de dissertação intitulado: "Um Modelo de Análise de Operações de Mixagens com Bitcoins em Serviços de Mistura Centralizada". Concluída a exposição, o candidato foi arguido pela Banca Examinadora que emitiu o seguinte parecer: "***aprovado***". Do ocorrido, eu, Ruy Alberto Pisani Altafim, Coordenador do Programa de Pós-Graduação em Informática, lavrei a presente ata que vai assinada por mim e pelos membros da banca examinadora. João Pessoa, 28 de julho de 2020.

Prof. Dr. Ruy Alberto Pisani Altafim

Prof. Rostand Edson Oliveira Costa
Orientador (PPGI-UFPB)

Prof. Guido Lemos de Souza Filho
Examinador Interno (PPGI-UFPB)

Prof. Daniel Faustino L de Souza
Examinador Externo à Instituição (UFERSA)

Prof. Denio Mariz Timoteo de Sousa
Examinador Externo à Instituição (IFPB)

"Aos meus pais, irmão, madrinha e minha companheira que, com muito carinho me apoiaram durante todos os momentos, e à toda comunidade científica que vêm sendo atacada e, ao mesmo tempo, cobrada em tempos tão difíceis."

Agradecimentos

Inicialmente gostaria de agradecer ao meu Orientador Dr. Rostand Costa, pelo acolhimento, paciência, disponibilidade, pelo tempo compartilhado e as importantes contribuições para que este trabalho fosse concluído.

Gostaria de agradecer também ao corpo docente do PPGI-UFPB pela dedicação e ensinamentos.

Ao IFRN, minha instituição de trabalho, pela oportunidade de dedicar-me exclusivamente ao mestrado durante parte do período necessário, bem como aos meus amigos desta instituição que sempre me apoiam e incentivam ao crescimento profissional e científico.

Aos colegas do programa e do PPGCA pelas trocas de ideias e ajuda mútua.

Aos familiares, em especial meus pais, irmão, madrinha e companheira por serem sempre incentivadores incondicionais de todas as minhas empreitadas.

Por fim, agradeço a todos que estiveram envolvidos direta ou indiretamente para a conclusão deste mestrado

Obrigado.

Resumo

Por concepção, uma *blockchain* permite que qualquer interessado possa analisar todas as transações já realizadas na rede, além de consultar o saldo de moedas que cada carteira contém, bem como qualquer relação que possa existir entre elas. Em contrapartida, informações financeiras pessoais são dados sensíveis que necessitam de privacidade, e sua exposição pode provocar desconforto aos proprietários. Portanto, a privacidade dos detentores dos ativos nesse sistema reside, por concepção, no pseudoanonimato fornecido pelos endereços de carteiras, os quais não possuem dados pessoais associados, apenas um código identificador. Porém, a qualquer momento que um endereço de carteira seja relacionado a um usuário, toda a sua privacidade será perdida. Por outro lado, buscando o direito ao sigilo financeiro e com a perspectiva de alcançar a privacidade desejada na origem da *Bitcoin*, nasce um tipo de serviço que utiliza de artifícios como a troca e embaralhamento de criptomoedas para atingir o anonimato na rede. Estes serviços são chamados de *cryptocurrency mixers* ou *cryptocurrency tumblers*. O objetivo deste trabalho foi desenvolver um modelo de análise da *Blockchain* para auxiliar no processo de rastreamento de criptomoedas embaralhadas por esses serviços. Para tal, foram realizados testes e análises de padrões de misturas de quatro mixers que atuam na *blockchain Bitcoin* e o desenvolvimento de uma estratégia para representação em grafos das transações envolvidas no embaralhamento. Dentre as conclusões obtidas, mesmo considerando que alguns dos usuários de tais serviços possam ter direito ao anonimato e sigilo financeiro, além do risco oferecido por tais serviços também é nítido que a existência das mixers favorece o cometimento de crimes fiscais, como a lavagem de dinheiro e sonegação de impostos, e a sua utilização para o apoio de outras atividades ilegais. Por outro lado, ferramentas e metodologias, como as apresentadas neste trabalho, permitem que forças da lei, governos e outros interessados possam rastrear a origem das criptomoedas em cenários onde isso seja necessário.

Palavras-chave: Bitcoin, misturadores de criptomoedas, mixers, análise de blockchain

Abstract

By design, a blockchain allows anyone interested to analyze every transactions already made on the network, in addition to consulting the balance of currencies that each wallet contains, as well as any relationship that may exist between the addresses of wallets in the network. In contrast, personal financial information is sensitive data that needs privacy, and its exposure can cause discomfort to owners. Therefore, the privacy of the holders of the assets in this system resides, by design, in the pseudo-anonymity provided by the addresses of portfolios, which do not have associated personal data, only an identifying code. However, anytime a wallet address is related to a user, all of their privacy will be lost. On the other hand, seeking the right to financial secrecy and with the prospect of achieving the desired privacy at the origin of Bitcoin, a type of service is born that uses artifices such as cryptocurrency exchange and shuffling to achieve anonymity on the network. These services are called cryptocurrency mixers or cryptocurrency tumblers. The objective of this work was to develop a blockchain analysis model to assist in the process of tracking cryptocurrencies mixed by these services. To this end, tests and analysis of the shuffling patterns of four mixers that operate on the Bitcoin Blockchain were carried out and the development of a strategy for graphing the transactions involved in the shuffling. Among the conclusions obtained, even considering that some of the users of such services may have the right to anonymity and financial secrecy, in addition to the risk offered by such services, it is also clear that the existence of mixers favors the commission of tax crimes, such as money laundering. money and tax evasion, and their use to support other illegal activities. On the other hand, tools and methodologies, such as those presented in this paper, allow law enforcement, governments and other stakeholders to trace the origin of cryptocurrencies in scenarios where this is necessary.

Keywords: Bitcoin, cryptocurrency mixers, mixers, blockchain analysis.

Conteúdo

Lista de Símbolos

ANS : Address Name System

API : Application Programming Interface

BTC : Bitcoin

DAG : Grafo AcíclicoDirecionado

dApps : Decentralized Applications

DLT : Distributed Ledger Technologies

DoS : Denial of Service

dPOS : Delegated Proof of Stake

ECB : European Central Bank

EUA : Estados Unidos da América

EVM : Ethereum Virtual Machine

FBI : Federal Bureau of Investigation

GMT : Greenwich Mean Time

IoT : Internet of Things

IP : Internet Protocol

PoET : Proof of Elapsed Time

PoS : Proof of Stake

PoW : Proof of Work

RPCA : Ripple Protocol Consensus Algorithm

SCP : Stellar Consensus Protocol

TPS : Transações por Segundo

USD : United States Dollar

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Na segunda metade da década de 2000, iniciou-se a mais grave crise econômica e financeira desde a Grande Depressão dos anos 1930. De acordo com Alexandre et al. (2009), esta crise teve início com o endividamento "acumulado essencialmente pelas famílias (Estadunidenses) para a aquisição de habitação e consumo". Isso levou a uma bolha imobiliária no mercado norte americano que mais tarde seria acompanhada de uma recessão nos setores não financeiros e nas economias, não apenas dos EUA mas mundial, como afirmou Kotz (2009).

Com a baixa credibilidade de bancos e do sistema financeiro, surge neste cenário, em 2008, uma nova proposta de moeda eletrônica que viria para revolucionar a forma como pessoas e instituições poderiam transferir dinheiro entre si. 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".

Ao se fazer uso do sistema então apresentado, torna-se possível realizar transações financeiras através da internet, sem a necessidade de um banco, operadoras de cartão de crédito ou qualquer outra instituição financeira intermediadora.

Para atingir o objetivo, Nakamoto propôs um livro caixa público e compartilhado entre os participantes da rede. Este livro caixa da Bitcoin, denominado *Blockchain*, é utilizado para registrar de forma pública todas as transações realizadas na rede. Dessa forma, fazendo uso do acesso público aos registros, é possível identificar qual a origem e o destino de todas as moedas, permitindo o rastreamento até o momento de sua criação. Assim, protegendo o

sistema contra adulteração de contas, gastos duplos ou criação indevida de novas moedas na rede. Este novo paradigma permite uma maior transparência nas grandezas envolvidas de um determinado ativo financeiro digital, inibindo, por exemplo, alavancagens extremas como a que caracterizou a crise financeira de 2008.

Por concepção, a *blockchain* permite que qualquer interessado possa analisar todas as transações já realizadas no sistema, além de consultar o saldo de moedas que cada carteira contém, bem como qualquer relação que possa existir entre os endereços de carteiras da rede.

Em contrapartida, informações financeiras pessoais são dados sensíveis que necessitam de privacidade, e sua exposição pode provocar desconforto aos proprietários. O modelo de base de dados descentralizada, global e de acesso público da *blockchain*, permite que todas as transações realizadas na rede possam ser visualizadas. Portanto, a privacidade dos detentores dos ativos nesse sistema reside, por concepção, no pseudoanonimato fornecido pelos endereços de carteiras, os quais não possuem dados pessoais associados, apenas um código identificador. Porém, a qualquer momento que um endereço de carteira seja relacionado a um usuário, toda a sua privacidade será perdida.

Ainda que a transparência da *blockchain* possua características negativas, não apenas a Bitcoin mas também diversas criptomoedas que surgiram posteriormente sofreram rápida valorização na segunda metade da década de 2010. No ano de 2017, a cotação do Bitcoin saltou de $1.000 em janeiro, chegando a quase $20.000 em dezembro. A nova febre financeira criada pelas criptomoedas fez a procura por esses ativos tornar-se altíssima o que contribuiu para o aparecimento de diversas *exchanges*, possibilitando a troca de moedas convencionais por moedas digitais.

O fortalecimento e a aparição destas novas moedas estavam ocorrendo para além do mercado financeiro tradicional, deixando governos sem a correta arrecadação de impostos. Esta realidade foi alterada com o surgimento e uso de exchanges, que permitiu aos governos realizarem a cobrança de tais valores. 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".

[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/.

Em território brasileiro, a Receita Federal, em 31 de Outubro de 2018, passou a exigir das corretoras declarações mensais de todas as operações de vendas de criptomoedas[2]. Outros países também deram início a processos no sentido de cercear o anonimato das *blockchains*, como a China[3], onde órgãos reguladores da internet "propõem que todas as operações com a ferramenta (blockchain) realizadas no país sejam identificadas".

A regulação dessas tecnologias emergentes trazem para governos, empresas e demais instituições envolvidas, a necessidade de mecanismos e ferramentas que forneçam condições de analisar as *blockchains* e identificar transações e indivíduos. Torna-se então essencial o desenvolvimento de metodologias e aplicações capazes de colaborar não apenas com questões fiscais mas também no combate ao crime.

Por outro lado, buscando o direito ao sigilo financeiro e com a perspectiva de alcançar a privacidade desejada na origem da Bitcoin, nasce um tipo de serviço que utiliza de artifícios como a troca e embaralhamento de criptomoedas para atingir o anonimato na rede. Estes serviços são chamados de *cryptocurrency mixers* ou *cryptocurrency tumblers* e surgem com a proposta de apagar os rastros das criptomoedas, fazendo com que ativos de carteiras que eventualmente tornaram-se conhecidas ou marcadas, sejam colocados em uma rede de embaralhamento e, posteriormente, moedas sem vínculos com as originais sejam depositadas em nova(s) carteira(s) do usuário.

1.1 Motivação e Justificativa

Com o passar do tempo as criptomoedas confirmaram sua viabilidade técnica e econômica e, cada vez mais, novos usuários aderiram aos cripto ativos. Porém, essa tecnologia de transferência eletrônica de valores, assim como outros meios analógicos já existentes, passou a ser utilizada com finalidades ilícitas. Dois casos podem ser citados pois tornaram-se conhecidos mundialmente: a cobrança de resgate de dados sequestrados por *Ransomwares* e negociações de mercadorias ilegais como no site *Silk Road*.

Os *Ransowares* são softwares maliciosos que bloqueiam arquivos digitais de usuários em

[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/.

seus computadores e cobram pagamento de resgate pela devolução dos mesmos. Para citar apenas um desses malwares, “com mais de 230.000 PCs com Windows infectados em todo o mundo, muitos deles em agências governamentais e hospitais, o WannaCry é o ataque de ransomware mais difundido visto até agora", afirmou a empresa de antivírus Avast[4].

No artigo desenvolvido por Conti et al. (2018), encontra-se um estudo econômico acerca dos ransomwares mais recentes. O WannaCry, que teve sua primeira aparição em maio de 2017, cobrava de suas vítimas um valor de resgate equivalente a USD 300 em Bitcoins. Este valor precisava ser pago no prazo de até três dias após o bloqueio, depois desse período o valor dobrava para USD 600. De acordo com Conti et al. (2018), em apenas três das carteiras digitais utilizadas pelo malware foram encontradas mais de 53 Bitcoins (aproximadamente USD 100.000 para a cotação da época).

O outro caso mencionado anteriormente foi o Silk Road. Como visto no estudo realizado por Christin (2013), o Silk Road foi um mercado online anônimo que teve sua operação iniciada em fevereiro de 2011, “o site não era uma loja por si, ele fornecia a infraestrutura para vendedores e compradores conduzirem transações em um ambiente online”. O que diferenciou o Silk Road de outros mercados online foi sua particularidade de “focar em garantir o máximo possível de anonimato para compradores e vendedores”. A maneira utilizada para auxiliar seus usuários a realizarem os pagamentos de forma anônima foi através da criptomoeda Bitcoin.

No estudo citado acima, os autores coletaram e analisaram dados do site de vendas por 6 meses, entre 3 de fevereiro de 2012 e 24 julho de 2012. Dentre as principais categorias de produtos encontrados estavam: “maconha”, “drogas“, “prescrições médicas”, “cocaína” e outros. O Silk Road teve suas vendas estimadas em 22 milhões de dólares anuais de acordo com a Forbes[5] e o lucro dos seus criadores foi estimado em 1,7 milhão de dólares americanos Christin (2013).

Neste mercado, os pagamentos de todas as transações executadas entre clientes e vendedores eram centralizadas em carteiras pertencentes ao próprio site e, só após a avaliação do vendedor ser realizada pelo respectivo cliente, os pagamentos eram transferidos para ele.

[4]“WannaCry Ransomware – o que é isso e como proteger seu PC | Avast” https://www.avast.com/pt-br/c-wannacry. Acesso em Março de 2020

[5]“Black Market Drug Site ‘Silk Road’ Booming: $22 Million In Annual Sales” https://www.forbes.com/sites/andygreenberg/2012/08/06/black-market-drug-site-silk-road-booming-22-million-in-annual-mostly-illegal-sales/

Como visto em Christin (2013), "O Silk Road aprimorava o fator anonimato ao prover o serviços de mistura" das moedas, antes de entrega-las à carteira de destino do vendedor. O método consistia em inserir carteiras intermediárias de uso único entre quem pagava e quem recebia. Ou seja, ao invés de $Comprador \rightarrow Vendedor$, o pagamento seguia através de uma cadeia de transações: $Comprador \rightarrow I_1 \rightarrow I_2... \rightarrow I_n \rightarrow Vendedor$, onde *I* representa as carteiras intermediárias e de uso único.

Em outubro de 2013 o site foi fechado pelo FBI que conseguiu chegar até o seu administrador, após uma longa e complexa investigação[6].

Os dois exemplos mencionados acima possuem em comum, além da utilizacão da Bitcoin para fins ilegais, a busca pelo anonimato em suas atividades. Para esses casos, a utilização de misturadores de criptomoedas podem dificultar extremamente ou até mesmo impedir que autoridades rastreiem os recursos e consigam identificar os envolvidos nos crimes.

Em suas páginas web, os serviços de mistura apelam para o direito à privacidade de cada indivíduo, porém levantam uma discussão sobre sua legalidade, pois o processo de mistura de criptomoedas assemelha-se a ao processo de lavagem de dinheiro físico, que é um crime tipificado em diversos países, como no Brasil, que foi definido na lei Nº 9.613, de 3 de março de 1998. A lei, em seu artigo primeiro descreve: "Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal".

A partir do cenário exposto, encontra-se um ambiente polarizado onde um grupo de entidades buscam identificar os usuários de criptomoedas, no lado oposto, outro grupo busca garantir a privacidade e o anonimato dos mesmos. Portanto, a necessidade de estudar esses serviços, analisa-los, encontrar possíveis falhas e padrões de funcionamento torna-se imprescindível não apenas para governos e agentes de segurança, como também aos próprios usuários das criptomoedas.

1.2 Objetivos

Nesta seção encontram-se descritos quais os objetivos geral e específico que este trabalho deseja alcançar.

[6]"Como o FBI capturou 'Dread Pirate Roberts' e fechou o Silk Road" https://canaltech.com.br/internet/Como-o-FBI-capturou-Dread-Pirate-Roberts-e-fechou-o-Silk-Road/

1.2.1 Objetivo Geral

Uma vez apresentada a problemática relacionada às questões de privacidade de criptomoedas como a Bitcoin, este trabalho tem como objetivo geral realizar um estudo acerca do funcionamento dos serviços de mistura e embaralhamento centralizado de Bitcoins, que buscam anonimizar usuários e confundir ferramentas de análise das *blockchains*, procurando avaliar e entender seu funcionamento, além de identificar padrões em seus algoritmos e, por fim, desenvolver uma ferramenta capaz de auxiliar a análise de blockchain visando mitigar o anonimato de usuários de misturadoras.

1.2.2 Objetivos Específicos

Visando atingir o objetivo geral, foram definidos os seguintes objetivos específicos:

- Selecionar e testar um subconjunto de prestadores do serviço de mistura centralizada de *bitcoins*;
- Analisar e descrever o funcionamento das *mixers* dentro da *blockchain*;
- Identificar possíveis falhas de misturadoras ao anonimizar seus usuários;
- Desenvolver uma ferramenta que auxilie a análise da *blockchain* em busca da carteira de origem de moedas embaralhadas.

1.3 Metodologia

Para o desenvolvimento deste trabalho, a metodologia utilizada divide-se em três etapas. A primeira delas consistiu no levantamento bibliográfico do objeto estudado, considerando-se que a tecnologia de *blockchain* possui muitos trabalhos abordando o tema nas mais diversas áreas: infraestrutura, segurança, consenso, aplicações, dentre outras. Porém quando trata-se de misturadoras de criptomoedas, poucos trabalhos acadêmicos abordaram o tema no passado. Por esta questão, fóruns, blogs e páginas web das próprias prestadoras de serviço de mistura e embaralhamento de Bitcoins também são utilizados para aprofundamento do referencial teórico.

Para a etapa seguinte, testes de utilização de mixers foram realizados com os objetivos de levantar dados, entender seu funcionamento e descobrir os possíveis riscos envolvidos. Para esta etapa, elaborou-se uma seleção de mixers com 4 serviços escolhidos. Estes foram submetidos aos testes de funcionalidades e, posteriormente, os dados resultantes serviram para analise, executando uma varredura dentro da *blockchain Bitcoin*, em busca de possíveis relacionamentos existentes entre as carteiras envolvidas.

Na terceira etapa, utilizando os dados levantados e analisados na fase anterior, deu-se a identificação e descrição de estratégias utilizadas nos serviços de mistura em busca de padrões que possam caracterizar vulnerabilidades nas mixers, e para validar o modelo, ocorreu o desenvolvimento de uma ferramenta capaz de rastrear a carteira de origem de uma transação de mistura, quando se tem conhecimento de carteiras de destino/saída, em duas das misturadoras testadas.

1.4 Estrutura da Dissertação

O presente documento está estruturado de forma que no Capitulo 2 é apresentada a fundamentação teórica necessária para este trabalho, envolvendo os temas Criptomoedas e DLTs; Anonimato e Privacidade em criptomoedas e Transações de Embaralhamento de Criptomoedas. No Capitulo 3, são apontados alguns trabalhos relacionados com a privacidade das criptomoedas, os quais foram utilizados como referencial nesta pesquisa. No Capítulo 4 são apresentados testes e análises iniciais de usos de misturadoras. Uma modelagem detalhada, com identificação de operações e endereços usados nas misturas são apresentados no Capítulo 5. O desenvolvimento da ferramenta para auxílio à análise da *blockchain* e seus testes, buscando mitigar o anonimado oferecido por mistura de bitcoins e validando o modelo apresentado no capítulo anterior, está presente no capítulo 6. Por fim, no capítulo 7, são apresentadas as conclusões obtidas após os estudos executados neste trabalho.

Capítulo 2

Fundamentação Teórica

Neste capítulo são apresentados conceitos importantes que fundamentam esta dissertação. Inicialmente, serão descritos os conceitos e características de criptomoedas e das Tecnologias de Livros Razão Distribuídos (DLTs), detalhando alguns exemplos como a Bitcoin, Ether e a Iota. Em seguida, são debatidos também os conceitos de anonimato e privacidade no contexto das criptomoedas e como mecanismos de embaralhamento e mistura de criptomoedas são usados em busca de segurança. Por fim, são feitas algumas considerações finais acerca dos fundamentos teóricos expostos.

2.1 Criptomoedas e DLTs

No seu famoso artigo de 2008 Nakamoto (2008), Satoshi Nakamoto, apresenta o conceito da criptomoeda *Bitcoin*, baseada em um sistema inovador de dinheiro eletrônico ponto-a-ponto que permite que pagamentos *online* sejam enviados diretamente de uma parte para a outra sem a necessidade de passar por uma instituição financeira, ou qualquer outra terceira parte de confiança.

Para viabilizar a implementação da *Bitcoin*, seu criador fez uso das Tecnologias de Livros de Registros Distribuído ou Tecnologias de Contabilidade Distribuída (ou DLT, do inglês *Distributed Ledger Tecnology*). Tais tecnologias, que possibilitaram o advento das criptomoedas, são, essencialmente, bases de dados distribuídas que armazenam suas informações em diversos nós da rede e que não necessitam de uma entidade centralizadora que controle as transações. O estado da rede é mantido através da utilização de algum algoritmo de con-

senso. Em DLTs públicas, Os registros gravados podem ser acessados por qualquer interessado enquanto que novos registros são adicionados de forma consensual pelos participantes da rede.

A DLT mais conhecida é a utilizada para armazenar as transações da rede *Bitcoin*. Ela recebeu o nome de *Blockchain*. Nela, as informações referentes às transações com a criptomoeda são agrupadas em blocos, e cada um deles está ligado ao anterior, formando uma cadeia de blocos. Cada um desses blocos é identificado por um código *hash*, calculado utilizando informações como: *dados das transações*, *timestamp*, *tamanho do bloco* e o *hash do bloco anterior*.

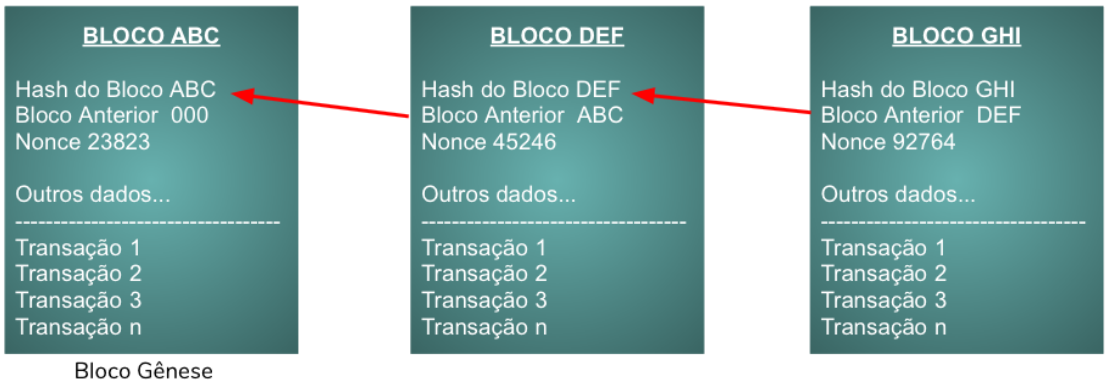

Figura 2.1: Encadeamento de Blocos

Calcular códigos *hash* é uma tarefa trivial para computadores modernos e por motivos de segurança, a serem discutidos adiante, a *Blockchain* não aceita que todo e qualquer código *hash* de bloco venha a ser inserido no seu livro de registros. Um mecanismo chamado *dificuldade* condiciona a validação do *hash* de um bloco àqueles que iniciem com uma determinada quantidade de bits iguais a 0 (zero), fazendo com que esse cálculo torne-se muito custoso.

Esse mecanismo, utilizando blocos encadeados por *hashes* calculados a partir de seus atributos e com um fator condicionante (dificuldade), permite a integridade dos registros e torna a estrutura de dados virtualmente imutável para seus blocos passados. Assim, se um participante desonesto tentar alterar qualquer das informações de um bloco anterior, será necessário um novo cálculo de *hash* considerando as informações modificadas. Nessa situação, O bloco seguinte da cadeia irá apontar para um *hash* inexistente, portanto, a cadeia terá sido quebrada e todos os blocos subsequentes estarão inválidos (Figura 2.2). Quanto mais an-

tigo for um bloco na cadeia, mais difícil será para um atacante quebrar sua integridade, pois torna-se necessário remontar a ligação de todos os blocos subsequentes com novos *hashes* válidos.

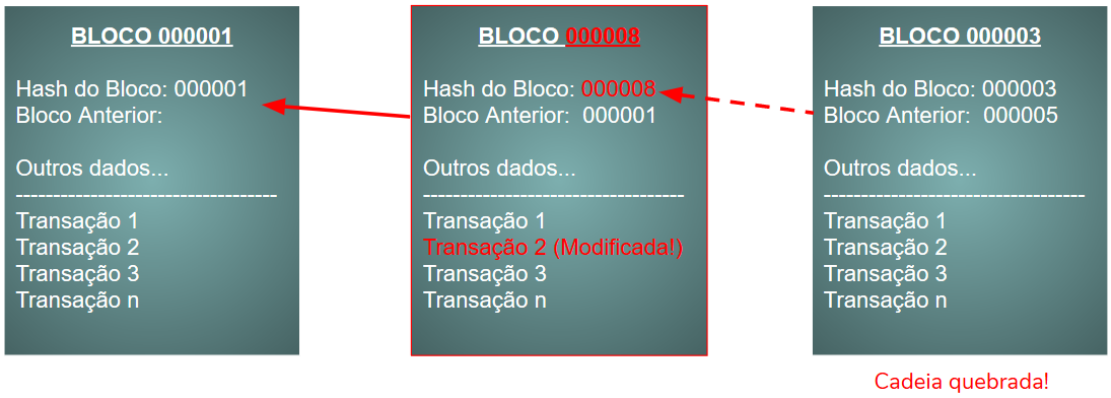

Figura 2.2: Exemplo de *Blockchain* corrompida

As informações contidas em uma DLT não podem ser apagadas ou modificadas. A medida que seu estado precisa ser alterado com a inclusão de novas transações, o livro de registros aumenta de tamanho e as novas operações realizadas são adicionadas ao final da cadeia. À vista disso, as Tecnologias de Contabilidade Distribuída possuem a característica da *imutabilidade*.

No que se refere ao acesso dos dados, é comum que o livro de registro das DLTs seja público, permitindo que qualquer usuário interessado possa obter informações sobre o histórico de todas as transações já realizadas, até mesmo rastreando a origem de moedas. Por outro lado, adicionar conteúdo ao livro de registro exige o cumprimento de regras bem definidas. Novas transações necessitam que os proprietários dos ativos assinem digitalmente as operações, comprovando a sua posse atual e identificando qual usuário será o novo dono do ativo (ou parte dele). Para validar as novas transações, elas precisam ser inseridas em um novo bloco e validadas através de um mecanismo de consenso para, só então, serem adicionadas à cadeia.

Após a implementação da Bitcoin, muitas novas criptomoedas surgiram acompanhando a nova tendência financeira e tecnológica. Em fevereiro de 2020, o site *CoinMarketCap*[1] já contabilizava 5.140 moedas diferentes no mercado. Algumas delas trouxeram modificações consideráveis em suas DLTs e apresentaram novas soluções, variando formas de armazena-

[1] https://coinmarketcap.com/

mento, acesso, validação de transações e expandido as possibilidades de aplicações dessas tecnologias.

2.1.1 Classificação das DLTs

O desenvolvimento das Tecnologia de Livro Razão Distribuídos fez surgir variações de *"blockchains"*, trazendo novos conceitos e aplicações para a tecnologia. A seguir serão discutidas as características que diferenciam cada DLT[2] e, naturalmente, ajudam a classificá-las.

Gerações de *Blockchains*

A *Bitcoin* deu início à *primeira geração* de *blockchains* ou *blockchains 1.0*, capazes de gerenciar e armazenar transações financeiras assinadas criptograficamente sem a necessidade de uma entidade centralizadora. Como expôs Yang et al. (2018), "A Blockchain 1.0 é completamente dedicada à descentralização de dinheiro e pagamentos, embora essa tenha sido a primeira implementação de uma Tecnologia de Livro Razão Distribuído (DLT)", e conclui: "a Blockchain 1.0 garante armazenamento distribuído, permite o compartilhamento de dados entre nós e transparência no processamento de transações."

Porém, estas DLTs da primeira geração possuem recursos reduzidos para execução de *scripts* e transações programáveis, limitando o poder da tecnologia.

A *segunda geração* chegou em 2013 com a proposição da *Ethereum*. Essa plataforma trouxe uma infraestrutura mais robusta que permite a execução de aplicações descentralizadas (*dApps*), armazenando os programas e os resultados de suas execuções no livro de registros. Estes programas receberam o nome de Contratos Inteligentes (*Smart Contracts*) e ampliaram imensamente as possibilidades de utilização das DLTs. Além de criptomoedas, essas plataformas também permitem a criação de mercados digitais, contratos de aluguel, jogos e outros, sem a presença de uma entidade controladora.

As tecnologias baseadas em DLTs continuam a evoluir trazendo novos algoritmos de consenso, estruturas de armazenamento e encadeamento, linguagens de *scripting* e outras funcionalidades adicionais.

[2]Neste documento, os termos *DLT* e *blockchain* serão usados de forma intercambiável com o mesmo sentido.

Em seu trabalho, Yang et al. (2018) adiciona ainda mais duas gerações de *blockchain* e as descreve brevemente. *A terceira geração*, atualmente em desenvolvimento, tem representantes como *Dfinity* (Hanke et al., 2018) , *NEO* (Coelho et al., 2019), *IOTA* (Divya e Biradar, 2018) e *Ethereum* (Buterin e Griffith, 2017) que usam diferentes abordagens. Elas visam suportar múltiplas linguagens de programação e o desenvolvimento de várias aplicações baseadas em dispositivos móveis. Na *Quarta geração*, a Blockchain 4.0 (também conhecido como *Seele* (Zeng et al., 2019)) introduz novos algoritmos de consenso baseados em Redes Neurais Artificiais que melhoram a tolerância a falhas do sistema. A proposta também inclui uma nova arquitetura de rede, com protocolo de conexão à Internet de baixa latência para permitir a integração com os recursos da Internet e o desenvolvimento de serviços baseados em *blockchain*.

Características de DLTs

Ao longo do desenvolvimento das DLTs, alguns trabalhos foram escritos buscando apresentar taxonomias para sistemas baseados em *blockchain*. Dentre eles podemos citar:

- Xu et al. (2017), que faz uma avaliação a partir dos projetos de arquitetura das blockchains. Classificando-os por: Projeto da arquitetura referente à *descentralização*; Projeto da arquitetura referente a *armazenamento e computação*; Projeto de arquitetura referente à *configuração da blockchain* e *Outros* projetos de arquitetura e implantação.

- Tasca e Tessone (2017), onde encontra-se uma taxonomia aprofundada, dividindo e categorizando as tecnologias de blockchain em oito componentes principais, cada um deles contendo diversos subcomponentes e sub-subcomponentes.

- Em Pinna e Ruttenberg (2016), publicado pelo *European Central Bank* (ECB), os autores categorizam as DLTs de acordo com três critérios: quanto a participação no livro de registros - restrito ou irrestrito; quanto ao método de validação e quanto a estrutura da base de dados compartilhada. Para apresentação e discussão das DLTs a serem enunciadas adiante, utilizaremos das descrições dessas características.

Acesso ao livro de registro

Com relação a acessibilidade dos DLTs, Pinna e Ruttenberg (2016) definem que "em termos de participação dos usuários, as DLTs podem ser divididas entre as que são **restritas** e as que são **irrestritas**. DLTs restritas são sistemas fechados cujos membros são entidades identificadas e responsáveis". Já as DLTs de acesso irrestrito podem ter seus dados lidos e adicionados por qualquer usuário que deseje participar da rede, fazendo com que esses livros de registros dependam de mecanismos de consenso robustos para manter os registros consistentes e confiáveis.

Métodos de validação de transações (algoritmos de consenso)

Com a evolução das DLTs, diversos mecanismos para validação das transações foram planejados e desenvolvidos.

Em redes privadas/permissionadas, de acesso restrito, os usuários recebem autorização para participar e possuem identidades conhecidas, como ocorre no *Hyperledger*, onde existem nós específicos para executar as transações e votar na validação das mesmas. Em DLTs de acesso irrestrito, usuários podem criar novos endereços na rede com custo computacional e financeiro desprezível. Desta forma, torna-se inviável validar transações utilizando um mecanismo que contabilize um voto por usuário. Para resolução desse problema, alguns algoritmos de consenso vem sendo utilizados pelas DLTs. Dentre eles, o **Proof of Work** (PoW) e o **Proof of Stake** (PoS).

Nos sistemas baseados em *Proof of Work*, os nós que desejam validar as transações realizadas na rede devem resolver problemas criptográficos, recebendo recompensas ao encontrar os resultados corretos. Esses nós, também chamados de mineradores, agrupam em blocos as transações ainda não validadas e, a partir deles, buscam a resolução do problema proposto: encontrar *hashes* específicos. Esse trabalho costuma consumir elevadas quantias de tempo, recursos computacionais e, por consequência, eletricidade. Após a solução (*hash*) ser encontrada para um bloco, ele passa a integrar o Livro de Registros e os mineradores devem procurar a solução para o bloco seguinte. Por outro lado, verificar se o resultado encontrado para um bloco de transações é valido é uma tarefa trivial.

A validação de novos blocos contendo transações nos sistemas baseados em *Proof of*

Stake não necessita de alto poder computacional de seus validadores. Nesse método, os nós recebem poder de voto baseado em sua participação na rede, medida por apostas feitas por aqueles que desejam participar do processo. Cada nó que desejar votar pela validação de novos blocos precisa apostar uma quantidade de ativos na rede, podendo ser recompensado para cada bloco válido criado ou votado. Um nó também pode ser punido, caso comporte-se de maneira desonesta, tentando prejudicar a rede (por exemplo, votando em blocos inválidos ou abstendo-se das rodadas de votação.

PoW e PoS são os mecanismos de consenso mais conhecidos e adotados pelas DLTs atualmente, porém uma oferta crescente de novos algoritmos está sendo apresentada. Para mencionar alguns: *Ripple Protocol Consensus Algorithm* - RPCA (Schwartz et al., 2014), *Stellar Consensus Protocol* - SCP (Mazieres, 2015), *Delegated Proof of Stake* - dPOS (Larimer, 2014) e *Proof of Elapsed Time* - PoET (Chen et al., 2017).

Estrutura do Livro de Registro (ou *Ledger* Distribuído)

Nas DLTs, as informações das transações são escritas nos livros de registros que seguem estruturas de dados planejadas para suportar o ecossistema. A primeira estrutura apresentada foi a **Blockchain**, onde conjuntos de transações são agrupadas em blocos, identificados por um código *hash*, e esses blocos são encadeados apontando para *hash* do bloco anterior (Figura 2.3).

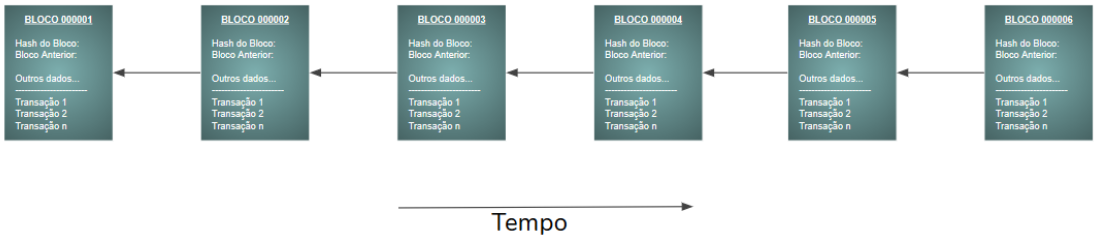

Figura 2.3: Estrutura Interna da DLT Blockchain

Na estrutura padrão de uma *blockchain*, novos blocos de transações precisam ser validados antes de fazer parte da cadeia, esse processo de validação é denominado mineração de blocos e é um processo concorrente entre todos os nós que desejam "minerar". Caso ocorra de dois blocos diferentes serem minerados ao mesmo tempo, o processo continuará a repetir-se até que a cadeia mais longa seja adotada como verdadeira e a outra descartada. Todo esse

mecanismo da *blockchain* costuma consumir muito recurso computacional e ter uma baixa taxa de validação de transações por segundo.

Outra estrutura DLT emergente é a **Tangle** (Popov, 2016). Criada originalmente para a IOTA (Divya e Biradar, 2018), baseia-se no conceito matemático DAG (Grafo Acíclico Direcionado) onde os vértices fazem ligações de forma que o grafo possua uma direção e, por ser acíclico, não existem *loops* nesta estrutura. Na DLT, os vértices são representados pelas transações da rede, não sendo agrupadas em blocos, como na blockchain, mas sim conectadas diretamente entre si (Figura 2.4). Deste modo, as transações não precisam esperar um bloco ser montado pra serem validadas. Essa arquitetura da DLT permite grande escalabilidade e alta velocidade de confirmação de transações por minuto. Outra característica da *Tangle* é que ela foi modelada para que o livro de registros não necessite ser baixado por completo em todos os nós de armazenamento na rede.

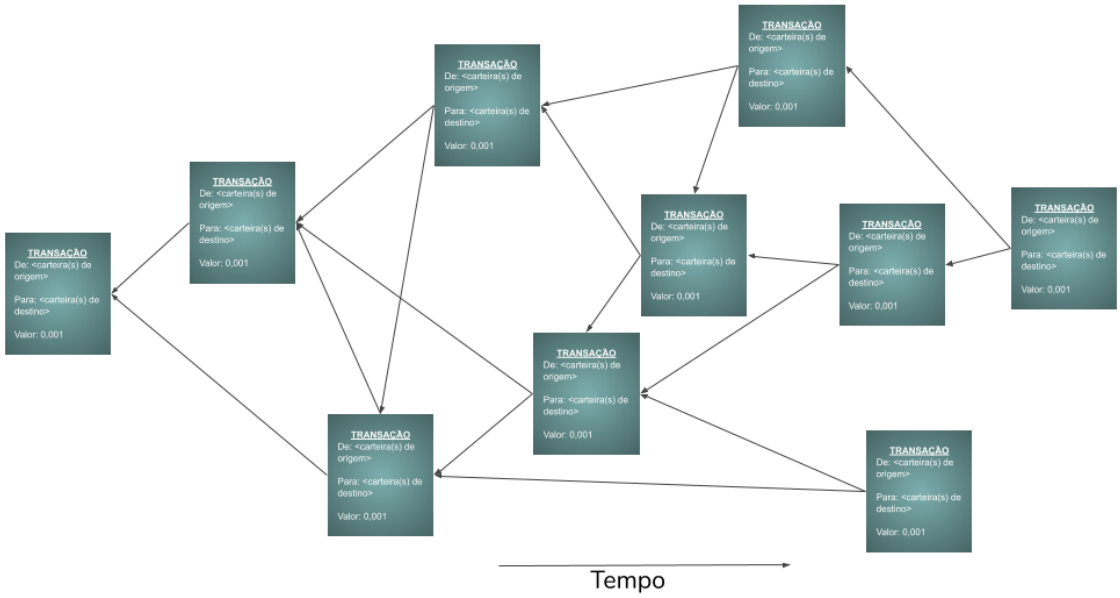

Figura 2.4: Estrutura Tangle

Assim como as demais características das DLTs, as estruturas de *ledgers* distribuídas também estão em constante mudança, surgindo novas tecnologias como *Hashgraph* (Baird, 2016) e *Holochain* (Harris-Braun et al., 2018), as quais prometem elevadas taxas de transações por segundo, novos mecanismos de consenso e diferentes finalidades de aplicação. A descrição dessas e demais estruturas está para além do escopo deste trabalho.

A seguir será feita uma descrição mais detalhada da dinâmica de funcionamento das três

criptomoedas mais utilizadas, as quais representam diferentes abordagens de DLTs.

2.1.2 Como funciona a Bitcoin

Em 09 de janeiro de 2009, Nakamoto lançou a primeira implementação da Bitcoin[3], a v0.1. A implementação fez uso de mecanismos já conhecidos como *hash*, infraestrutura de chaves públicas e redes ponto-a-ponto para compartilhar dados e armazena-los em uma estrutura de lista encadeada de blocos. Desta forma, a integridade dos dados presentes no livro de registro pode ser facilmente verificada, pois caso algum bloco tenha seus valores alterados, a cadeia será quebrada e todos os blocos posteriores tornam-se inválidos.

De acordo com o seu artigo publicado no ano anterior, Nakamoto define que uma moeda eletrônica é "uma cadeia de assinaturas digitais". Portanto, para executar uma transferência, o proprietário deve assinar digitalmente "um *hash* da transação anterior e uma chave pública do próximo proprietário", após esse procedimento, essas informações devem ser "adicionadas ao fim da moeda", ou seja, ao fim da cadeia de assinaturas. A Figura 2.5 representa as transações Bitcoin.

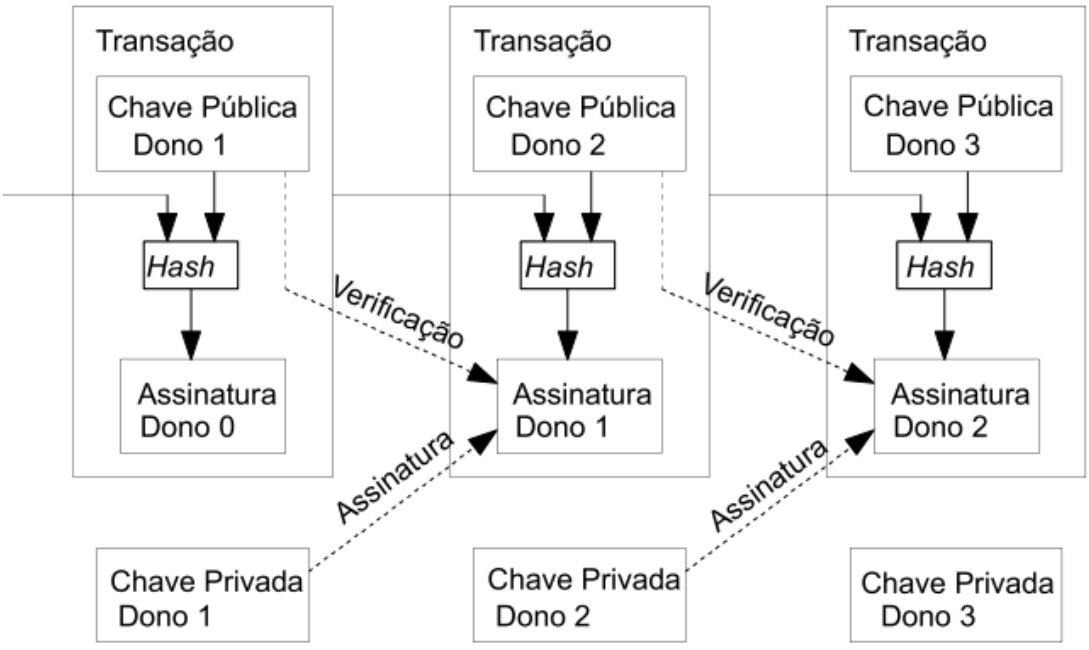

Figura 2.5: Transações da Bitcoin apresentadas em Nakamoto (2008)

[3]A mensagem de lançamento está disponível em "https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html"

Essas transações são protegidas através de assinatura digital e são destinadas para um endereço de carteira baseado na chave pública do destinatário e assinadas pela chave privada do remetente. Portanto, para gastar uma moeda, o usuário precisa provar que é o dono, através de sua chave privada daquela carteira, e todos as informações referentes as transações permanecem públicas no livro de registro.

Após a transação ser realizada, ela necessita passar pelo processo de validação seguindo algumas etapas. Quando um usuário Bitcoin realiza uma transação financeira enviando moedas para outro usuário, sua transação será depositada em um *pool* contendo todas as transações que ainda não foram inseridas em um bloco, portanto ainda não encadeadas na Blockchain. Os nós mineradores da rede, em troca de tarifas das transações e o direito de criar novas moedas para si, constroem blocos contendo transações não validadas e buscam por um *hash* que atenda as condições de dificuldade da rede. Essa dificuldade é variável e auto regulada para manter uma frequência de um bloco minerado a cada dez minutos.

Ao ser encontrado o *hash* adequado, o bloco é considerado minerado e enviado para os *full nodes* que armazenam todo o livro de registros. Todo *full node* deve efetuar uma série de verificações com o objetivo de confirmar a validade dos blocos e todas suas transações, bem como a integridade da cadeia. Só então, um bloco e suas transações são inseridos na *Blockchain* e sincronizados por toda a rede.

À medida que novos blocos são inseridos na cadeia, os anteriores tornam-se mais difíceis de serem modificados, pois se faz necessário ao usuário malicioso modificar todos os blocos subsequentes, e isso precisa ser feito em uma velocidade mais alta que a maioria dos nós participantes. Quanto mais antiga e profunda na *Blockchain* uma informação está, mais protegida contra modificações ela se torna.

Observando as características anteriormente apontadas, afirma-se que a *Bitcoin* é uma criptomoeda que possui uma DLT de primeira geração. Com acesso público ao livro de registros, seu mecanismo de consenso é a Prova de Trabalho (PoW) e a estrutura de dados utilizada para armazenamento de transações é a *blockchain*.

Em Fevereiro de 2020[4], a *Blockchain Bitcoin* estava adicionando à sua cadeia blocos com tamanho médio de 1,10MB. Um total de 616 mil blocos haviam sido validados e sua estrutura completa já ocupava o equivalente a 262GB, realizando 318 mil transações por dia.

[4]Valores extraídos de https://www.blockchain.com

2.1.3 Como funciona a Ethereum

Ether é uma moeda digital, nativa da *blockchain* denominada Ethereum, que surgiu alguns anos após a criação da Bitcoin. Essa criptomoeda, lançada em 2015, tem características bem similares à sua antecessora quando observada do ponto de vista funcional: é uma moeda puramente digital sem entidade centralizadora, com transações assinadas que necessitam aguardar validação para serem inseridas em uma *blockchain*.

As inovações trazidas pela Ethereum, dentre as quais destaca-se a capacidade de executar aplicações descentralizadas (*dApps*), e armazenar resultados na *blockchain* foram introduzidas por Buterin et al. (2014). Essas aplicações foram denominadas Contratos Inteligentes (*Smart Contracts*). O primeiro exemplo dado por Buterin para essas aplicações é um contrato onde "A pode retirar até X unidades monetárias por dia, B pode retirar até Y por dia, A e B juntos podem retirar qualquer valor e A pode interromper a capacidade de retirada de B".

> O que a Ethereum pretende fornecer é uma *blockchain* com uma linguagem de programação Turing-completa totalmente desenvolvida que possa ser usada para criar "contratos" que podem ser usados para codificar funções arbitrárias de transição de estado, permitindo que os usuários criem qualquer um dos sistemas descritos acima, assim como muitos outros, simplesmente escrevendo a lógica em algumas linhas de código. Buterin et al. (2014)

A linguagem de programação supracitada é chamada *Solidity*. Trata-se de uma linguagem orientada a objetos, de alto nível e para implementação dos contratos inteligentes - programas capazes de gerenciar o comportamento de contas dentro da *Ethereum*. A *Solidity* foi influenciada por *C++*, *Python* e *Javascript*, sendo projetada para executar dentro da *Ethereum Virtual Machine* (EVM), esse ambiente virtual encontra-se embutido em cada *Ethereum Full Node*. Ela é uma máquina virtual completamente isolada onde o código o qual está executando não tem acesso à rede, sistema de arquivos ou outros processos do computador hospedeiro, com exceção apenas à permissão de interagir com outros contratos.

Durante a execução de contratos inteligentes, a *Ethereum* utiliza a criptomoeda *Ether* como combustível para processar as instruções e pagar pelo seu esforço computacional aos nós que executam as aplicações. Esse mecanismo também de protege a rede de programas defeituosos ou maliciosos que possam ficar em execução por muito tempo ou para sempre, consumindo recursos dos nós.

Até 2020, a *Ethereum* utilizava-se apenas da Prova de Trabalho como algoritmo de consenso para validação de blocos em sua rede, assim como a *Bitcoin*. Mas, nesse ano, a DLT passa por uma atualização com maiores impactos na sua estrutura e uma dessas mudanças é o *Casper*, a implementação *Ethereum* do mecanismo de consenso por **Prova de Participação** (PoS).

Em resumo, *Ether* é uma criptomoeda pertencente a segunda geração de DLTs, a *Ethereum*. Ela é capaz de executar aplicações distribuídas que ficam armazenadas no seu livro de registros com o acesso público e, assim como a *Bitcoin*, a estrutura de dados utilizada para armazenamento de transações é a *blockchain*, utilizando dois mecanismos de consenso: a Prova de Trabalho (PoW) e a Prova de Participação (PoS).

2.1.4 Como funciona a IOTA

Pertencente terceira geração de criptomoedas, a **IOTA** é uma moeda otimizada para a Indústria 4.0 [5] e a Internet das Coisas (IoT) [6], buscando ser leve e rápida bastante para que dispositivos IoT possam realizar microtransações de maneira eficiente.

Dentre as mudanças para as DLTs utilizadas até então, a IOTA introduz uma nova estrutura para armazenamento de transações denominada *Tangle*. Essa solução apresentada é capaz de reduzir os efeitos de um dos pontos fracos da *blockchain*: a capacidade de validação de transações por segundo, pois a Prova de Trabalho em conjunto com a *blockchain* logram êxito em impedir o gasto duplo de usuários, sem a necessidade de uma entidade intermediária, mas o custo desse arranjo é a dificuldade de encadear muitos blocos em curto período de tempo.

A estrutura *Tangle* não agrupa as transações em blocos, elas são inseridas individualmente na DLT, o que exige que o usuário valide duas outras transações existentes no livro de registro. Dessa forma, não existe um limite definido para a quantidade de transações que possam ser confirmadas por segundo (TPS), quanto mais usuários transacionando, maior a capacidade da rede em verificá-las. Chamado de *pay-it-forward*, esse sistema de validação não cobra tarifas de seus participantes, demandando apenas um pouco de poder computacional para validação de transações prévias.

[5] Indústria 4.0 é um conceito que representa a quarta revolução industrial onde um conjunto de tecnologias, como a Inteligência Artificial, Robótica e Big Data, permitem a fusão do mundo físico, digital e biológico.

[6] Redes de objetos físicos conectados à internet com capacidade de execução de tarefas coordenadas.

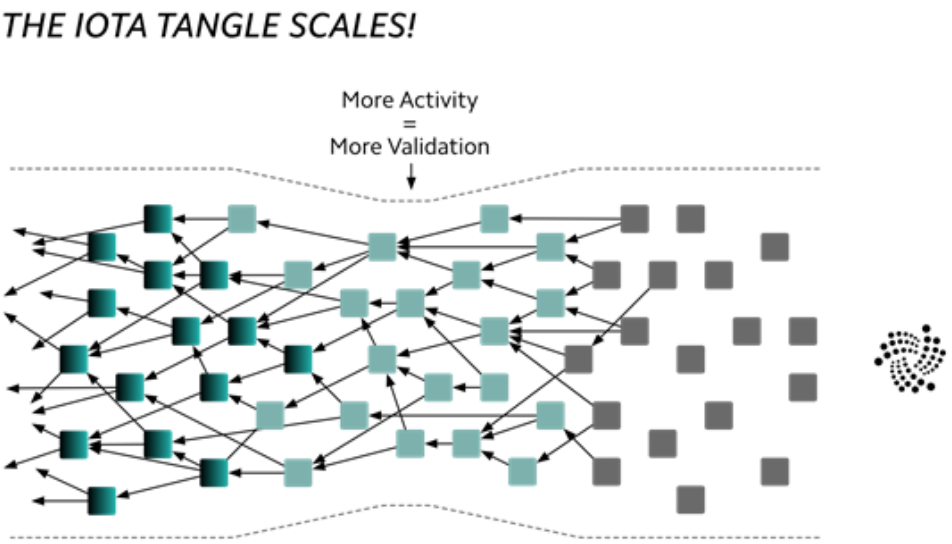

Figura 2.6: Iota e sua capacidade de validação, disponível em: *https://www.iota.org/get-started/faqs*

Outra característica da IOTA, apresentada por Popov (2016), é sua resistência à computação quântica. Esse é um problema futuro conhecido para a rede Bitcoin e demais DLTs que utilizem a Prova de Trabalho convencional. O campo *nonce* desta tecnologia foi projetado para que o tempo de encontra-lo não seja maior que o tempo para realização de outras tarefas da transação, fazendo com que o poder computacional de computadores quânticos não tenham muita relevância no processo de validação de transações.

Contratos inteligentes também estão sendo implementados para a Iota através do protocolo *Quibic* [7].

2.2 Privacidade, Anonimato e as Misturadoras de Criptomoedas

No intuito de equiparar às vantagens do sistema bancário tradicional, se faz necessário que as criptomoedas realizem a implementação de alguns princípios de segurança como, por exemplo, a privacidade das informações, pois quando o cliente de um banco tradicional efetua

[7]Mais informações podem ser encontradas no site do projeto https://qubic.iota.org/intro), o qual descreve soluções para *oracle machines*, *smart contracts*, *outsourced computations* e mais.

uma transferência de sua conta para conta de outro cliente, estas informações são conhecidas apenas pelas partes envolvidas na transação e o próprio banco. Para a proposição de uma moeda virtual eletrônica onde não encontre-se uma terceira parte de confiança, existe um problema de privacidade das informações pois, a *blockchain* permite que qualquer interessado possa verificar todas as transações já feitas pelo sistema, causando uma quebra no princípio da privacidade.

Em contexto de segurança digital, anonimato e privacidade costumam ser conceitos que têm seus significados misturados ou confundidos e, por vezes, mencionados de maneira errônea quando trata-se de criptomoedas. Como citado por Bradbury (2014), Khalilov e Levi (2018), privacidade diz respeito a esconder o conteúdo, enquanto anonimato refere-se a quem é o proprietário dele.

Blockchains públicas, como as apresentadas anteriormente, são transparentes e armazenam informações de modo que possam ser acessadas por qualquer usuário da rede interessado em obter esses dados, portanto os proprietários dessas criptomoedas não possuem privacidade sobre esse material. Dentre as informações disponíveis estão as listas de *Inputs* e *Outputs* contendo endereços de carteiras de origem e destino da transação. Entretanto, na cadeia de blocos nenhuma informação dos usuários é guardada, além dos valores transacionados e endereços de carteiras, sendo esses endereços pseudônimos para os usuários, logo podemos classificar a Bitcoin e outras criptomoedas como pseudoanônimas. Nelas não é registrada nenhuma relação entre usuários no mundo físico e suas carteiras virtuais como explica Nakamoto (2008), "O público pode ver que alguém está enviando uma quantidade para outra pessoa, mas sem informações que ligam a transação a qualquer um".

Outrossim, a característica de transparência pode ser explorada por indivíduos maliciosos, mesmo não havendo uma identificação obrigatória entre um usuário e seus endereços de carteiras, estes podem ser associados ao seus donos por diversos meios como: identificação de endereço IP de onde foram disparadas as transações, compras *on line* em lojas que necessitam identificar seus clientes; câmbio de moedas em exchanges, que exigem cadastros; pagamento ou transferência de criptomoedas entre pessoas conhecidas, dentre outros. Observando e rastreando os endereços também é possível identificar o saldo e todo o histórico de transações daquelas carteiras, como apontado por Moser (2013), "devido ao fato de que todas as transações são armazenadas publicamente na *blockchain*, o anonimato de um

remetente depende do pseudônimo não estar vinculado à sua verdadeira identidade". Dessa forma, o anonimato e a privacidade dos usuários de Bitcoin e outras criptomoedas podem ser ameaçados.

Por variados motivos, que vão do legítimo direito ao sigilo financeiro à ocultação de crimes, o anonimato e a privacidade podem ser desejo ou necessidade dos usuários de criptomoedas, por este motivo mecanismos foram criados para suprir tal necessidade, entre eles, as **mixers** de criptomoedas que também podem ser chamadas de **redes de mistura** ou **serviços de lavanderia** e "são usadas para impedir o rastreamento de atividades de mensagens através de uma rede, incluindo uma sequência de intermediários ou uma estrutura de *pool*" (Khalilov e Levi, 2018), "ofuscar as transações e reduzir o risco de desanonimização" (Feng et al., 2018).

Diversas técnicas de mistura de criptomoeda já foram registradas e debatidas por Valenta e Rowan (2015) e Feng et al. (2018), elas podem ser divididas em dois grandes grupos: as *Misturas Centralizadas* e as *Misturas Descentralizadas*. Dentre elas algumas técnicas são: *CoinSwap*, *Mixcoin*, *BlindCoin CoinJoin*, *CoinShuffle*, *JoinMarket*, *CoinParty*, além dos serviços publicados na web.

De acordo com Ruffing et al. (2014), um protocolo de mistura de Bitcoin deve prover os seguintes objetivos de privacidade e segurança:

- **Desconectabilidade**: Após uma transação de mistura bem sucedida, não pode haver ligação entre os endereços de entrada e saída de um participante honesto;
- **Verificabilidade**: Um atacante não pode ser capaz de roubar ou destruir moedas de um participante honesto
- **Robustez**: O protocolo deve eventualmente ser bem sucedido mesmo na presença de participantes maliciosos enquanto os links de comunicação permanecerem confiáveis.

2.2.1 Serviços de Misturas Centralizadas

Existem diversos prestadores de Serviços de Misturas Centralizadas na web oferecendo privacidade e anonimato na *blockchain* em troca de uma porcentagem do valor transacionado.

Para promover o anonimato para as carteiras finais, os serviços misturadores fornecem ao cliente um endereço de carteira para o qual devem ser enviadas as moedas que serão

embaralhadas/trocadas e o cliente informa para qual, ou quais, carteiras devem ser enviadas as novas moedas. As interfaces de usuário para operação desses sistemas costumam oferecer algumas personalizações de configuração, tais como:

- Dividir o destino das moedas para 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 (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, utilizando ativos de sua reserva e de outros clientes. Cada um dos prestadores desses serviços utilizam algoritmos próprios (e não revelados) que buscam embaralhar as moedas e evitam que sejam retornadas para os proprietários originais (Figura 2.7).

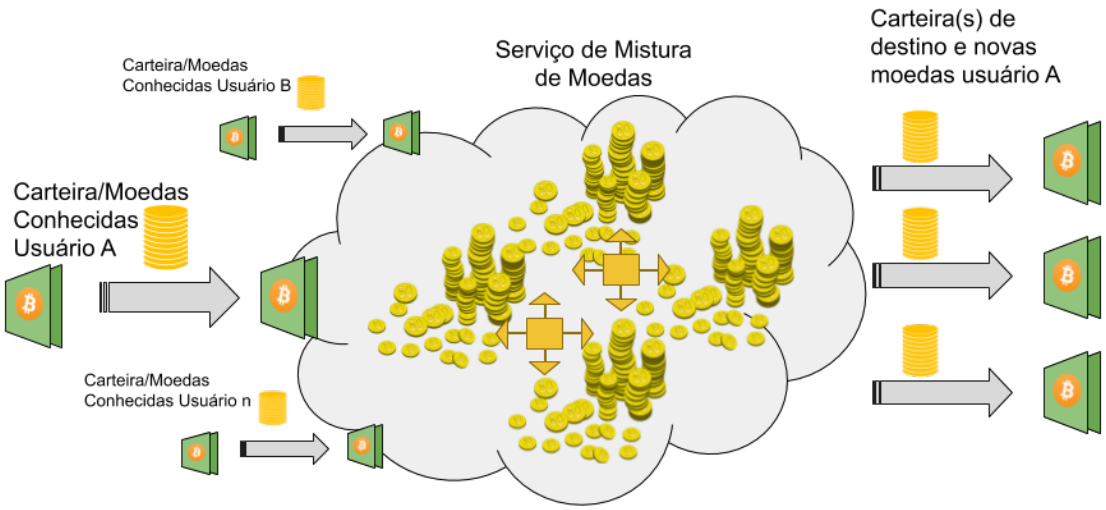

Figura 2.7: Serviço de mistura centralizada

Dois riscos estão envolvidos nesta modalidade de mistura (Feng et al., 2018): i) o provedor de serviço ser um atacante e roubar os ativos dos clientes; e ii) o prestador de serviço pode guardar registros das transações, não havendo garantias que os dados dos usuários não sejam divulgados. Alguns protocolos de mistura centralizada já foram propostos na tentativa de minimizar os riscos: *CoinSwap* (Maxwell, 2013b), *Mixcoin* (Bonneau et al., 2014) e o *Blindcoin* (Valenta e Rowan, 2015).

2.2.2 Serviços de Mistura Descentralizadas

Diferente dos serviços anteriores, estes protocolos de mistura não possuem um ponto central que possa roubar ativos dos usuários, registrar operações, sofrer ataques de DoS ou cobrar taxas, além de ser mais próximo e mais compatível com a estrutura descentralizada da *Blockchain* (Feng et al., 2018). Essa estatégia foi primeiramente descrita por Maxwell (2013a) no Bitcoin Forum[8], com o intuito de recuperar a privacidade de usuários evitando a marcação de moedas, ele propõe que "Quando você quiser realizar um pagamento, encontre outra pessoa que também queira efetuar um pagamento e façam um pagamento conjunto". O objetivo é unir várias transações em uma só, multi assinada, contendo ***n*** entradas e saídas, desta forma eliminando os custos de tarifas cobradas pelas mixers centralizadas. Maxwell batizou o procedimento como *CoinJoin*.

A estratégia *CoinJoin* consegue reduzir as taxas cobradas pelas mixers centralizadas, por motivo das moedas serem misturadas pelos próprios usuários, além de não poderem ser impedidas por autoridades e governos, porém também possuem falhas. Conseguir eficiência em anonimato, pode ser difícil e requer um alto número de participantes nas transações, pois quanto menos usuários ingressarem, mais fácil se torna identificar a origem das moedas.

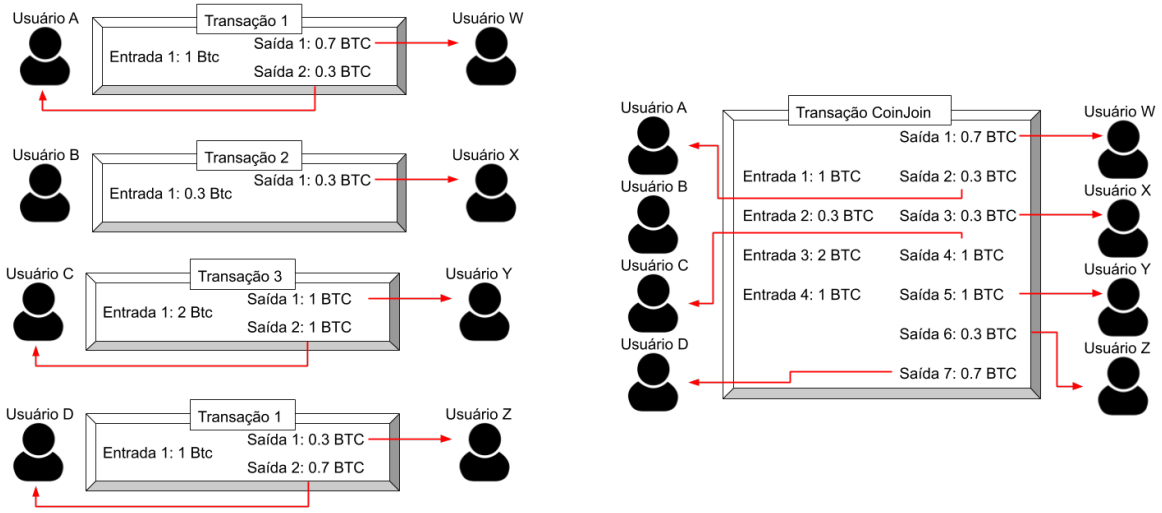

Figura 2.8: Protocolo CoinJoin

Implementações da estratégia de mistura descentralizada *CoinJoin* foram publicadas nos anos subsequentes, utilizando de criptografia para aumento de anonimato das transações.

[8]Disponível em: https://bitcointalk.org/index.php?topic=279249.0

Entre eles: *CoinShuffle* (Ruffing et al., 2014), *JoinMarket* (Belcher, 2015), *CoinParty* (Ziegeldorf et al., 2015).

2.2.3 Criptomoedas com Prioridade em Anonimato

Desenvolvedores e usuários mais inquietos com a segurança de suas informações nas DLTs públicas, considerando insuficiente o nível de segurança fornecido por elas, criaram novas criptomoedas capazes de elevar o grau de privacidade e anonimato através da implementação de novas tecnologias e conceitos, como pode-se observar nos exemplos a seguir:

- A criptomoeda **Monero**[9], descrita em Noether (2015), esconde origem e destino de suas transações ao utilizar *assinaturas em anel*, *transações confidenciais* e *endereços sigilosos*, impedindo o rasteamento das moedas e identificação dos usuários;

- A moeda **Zcash** [10] utiliza a tecnologia *zn-SNARKs* (*Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*), uma implementação da criptografia *Zero-Knowledge Proof* Hopwood et al. (2016) capaz de proteger a privacidade dos usuários realizando verificação de transações sem a necessidade de revelar seu emissor ou receptor;

- A **Dash**[11], publicada em Duffield e Diaz (2018), disponibiliza para seus usuários uma opção denominada Envio Privado (*PrivateSend*) onde, pagando um pouco mais de taxas, a rede utiliza um mecanismo de embaralhamento descentralizado por *coinjoin* para mitigar tentativas de rastreamento de suas moedas.

2.3 Considerações Finais

A Bitcoin concretizou o conceito de moeda digital ponto a ponto e sem uma terceira parte a qual os usuários precisassem confiar para controlar e armazenar as transações, assim iniciando um período efervescente em surgimento e desenvolvimento de criptomoedas. Assim como o dinheiro físico e cartões de crédito possuem falhas, sofrem ataques e fraudes, o novo

[9] https://web.getmonero.org/
[10] https://z.cash/
[11] https://www.dash.org

dinheiro digital também possui seus infortúnios e fraquezas. Seus usuários utilizam-no para os mais diversos fins e a privacidade financeira continua a ser um direito requerido, ainda que, por concepção, a Bitcoin e outras criptomoedas não consigam manter a privacidade das transações registradas no livro razão. As DLTs públicas são legíveis por quaisquer interessados e os registros são armazenados por estruturas de dados amplamente replicadas.

Para fornecer uma alternativa de privacidade e anonimato, protocolos, novas criptomoedas focadas em sigilo e serviços de mistura estão disponíveis aos interessados. A análise dos serviços de mistura centralizados, abordados acima e facilmente encontrados na web estarão em foco nos próximos capítulos deste trabalho.

Capítulo 3

Trabalhos Relacionados

A Bitcoin e a Blockchain são tecnologias que estão sendo pesquisadas por toda a última década em diversas áreas incluindo a segurança. 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* através de rastreamento das transações na blockchain. Já em 2018, Hong et al. publicaram um trabalho onde executaram testes em 5 mixers durante o ano de 2017, com auxílio de uma ferramenta chamada *Chainalysis*[1], chegando a um algoritmo de *de-mixing* baseado em horários de transação. Os próprios criadores da Bestmixer (uma das *mixers* estudadas neste trabalho) publicaram no fórum em Bestmixer (2018), falhas das misturadoras 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

[1]Software proprietário de monitoramento de transações. `https://www.chainalysis.com/`

esquemas atuais e futuros de lavagem de dinheiro". Outros autores também publicaram trabalhos acerca de como criptomoedas podem favorecer a crimes financeiros e discutem sobre a necessidade de regulamentação, como Albrecht et al. (2019) e Foley et al. (2019).

Em Khalilov e 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 de Janeiro de 2009 até 01 de Janeiro de 2017, 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 realizada 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 e Costa (2018) apresenta uma proposta de identificação de carteiras. Um serviço chamado *Address Name System* ou ANS. Nesta proposta apresentam-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 e um endereço de carteira, e retorna ao usuário a identidade declarada, se houver uma.

Outro trabalho que busca a identificação de usuários *Bitcoin* pode ser encontrado em Juhász et al. (2018), aqui os autores utilizaram softwares clientes modificados para realizar o monitoramento de mensagens na rede *Bitcoin*, reconhecendo os endereços IP envolvidos e, após meses de capturas de mensagens, foram capazes de relacionar milhares de usuários e endereços de carteiras vinculando-os a localizações geográficas através de uma abordagem *bayesiana*.

Capítulo 4

Avaliação do Funcionamento de *Mixers*

Os serviços de **mistura centralizada** de criptomoedas são o objeto de estudo deste trabalho e, neste capítulo, encontra-se uma análise a respeito do funcionamento desses serviços, sua eficácia, custos envolvidos, riscos para o usuário e a tentativa de compreensão dos protocolos utilizados para essa categoria de mistura de criptomoedas.

4.1 Modalidades de Rastreamento

Embora o sigilo financeiro com anonimato e privacidade sejam justificativas legítimas para que proprietários de criptomoedas possam fazer uso das misturadoras, a quebra de seus protocolos, a descoberta do relacionamento entre as carteiras de origem e destino, bem como a identificação de carteiras pode tornar-se uma necessidade em situações que envolvam crimes como sonegação, lavagem de dinheiro e mercado ilegal.

De acordo com o relatório Trace (2019), o total de fraudes e roubos relacionados a criptomoedas no ano de 2019 foi de US $ 4,5 bilhões, dos quais US $ 370,7 milhões foram perdidos em roubos de *exchanges* e falhas de segurança, e US $ 4,1 bilhões em perdas decorrentes de fraude e apropriação indébita de fundos.

A análise e investigação da *blockchain* em busca de crimes se faz, cada vez mais, uma necessidade das forças da lei e de governos, como cita o delegado Zumas (2020) “o conhecimento mínimo acerca do tema (e em diversos outros ligados à investigação e tecnologia) pode proporcionar o início para o deslinde de vários crimes, antes vistos como insolucionáveis caso o agente não tivesse (sic) atento à “criptoinvestigação”.

Empresas voltadas pra segurança e análise de criptomoedas e blockchains iniciaram seus trabalhos e já divulgam o desenvolvimento de ferramentas de criptoanálise em seus websites, como a *Chainalysis*[1] e a *Ciphertrace*[2], contudo o acesso a essas ferramentas é restrito ao seus clientes, para mais os algoritmos e protocolos implementados nos sistemas são caixas pretas, assim como nas misturadoras de criptomoedas, tornando-se de difícil acesso acadêmico.

Os serviços de mistura e embaralhamento, por definição, precisam entregar moedas que não possuam relação com as enviadas pelo usuário no início do processo, fornecendo assim o anonimato que fora perdido após uma possível marcação de criptomoedas. Para isso, não deve existir qualquer vínculo entre as carteiras de origem e destino dos ativos, seja antes ou após a mistura. Quando as transações bitcoin ocorrem de maneira comum e direta, de uma carteira A para outra carteira B, essa localização é facilmente rastreada no livro de registros, porém, ao passar pelas lavanderias de criptomoedas a ligação $A \rightarrow B$ é perdida.

Dessa forma, haveriam dois possíveis caminhos a serem investigados para identificação das moedas e carteiras que passaram por uma misturadora:

- *Rastreamento da Carteira de Destino;* e
- *Rastreamento da Carteira de Origem*.

4.1.1 Rastreamento da Carteira de Destino

Essa estratégia de rastreamento das criptomoedas é aplicável quando a parte interessada na localização dos ativos conhece algum endereço de carteira onde as moedas estiveram sob posse em um determinado momento T_0 e deseja identificar em qual endereço estão as criptomoedas (ou parte delas) em um momento posterior T_1.

Uma situação onde um criminoso tenha fornecido um endereço de carteira para depósitos de pedido de resgate por sequestro de dados, e agora o endereço não possua mais moedas, é um exemplo onde essa estratégia faz-se desejada.

[1] https://www.chainalysis.com/
[2] https://ciphertrace.com/

4.1.2 Rastreamento da Carteira de Origem

Essa estratégia se aplica quando a necessidade de rastreamento de criptomoedas parte de maneira inversa no tempo, desejando a localização de onde estavam os ativos no instante T_0, sabendo-se da localização delas no instante $T_1 > T_0$.

Como exemplo da utilização dessa estratégia, supõe-se o cenário onde um suspeito de lavagem de dinheiro, com localização atual de seus criptoativos conhecida, pode ter suas transações rastreadas dessa maneira, em busca de uma possível confirmação de que aquelas moedas passaram por uma misturadora e identificar a real carteira de origem, a qual poderia estar diretamente vinculada à origens e motivações espúrias.

Ambas as estratégias podem ser usadas de forma complementar para a comprovação da relação entre dois endereços de carteiras aparentemente sem ligação na *blockchain* mas que estão vinculadas à operações de mixagem de moedas.

4.2 Dinâmica de Funcionamento de *Mixers*

Para entender a dinâmica de funcionamento das *misturadoras* de criptomoedas, foi realizada uma avaliação exploratória de algumas delas. Neste sentido, foi testado e analisado o serviço de quatro *mixers* centralizadas.

O primeiro passo foi a identificação e seleção dos serviços a serem testados. Como não foram encontrados textos acadêmicos que catalogam ou ranqueiam os serviços dos mixers, foi utilizada como referência uma lista contendo as "9 melhores serviços misturadores de Bitcoin" [3].

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 três serviços foram rotulados como sendo "não aprovados" e de "muito grande risco": *Grams Helix*, *BTC Blender* e *Coinmixer*.

Mais tarde viria a ser publicado o relatório *Q2 2018 cryptocurrency anti-money laundering report* (Trace, 2018) onde seriam catalogados treze serviços de mistura: *Bitblender*, *Bitcloak*, *BitcoinFog*, *BitLaunder*, *Bitmixer*, *Coinmixer*, *DarkLaunder*, *Helix*, *Helix2*, *Helix-light*, *HelixMixer*, *Outlawtumbler* e *Penguinmixer*.

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

Os testes exploratórios foram realizados com dois dos serviços considerados "melhores e mais populares" (**Bestmixer**[4] e **Blender.io**[5]) e com dois dos considerados de grande risco (**Helix Light Grams**[6] e **BTC Blender**[7]).

4.2.1 Realizando Transações de Mixagem

Os serviços de mistura apresentam alguns parâmetros comuns entre si para que um cliente inicie seu processo de anonimização de moedas. A prestadora fornece um endereço de carteira para onde o cliente deve enviar as moedas a serem trocadas, e um conjunto de parâmetros que precisam ser configurados:

- Quantidade de carteira onde as novas moedas serão entregues;
- Endereço das carteiras de entrega;
- Taxa de serviço a ser cobrada pela misturadora;
- Tempo de atraso entre as entregas das moedas após a confirmação de depósito.

A depender do serviço utilizado, outros parâmetros podem ser fornecidos para configuração, mas os apresentados acima estão presentes em todas as misturadoras estudadas. A Figura 4.1 apresenta o exemplo de uma página web de misturadora para configuração dos parâmetros mencionados.

A configuração padrão para os testes realizados neste trabalho 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 a confirmação do envio e o recebimento das novas moedas é de 2 horas para cada carteira de destino.

O serviço *BTC Blender* 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%.

[4] `https://bestmixer.io/`
[5] `https://blender.io/`
[6] `https://helixmixer.org/helix/light.html`
[7] `https://btcblender.com/`

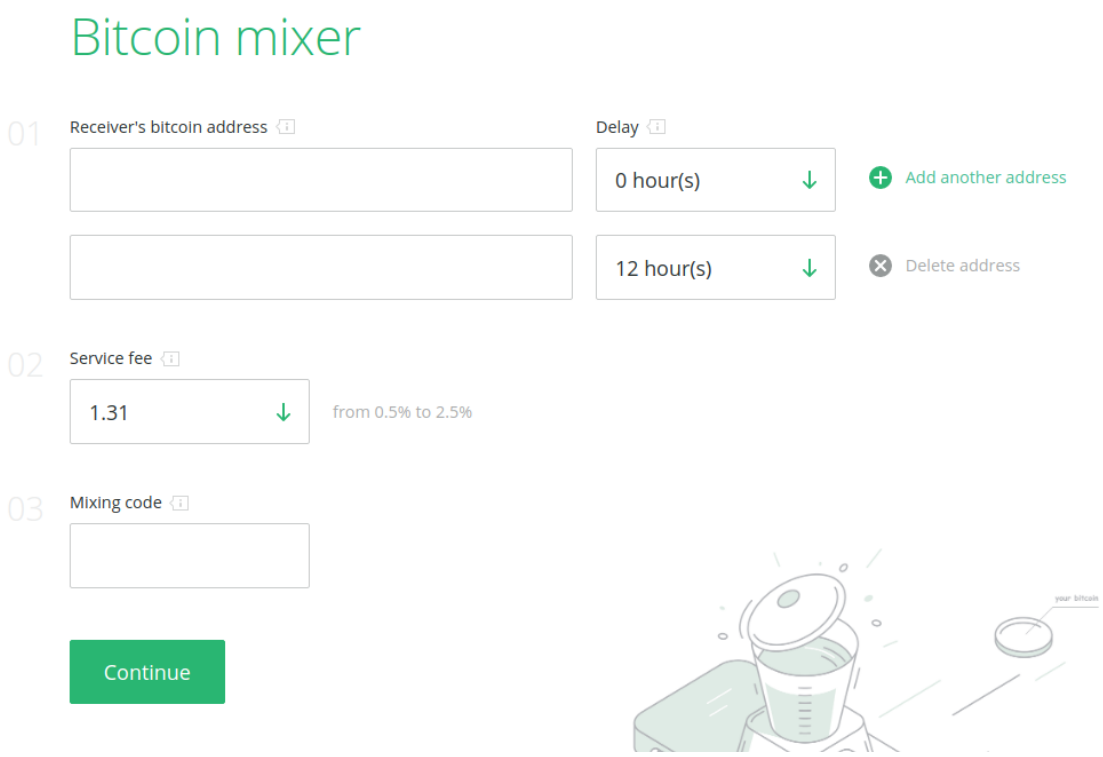

Figura 4.1: Página web de configuração de uma misturadora
Fonte: https://blender.io/

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 4.1. Nela encontram-se as datas das transações, bem como as taxas cobradas nominalmente para a mistura, o total recebido pelo cliente e especificação dos valores reais que foram "consumidos"durante as operações.

Tabela 4.1: Configurações dos experimentos e saldos pós mistura

Data	Mixer	Taxa (%)	Enviado	Total Recebido	Total Consumido	Taxa Efetiva(%)
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*	1,350	0,001	0,00078650	0,00021350	21,35
16/11/2018	*Blender.io*	1,350	0,001	0,00078650	0,00021350	21,35
31/10/2018	BTCBlender	1,000	0,001	0	0,00100000	100
31/10/2018	Helix	2,500	0,001	0	0,00100000	100

A etapa seguinte ao processo de testes dos serviços foi 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.

4.2.2 Rastreando as Transações de Mixagem

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*[8], desenvolvidos em Python para este experimento, utilizando o módulo *blockexplorer* da *api-v1-client-python*[9].

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, as carteiras de destino.

O valor utilizado por padrão para o parâmetro **T** foi 10, que recebeu esse valor pois consultas com carteiras possuindo mais de 10 transações costumam retornar movimentações muito antigas. 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 possíveis endereços pertencentes aos núcleos dos *pools*. A estratégia adotada para chegar ao núcleo foi aumentar gradativamente o valor de **N** até encontrar interseções com 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 vari-

[8]Disponível para download em: `http://bit.ly/mixersscript`
[9]Disponível em: `https://github.com/blockchain/`

ando 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 4.4, 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*[10], uma plataforma de código aberto para visualização de redes complexas e integração com qualquer tipo de atributo de dados.

4.2.3 Rastreando os Endereços de Carteiras Envolvidos

A tarefa de rastrear o caminho percorrido pelas moedas, seja da entrada nas *mixers* até um provável núcleo das redes misturadas, ou o seu inverso, da chegada nas novas carteiras até o núcleo, foi automatizado como descrito na Seção 4.2.2.

A análise dos dados levantados apontam para: i) valores elevados de Bitcoins sendo repassados através dessas redes de mistura; ii) carteiras que podem participar da rede de mais de uma misturadora e iii) uma rede complexa de carteiras transacionando entre si.

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 enormes em criptomoedas. Nas Tabelas 4.2 e 4.3 encontram-se dados dos 10 (dez) endereços de carteiras identificadas no núcleo das transações de mistura que mais movimentaram criptomoedas.

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

Tabela 4.2: 10 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
8	<38f8RHFQ...>	77.213,8821	77.119,2209	94,6613
9	<1NyfNYAX...>	76.709,4172	76.709,4172	0,00
10	<14scL4Vj...>	74.326,5540	74.326,5540	0,00

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*[11] em 18 de Novembro de 2018, cujo valor da Bitcoin era de $5.594,97. De acordo com esse ranking mostrado na Tabela 4.2, as 10 primeiras carteiras também movimentaram cifras milionárias.

Tabela 4.3: As dez 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
8	<1Lsqcv4c...>	1.943.532,7903	1.943.532,7903	0,00
9	<1J37CY8h...>	1.620.483,2415	1.614.471,3025	6.011,9390
10	<1DrrYDDR...>	263.015,5788	262.484,7745	530,8043

Na Tabela 4.3, 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

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

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 dos dados é a existência de uma mesma carteira encontrada nas redes de embaralhamento das duas mixers, o endereço <1NDyJtNT...>, uma das carteiras com alto volume e valor de transações. Esse endereço pertence a Exchange Binance[12], como revelado pelo perfil oficial da mesma no twitter[13]. Após essa constatação, também foram descobertos outros endereços de carteiras pertencentes as *exchanges* que também estão presentes nas Tabelas 4.2 e 4.3, entre eles: <1Kr6QSyd...> [14] pertencente a Bitfinex[15], <1J37CY8h...>[16] pertencente a Gemini[17] e <1N52wHoV...>[18] de propriedade da Bittrex[19].

Outro endereço de carteira que foi encontrado no rastreamento das transações nas duas misturadoras é o <1BestMix...>. Esta carteira pertence ao *pool* da *Bestmixer* e, em diversas transações onde foi encontrada, é usada para receber e efetuar transferências de valores menores que 1BTC. Consultando a *blockchain* encontra-se milhares de envios de valores iguais a 0,00000888 saindo desse "hub" para diferentes carteiras.

A quantidade de carteiras encontradas durante o rastreamento, bem como suas ligações através de transações, é elevada e difícil de serem analisadas caso a caso, por isso estão apresentados a seguir gráficos que buscam demonstrar as relações rastreadas nessas redes de mistura.

[12] https://www.binance.com/

[13] https://twitter.com/binance/status/961666467325358081

[14] Identificada em: https://www.reddit.com/r/bitfinex/comments/7ihnz5/now_almost_350000000_in_hot_wallet_bitfinex/

[15] https://www.bitfinex.com/

[16] Identificada em: https://www.reddit.com/r/Gemini/comments/7duvl7/dear_gemini_please_stop_wasting_precious/

[17] https://gemini.com/

[18] Identificada em: https://www.reddit.com/r/Bitcoin/comments/7kxblo/is_bittrex_helping_to_manipulate_btc_drop/

[19] https://global.bittrex.com/

4.3 Visualização Gráfica das Operações de Mixagem Rastreadas

Após o levantamento de dados da *blockchain* explicado na Seção 4.2.2, 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.

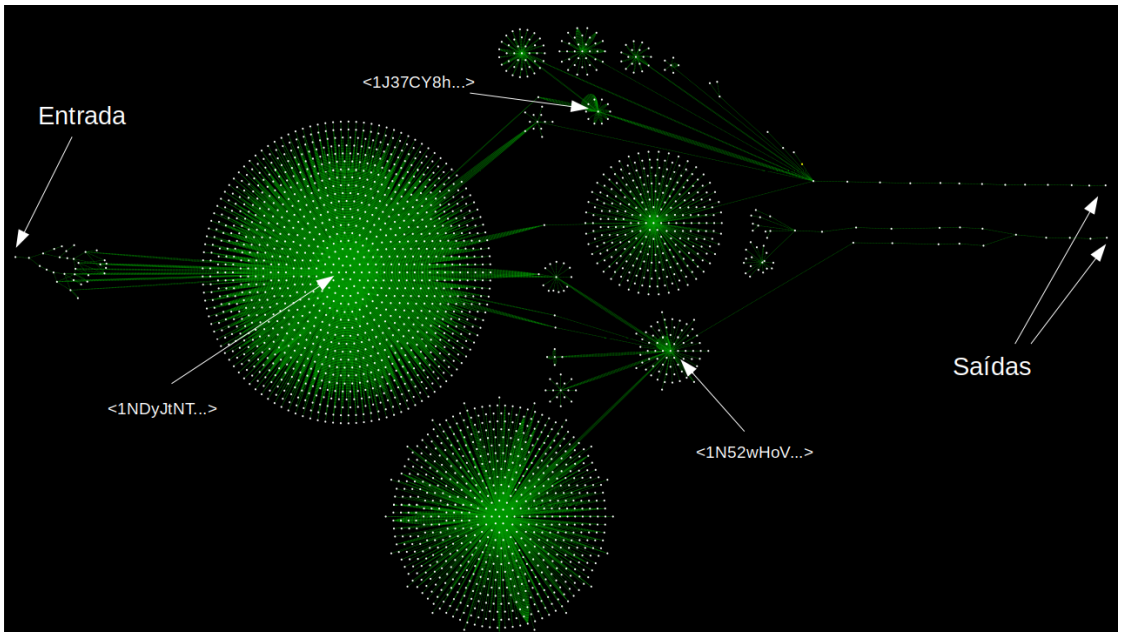

Figura 4.2: Grafo de rastreamento da Bestmixer

Nos grafos apresentados nas Figuras 4.2 e 4.3, 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.

Na Figura 4.2, está representado o rastreamento realizado em uma das operações de mistura testadas com o serviço *Bestmixer* e nela estão identificadas também três carteiras entre as que possuem maiores valores de movimentação de moedas durante o período de testes (prováveis exchanges), conforme Tabela 4.2. 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.

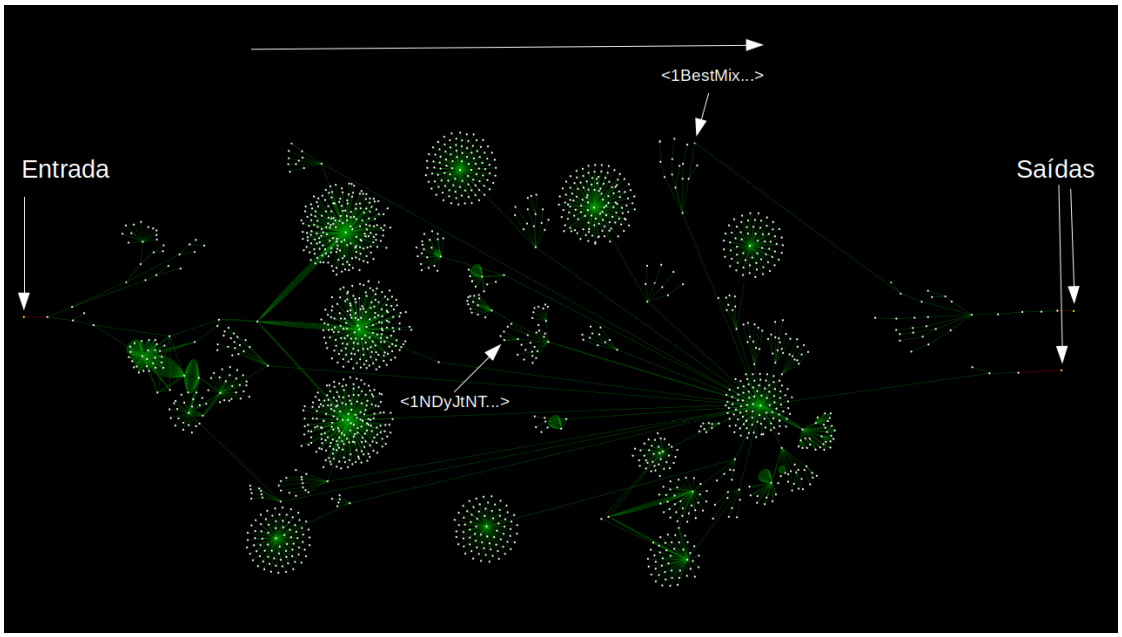

Figura 4.3: Grafo de rastreamento da Blender.io

A Figura 4.3, 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...>, assim fazendo surgir a suspeita de adoção da *API Bestmixer*, por parte da Blender.io, em sua rede de misturas.

4.3.1 Centralidade de Grau das Carteiras Envolvidas

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

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

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

Tabela 4.4: Carteiras com maior centralidade de grau

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

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 4.4.

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.

Carteiras com alto grau de entrada ou de saída não são encontradas nas bordas das redes analisadas, pois carteiras de entrada nas redes de mistura costumam possuir apenas 2 transações (k_i), bem como os endereços que realizam a entrega das moedas aos clientes. Esta medida pode ser utilizada para identificar carteiras no núcleo das lavanderias, suas reservas.

4.4 Considerações Finais

Como dito em Böhme et al. (2015) os protocolos de mistura geralmente não são públicos, portanto difíceis de terem sua eficiência avaliada. Até esta fase algumas informações relevantes foram levantadas acerca da dinâmica operacional e do nível de eficiência dos serviços em pauta.

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", após completadas todas as etapas de mistura, terá duas transações: i) uma de recebimento do valor depositado pelo cliente e ii) uma de envio para uma (ou mais) carteira(s) seguinte(s) que também são de posse da mixer. Logo, as carteiras de entrada das *mixers* são endereços de uso único.

Ao consultar na *blockchain* a carteira de entrada fornecida pelo serviço *Helix Light Grams* <13jnQqaJ...>[20], 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 e nenhuma de saída.

Os serviços *Bestmixer* e *Blender.io* realizaram a entrega das novas moedas nos endereços previamente configurados. Quanto aos valores devolvidos, são variáveis e uma parcela bem superior à taxa de serviço cobrada pela misturadora 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 4.1 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

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

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 dos ativos, em geral, são serviços apócrifos e desvinculados 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 4.3, a qual relaciona um sumário do possível 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 nas seções anteriores. Em ambos os casos é plausível identificar comportamentos comuns de seus algoritmos. Ao analisar o serviço dessas duas *mixers* conclui-se que a mistura dos bitcoins pode custar mais de 20% do valor de entrada enviado pelo cliente.

No que tange a eficiência, quando tentado estabelecer um caminho a partir dos endereços de entrada das moedas, não é possível encontrar a carteira de destino fazendo uso das ferramentas públicas de análise da *blockchain*. É notado que os serviços testados com sucesso mantém as moedas de entrada paradas e só as movimentam após as novas moedas serem entregues às carteiras finais dos clientes, desta forma impedindo a relação direta entre as moedas de entrada e as moedas 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 e 21 horas* e *2 dias e 18 horas*, não sendo possível encontrar padrões precisos no tempo de armazenamento e repasse dessas moedas.

Ainda tratando-se de horário de transações, desenvolvedores da *Bestmixer* (2018) descobriram e reportaram uma falha de misturadoras da época que não randomizavam o horário de entrega das novas moedas aos clientes. Chegaram a construir uma ferramenta denominada CAE-check (*Coin Anonymisation Event-check*) que era capaz de analisar essa vulnerabilidade nas *mixers* existentes. Na prática, a ferramenta verificava 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 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 nos experimentos aqui apresentados 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 da terceira confirmação de cada uma das transações de entrada e, em especial, os horários de criação das transações de saída (pagamento ao cliente) vindas das *mixers* testadas, é possível identificar que a *Bestmixer* utilizou um maior fator de aleatoriedade para efetuar os pagamentos de cada uma das carteiras de destino, enquanto que a *Blender.io* demonstra ter períodos de tempo de pagamento mais constantes que podem auxiliar a análise da mistura em busca de origem ou destino. Os dados podem ser encontrados na Tabela 4.5.

Tabela 4.5: Horários de confirmação de envio e devolução de novas moedas

	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	15:43:25
Recebimento Carteira 1	13:50:09	02:03:09	01:11:04	17:44:33
Recebimento Carteira 2	15:59:07	04:11:08	01:11:05	19:44:04

Considerando as informações apresentadas anteriormente, em conjunto com a informação de que o serviço *Bestmixer* fornece gratuitamente uma API (*Application Programming Interface*)[21] 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.

Verifica-se também que diversos endereços rastreados durante esse experimento, que acumulam ou já acumularam elevadas quantidades de moedas e transações (maior centralidade de grau), pertencem à casas de câmbio digitais, um parâmetro que pode ser utilizado para observar a quantidade de usuários desses serviços que estariam passando seus ativos por lavanderias de criptomoedas. Conseguir reconhecer a maior quantidade possível de endereços das *exchanges* ajuda a identificar quais carteiras são realmente parte da reserva das misturadoras e não das casas de câmbio. Ademais, existe ainda a possibilidade de carteiras de *exchanges* estarem diretamente ligadas às redes de mistura.

[21] Disponível em: `https://bestmixer.io/en/api`

Capítulo 5

Um Modelo para Rastreamento de Operações de Mixagem

Este capítulo apresenta e descreve uma nova etapa de investigação, mais pontual e minuciosa, tomando como base as observações e os resultados obtidos no capítulo anterior. Inicialmente são detalhadas as estratégias de mistura identificadas que foram implementadas pelas lavanderias testadas neste trabalho, apontando as transações executadas e os papéis desempenhados pelos endereços de carteiras nas redes. Em seguida é descrito um modelo base para mixagem centralizada de criptomoedas que busque a garantia do anonimato e privacidade dos usuários. Posteriormente, na seção 5.2, é apresentada uma proposta de rastreamento de misturas em operações que envolvam duas carteiras de destino. Por fim, são apresentadas as conclusões sobre os serviços das mixers testadas.

5.1 Estratégias de Mixagem Observadas

A análise apresentada na seção 4.2 é muito ampla e generalista para entender a complexidade da Blockchain e as minúcias do processo de mistura das criptomoedas. Um estudo mais pontual a partir das carteiras de entrada e saída das lavanderias permitem a identificação de alguns padrões utilizados no processo de mistura em ambas as mixers testadas.

Uma observação mais criteriosa mostra que após o recebimento das transações nas carteiras de entrada, as misturadoras podem executar dois tipos de operações com as moedas que estão circulando em suas redes: **Fracionamento** e **Acumulação**. A utilização dessas

operações em sequência extrai os valores referentes as taxas do serviço e obtém as quantias específicas para a entrega das novas moedas aos clientes.

Nas operações de **Fracionamento**, as misturadoras dividem o valor contido em uma carteira, enviando o saldo existente no endereço para outros dois (ou mais) (Figura 5.1). A finalidade é reduzir a cifra recebida nas transações de entrada da carteira e obter valores específicos necessários para devolução de moedas aos demais clientes. Essa operação pode continuar ocorrendo recursivamente até que seja obtido o montante desejado.

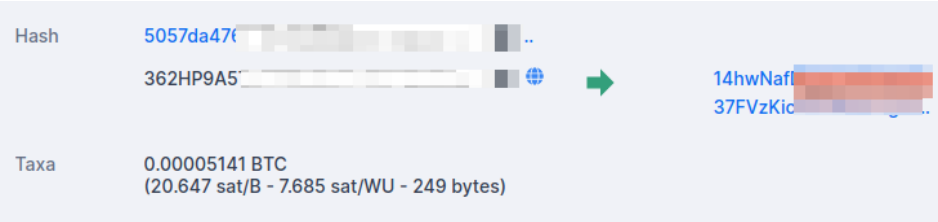

Figura 5.1: Exemplo de **Operação de Fracionamento**. Fonte: `http://blockchain.com`

Por outro lado, a operação de **Acumulação** utiliza as moedas de duas ou mais carteiras das mixers para reunir quantias maiores (Figura 5.2). É comum ocorrer operações deste tipo utilizando carteiras que foram empregadas para guardar pequenas quantias de trocos de outras transações. Também foram encontradas operações de acumulação ocorrendo de maneira recursiva como ilustra a Figura 5.3.

Utilizando-se das operações acima mencionadas, as misturadoras aplicam suas estratégias para o embaralhamento das moedas de seus clientes e, ao observar a blockchain em busca de relações entre as carteiras envolvidas, identificou-se endereços que foram empregados para realizar papéis recorrentes nas redes de mistura. Os papéis, a serem descritos adiante, são: **Entrada**, **Salto**, **Acumulador** e **Pool Temporário**. Além deles, também foi possível identificar alguns endereços de *Exchanges* nas margens das operações.

O primeiro papel observado nessas redes diz repeito ao **Endereço de Entrada** (suas representações podem ser vistas nas Figura 5.4 e 5.5), essas carteiras são fornecidas pela mixer para que o cliente envie as moedas a serem misturadas pelo serviço. O endereço de entrada é utilizado apenas uma vez, isso significa que esta carteira deve possuir 0 (zero) transações antes que o cliente realize o depósito na mixer, depois ela executa uma transação de saída, enviando todo o seu saldo e não voltando a receber moedas. Durante os experimentos re-

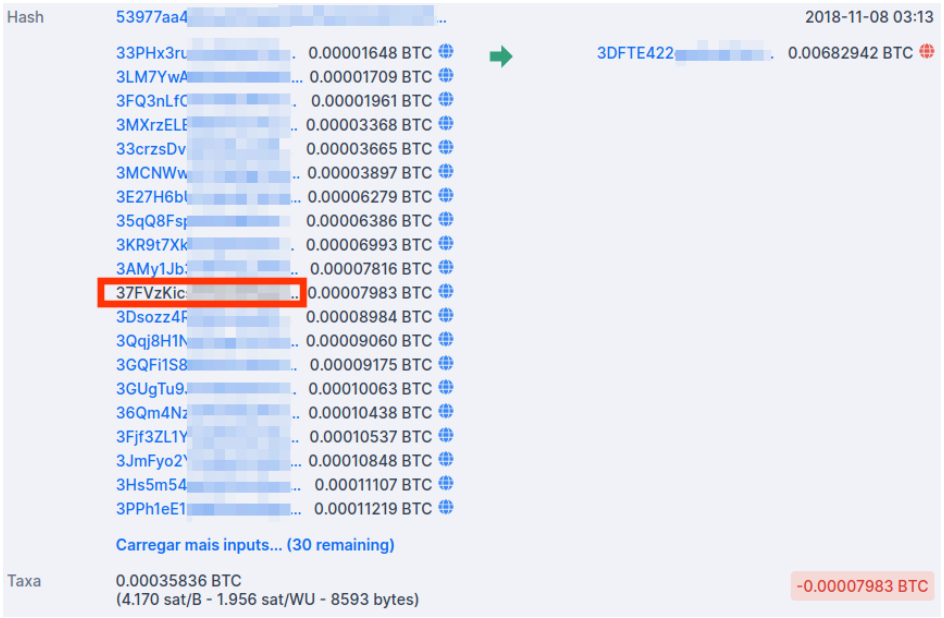

Figura 5.2: Exemplo de **Operação de Acumulação**. Fonte: `http://blockchain.com`

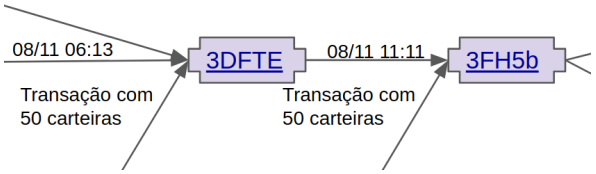

Figura 5.3: Exemplo de **Operação Recursivas de Acumulação**. Cada uma das caixas representa uma carteira acumuladora e as setas são transações. Fonte: do autor

alizados, os endereços de entrada das misturadoras mantiveram as moedas guardadas, no mínimo, até o momento em que novas moedas eram devolvidas ao cliente, podendo manter esses ativos sem movimentação durante dias.

O segundo papel identificado neste estudo é o das carteiras **Salto** (Figura 5.6). São endereços intermediários, também de uso único, que possuem as funções de efetuar pagamentos aos clientes, receber trocos de transações e participar de operações de acumulação enviando moedas para as carteiras **Acumuladoras** que, por sua vez, também são endereços de uso único nas redes de misturas, e sua principal característica é receber transações com moedas de duas ou mais origens (Figura 5.3).

Outras vezes, particularmente nas misturas operadas pela *Bestmixer*, endereços de carteiras foram utilizados em operações de acúmulo por mais de uma ocasião (grau de entrada $k_i^{in} > 1$), reunindo determinadas quantias de moedas, repassando o valor adiante e voltando a acumular, essas carteiras foram denominadas como **Pool Temporário**. Quando observado o

Figura 5.4: Exemplo de **Endereço de Entrada**. Fonte `http://blockchain.com`

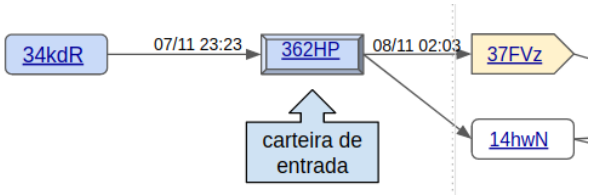

Figura 5.5: Exemplo de **Endereço de Entrada** e operação de **Fracionamento**. A caixa da esquerda representa a carteira pela qual o cliente enviou suas moedas para a misturadora. Fonte: do autor

número de transações de entrada e saída, essas foram as únicas carteiras com centralidade de grau total $k_i > 2$. A Figura 5.7 apresenta um desses endereços, o qual realizou 12 transações (6 de entrada e outras 6 de saída), acumulando e repassando valores de aproximadamente 1,9 bitcoin em cada transação.

Ao analisar as misturas executadas pela *Blender.io* não foi possível identificar nenhuma carteira da rede do serviço que possuísse centralidade de grau $k_i > 2$, isto é, nenhuma delas foi utilizada por mais de uma vez, possuindo apenas uma transação de entrada e outra de saída. Em contrapartida, a recursividade da operação de acumulação foi mais frequente, repassando quantias cada vez mais elevadas para novas carteiras (Figuras 5.8 e 5.9).

Por fim, como pode ser observado na seção 4.2.3, endereços de *exchange* costumam ser

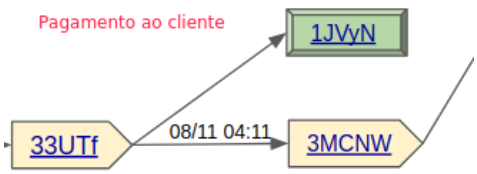

Figura 5.6: Exemplo de **Carteiras de Salto**. Fonte: do autor

Endereço	1CataJ7
Formato	BASE58 (P2PKH)
Transações	12
Total Recebido	11.85305282 BTC
Total Enviado	11.85305282 BTC
Balanço final	0.00000000 BTC

Figura 5.7: Exemplo de **Carteira Pool Temporário**. Fonte: `http://blockchain.com`

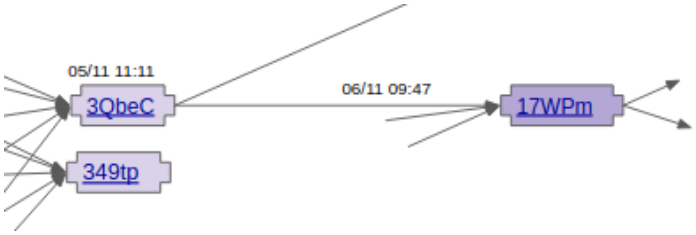

Figura 5.8: Exemplo operações recursivas de grandes valores em carteiras Acumuladoras da Blender.io. Fonte: do autor

alcançados quando transações de mistura são rastreadas, sejam eles depositando ou recebendo moedas das lavanderias, o que aparentam ser operações disparadas e recebidas por clientes dessas casas de câmbio digitais. Esses endereços, como apontado anteriormente, possuem elevado grau de centralidade na *blockchain* e podem ser facilmente identificados pela exagerada atividade, o que torna o seu número de transações muito alto. Nesta análise, um endereço em particular foi frequente nas transações *Bestmixer*, o <1NDyJtNT...> de propriedade da exchange Binance, que recebeu transferências diretamente de carteiras classificadas neste trabalho como *Pools Temporárias* da mixer.

A seguir estão apresentados e descritos os grafos contendo apenas operações e carteiras que fizeram parte dos processos de mistura aqui estudados, desta forma as Figuras de 5.10 até 5.19 são representações das observações pontuais dos casos que enquadram apenas carteiras e transações diretamente relacionadas com as operações de mistura e estão organizadas em função da dimensão tempo, os horários estão impressos em GMT. Como é sabido, a Blockchain possui enormes quantidades de informações e a representação de todas as relações entre carteiras próximas as estudadas podem ser observadas em 4.3.

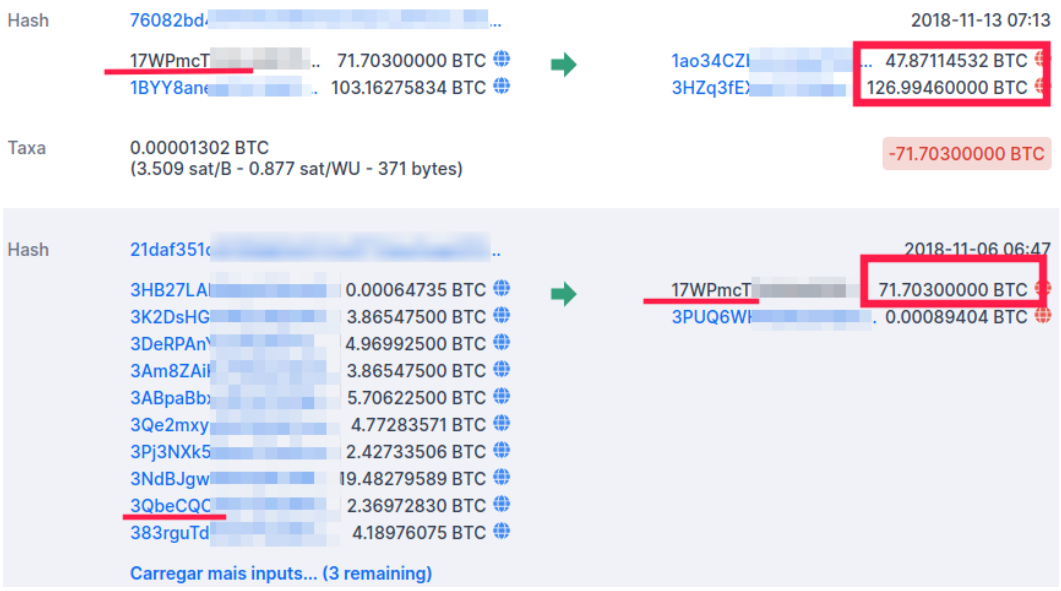

Figura 5.9: Exemplo operações recursivas de grandes valores em carteiras Acumuladoras da Blender.io. Fonte: `http://blockchain.com`

5.1.1 Dinâmicas Bestmixer

Seguindo-se o fluxo das moedas (Figura 5.10 e 5.11) enviadas para a misturadora através da carteira de entrada <3MB63...>, bem como das moedas chegando às carteiras do cliente (<3MB63...> e <1HnSi...>), confirma-se que as moedas devolvidas não possuem relação com as moedas enviadas para a misturadora pelo cliente. No padrão notado para a devolução ao cliente, as moedas vieram de fluxos diferentes, de transações ocorridas em um momento anterior ao pedido de mistura, chegaram através de uma carteira Salto e o troco resultante dessas transações foram enviados para outras carteiras Salto. Percebeu-se também que após algumas transações, os trocos são encaminhados para uma operação de acumulação, incluso aqui as moedas originárias do cliente (Figura 5.11).

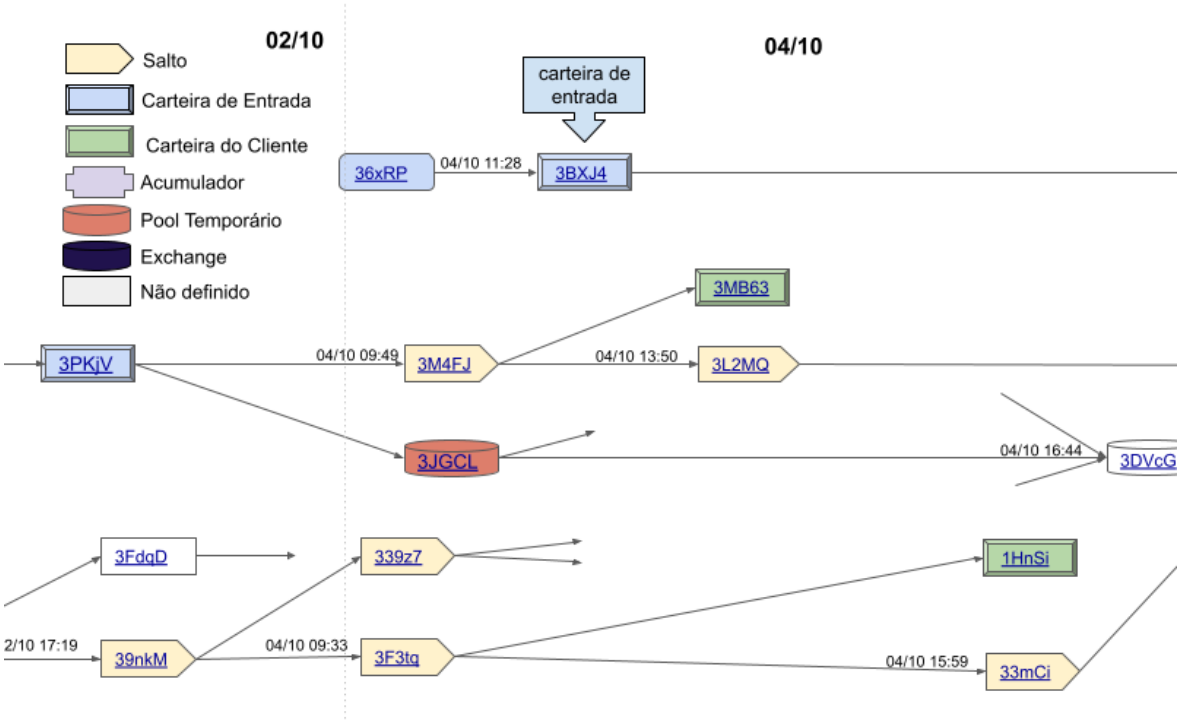

Figura 5.10: Avaliação detalhada da primeira mistura *Bestmixer* (Recorte A). Fonte: do autor

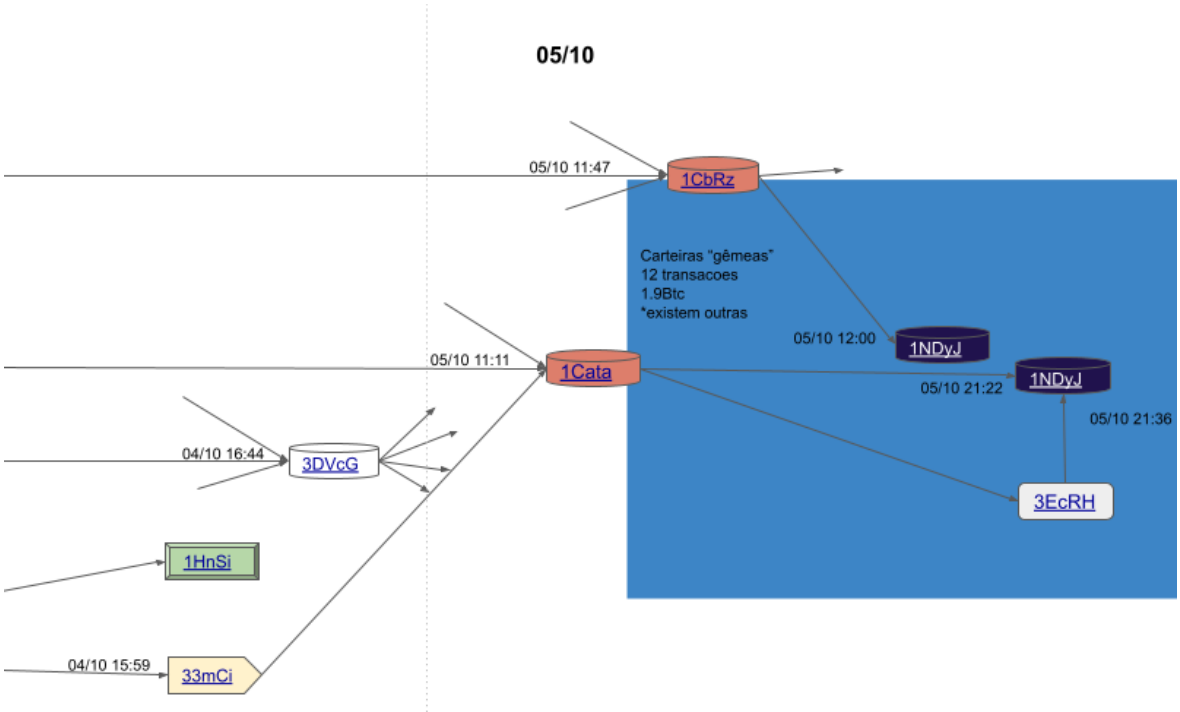

Figura 5.11: Avaliação detalhada da primeira mistura *Bestmixer* (Recorte B). Fonte: do autor

As operações descristas para a primeira operação *Bestmixer* também foram encontradas na segunda (Figuras 5.12 e 5.13), a destacar que a transação de acumulação realizada na primeira mistura (Figura 5.11) ocorreu em endereços de Pools Temporários, enquanto que na segunda mistura elas foram realizadas em carteira Acumuladora (Figura 5.13).

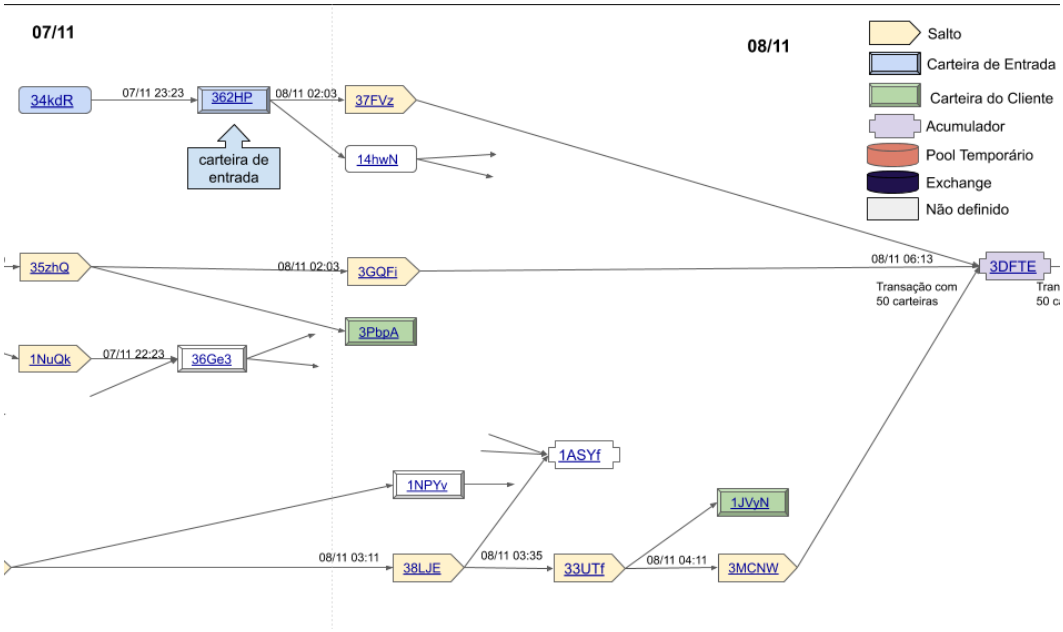

Figura 5.12: Avaliação detalhada da segunda mistura *Bestmixer* (Recorte A). Fonte: do autor

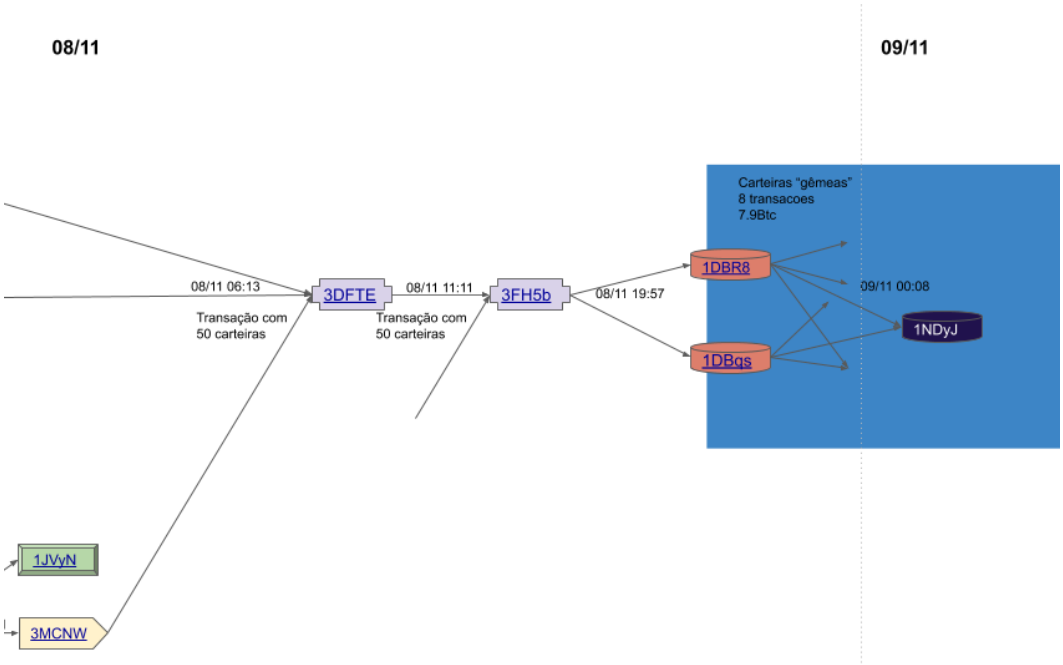

Figura 5.13: Avaliação detalhada da segunda mistura *Bestmixer* (Recorte B). Fonte: do autor

Figura 5.14: Carteiras Gêmeas da primeira mistura *Bestmixer*. Fonte:`http://blockchain.com`

Figura 5.15: Carteiras Gêmeas da segunda mistura *Bestmixer*. Fonte: `http://blockchain.com`

Em ambas operações de mistura, o fluxo das moedas levou para endereços de *Pool Temporários* e que possuíam algumas peculiaridades. Esses endereços encontrados dispõem de uma carteira espelho a qual realizou a mesma quantidade de transações envolvendo os mesmos valores ou valores muito próximos, e foram aqui denominadas de **Carteiras Gêmeas**. Na primeira mistura, esses endereços executaram seis transações de entrada e seis transações de saída cada um deles (Figura 5.14) Entre os dias 18/09/2018 e 08/12/2018, enquanto que na segunda mistura as Carteiras Gêmeas executaram oito transações, sendo quatro de entrada e outras quatro de saída (Figura 5.15) Entre os dias 21/09/2018 e 03/12/2018. Dentre os endereços envolvidos nas transações de saída das Carteiras Gêmeas, um deles foi recorrente, o <1NDyJtNT...>, como é sabido este endereço pertence a casa de câmbio *Binance*.

Transferências realizadas a clientes de casas de câmbio virtuais não costumam ser enviadas diretamente para as carteiras do núcleo das *exchange* como é o caso do endereço <1NDyJtNT...>, logo as Carteiras Gêmeas encontradas neste estudo pertencem a clientes da Binance. Não foi possível definir se (i) a *Bestmixer* é o cliente da *exchange* e seu pool é operado a partir de lá, (ii) esses endereços gêmeos são de clientes recorrentes da Misturadora ou (iii) a Binance faz parte da rede de misturas *Bestmixer*.

5.1.2 Dinâmicas Blender.io

O fluxo de moedas encontrado nas operações Blender.io, representados nas Figuras 5.16, 5.17, 5.18 e 5.19, seguem padrões semelhantes aos percebidos nas operações *Bestmixer*: as novas moedas recebidas vieram de fluxos diferentes, entregues por carteiras Salto, em transações envolvendo troco e que seriam reunidos em carteiras Acumuladoras. As principais diferenças encontradas entre as mixes são a falta de um endereço de Pool Temporário e operações de Fracionamento em conjunto com operações de Acumulação.

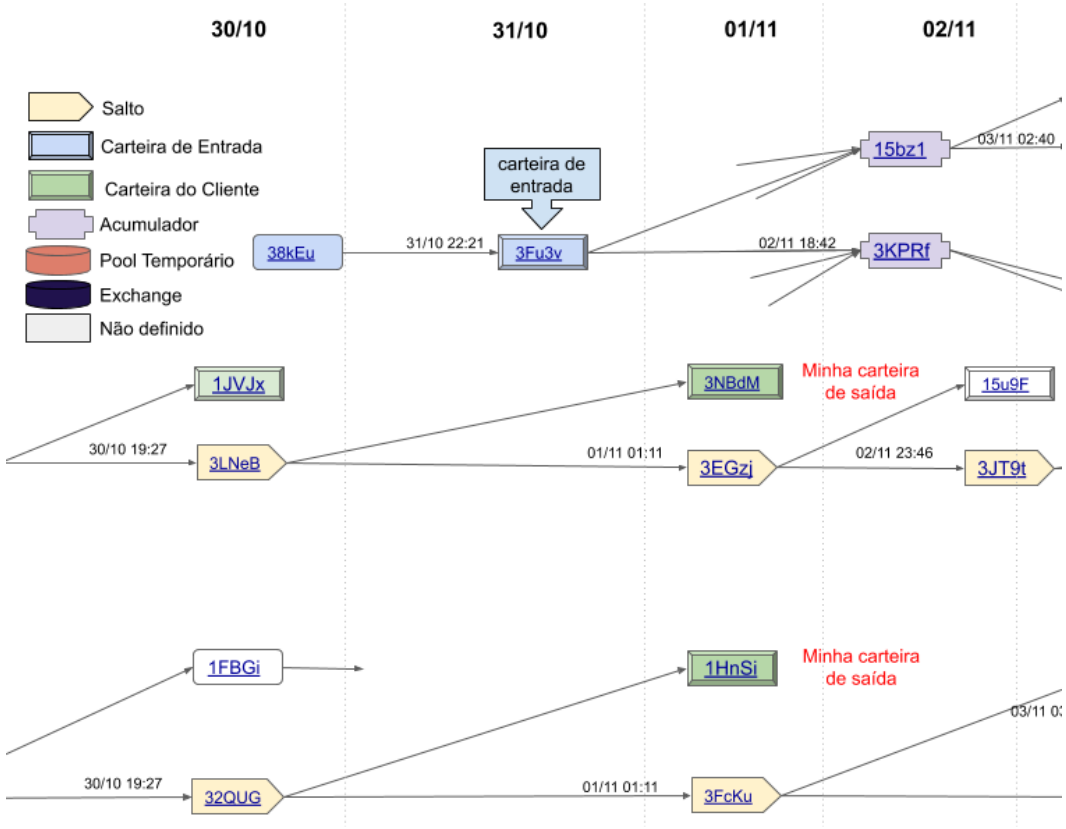

Figura 5.16: Avaliação detalhada da primeira mistura *Blender.io* (Recorte A). Fonte: do autor

Dentro dos fluxos analisados não foi possível identificar endereços com $k_i > 2$, todas as carteiras encontradas e que aparentam fazer parte da rede de mistura são de uso único. Possivelmente, as reservas de moedas da misturadora estão em constante deslocamento na blockchain e essa hipótese sustenta-se a partir do conjunto de carteiras Acumuladoras encontradas, como podem ser observadas nas Figuras 5.17 e 5.19, que executam recursivas operações de acumulação e fracionamento encaminhando elevadas quantias de moedas (Figuras 5.9 e 5.20).

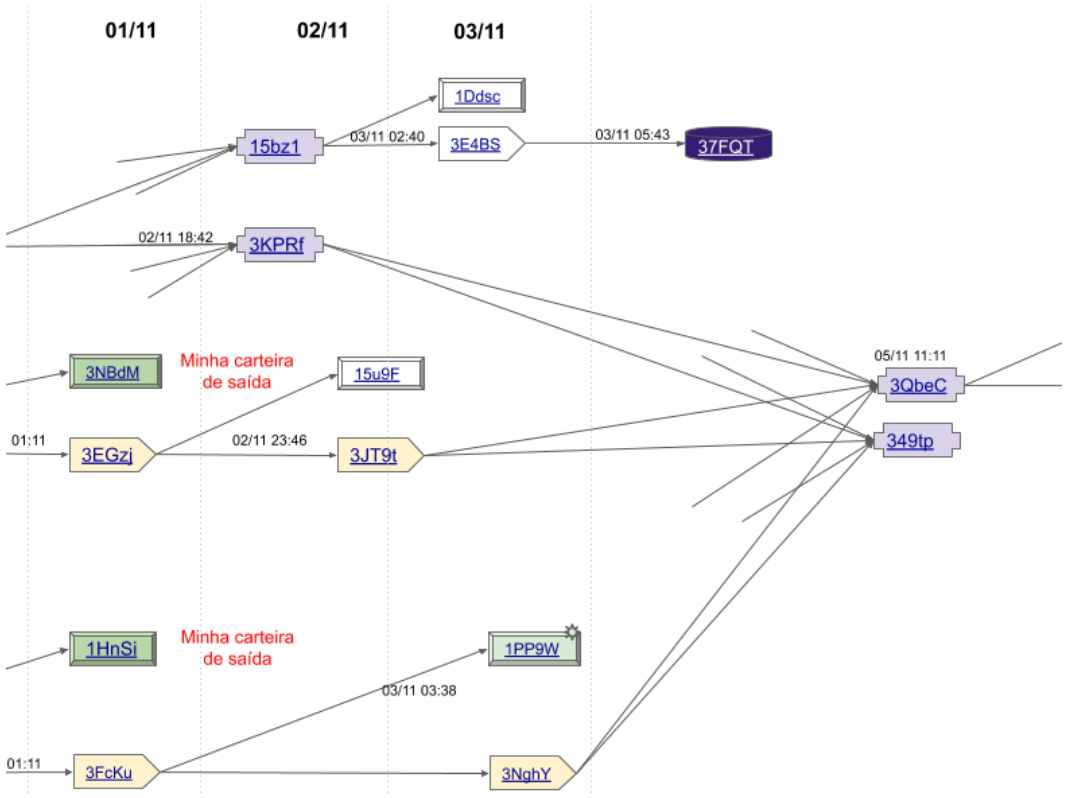

Figura 5.17: Avaliação detalhada da primeira mistura *Blender.io* (Recorte B). Fonte: do autor

A outra diferença notada entre as misturas é que para a *Bestmixer* as operações de Acumulação foram sempre executadas com a relação de carteiras em $N : 1$, enquanto que nas misturas da *Blender.io* essas operações ocorreram de maneira $N : N$. São diferentes transações de Fracionamento acumulando moedas em outras duas carteiras, como podem ser vistas nas Figuras 5.19 e 5.17.

Ainda durante a investigação na dinâmica das misturas feitas pela *Blender.io* foi identificada uma carteira de saída ($< 1PP9W... >$) diferente das utilizadas no experimento, esse endereço esteve presente no fluxo de transações da primeira operação de teste realizada com a operadora (Figura 5.17). A carteira foi investigada e apresenta todas as características de um endereço que recebeu moedas de duas operações de misturas distintas que utilizaram duas carteiras como destino (Figuras 5.21 e 5.22). A relação entre essas carteiras pode ser notada na terceira transação de ambas onde, juntas, realizam uma transferência de moedas para novos endereços utilizando as moedas recebidas anteriormente nas misturas.

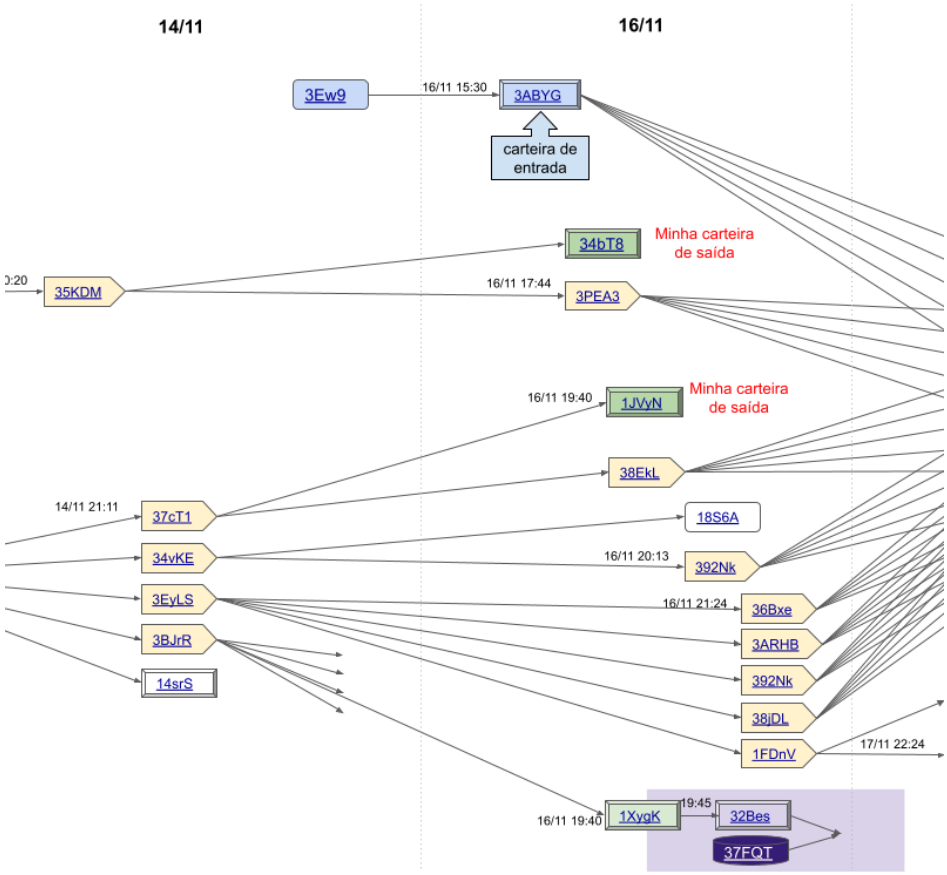

Figura 5.18: Avaliação detalhada da segunda mistura *Blender.io* (Recorte A). Fonte: do autor

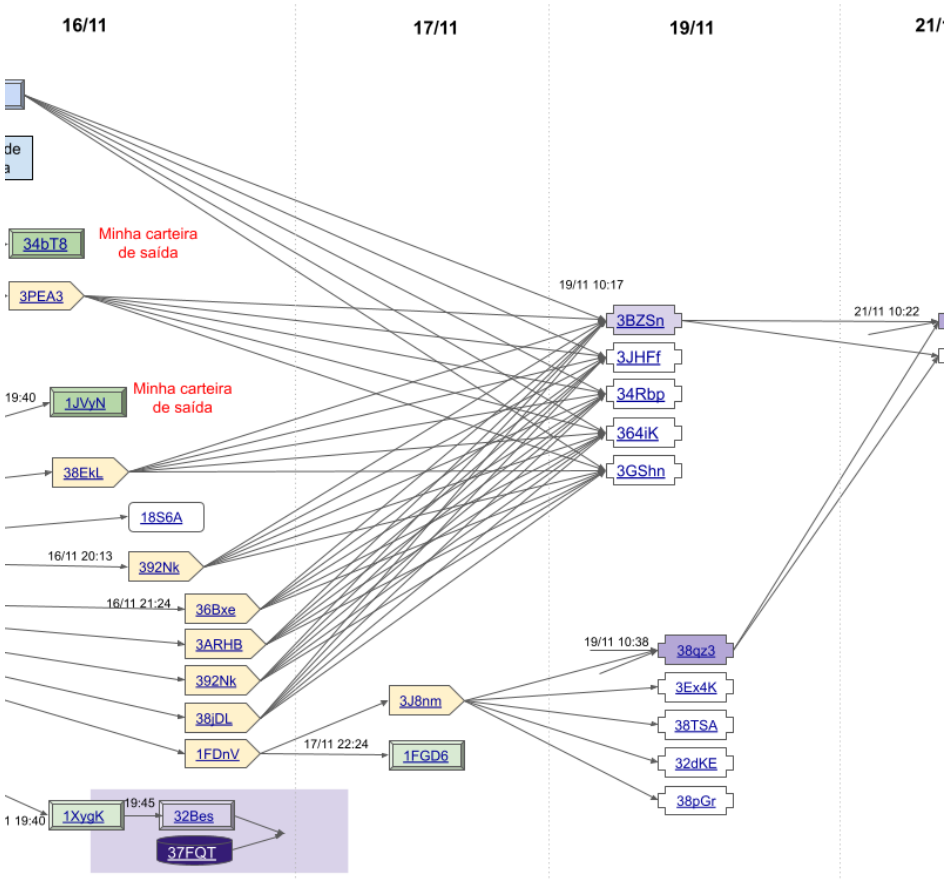

Figura 5.19: Avaliação detalhada da segunda mistura *Blender.io* (Recorte B). Fonte: do autor

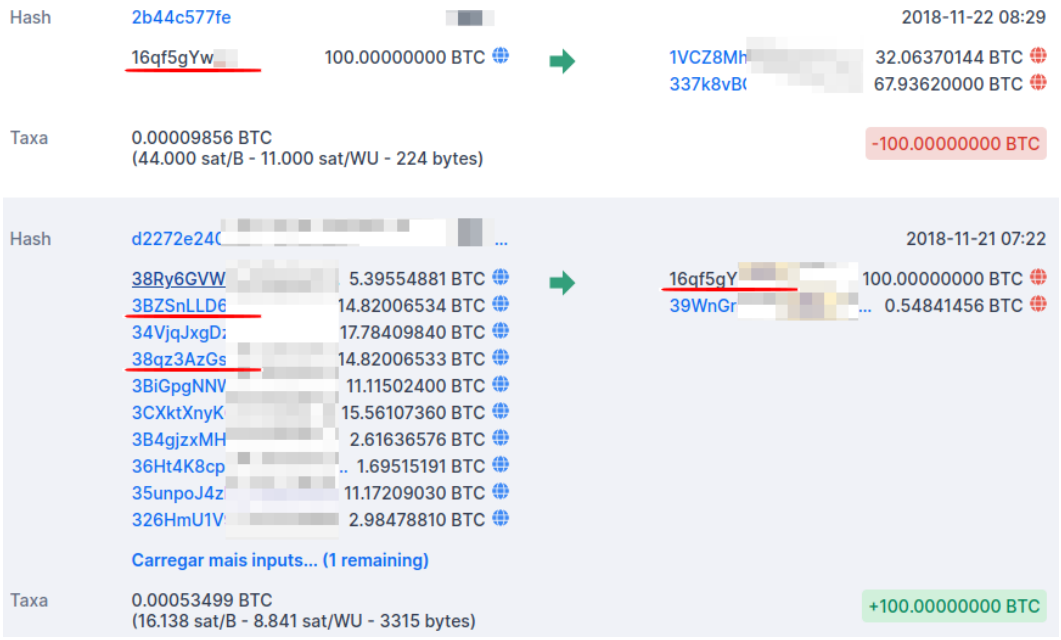

Figura 5.20: Carteiras Acumuladoras em operações recursivas de alto valor na segunda mistura Blender.io. Fonte: `http://blockchain.com`

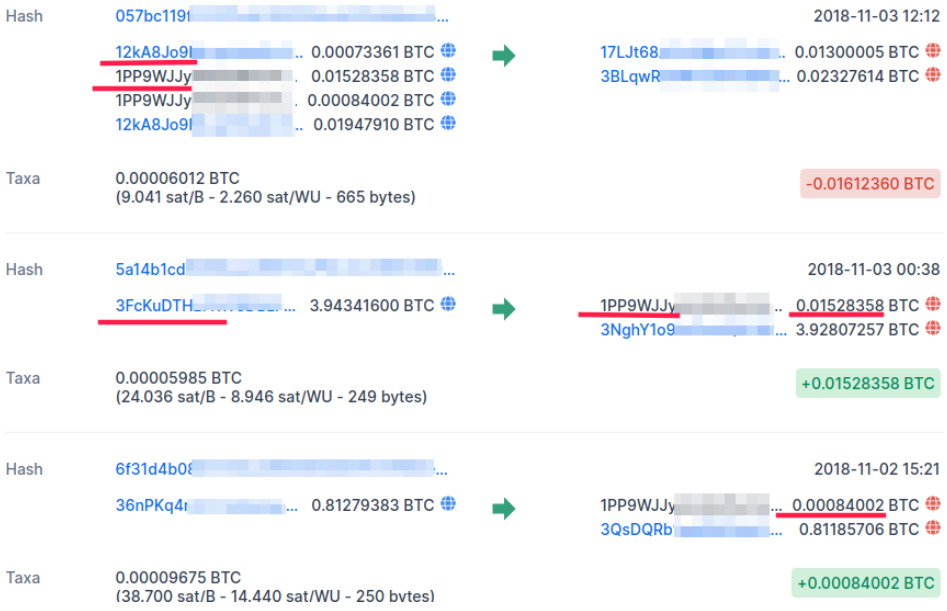

Figura 5.21: Carteira $< 1PP9WJJy... >$, por duas vezes recebeu moedas de mistura em conjunto com a carteira $< 12kA8Jo9... >$. A segunda operação, onde recebe moedas de $< 3FcKuDTH... >$ foi identificada em 5.17). Fonte: `http://blockchain.com`

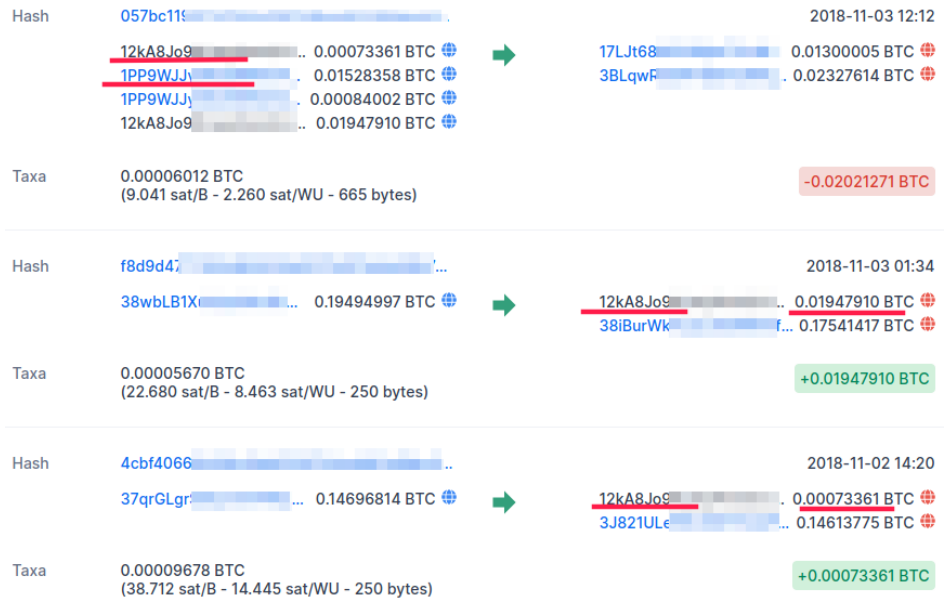

Figura 5.22: Carteira $< 12kA8Jo9... >$, por duas vezes recebeu moedas de mistura em conjunto com a carteira $< 1PP9WJJy... >$. Fonte: `http://blockchain.com`

5.2 Abordagem de Rastreamento Proposta

As operações de mistura de moedas apresentadas e investigadas nas seções anteriores apontam para um padrão que pode ser utilizado com o propósito de rastrear tanto a origem quanto o destino real das moedas que passam pelo serviço, bem como identificar carteiras de outros clientes. Conhecendo duas ou mais carteiras de saída (pelas quais o cliente da *mixer* recebeu suas novas moedas), essa vulnerabilidade no processo de mistura ocorre quando existe um ou mais endereços de carteira onde trocos dos pagamentos das misturas convergem. Essa falha será chamada de **Parentes Convergentes** neste trabalho.

Como observado nos experimentos, todas as novas moedas entregues ao cliente fazem partem de uma transação que envolve troco e este é enviado para uma carteira Salto. As próximas transações com as moedas do troco seguirão um fluxo em paralelo com outras carteiras e transações da misturadora, podendo ser usado para efetuar novos pagamentos, até que finalmente participará de uma transação de Acumulação. Em três dos quatro experimentos, essa carteira Acumuladora foi utilizada para convergir o fluxo das moedas enviadas para mistura e o troco das transações das moedas recebidas (Figuras 5.11 e 5.19).

Utilizando os Parentes Convergentes como referencial dentro da Blockchain, considerando que nos experimentos realizados não mais que 5 saltos ocorreram entre carteiras paga-

doras, carteiras de entrada e os Parentes Convergentes, torna-se computacionalmente viável executar uma varredura na blockchain em busca de transações com valores próximos aos esperados para entrada ou saída de uma mistura.

Em especial, o rastreamento da carteira de entrada e origem torna-se mais fácil de ser realizado, quando sabe-se quais as carteiras de saída ou destino, pois é sabido que a mistura começou em uma carteira, e não duas ou mais. O oposto, rastrear a partir da origem, requer um custo computacional maior, dado que há a necessidade de procurar por conjuntos de transações, em um determinado período de tempo, cujo o somatório de seus valores possua a quantia estimada pós lavagem das moedas (entre 78,65% e 96,95% do valor de entrada, para as operações realizadas neste trabalho, como podem ser vistas na Tabela 4.1).

Inicialmente localiza-se quais carteiras Acumuladoras ou Pools Temporários são candidatos a Parentes Convergentes, partindo da transação de entrada na mixer ou das transações de saída.

Na segunda etapa, para cada carteira candidata a Parentes Convergentes, deve-se realizar um rastreamento reverso na blockchain em busca de transações com valores e horários compatíveis para identificação de endereços candidatos à entrada ou saída.

Isso posto, três das quatro operações de mistura realizadas neste estudo puderam ter suas carteiras de entrada rastreadas a partir das carteiras de destino ao executar o Algoritmo 5.1

Código Fonte 5.1: Algoritmo de Rastreamento Destino - Origem

```
1  Localizar_Convergencia(transacoes_recebimento[])
2      Para cada transacoes_de_recebimento
3          Selecionar carteira_de_troco
4          Varrer recursivamente carteira_de_troco.transacoes_de_saida ate limite_de_niveis
5              Se Parente_Convergente encontrada
6                  Rastreamento_Reverso(Parente_Convergente)
7
8  Rastreamento_Reverso(Parente_Convergente)
9      Para cada Parente_Convergente.transacao_entrada.carteiras
10         Recuar recursivamente na blockchain ate limite_de_niveis
11             Para cada transacao_de_entrada.carteiras_destino
12                 se carteiras_destino.transacoes = 2 e
13                    carteiras_destino.total_recebido > total_recebido_pos_mistura e
14                    carteiras_destino.total_recebido < teto_estimado e
15                    carteiras_destino.saldo = 0 e
16                    transacao_de_entrada.horario < transacoes_de_recebimento.horario
17                      "Encontrada uma candidata carteira de entrada da mixer!"
```

5.3 Modelo Base de Mixagem

Considerando as definições estudadas de mixers, pode-se afirmar que uma modelagem básica de misturas centralizadas de criptomoedas M é a composição de um conjunto de moedas de entrada (transações) C_I enviado pelo cliente, a ser operado por um conjunto de operações O, que devolverá um conjunto de moedas na saída C_O aos clientes, tal que não possua nenhuma moeda em comum com o conjunto de entrada daquele mesmo cliente. Deste modo, pode-se definir um modelo base de mistura M como:

$$M = \{C_I, O, C_O \mid C_I \cap C_O = \emptyset\} \tag{5.1}$$

Porém, para assegurar a privacidade e o anonimato dos usuários, como visto a na Seção 5.2, outros requisitos precisam ser inseridos em uma mistura M, considerando a possibilidade de falha dos Parentes Convergentes ou similares, deve-se notar a necessidade da não existência de relações entre as operações realizadas nas moedas de entrada com as operações realizadas nas moedas de saída, $O(C_I, C_O) = \emptyset$, logo, um modelo mais confiável para misturas de criptomoedas poderia ter em sua definição:

$$M = \{C_I, O, C_O \mid (C_I \cap C_O = \emptyset) \wedge O(C_I, C_O) = \emptyset\} \tag{5.2}$$

5.4 Considerações Finais

Após uma análise mais detalhada de recortes das operações de mistura de criptomoedas testadas, foi possível reconhecer padrões utilizados pelas mixers para o embaralhamento das moedas em suas redes, como funcionam suas transações e como comportam-se as carteiras utilizadas. Portanto, usuários e entidades com interesse em rastrear a origem ou o destino dos criptoativos que passam por essas lavanderias podem criar algoritmos capazes de apontar carteiras envolvidas no processo de lavagem das moedas. Executar operações nessas redes, testando os serviços que deseja-se analisar e rastrear, são formas efetivas de ter compreensão acerca de seu funcionamento, permitindo a identificação de carteiras de usuários que participaram do embaralhamento, assim como os valores envolvidos nessas operações, características essas importantes para a criptoanálise de crimes.

Nos dois testes executados com a *Bestmixer*, os fluxos das moedas convergiram para carteiras pertencentes à rede da *exchange Binance*, onde os reais proprietários dessas carteiras podem ser a própria lavanderia ou clientes recorrentes da *Bestmixer*, pois verificaram-se sucessivas transações semelhantes. Nesses casos, autoridades seriam capazes de requerer a identificação dos portadores desses endereços e cobrar eventuais taxas e devidos impostos, pois *exchanges* são obrigadas.

Por outro lado, o fluxo das transações *Blender.io* convergem para carteiras de uso único que acumulam fundos temporariamente, sempre encaminhando todo o saldo a cada transação.

As lavanderias testadas cumpriram o papel de devolver moedas que aparentemente não possuíam relação com aquelas enviadas pelo cliente, todavia, por não garantir isolamento nos fluxos de transações entre as carteiras participantes, uma vulnerabilidade foi encontrada, os Parentes Convergentes. Essa brecha de segurança nos algoritmos das mixers estudadas, permite localizar endereços participantes dos embaralhamentos e, portanto, o rastreamento da origem ou do destino dos bitcoins torna-se viável.

Capítulo 6

Avaliação do Modelo Proposto

Após a execução dos experimentos de mistura de criptomoedas utilizando mixers centralizadas, seguida de análises da blockchain de formas macro e pontual, foi então encontrada uma vulnerabilidade nos mecanismos de embaralhamento e um algoritmo de rastreamento de carteira de origem foi esboçado. Neste capítulo, a heurística do rastreamento por meio do Parente Convergente será avaliada através da implementação do algoritmo e testagem de sua eficiência.

6.1 Metodologia

A partir da análise do comportamento das misturas e a descoberta dos Parentes Convergentes, o algoritmo apresentado em Código Fonte 5.1 foi implementado em linguagem de programação *Python 2.7*, com ajuda da biblioteca *Blockchain/api-v1-client-python*[1]. O objetivo desse software é identificar na *Blockchain* quais os endereços que possivelmente são a origem de uma mistura de bitcoins que utilizou duas carteiras como destino, as quais são conhecidas.

Os parâmetros de entrada do programa são os *hashes* que representam as transações de recebimento das novas moedas, dessa forma, foram utilizados os quatro pares de *hashes* das transações dos experimentos anteriormente apresentados (Capítulo 5), portanto as carteiras de origem já eram conhecidas para essas quatro misturas. Outros dois pares de *hashes*, de transações identificadas durante a fase de análise, também participaram dos testes, estes não possuem carteiras de origem confirmada.

[1] Disponível em `https://github.com/blockchain/api-v1-client-python/`

O software desenvolvido trabalhou em duas etapas sequenciais: (i) uma varredura na *Blockchain* para frente no tempo, a procura de um Parente Convergente em comum entre os fluxos de envio e recebimento dos bitcoins; (ii) uma varredura para trás no tempo, a partir do Parente Convergente, em busca de transações que possuam horário e valor compatíveis com a saída, de acordo o modelo esboçado.

Após a execução, foi avaliado (i) se existe Parente Convergente para as transações de saída, (ii) se existem candidatas para carteiras de entrada da mistura (iii) tempo de execução do rastreamento.

A seguir estão o planejamento da execução, os resultados e análises do experimento.

6.2 Planejamento Experimental

Para a execução do software de rastreamento, os *hashes* que identificam as transações de saída da misturadora foram passados como entrada para a aplicação. As quatro misturas realizadas para testes neste trabalho estão com seus *hashes* representados na Tabela 6.1, os outros dois códigos de transações encontradas durante a investigação estão mostrados na Tabela 6.2, somando seis pares, consequentemente seis rastreamentos.

Tabela 6.1: Códigos Hashes de recebimento das transações

	Bestmixer 04/10/2018	Bestmixer 08/11/2018	Blender.io 31/10 e 01/11	Blender.io 16/11/2018
Transação de Recebimento 1	b6d71a1f...	3f2204b7...	70909fe9...	57428961
Transação de Recebimento 2	b0fc79c7...	a11ad650...	2b828ed4...	b2774e14

Tabela 6.2: Códigos Hashes de recebimento das transações - carteira encontrada durante análise

	Blender.io 02/11/2018	Blender.io 03/11/2018
Transação de Recebimento 1	4cbf4066...	5a14b1cd...
Transação de Recebimento 2	6f31d4b0...	f8d9d477...

A aplicação foi executada em um computador com processador *Intel Core i7-4510U*, com 8GB de memória Ram e rodando sobre sistema operacional com *Kernel Linux 4.15.0 64 bit*.

Para um endereço ser considerado candidato à carteira de entrada da mistura ele precisou cumprir os requisitos: (i) Possuir apenas duas transações, uma de entrada e outra de saída; (ii) não estar a mais de três saltos do Parente Convergente; (iii) a data e hora da transação de entrada precisava ter ocorrido a até seis horas antes da primeira transação de saída; (iv) o saldo atual ser igual a zero; (v) saldo total necessita ser maior que a soma das transações de saída da mistura e menor que a soma mais 30%.

Os totais que foram recebidos nas saídas das misturas podem ser encontrados nas Tabelas 4.1 e 6.4. O valor do saldo total das carteiras de entrada pode sofrer uma redução de até 22% da quantia depositada, como visto na tabela 4.1. Por esse motivo, o teste no saldo das carteiras candidatas utilizam um teto de até 130% da soma dos valores de saída da mistura, o que representa aproximadamente 23% do valor enviado para a mixer, 1% acima do custo mais caro encontrado nos experimentos anteriores.

O software de rastreamento foi executado seis vezes, uma para cada mistura, e os resultados podem ser encontrados na seção a seguir.

6.3 Resultados e Análise

Após a execução do software conforme os parâmetros expostos anteriormente, ele foi capaz de encontrar o Parente Convergente em cinco das seis misturas investigadas. Por sua vez, para as candidatas à carteira de entrada, a aplicação foi capaz de localizar quatro das seis envolvidas nas operações analisadas, sabe-se também que três delas estão corretas, por já serem de conhecimento pregresso ao experimento aqui posto e a quarta candidata, de uma operação executada por usuário desconhecido, atende a todos os requisitos previamente determinados. A Tabela 6.3 ilustra o resumo de execução dos testes.

Tabela 6.3: Resultados das execuções do programa de rastreamento de carteira de origem

Mistura	Parente Convergente	Carteira de Entrada	Valor Enviado	Tempo de Execução (s)	Data da Transação
Bestmixer 1	$< 1CataJ7w... >$	Não Encontrada	?	57	?
Bestmixer 2	$< 3DFTE422... >$	$< 362HP9A5... >$	0,001	140	07/11 23:23
Blender.io 1	$< 3QbeCQCX... >$	$< 3Fu3vHoa... >$	0,001	47	31/10 22:21
Blender.io 2	$< 3BZSnLLD... >$	$< 3ABYGhu6... >$	0,001	1236	16/11 15:30
Outra 1	$< 3NdBJgwG... >$	$< 3P5nc6uM... >$	0,00178254	143	02/11 14:55
Outra 2	Não Encontrada	Não Encontrada	?	30	?

As consultas à *Blockchain* efetuadas pelo software de rastreamento ocorreram através da rede mundial de computadores, acarretando em um tempo de resposta bem mais lento se comparado com o desempenho de uma consulta em base de dados local, devido aos atrasos envolvidos. Apesar disso, o período necessário para o rastreamento foi superior a três minutos em apenas uma das execuções, quando em busca da carteira de origem da mistura *Blender.io 2*, que chegou a mais de 20 minutos para conclusão da tarefa. Os fluxos de transações envolvidas nessa mistura possuem muitos fracionamentos e acúmulos, fazendo uso de uma grande quantidade de carteiras no processo (Figuras 5.18 e 5.19).

A aplicação foi capaz de identificar uma possível carteira de origem para a mistura nomeada como *Outra 1* (mistura de terceiros, identificada durante investigação dos experimentos), a qual o valor de entrada na operação foi de 0,00178254 btc. Sendo assim, a misturadora haveria descontado 0,00020891 btc equivalente a 11,72% do valor de entrada para a operação (Tabela 6.4.

Tabela 6.4: Rastreamento de misturas de cliente encontrado na *Blender.io*

	Primeira Mistura 02/11/2018		Segunda Mistura 03/11/2018	
Entrada	0,00178254	14:55	?	?
Recebimento Carteira 1	0,00073361	17:20	0,01528358	03:38
Recebimento Carteira 2	0,00084002	18:21	0,01947910	04:34
Total Recebido	0,00157363	88,28%	0,03476268	04:34
Valor descontado	0,00020891	11,72%	?	?

Após os resultados apresentados acima, novas rodadas de rastreamento foram executadas alterando parâmetros de saltos limites entre Parentes Convergentes e carteiras de entrada para quatro, cinco e seis; e o fator multiplicador de valor de entrada para 1,5 (50%), no entanto as únicas variações de resultado foram relativas ao tempo de execução, devido a uma maior quantidade de transações e carteiras que foram testadas.

6.4 Considerações Finais

A implementação do algoritmo de rastreamento de carteira de origem a partir de duas carteiras de saída, baseado na vulnerabilidade do Parentes Convergentes, obteve exito superior a 66% em encontrar carteiras candidatas à carteira de entrada da mistura. Esse resultado

aponta para uma falha que não está presente em todas as misturas realizadas pelas lavanderias mas que auxilia a criptoanálise, identificando e agilizando o processo e, em muitos casos, podendo fazer a ligação direta entre as carteiras de entrada e saída das misturadoras, conservando a relação entre as moedas e seus proprietários, rastreando-os pela *Blockchain*.

O experimento aqui apresentado é a implementação de um algoritmo de mitigação de lavagem de criptomoedas, em misturas centralizadas, que pode ser refinado a partir de novas relações descobertas dentro das misturas investigadas, tendo potencial para uma retro alimentação de dados a cada operação encontrada.

Por fim, os resultados obtidos validam as análises postas no Capítulo 5 e abrem espaço para desenvolvimento e implementação de algoritmos que sejam capazes de executar o rastreamento origem - destino das moedas e identificação de lavanderia utilizada no procedimento. Também é preciso ter em mente que as mixers continuam em evolução e seus mecanismos podem ser constantemente alterados, entretanto a *Blockchain* é imutável e misturas ocorridas no passado não podem ter suas carteiras alteradas.

Capítulo 7

Conclusão e Trabalhos Futuros

Diante do novo paradigma financeiro pós surgimento da Bitcoin, onde moedas completamente digitais tornaram-se realidade ao agrupar tecnologias como a criptografia e livros de registros distribuídos, permitindo assim a transferência de valores direta entre usuários da internet, protocolos e serviços surgiram buscando oferecer anonimato e privacidade aos proprietários de criptomoedas. O presente trabalho apresentou um estudo acerca do funcionamento dos serviços de misturas centralizas de criptomoedas (*criptocurrency mixers* ou *tumblers*), também conhecidos como serviços de embaralhamento ou lavanderias. Procurando o entendimento mais aprofundado dos serviços de misturas disponíveis na internet, foram realizados testes em quatro *mixers* e o resultado dessas operações foi avaliado sob diversos aspectos.

Quanto à esfera econômica, os riscos de perda dos ativos são reais e duas das quatro lavanderias testadas não devolveram moeda alguma para o cliente. Entre as que devolveram, os encargos totais para uso do serviço podem chegar a 21% do valor depositado. Com tantos riscos envolvidos surgem alguns questionamentos, entre eles: a quem pode interessar um serviço sem garantias e com tarifas tão elevadas para conseguir anonimato? Apesar dos questionamentos, as *mixers* estão diariamente interagindo com muitos clientes, é o que apontam as diversas carteiras encontradas ao analisar o fluxo de transações registrados na *Blockchain*. 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 misturadoras”.

No que diz respeito a análise mais técnica dos serviços, inicialmente a *Blockchain* foi varrida por scripts para examinar os caminhos percorridos pelas moedas e quais carteiras estariam envolvidas nos processos de mistura. Em seguida, os fluxos das transações foram analisados de forma mais pontual e cuidadosa para encontrar padrões empregados pelas lavanderias, descobrindo quais carteiras podem ser de clientes, das misturadoras ou de casas de câmbio. Esta última, inclusive, foi destino de moedas nos fluxos dos dois embaralhamentos efetuados pela *Bestmixer*, onde carteiras receberam repetidas transações e enviaram seus saldos para um endereço conhecido da exchange *Binance*. Levantando mais um questionamento sobre quem seria o proprietário dessas carteiras, um cliente recorrente ou a própria *mixer*? Para ambos os casos esses endereços podem ter seus donos identificados par casos de necessidade fiscal ou jurídica.

Dentro dos padrões descobertos, uma vulnerabilidade nos protocolos de mistura foi encontrada: Os Parentes Convergentes, essa falha pode possibilitar o rastreamento de bitcoins utilizados nas misturas. Um algoritmo de rastreamento da origem de ativos, a partir do conhecimento de carteiras destino, foi modelado, implementado e conseguiu chegar a carteira de entrada da lavagem em em 66% dos experimentos executados. A modelagem dos processos usados pelas lavanderias, esboçada por esse trabalho, validada pela implementação e execução de um software de rastreamento, possibilitou também a identificação de outros clientes participantes das misturas, indicando a chance de exposição desses usuários, bem como suas carteiras e saldos.

Portanto, usuários de serviços de lavanderia de criptomoedas não possuem garantias de entrega das atividades prometidas, seja por não terem suas moedas devolvidas ou por *mixers* não conseguirem assegurar o anonimato de seus clientes. Naturalmente, a desanonimização dos usuários pode levar a criação de novos protocolos de mistura, fazendo com que os serviços evoluam, até o surgimento de novas formas de rastreamento. Por outro lado, é importante destacar que a *Blockchain* é imutável e aqueles que desejavam ter seu anonimato garantido, trocando suas moedas marcadas através das misturadoras, não conseguirão faze-lo por muito tempo, obrigando-os a trocas contínuas que podem custar muito de seu patrimônio.

Este trabalho possui limitações claras devido a pequena quantidade de amostras. Para continuar investigando esses serviços, participando do jogo de gato e rato das lavanderias, faz-se necessário uma quantia de recursos financeiros, tornando assim uma pesquisa custosa.

Logo, para trabalhos futuros, abre-se um leque de possibilidades para continuidade do tema aqui abordado. A partir do modelo já examinado, novas heurísticas de rastreamento podem ser desenvolvidas para localização de carteiras destino, bem como identificação da lavanderia utilizada, e ainda implementações em software para automatizar o reconhecimento das operações e carteiras nos fluxos de misturas. Os gráficos detalhados encontrados no Capítulo 5, foram modelados manualmente, assim sendo, uma ferramenta capaz de desenhar e identificar os papéis de carteiras como apresentados no capítulo também será de grande valia para a análise dos livros de registro. Destaque-se também a constante evolução dos serviços estudados e a provável atualização de seus protocolos, fazendo importante que novos experimentos sejam realizados com alguma frequência para fins de catalogação de seus algoritmos a cada recorte temporal. Naturalmente, novas criptomoedas continuam a surgir e as lavanderias também podem migrar para esses ativos, fica em aberto então o estudo das misturadoras nas demais moedas e redes como a Ethereum.

Bibliografia

Albrecht, C., Duffin, K. M., Hawkins, S., e Rocha, V. M. M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*.

Alexandre, F., Martins, I., Andrade, J., Castro, P., e Bação, P. (2009). *A Crise Financeira internacional*. Estado da Arte. Imprensa da Universidade de Coimbra / Coimbra University Press.

Baird, L. (2016). Hashgraph consensus: fair, fast, byzantine fault tolerance. *Swirlds Tech Report, Tech. Rep.*

Belcher, C. (2015). Joinmarket release on mainnet. Disponível em: <https://www.reddit.com/r/joinmarket/comments/358dlv/joinmarket_released_on_mainnet/>. Acesso em: 02 de Fev. de 2020.

Bestmixer (2018). Bestmixer.io the future of bitcoin mixing! technology is here. Disponível em: <https://bitcointalk.org/index.php?topic=3140140>. 10 de Out de 2018.

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

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., e Felten, E. W. (2014). Mixcoin: Anonymity for bitcoin with accountable mixes. Em *International Conference on Financial Cryptography and Data Security*, pgs. 486–504. Springer.

Bradbury, D. (2014). Anonymity and privacy: a guide for the perplexed. volume 2014, pgs. 10–14. Elsevier.

Buterin, V. et al. (2014). A next-generation smart contract and decentralized application platform. *white paper*, 3(37).

Buterin, V. e Griffith, V. (2017). Casper the friendly finality gadget. *arXiv preprint arXiv:1710.09437*.

Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., e Shi, W. (2017). On security analysis of proof-of-elapsed-time (poet). Em *International Symposium on Stabilization, Safety, and Security of Distributed Systems*, pgs. 282–297. Springer.

Christin, N. (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. Em *Proceedings of the 22nd international conference on World Wide Web*, pgs. 213–224. ACM.

Coelho, I. M., Coelho, V. N., Lin, P., e Zhang, E. (2019). Community yellow paper: A technical specification for neo blockchain.

Conti, M., Gangwal, A., e Ruj, S. (2018). On the economic significance of ransomware campaigns: A bitcoin transactions perspective. *Computers & Security*.

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

Divya, M. e Biradar, N. B. (2018). Iota-next generation block chain. *International journal of engineering and computer science*, 7(04):23823–23826.

Duffield, E. e Diaz, D. (2018). Dash: A payments-focused cryptocurrency. *Whitepaper, https://github.com/dashpay/dash/wiki/Whitepaper*.

Feng, Q., He, D., Zeadally, S., Khan, M. K., e Kumar, N. (2018). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*.

Foley, S., Karlsen, J. R., e Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, 32(5):1798–1853.

Hanke, T., Movahedi, M., e Williams, D. (2018). Dfinity technology overview series, consensus system. *arXiv preprint arXiv:1805.04548*.

Harris-Braun, E., Luck, N., e Brock, A. (2018). Holochain: scalable agent-centric distributed computing. *GitHub. URL: https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf*.

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

Hong, Y., Kwon, H., Lee, J., e Hur, J. (2018). A practical de-mixing algorithm for bitcoin mixing services. Em *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, pgs. 15–20.

Hopwood, D., Bowe, S., Hornby, T., e Wilcox, N. (2016). Zcash protocol specification. *GitHub: San Francisco, CA, USA*.

Juhász, P. L., Stéger, J., Kondor, D., e Vattay, G. (2018). A bayesian approach to identify bitcoin users. *PloS one*, 13(12):e0207000.

Khalilov, M. C. K. e Levi, A. (2018). A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Communications Surveys & Tutorials*, 20(3):2543–2585.

Kotz, D. M. (2009). The financial and economic crisis of 2008: A systemic crisis of neoliberal capitalism. *Review of radical political economics*, 41(3):305–317.

Larimer, D. (2014). Delegated proof-of-stake (dpos). *Bitshare whitepaper*.

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

Maxwell, G. (2013a). Coinjoin: Bitcoin privacy for the real world. Em *Post on Bitcoin forum*.

Maxwell, G. (2013b). Coinswap: Transaction graph disjoint trustless trading. *CoinSwap: Transactiongraphdisjointtrustlesstrading (October 2013)*.

Mazieres, D. (2015). The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, 32.

Moser, M. (2013). Anonymity of bitcoin transactions.

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

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

Noether, S. (2015). Ring signature confidential transactions for monero. *IACR Cryptology ePrint Archive*, 2015:1098.

Pinna, A. e Ruttenberg, W. (2016). Distributed ledger technologies in securities post-trading revolution or evolution? *ECB Occasional Paper*, (172).

Popov, S. (2016). The tangle. *cit. on*, pg. 131.

Ruffing, T., Moreno-Sanchez, P., e Kate, A. (2014). Coinshuffle: Practical decentralized coin mixing for bitcoin. Em *European Symposium on Research in Computer Security*, pgs. 345–364. Springer.

Schwartz, D., Youngs, N., Britto, A., et al. (2014). The ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, 5(8).

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

Tasca, P. e Tessone, C. J. (2017). Taxonomy of blockchain technologies. principles of identification and classification. *arXiv preprint arXiv:1708.04872*.

Trace, C. (2018). Q2 2018 cryptocurrency anti-money laundering report. Disponível em: <https://ciphertrace.com/q2-2018-cryptocurrency-anti-money-laundering-report/>.

Trace, C. (2019). Q4 2019 cryptocurrency anti-money laundering report. Disponível em: <https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/>.

Valenta, L. e Rowan, B. (2015). Blindcoin: Blinded, accountable mixes for bitcoin. Em *International Conference on Financial Cryptography and Data Security*, pgs. 112–126. Springer.

van Wegberg, R., Oerlemans, J.-J., e 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.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., e Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. Em *2017 IEEE International Conference on Software Architecture (ICSA)*, pgs. 243–252. IEEE.

Yang, W., Garg, S., Raza, A., Herbert, D., e Kang, B. (2018). Blockchain: trends and future. Em *Pacific Rim Knowledge Acquisition Workshop*, pgs. 201–210. Springer.

Zeng, L., Xin, S., Xu, A., Pang, T., Yang, T., e Zheng, M. (2019). Seele's new anti-asic consensus algorithm with emphasis on matrix computation. *arXiv preprint arXiv:1905.04565*.

Ziegeldorf, J. H., Grossmann, F., Henze, M., Inden, N., e Wehrle, K. (2015). Coinparty: Secure multi-party mixing of bitcoins. Em *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, pgs. 75–86.

Zumas, V. F. (2020). Criptomoedas, criptocrime e criptoinvestigação. Disponível em: <https://www.direitonet.com.br/artigos/exibir/11637/Criptomoedas-criptocrime-e-criptoinvestigacao>. Acesso em: 10 de Maio de 2020.