Universidade Federal do Rio de Janeiro
Instituto de Matemática
Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais
Programa de Pós-Graduação em Informática

Caracterizações Quantitativas de redes descentralizadas baseadas no Blockchain

Saulo Marques Ribeiro Ricci

Rio de Janeiro
2017

Saulo Marques Ribeiro Ricci

Caracterizações Quantitativas de redes descentralizadas baseadas no Blockchain

Dissertação de Mestrado submetida ao Programa de Pós-Graduação em Informática, Instituto de Matemática e Instituto Tércio Parcitti da Universidade Federal do Rio de Janeiro (área de concentração: Redes de Computadores e Sistemas Distribuídos) como parte dos requisitos necessários para a obtenção do Título de Mestre em Informática.

Orientador: Prof. Daniel Sadoc Menasché, D.Sc.

Coorientador: Prof. Alex Borges Vieira, D.Sc.

Rio de Janeiro

2017

CIP - Catalogação na Publicação

M491c

Marques Ribeiro Ricci, Saulo
Caracterizações Quantitativas de redes descentralizadas baseadas no Blockchain / Saulo Marques Ribeiro Ricci. -- Rio de Janeiro, 2017.
68 f.

Orientador: Daniel Sadoc Menasché.
Dissertação (mestrado) - Universidade Federal do Rio de Janeiro, Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Programa de Pós-Graduação em informática, 2017.

1. Bitcoin. 2. Ethereum. 3. Aprendizado de Máquina. 4. Caracterização. I. Sadoc Menasché, Daniel, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

SAULO MARQUES RIBEIRO RICCI

Caracterizações quantitativas de redes descentralizadas baseadas no Blockchain

Dissertação de Mestrado submetida ao Corpo Docente do Departamento de Ciência da Computação do Instituto de Matemática, e Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para obtenção do título de Mestre em Informática.

Aprovado em: Rio de Janeiro, 17 de AGOSTO de 2017.

Prof. Dr. Daniel Sadoc Menasché (Orientador)

Prof. Alex Borges Vieira, Dr.

Prof. Artur Ziviani, Dr.

Prof. Felipe Maia Galvão França, Ph.D.

Profa. Priscila Machado Vieira Lima, Ph.D.

Dedico este trabalho ao meu orientador e mentor que sempre estiveram disponíveis para ajudar e me guiaram ao longo do processo de pesquisa e aperfeiçoamento acadêmico. Dedico também a start-up Skry e Casa da Moeda do Brasil pela oportunidade e disponibilidade para realizarmos juntos esse trabalho de pesquisa.

AGRADECIMENTOS

Agradeço ao meu orientador, mentor e todos aqueles que de alguma forma contribuíram com a minha vida acadêmica. Em especial agradeço a *start-up Skry* e *Casa da Moeda do Brasil* por terem me proporcionado o ambiente e oportunidade para execução deste trabalho.

RESUMO

O presente trabalho caracteriza os tempos de confirmação das transações do *Bitcoin*, modela a dinâmica de mineração visando analisar os tempos de confirmações, considerando fatores intrínsecos da rede *Bitcoin* tais como tempos de atividade de blocos e tempos de chegadas de transações nos mineradores através da teoria de filas. Considerando as caracterizações, foi proposto um modelo para previsão de confirmação das transações baseado numa árvore de decisão e rede neural sem peso *WiSARD*. Além disso, verificamos dois modelos para detecção de transações anômalas tanto para o *Bitcoin* quanto para o *Ethereum*. Tais modelos são baseados em misturas gaussianas.

Palavras-chaves: Bitcoin. Ethereum. Aprendizado de Máquina. Caracterização.

ABSTRACT

In this work, we characterize the confirmation time of Bitcoin's transactions using a queueing theory model that accounts for factors such as the activity time of blocks and the mean time between transactions. Based on the confirmation time characterization we build a predictive model to decide if a given unconfirmed transaction will be confirmed. The model consists of a causal decision tree coupled with a WiSARD neural network. The decision tree is used to perform an initial classification between confirmed, unconfirmed and inconclusive transactions. The inconclusive transactions are then set as input to the WiSARD neural network. Finally, we conclude with two anomaly detection models for Bitcoin and Ethereum transactions. These models are based on gaussian mixtures.

Keywords: Bitcoin. Ethereum. Machine Learning. Characterization.

LISTA DE ILUSTRAÇÕES

Figura 1 – Evolução do preço do *Bitcoin* em dólares americanos, face à quantidade de transações efetuadas na rede. 14
Figura 2 – Uso do endereço como chave pública em conjunção com a chave privada para efetivar transações. 20
Figura 3 – Típica transação no Bitcoin com vários endereços pertencentes ao mesmo usuário e com dois endereços de saída: um deles do destinatário e o outro gerado pelo cliente Bitcoin e pertencente ao mesmo usuário que está pagando a fim de receber o troco. 21
Figura 4 – CDF do tempo de confirmação para as transações confirmadas 26
Figura 5 – Caracterizaçao do tempo de confirmação. 27
Figura 6 – Fittings de métricas para a dinâmica de confirmação e tempos relacionados com transações e blocos 28
Figura 7 – Blocos ativos: (a) cada barra inicia quando ocorre a primeira transação associada ao bloco, e termina quando o bloco é confirmado; (b) número de blocos ativos em função do tempo. A área embaixo desta curva divida pelo tempo produz o número médio de blocos ativos. 29
Figura 8 – Histograma da distribuição dos tamanhos das transações que estão representados via escala de cinza entre os bins de intervalos de tempo de confirmação. O último bin se refere as transações que não foram confirmadas em 24 horas 34
Figura 9 – Histograma da distribuição da quantidade de endereços de saída que estão representados via escala de cinza entre os bins de intervalos de tempo de confirmação. O último bin se refere as transações que não foram confirmadas em 24 horas 35
Figura 10 – Histograma da distribuição da razão entre o fee pelo valor transacionado que estão representados via escala de cinza entre os bins de intervalos de tempo de confirmação. O último bin se refere as transações que não foram confirmadas em 24 horas 35
Figura 11 – Árvore de Decisão usada para classificar transações em confirmadas e não confirmadas. Baseada em algumas *features*, a árvore classifica preliminarmente as transações que não serão confirmadas. O conjunto que não tem-se certeza é verificado junto a *WiSARD* proposta no modelo. 36
Figura 12 – *Scatter plot* das percentagens de acertos e erros considerando a discretização *Chi2*. 38

Figura 13 – *Scatter plot* das percentagens de acertos e erros considerando a discretização *ChiMerge*. 39
Figura 14 – Grafo de fluxos de 3 *hops* de profundidade para cálculo de anomalia da transação Tx1 41
Figura 15 – Exemplo do grafo de fluxos de 3 *hops* de profundidade para cálculo de anomalia da transação Tx1 43
Figura 16 – *Boxplot* para cada uma das *features* normalizadas 45
Figura 17 – Matriz de correlação entre as features do grafo de fluxos. A escala de cor representa o valor das correlações calculadas. 45
Figura 18 – Histograma dos scores de anomalia finais para o modelo univariado . 47
Figura 19 – Histograma dos scores de anomalia finais para o modelo multivariado 48
Figura 20 – Boxplot das *features* para as transações de cada conjunto de dados utilizado 56
Figura 21 – Boxplot das *features* para os blocos de cada conjunto de dados utilizado 57
Figura 22 – Matriz de correlação entre as *features* para blocos 58
Figura 23 – Matriz de correlação entre as *features* para transações 59
Figura 24 – Curva ROC para os dados de validação 61

LISTA DE TABELAS

Tabela 1 – *WiSARD* sem *bleaching* 38
Tabela 2 – Tabela das estatísticas descritivas das métricas das transações do grafo de fluxos 42
Tabela 3 – Cálculo das métricas relacionadas com os caminhos do grafo de fluxos 43

SUMÁRIO

1 INTRODUÇÃO 12
1.1 BITCOIN E SEU PREÇO 13
1.2 TECNOLOGIA *BLOCKCHAIN* 15
1.2.1 Consenso descentralizado 15
1.2.2 O *blockchain* 15
1.2.3 Contratos Inteligentes 15
1.2.4 Computação confiável 16
1.2.5 Prova de trabalho e de participação 16
1.3 O QUE É UM HARDFORK NA CADEIA DO BLOCKCHAIN? 16
1.4 MOEDAS ALTERNATIVAS 16
1.5 OBJETIVOS PROPOSTOS NO TRABALHO 17

2 FUNDAMENTOS SOBRE BITCOIN E BLOCKCHAIN 20

3 CARACTERIZAÇÃO DA DINÂMICA DAS TRANSAÇÕES DO BITCOIN 23
3.1 DADOS UTILIZADOS 24
3.2 TEMPO DE CONFIRMAÇÃO DE TRANSAÇÕES 25
3.3 CARACTERIZAÇÃO DO TEMPO DE CONFIRMAÇÃO 26

4 CLASSIFICAÇÃO DE TRANSAÇÕES SOB A ÓTICA DE REDES NEURAIS 32
4.1 TRABALHOS RELACIONADOS 32
4.2 *DATASET* E MODELAGEM 33
4.3 RESULTADOS 33
4.4 ANÁLISE E FILTRAGEM 34
4.5 ÁRVORE DE DECISÃO 34
4.6 CONJUNTOS DE TREINO E TESTE 36
4.7 MAPEAMENTO PARA RETINA 36
4.8 RESULTADOS 37

5 DETECÇÃO DE ANOMALIAS NA REDE BITCOIN 40
5.1 DADOS E PRÉ-PROCESSAMENTO 40
5.2 MODELO GAUSSIANO 46
5.3 MODELO DE MISTURA GAUSSIANA 47
5.4 CONCLUSÕES 48

6 DETECÇÃO DE ANOMALIAS NA REDE ETHEREUM 50
6.1 INTRODUÇÃO 50
6.1.1 Por que criar novas moedas virtuais? 51
6.1.2 Estrutura deste capítulo 51
6.2 DETECÇÃO DE ANOMALIAS 51
6.3 DADOS UTILIZADOS 52
6.4 METODOLOGIA E EXPERIMENTOS 54
6.5 CONCLUSÕES 62

7 CONCLUSÃO 63

REFERÊNCIAS 64

1 INTRODUÇÃO

O Bitcoin é uma criptomoeda que oferece flexibilidade na forma como as transações financeiras são efetuadas. Diferentemente das moedas convencionais, não existem entidades financeiras centralizadas que manipulam, fiscalizam e validam transações. Ao invés de contarem com bancos, todas as movimentações são realizadas ponto a ponto de forma que as entidades envolvidas na transação interagem diretamente. Criado formalmente em (NAKAMOTO, 2008), no auge da crise financeira, o Bitcoin ainda é alvo de muitas especulações, seja apenas como uma simples moeda virtual ou até mesmo suposições de que se trata de um esquema de pirâmide.

Evidentemente, o interesse pela moeda têm aumentado ao longo dos últimos anos, no permear de muito ceticismo e de propagandas onde usuários conseguiram rendimentos acima de 100% em menos de um ano, se Bitcoin é entendido como um investimento. Segundo um recente levantamento nota-se que em cada ano, a partir de 2013, há dezenas de milhões de transações e desde o começo do ano de 2016 até o mês de novembro foram contabilizadas quase 69 milhões de transações.[1]

Em termos de volume só no ano de 2016 o Bitcoin foi responsável por transacionar 40 bilhões de dólares até o mês de novembro.

Bitcoin não apenas criou uma moeda digital, mas, também, uma moeda descentralizada. Tal arranjo se faz necessário para evitar o famoso problema do gasto duplo. O problema do gasto duplo é nada mais que a habilidade de enviar mais de uma vez para o mesmo destinatário o mesmo valor já transacionado no passado. Para que uma transação seja de fato confirmada, ela precisa de ser concordada pelo consenso comum da rede. Todos os participantes têm de concordar e confirmar aquela transação. Isto é o que é denominado Prova de Trabalho, do inglês Proof of Work.

Por outro lado, o Bitcoin pode ser considerado uma revolução na Ciência da Computação, sendo na sua essência, um protocolo pelo qual se comunicam os computadores conectados na rede *p2p* do sistema. Não existe portanto nenhuma empresa ou entidade proprietária do protocolo. Assim, não pode-se afirmar que o Bitcoin é um esquema de pirâmide ou Ponzi, pois não há ninguém operando o esquema e não há nenhuma espécie de retorno prometido.

[1] <https://blockchain.info/charts>

(ANDROULAKI et al., 2013) e (REID; HARRIGAN, 2013) chamam atenção para o fato de que as medidas que o sistema Bitcoin adota para tratar o anonimato de seus usuários já não são suficientes. Os trabalhos utilizam técnicas de agrupamento de usuários em função do histórico de transações envolvidas para tentar desvendar características dos mesmos. A quebra de anonimato pode ocorrer mesmo que o usuário crie inúmeros endereços na tentativa de dificultar sua identificação.

1.1 BITCOIN E SEU PREÇO

O valor da moeda Bitcoin é conhecida por grandes oscilações. No ano de 2016 até o mês de novembro o valor máximo de cotação de 1 bitcoin foi equivalente à 762 dólares enquanto a cotação mínima até então para o ano de 2016 foi de 368 dólares. A moeda valorizou rapidamente desde 2009/2010 (quando o valor máximo era de 0.50 centavos de dólares) e em 2013 a cotação mínima foi de 293 dólares. Os gráficos na Figura 1 mostram tal comportamento da valorização da moeda *Bitcoin* desde a sua criação em 2009 até o mês de julho de 2017. Nota-se o quanto a moeda valorizou durante os últimos anos, face ao volume de transações, cujo pico foi no ano de 2016.[2]

[2] Gráfico extraído de <http://www.worldcoinindex.com>

Figura 1 – Evolução do preço do *Bitcoin* em dólares americanos, face à quantidade de transações efetuadas na rede.

Desde o começo do ano de 2017, o Bitcoin têm batido recordes de preço, e em agosto de 2017 a cotação de 1 BTC equivalia mais de 4 mil dólares. Não se sabe qual o valor máximo da criptomoeda, porém o risco de uma queda iminente é maior. O preço a curto prazo é fortemente atrelado aos acontecimentos importantes, como as definições de mercado para o futuro da moeda, tais como fatores políticos dos países, protecionismo e fatores internos como *hardforks* no *blockchain* do Bitcoin.

Outro ponto importante, é que o preço do Bitcoin não deriva de nenhuma moeda nacional ou *commodity*, pois ele não é lastreado por nenhum ativo, uma vez que o Bitcoin pode ser entendido como a própria mercadoria e ativo em si. Desta forma, pode ser entendido como um ativo digital baseado na matemática que é emitido por meio de uma rede descentralizada e regido por criptografia.

1.2 TECNOLOGIA *BLOCKCHAIN*

Segundo (MOUGAYAR, 2016), sob o ponto de vista tecnológico, o *blockchain* é um novo tipo de banco de dados, ambos contém informações históricas sobre o contexto em que estão inseridos, porém são projetados para diferentes tipos de interações.

Para os desenvolvedores, o *blockchain* representa um novo paradigma de como projetistas e engenheiros de *software* escreverão novas aplicações.

A tecnologia *blockchain* pode ser entendida através de 5 principais conceitos e como eles se interrelacionam: o *blockchain*, consenso descentralizado, computação confiável, contratos inteligentes e prova de trabalho ou de participação.

1.2.1 Consenso descentralizado

Consenso descentralizado quebra o velho paradigma da centralização, onde uma entidade ou banco de dados central é primariamente utilizado para regrar e validar transações. O esquema descentralizado, no qual o *Bitcoin* é baseado, transfere autoridade para os próprios participantes da rede e possibilita que todos os participantes gravem transações contidas em blocos públicos, assim formando uma única cadeia pública: o *blockchain*.

1.2.2 O *blockchain*

O *blockchain* é como um local onde informações podem ser armazenadas em sequência linear do tempo. Todos podem verificar que algum participante depositou informação neste local, porém somente o criador da informação pode manipulá-la, porque somente ele possui a chave privada, uma vez que todo o conteúdo é assinado.

Desta forma o *blockchain* é a sequência linear destes espaços, denominados blocos públicos que são verificados e validados pelo consenso descentralizado.

1.2.3 Contratos Inteligentes

Os contratos inteligentes são os principais componentes para a construção de aplicações descentralizadas. Eles são equivalentes à pequenos programas que são alimentados com moeda ou *tokens* . A principal ideia dos contratos inteligentes é a aplicação de regras e governança sobre transações concordadas por diferentes participantes e que podem ser verificadas de forma automática pelo *blockchain*.

1.2.4 Computação confiável

Combinados os conceitos do *blockchain*, consenso descentralizado e contratos inteligentes, percebe-se que eles aumentam o grau de confiança e de responsabilidade entre todos os participantes da rede.

Desta forma, as funções das autoridades centrais podem ser codificadas em contratos inteligentes e governadas pelo consenso descentralizado num *blockchain*.

1.2.5 Prova de trabalho e de participação

O núcleo da operação do *blockchain* envolve o conceito de prova de trabalho, referenciado em (NAKAMOTO, 2008). Tal conceito é, na verdade, o direito de participação no sistema do *blockchain*, cujo principal objetivo é prevenir que outros usuários mudem as informações no *blockchain* sem ter um grande custo para isto. Portanto prova de trabalho é crucial na formação do *blockchain* pois ele não pode ser desfeito e é baseado em criptografia, assim assegurando sua autenticidade.

Porém prova de trabalho é caro de manter, estima-se que há gastos em torno de 600 milhões de dólares ao ano no Bitcoin para ser mantido. Como alternativa, surgiu a prova de participação que é mais barata para ser implementada.

1.3 O QUE É UM HARDFORK NA CADEIA DO BLOCKCHAIN?

O código do Bitcoin é aberto, portanto todos podem modificá-lo e sugerir mudanças. Porém, isto introduz outra dificuldade na rede: tem de haver um consenso por parte de todos que participam da rede, para que a mudança seja implementada. Na maioria dos casos, o consenso não é 100% aceito pela comunidade e portanto a moeda tem de ser divida e seguir cadeias diferentes do *blockchain* à partir do ponto que ela se dividiu. O *hardfork* é, justamente, o processo de separação pelo qual a cadeia do *blockchain* passa no momento em que novas versões do protocolo são implementadas.

Desta forma os eventos *hardfork* podem causar turbulência na rede, de forma a desvalorizar a cotação da moeda e aumentar especulações e movimentações de venda por parte dos investidores, com o objetivo de minimizar as prováveis perdas.

1.4 MOEDAS ALTERNATIVAS

Ao longo dos últimos anos várias criptomoedas surgiram. Algumas são idênticas ao Bitcoin, e outras como o Ethereum, são plataformas mais complexas, que

introduzem conceitos que vão além de apenas dinheiro eletrônico, como o conceito de contratos inteligentes, do inglês *Smart Contracts*. Hoje, Bitcoin bem como todas as outras criptomoedas são consideradas ramificações de algo maior, denominado tecnologia Blockchain.

1.5 OBJETIVOS PROPOSTOS NO TRABALHO

Um dos desafios chaves associados à rede Bitcoin refere-se ao tempo de confirmação de transações. Uma vez que um cliente sinalize que deseja efetivar uma transação com um vendedor, esta transação é anunciada na rede Bitcoin. O tempo de confirmação de uma transação é o tempo entre o anúncio da transação e a confirmação de sua autenticidade. Esta confirmação envolve múltiplas etapas, incluindo a verificação de sua integridade por parte de mineradores, a inclusão da transação em um bloco e a inclusão do bloco na cadeia principal de transações do Bitcoin (*blockchain*).

Neste trabalho estudamos estatísticas sobre previsão de confirmação de transações, tempo de confirmação e graus das mesmas. Dentre os trabalhos de caracterização da rede Bitcoin, destacamos (RON; SHAMIR, 2013). Neste trabalho, os autores analisam diversas propriedades estatísticas associadas às transações: como os usuários gastam seus bitcoins, o saldo de bitcoins dos usuários, como os usuários movem bitcoins entre seus diversos endereços para manter sua privacidade etc.

Outro trabalho de caracterização do Bitcoin é (MEIKLEJOHN et al., 2013). Neste trabalho, os autores identificam vários participantes do sistema e os separam em grupos. Os usuários identificados no trabalho são usuários com forte atuação no sistema: mineradores, vendedores, casas de câmbio e casas de jogos, além de outros usuários influentes. O trabalho apresenta duas heurísticas de como agrupar esses usuários e defini-los, mostrando mais uma vez que o anonimato no sistema não é tão forte como supostamente foi apresentado. O trabalho também caracteriza variáveis referentes à rede do sistema como: média de transações, menores transações, transações recebidas e um balanço de quanto que cada usuário transaciona com os usuários categorizados pelo trabalho.

Embora a literatura sobre o sistema Bitcoin seja vasta, não é de nosso conhecimento nenhum trabalho anterior que tenha proposto um modelo de filas para estimar o tempo de espera experimentado pelas transações.

O advento do Bitcoin trouxe plataformas de pagamento que são intermedi-

adores entre as partes envolvidas.[3] O objetivo é criar uma camada de segurança nas transações e oferecer garantias de que as transações serão de fato efetivadas. Conforme caracterizado na seção 3.3 quase 90% das transações foram confirmadas em até 30 minutos, o que é demasiadamente demorado para liberação do crédito a fim de efetivar transações via tais plataformas.

Os objetivos do presente trabalho consistem na criação de um conjunto de ferramentas que auxiliem entidades financeiras que utilizam o Bitcoin como moeda de pagamento a preverem a confirmação das transações recebidas rapidamente, bem como monitoramento de transações anômalas em relação às últimas transações efetivadas.

As três contribuições principais desta tese são listadas a seguir:

1. **Caracterização do tempo de confirmação de transações:** caracterizações sobre os tempos de confirmações das transações, incluindo descrição dos dados usados, bem como proposta de um modelo de fatores externos que podem influenciar o comportamento dos mineradores e consequentemente os tempos de confirmações são tema do capítulo 3. A dinâmica da mineração é modelada sob a ótica de modelo de filas na seção 3.3, considerando o ecosistema como a composição de mineradores. O modelo considera fatores como a chegada de novas transações para serem mineradas, o tempo entre os blocos minerados, bem como o tempo de atividade dos blocos (RICCI et al., 2016).

2. **Previsão de confirmação de transações:** O capítulo 4 utiliza uma rede neural sem peso *WiSARD* para prever se transações serão confirmadas ou não. Primeiramente é aplicada uma árvore de decisão com base em algumas *features* da transação tais como quantidade de endereços de saída e razão entre o *fee* e volume transacionado para decidir rapidamente quais transações serão confirmadas. Aquelas restantes que não estão certas se não serão confirmadas são direcionadas para a rede neural a fim de classificá-las. O melhor resultado obtido para este conjunto é de 60% de acerto.

3. **Detecção de transações anômalas:** Uma transação é considerada anômala caso possua indicativos de comportamentos maliciosos, como lavagem de dinheiro ou até mesmo casos de roubo de moedas. Neste trabalho propomos algoritmos de aprendizado por máquina para identificação de transações anômalas.

   Ortogonalmente à predição da confirmação de transações é de valia o monitoramento de anomalias que, em última instância, pode ter um caráter investigativo.

[3] *bitpay* <https://bitpay.com> é um exemplo de plataforma de pagamento que utiliza bitcoins

Neste âmbito o capítulo 5 utiliza três modelos a fim de calcular o *score* de anomalia para cada transação. Cada transação é modelada no seu grafo de fluxos, retratando o comportamento do fluxo de moedas até alcançar a transação a ser avaliada. Os modelos apresentados neste trabalho podem ser usados em investigações mais aprofundadas do caráter das transações com alto *score* calculado com padrões maliciosos já reportados na literatura (FERRIN, 2013; MÖSER; BÖHME; BREUKER, 2013; KHAC et al., 2011; LUO, 2014). Os dois modelos de detecção de *outliers* são baseados na utilização da distribuição gaussiana para aproximar o comportamento de cada *feature* do grafo de transações do *Bitcoin* como aplicado no capítulo 5 e nas transações e blocos do *Ethereum* no capítulo 6.

2 FUNDAMENTOS SOBRE BITCOIN E BLOCKCHAIN

Neste capítulo são abordados os principais conceitos para o entendimento do Bitcoin (NARAYANAN et al., 2015). Em particular, focamos nos conceitos relevantes para a compreensão do restante da dissertação.

Endereço: Para participar da rede e realizar transações, um usuário precisa de uma chave pública (referida como endereço público, ou simplesmente endereço) e uma chave privada. Desta forma, a chave pública identifica o usuário e a chave privada é utilizada para fazer pagamentos. Um pagamento, na rede Bitcoin, é implementado por meio de uma transação que gera uma saída de recursos, recursos esses previamente registrados em uma transação anterior. Na Figura 2 o usuário do Bitcoin identificado pelo endereço/chave pública *123ea...* utiliza sua chave privada *4hgrT...* para assinar o *script* que usa recursos da transação anterior *xdaw3...:0* e desta forma liberar o valor que possui e assim efetivar uma transação que utilize tal valor como entrada.

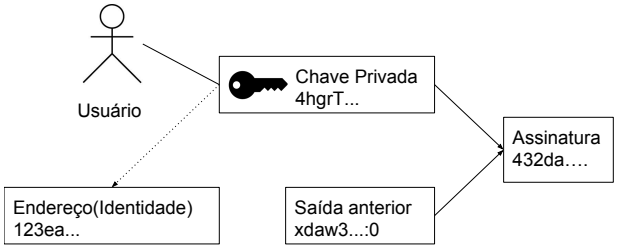


Figura 2 – Uso do endereço como chave pública em conjunção com a chave privada para efetivar transações.

Transação: Uma transação contém a informação da movimentação de moedas entre endereços. Ela está associada a duas listas de endereços, uma de entrada e uma de saída. Os endereços de entrada (resp., saída) transferem (resp., recebem) moedas. Uma transação típica pode conter, por exemplo, dois endereços de entrada correspondentes a duas carteiras de um mesmo usuário físico e duas saídas - uma correspondente à carteira do destinatário e a outra ao troco. A Figura 3 mostra uma típica transação do Bitcoin, onde todos os endereços de entrada *Input 1, Input 2,..., Input n* pertencem ao mesmo *Usuário 1*. Os valores em cada endereço devem ser totalmente utilizados, e o usuário pode utilizar vários endereços para que a soma de seus valores seja o suficiente para efetuar o pagamento. Por outro lado, tem-se duas saídas *Output 1* e *Output 2*. *Output 1* é referente ao endereço *addrx* e pertencente ao *Usuário 2* e destinatário. *Output 2* está associado com o endereço *addrz*, pertencente ao *Usuário 1* e gerado pelo cliente Bitcoin

no momento que a transação foi gerada. Este endereço possui a finalidade de troco para o *Usuário 1*.

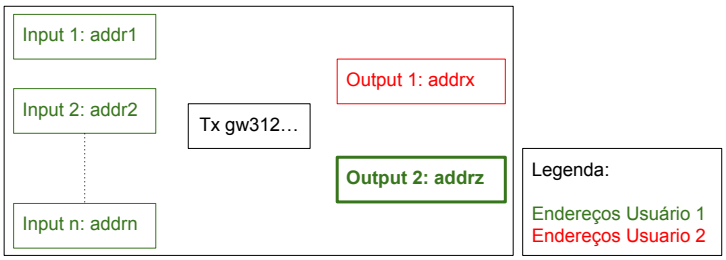


Figura 3 – Típica transação no Bitcoin com vários endereços pertencentes ao mesmo usuário e com dois endereços de saída: um deles do destinatário e o outro gerado pelo cliente Bitcoin e pertencente ao mesmo usuário que está pagando a fim de receber o troco.

Grau da transação: O grau de entrada (resp., saída) de uma transação é o número de endereços na lista de entrada (resp., saída). O grau da transação é a soma dos graus de entrada e saída.

Bloco: Consiste de um conjunto de transações. A tarefa dos mineradores é coletar transações pendentes de confirmação, formar blocos a partir destas e validar os blocos formados. O instante em que cada bloco é validado é estampado no próprio bloco.

Mineração: O ato de emitir novos blocos é chamado de mineração. Em dado momento existem diversos mineradores competindo entre si para serem os primeiros a validar o próximo bloco e ganharem as respectivas recompensas em *satoshis*.[1]

Bloco confirmado: Um bloco validado por um minerador e efetivado no *blockchain*.

Transação confirmada: Transação que faz parte de um bloco confirmado.

Prova de trabalho (proof of work): O primeiro minerador a validar um bloco recebe uma recompensa. Validar o bloco envolve resolver um desafio criptográfico, e desta forma pode-se dizer que a recompensa é fruto da prova de trabalho (*proof of work*). O fato de o estado atual da rede ser fruto da solução de inúmeros desafios criptográficos é uma das medidas usadas para minimizar ataques, tornando tais ataques muito custosos.

Cadeia de blocos: Uma sequência (lista encadeada) de blocos de transações confirmadas, considerada como registro de todas as transações realizadas pelo sistema.

Cadeia de blocos principal (*blockchain*): A maior sequência de blocos de transações confirmadas existente na rede. A cadeia de blocos principal é muito longa (acumulando

[1] O satoshi é a menor unidade da moeda Bitcoin. Uma unidade de satoshi equivale a 10^{-8} Bitcoin.

mais de 121 milhões de transações em abril de 2016), e envolveu uma quantidade de trabalho grande para ser criada tendo em vista que a inclusão de cada bloco requer a solução de um desafio criptográfico. Assim, existe um consenso sobre a natureza da maior parte dos blocos da cadeia principal do Bitcoin. Eventualmente, pode existir ambiguidade apenas sobre os últimos blocos incluídos na cadeia. Os blocos que não venham a ser considerados como parte da cadeia principal constituem cadeias órfãs.

Prioridade de transações: Existe um limite na quantidade de transações que podem ser incluídas por bloco. Para determinar quais transações incluir em cada bloco, os mineradores em geral utilizam uma fórmula padrão de prioridades que envolve a idade da transação, seu tamanho e incentivos na forma de taxas oferecidos por cada transação. Conforme veremos na Seção 3.3, prioridades afetam de forma significativa o tempo de confirmação experimentado pelas transações.

Taxa da transação (*fee*): Gorjeta não obrigatória oferecida pelos proponentes da transação para recompensar os mineradores que venham a confirmar tal transação. Valores maiores de gorjeta aumentam a prioridade na validação da transação, mas valores muito altos podem gerar suspeitas de operações ilícitas (*high-fee spam*). Como abordado em (BUNTIX, 2017) existem, a priori, duas principais hipóteses que explicam a razão da criação de tais transações com alta gorjeta: o primeiro cenário onde há um erro ou configuração errada do cliente Bitcoin responsável por criar transações, ou, sob um segundo aspecto mais nefasto os atacantes de fato elevam os *fees* das suas transações a fim de forçar que a média das gorjetas das demais transações subam, assim beneficiando os mineradores.

3 CARACTERIZAÇÃO DA DINÂMICA DAS TRANSAÇÕES DO BITCOIN

Apesar do crescente interesse em criptomoedas, tanto indústria quanto a academia sentem falta de análises quantitativas desses sistemas. Neste capítulo caracterizamos quantitativamente algumas das métricas associadas à rede Bitcoin. São visadas métricas importantes relacionadas a transações, como a probabilidade uma transação ser confirmada e o tempo decorrido para essa confirmação. Os resultados mostram que há um número não negligenciável de transações que não são confirmadas 24 horas após serem postadas na rede. Nesse caso, é observada uma alta correlação entre a taxa oferecida aos minerados pela confirmação de uma transação, seu volume (valor da transação) e a suspeita de que a transação não será confirmada. O capítulo mostra que transações do Bitcoin geralmente são confirmadas em períodos curtos, mas ainda assim, muito acima de tempos usuais de sistemas de cartão de crédito.

Neste capítulo são destilados alguns aspectos fundamentais relacionados às transações que circulam na rede Bitcoin. Para tal, contamos com dados públicos, disponíveis na rede, bem como dados colhidos ao longo de um ano por centenas de monitores instrumentados em diversos pontos do mundo. Os monitores obtém informações que não estão convenientemente acessíveis ao público geral, por exemplo, sobre transações que não foram confirmadas bem como o instante em que cada transação foi publicada na rede Bitcoin. As informações colhidas pelos monitores são enviadas para um banco de dados administrado pela startup *Skry*. A partir delas, podemos inferir propriedades sobre o tempo de espera experimentado pelos clientes, bem como sobre a chance de uma dada transação ser eventualmente confirmada.

Dentre as perguntas que visamos responder neste capítulo e no próximo, temos:

1. é possível inferir se uma dada transação será efetivamente confirmada ou não, no momento em que ela é primeiramente observada na rede Bitcoin? Esta pergunta é tema do capítulo 4.
2. qual a distribuição do tempo de confirmação das transações que são confirmadas? Esta pergunta é tema do presente capítulo.

Com a finalidade de responder estas perguntas, assumimos que uma transação que não é confirmada em 24 horas é considerada como inválida. Analisando os *datasets* coletados, as contribuições, com relação às perguntas anteriores são:

1. várias das transações inválidas possuem propriedades que permitem prever de forma precoce, com alto grau de acurácia, que de fato tais transações não serão confirmadas;
2. caracterização da distribuição do tempo de confirmação das transações válidas, e parametrização por distribuições clássicas a fim de que se possa utilizar as caracterizações de forma simples e conveniente em trabalhos futuros.

3.1 DADOS UTILIZADOS

Nesta seção, são descritos os dois *datasets* utilizados neste trabalho.

O primeiro conjunto de dados, usado na seção 3.2, foi coletado no período de 23-29/05/2015 referente às transações confirmadas e não confirmadas. Os dados são originários de um *streaming* do sistema de nós monitores desenvolvidos pela *Skry* e que estão espalhados por todos os continentes. Cada transação, portanto, é anotada com o *timestamp* do momento em que ela foi primeiro vista por alguns dos nós da rede de monitores. Cada transação, assim que coletada, é armazenada durante 24 horas[1] e verifica-se se de fato esta foi confirmada usando uma API desenvolvida também pela *Skry*. Ao final desse processo, foram gravadas 697,392 transações, cada uma possuindo informações como o tamanho em KB, o *fee* associado, o volume transacionado, grau de entrada e de saída e o tempo de confirmação.

O segundo *dataset*, usado na seção 3.3, é uma composição de registros do banco de dados proveniente da empresa *Skry* que compreende transações confirmadas entre 22/09/2015 e 11/01/2016. Para cada transação é anotado o instante em que esta foi vista pela primeira vez por algum dos monitores. Este *dataset* contém 12,725,212 transações confirmadas e que foram incluídas no *blockchain*.

[1] Aqui, uma transação é considerada como não confirmada se não houve sua efetivação no *blockchain* em até 24 horas

3.2 TEMPO DE CONFIRMAÇÃO DE TRANSAÇÕES

Nesta seção descrevemos uma metodologia para previsão de confirmação de transações conforme elas são geradas.[2] De fato, como é de conhecimento comum, o tempo de confirmação no Bitcoin é bem maior que o de transações em cartões de crédito. Assim, a previsão se faz necessária e interessante para instituições que analisam riscos de créditos e que desejam ter relacionamento com a rede do Bitcoin.

No Bitcoin, assim que uma transação é gerada, suas informações são imediatamente espalhadas ao longo da rede a fim de serem, eventualmente, efetivadas dentro de um bloco a ser confirmado. Nesse trabalho, definimos como tempo de confirmação de uma transação como a diferença entre os instantes de tempo em que o bloco em que ela está inserida é confirmado por algum minerador e o instante em que a transação foi primeiro vista por um dos monitores.

Conforme a definições do protocolo usado no Bitcoin, cada bloco leva em média 10 minutos para ser confirmado (BONNEAU, 2015). Portanto as caracterizações e estimativas dos tempos de confirmação das transações abordado neste trabalho são entendidos como um problema fundamental intrínseco ao protocolo e definições do Bitcoin.

Para construção do modelo de previsão, é necessária a caracterização prévia de aspectos que podem ser agrupados dentre aqueles inerentes à própria transação bem como aqueles referentes aos estado e dinâmica de todo o sistema de nós e mineradores. Assim, essa seção se concentra nos fatores pontuais das transações como a quantidade de endereços creditados pela transação, razão entre o *fee* e o volume total pago de satoshis e o próprio tamanho das transações.

A CDF na Figura 4 mostra o cenário geral para as transações recém geradas e que foram confirmadas durante a semana de maio de 2015. Em torno de 90% delas foram confirmadas em até 30 minutos a partir do momento que foram vistas pela primeira vez pelos monitores.[3] Portanto para entidades que desejam utilizar o *Bitcoin* como meio de pagamento é desejável que o tempo de confirmação de transações seja o menor possível e portanto pode haver um impacto significativo no nivel de negócio.

No grupo de transações não confirmadas houve casos em que uma transação

[2] Os experimentos e programas criados para *streaming* e monitoramento de transações foram implementadas usando o ambiente do *Google Cloud Compute Engine* <http://cloud.google.com/compute>. Cada monitor de transações foi configurado numa instancia *Standard* de 4 *cores*

[3] A precisão do tempo de confirmação está atrelada à cobertura dos monitores. Nossos monitores estão espalhado por todos os continentes. Assim temos uma visão abrangente da rede.

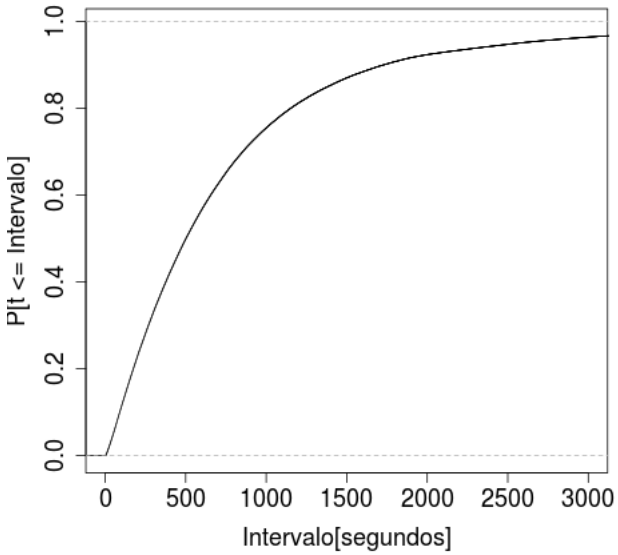


Figura 4 – CDF do tempo de confirmação para as transações confirmadas

possui mais de 100 endereços de saída, ou cujo o *fee* foi superior a mais de 20 vezes o valor da própria transação, ou cujo tamanho foi maior do que 20MB. Uma árvore de decisão, baseada nestas *features* é utilizada no capítulo 4, para realizar uma primeira separação entre aquelas transações com alta chance de serem confirmadas, daquelas que não serão. Este cenário é inexistente no grupo de transações confirmadas e pode explicar o fator de *delay* no tempo de confirmação por parte dos mineradores.

Os mineradores optam por não adicionarem transações relativametne grandes, ou que possuem o seu *fee* destoante do valor de referência definido pelo protocolo do Bitcoin (i.e. 0.0001 BTC/KB (BITCOINWIKI, 2015)). Atacantes que geram tais transações sugerem induzir interesse ou até mesmo burlar o minerador para que suas transações sejam confirmadas. Estas transações foram reportadas em fórums tais como em (BITCOINTALK, 2016) e são conhecidas como *high-fee spam*.

3.3 CARACTERIZAÇÃO DO TEMPO DE CONFIRMAÇÃO

Nesta seção, são caracterizados alguns aspectos relacionados com a dinâmica e estado da rede no Bitcoin tais como o tempo entre geração de blocos, tempo entre chegadas de transações e quantidade de blocos ativos no sistema. Além disso é proposto um modelo que relaciona tais aspectos com o tempo de confirmação das transações.

A linha de tempo na Figura 5 mostra a dinâmica relacionada com o processo de chegada de transações para serem mineradas, bem como a indicação dos intervalos entre chegada de transações dentro de um bloco. T e B denotam intervalos entre divulgação de

transações e entre confirmação de blocos, respectivamente. $T_{j,i}$ denota o intervalo entre a divulgação da i-ésima transação pertencente ao bloco j e a divulgação da transação imediatamente anterior a ela. B_j denota o intervalo de tempo entre a confirmação do j-ésimo bloco e a confirmação do bloco $j-1$.

Seja $D_{j,i}$ o tempo de confirmação da i-ésima transação do bloco j. $D_{j,i}$ é igual ao instante de tempo em que o bloco no qual a transação está contida foi confirmado, menos o instante de tempo no qual tal transação foi primeiro divulgada.

O tempo de atividade do bloco j é denotado por S_j. Ele é igual ao intervalo de tempo entre a primeira transação do bloco j ter sido divulgada e o instante em que o bloco j foi confirmado.

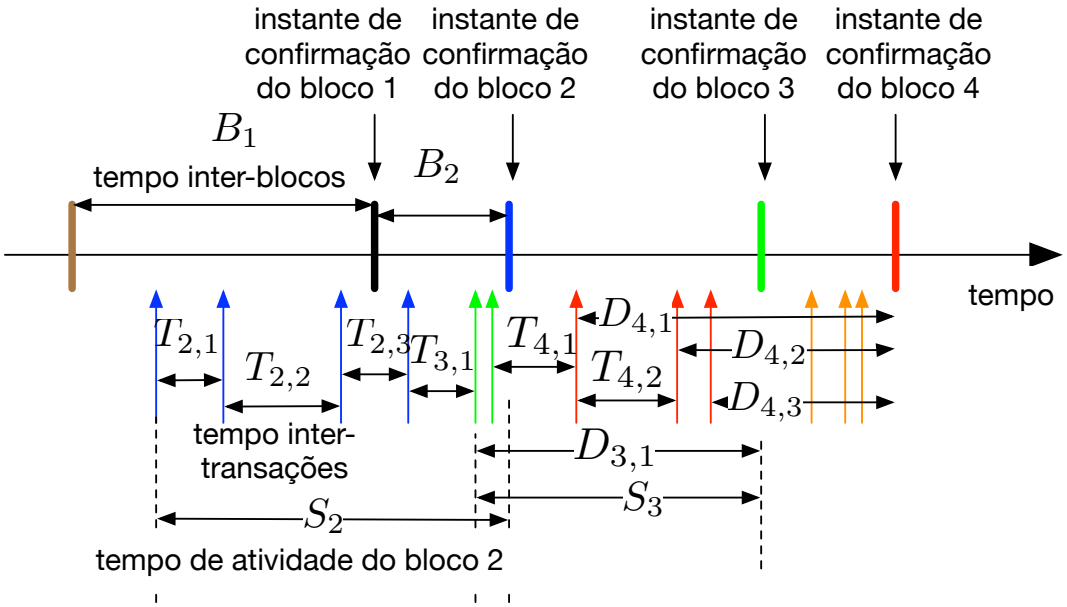
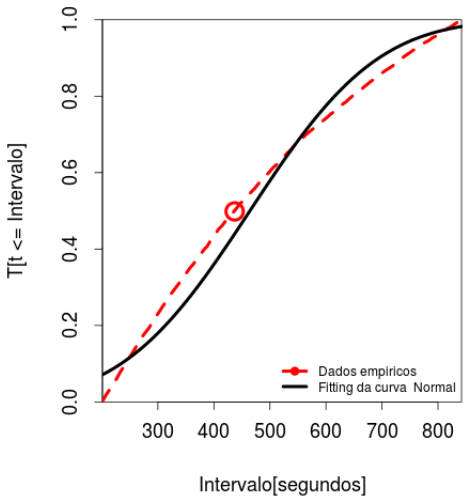


Figura 5 – Caracterizaçao do tempo de confirmação.

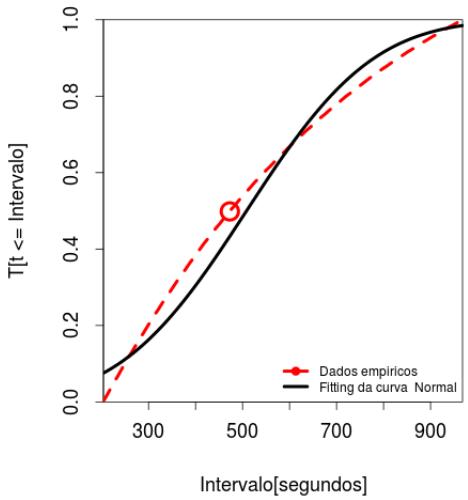
A fim de minimizar o efeito de ruídos gerados pelas ferramentas de coleta de dados executadas pelos monitores, foi realizada uma filtragem dos dados da série temporal de tempo entre transações, e consideramos apenas valores que estão entre o primeiro e terceiro quartis da distribuição. Após feita esta filtragem, os tempos entre transações consecutivas no *trace* analisado variou entre 0 e 1 segundo.

A CDF da distribuição dos tempos entre blocos, bem como a curva que melhor se adequa à distribuição empírica, estão representadas na Figura 6a. Recordando, seja B a variável aleatória que caracteriza o tempo entre confirmação de blocos. A melhor distribuição que descreve o intervalo entre confirmação de blocos é a normal com parâmetros $E(B) = 464.30$ segundos e $V(B) = 179.57$. Desta forma tem-se um coeficiente de variação de 0.029. Em média os blocos gastam quase 8 minutos para serem

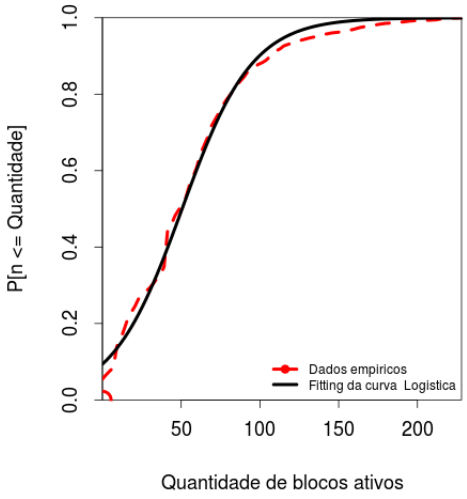
minerados. Note que esse valor é um pouco menor que o alvo de 10 minutos visado no projeto da rede Bitcoin (vide <https://bitcoinwisdom.com/bitcoin/difficulty> para mais detalhes).



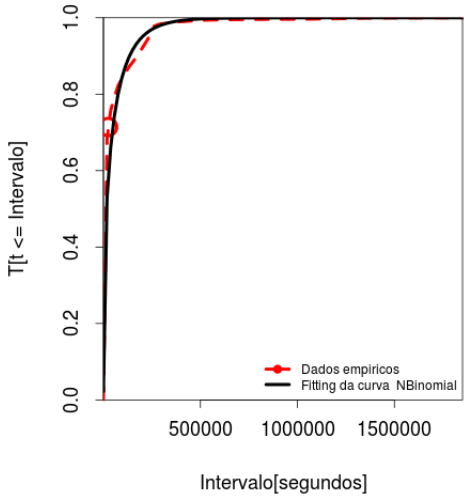
(a) Fitting da CDF do tempo entre blocos, B



(b) Fitting da CDF do tempo de confirmação das transações, D



(c) Fitting da CDF da quantidade de blocos ativos, M



(d) Fitting da CDF do tempo de atividade dos blocos, S

Figura 6 – Fittings de métricas para a dinâmica de confirmação e tempos relacionados com transações e blocos

Já a CDF representada na Figura 6b reflete o intervalo de tempo que uma determinada transação espera por sua confirmação. Seja D a variável aleatória que caracteriza o tempo de confirmação de uma transação. Percebe-se que, assim como para a distribuição dos tempos entre blocos, a melhor distribuição que descreve os dados empíricos foi a normal, com parâmetros $E(D) = 508.51$ segundos e $V(D) = 212.11$, cujo coeficiente de variação calculado é 0.029. Portanto, em média as transações esperam um

pouco mais de 8 minutos para serem confirmadas. Note que $E(D) > E(B)$, o que reflete o fato de que as transações tipicamente precisam esperar, na média, por pelo menos uma validação de bloco antes de serem consideradas como candidatas a validação.

Seja $E(B_r)$ o valor esperado da vida residual do tempo entre blocos. Quando uma nova transação chega ao sistema, ela espera $E(B_r)$ até enxergar o próximo bloco sendo confirmado,

$$E(B_r) = E(B^2)/(2E(B)) \tag{3.1}$$

O tempo médio de confirmação de uma transação é dado pela vida residual do tempo até a confirmação do próximo bloco, somada à espera pela confirmação de blocos adicionais até que esta seja efetivamente confirmada. Seja α o parâmetro que quantifica o número médio de blocos adicionais que se aguarda até uma confirmação. Então,

$$E(D) = \alpha E(B) + E(B_r) \tag{3.2}$$

Podemos estimar α experimentalmente. Conforme descrito nesta seção, temos que $E(B_r) = (179.57 + (464.30)^2)/(2(464.30)) = 232.34$, $E(D) = 508.51$ e $E(D) - E(B_r) = 276.16$. Ou seja, $\alpha = 0.6$, o que significa que na média as transações precisam esperar a vida residual de um bloco mais aproximadamente 0.6 do tempo entre blocos para serem servidas. Em outras palavras,

$$E(D) = 0.6(E(B) + E(B_r)) + 0.4E(B_r) \tag{3.3}$$

Na média 40% das transações já são atendidas no primeiro bloco que tem oportunidade de encontrar ao chegarem no sistema, e 60% tem de esperar por mais um bloco para serem confirmadas.

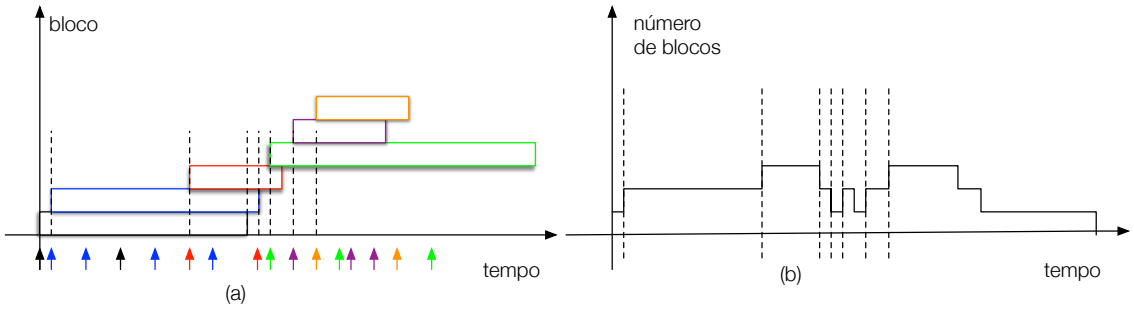


Figura 7 – Blocos ativos: (a) cada barra inicia quando ocorre a primeira transação associada ao bloco, e termina quando o bloco é confirmado; (b) número de blocos ativos em função do tempo. A área embaixo desta curva divida pelo tempo produz o número médio de blocos ativos.

Para obter maior entendimento sobre o tempo experimentado pelas transações, estudamos também o número de blocos ativos no sistema. Seja $E(M)$ o número esperado

de blocos encontrados no sistema. $E(M)$ é igual à área embaixo da curva mostrada na Figura 7 divida pelo tempo de observação.

A Figura 6c representa a CDF empírica da quantidade de blocos ativos, bem como a curva de *fitting* que melhor se adequou aos dados: a distribuição logística com $E(M) = 50.60$ blocos ativos e $V(M) = 22.30$. Em princípio, tal média de blocos ativos é alta se comparada com o número médio de confirmações de blocos que uma transação típica observa antes de ser confirmada (em torno de 1.6 confirmações, conforme discutido acima). Um dos fatores que explicam tal discrepância é o esquema de prioridades implementado na rede (vide Seção 2). Algumas transações precisam aguardar muito mais que outras para serem confirmadas, o que favorece um aumento do número de blocos ativos.

Em relação ao tempo de atividade de cada bloco, a Figura 6d mostra a sua CDF empírica, bem como o melhor *fitting* encontrado, dado pela distribuição binomial com $n = 47158$ e probabilidade de sucesso $p = 0.37$. Denotemos por $\hat{S}$ o estimador do tempo de atividade de cada bloco. Temos a média estimada $E(\hat{S}) = np = 17448.46$ segundos e variância $V(\hat{S}) = np(1-p) = 104.85^2$, com coeficiente de variação em torno de 0.006. Em média os blocos estão ativos em torno de 5 horas. Esse número, bem maior que o tempo médio entre gerações de novos blocos que é de aproximadamente 8 minutos, mais uma vez reflete o fato de que algumas transações ficam pendentes no sistema por muito tempo antes de serem confirmadas, acarretando em tempos de atividades de blocos na ordem de horas (Figura 6(b)).

De acordo com o resultado de Little, temos que $E(M) = \lambda_B E(S)$, onde λ_B denota a taxa média de chegada de blocos, $\lambda_B = 12968/9605710 = 0.00135$ blocos/segundo (observamos 12,968 blocos de 22/09/2015 19:36:06 até 11/01/2016 23:51:16). Logo, $E(S) = 50.6/0.00135 \approx 10.4$ horas. Note que $E(S)$ é aproximadamente igual ao dobro do valor de $E(\hat{S})$ estimado pelo *fitting* da distribuição binomial discutido no último parágrafo. A discrepância pode ser consequência do fato de o sistema não encontrar-se em estado estacionário ou em equilíbrio. Ao aplicarmos o mesmo modelo em dados colhidos mais recentemente, e reportados no projeto de final de curso de Eduardo Ferreira (UFRJ, 2016), obtivemos a concordância entre os resultados empíricos e aqueles obtidos via lei de *Little*.

O tempo médio de confirmação de uma transação envolve vários fatores, incluindo as taxas associadas, incentivos etc. Neste trabalho, apresentamos um modelo preliminar para relacionar o tempo médio de confirmação de uma transação e o tempo entre blocos. Trabalho futuro consiste em analisar os diferentes fatores que afetam o

tempo de confirmação, levando em conta prioridades.

4 CLASSIFICAÇÃO DE TRANSAÇÕES SOB A ÓTICA DE REDES NEURAIS

O presente capítulo tem por objetivo principal o uso da rede neural sem peso *WiSARD* (com e sem *bleaching*) para classificação da confirmação de transações no Bitcoin. Um de nossos objetivos é encontrar qual a melhor combinação de parâmetros da rede neural para tomada de decisões rápidas sobre se uma transação será confirmada ou não.

4.1 TRABALHOS RELACIONADOS

A rede Bitcoin pode ser vista como um grafo de transações modelado de tal forma onde os vértices são transações e as arestas são entendidas como o fluxo de bitcoins entre transações. Trabalhos como (MÖSER; BÖHME; BREUKER, 2014; MÖSER; BÖHME; BREUKER, 2013; MÖSER; BÖHME, 2015) buscam analisar a rede de transações sob perspectiva de grafos e assim criar modelos de lavagem de dinheiro, de influências e detecção de anomalias.

Em particular (MÖSER; BÖHME; BREUKER, 2014) descreve um modelo de risco de transações para entidades de crédito e para até mesmo mineradores avaliarem o risco associado à lavagem de dinheiro e outros comportamentos maliciosos. Porém os autores não levaram em conta uma camada que analisasse se uma transação é ou não confirmada com base em suas características.

Este capítulo visa cobrir esta lacuna e assim aplicar no contexto de classificação de transações um classificador baseado em rede neural sem pesos como retratado em (ALEKSANDER et al., 2009; CARVALHO et al., 2013).

Ainda no âmbito de confirmação de transações, já é uma prática predizer a probabilidade de confirmação de uma transação não confirmada para liberação do pagamento efetuada pela plataforma. A plataforma de pagamentos via Bitcoin tratada em (PEREZ, 2014) utiliza verificação por *double-spending* e confiança associada ao minerador responsável pela mineração para predizer a confirmação da transação. Neste capítulo, em contrapartida, fazemos uso apenas de dados disponíveis publicamente sobre as transações sendo analisadas.

4.2 *DATASET* E MODELAGEM

Os dados utilizados são os mesmos usados no capítulo 3, referentes à transações que não foram ainda confirmadas no momento da coleta.

Cada transação é modelada como um vetor de *features*. Aquelas utilizadas neste trabalho são básicas e não demandam nenhuma derivação para serem calculadas, pois todas as informações consideradas estão explícitas no corpo da transação recebida.

Portanto as *features* consideradas para este trabalho são:

- Tamanho em KB;
- *Fee* em bitcoins BTC;
- Valor transacionado em BTC;
- Quantidade de endereços usados como entrada/pagadores da transação;
- Quantidade de endereços a serem pagos na saída da transação;
- Razão entre *fee* e o valor transacionado.

4.3 RESULTADOS

As Figuras 8, 9 e 10, ilustram os resultados obtidos da coleta. Em cada figura, no eixo x temos os *bins* referente à cada intervalo dos tempos de confirmação das transações e no eixo y a frequência de transações para cada um dos *bins*. O último elemento do eixo x, marcado com UTx (unconfirmed transactions) corresponde à transações que, após 24 horas, ainda não tinham sido confirmadas. Estas transações são por nós consideradas como não confirmadas (ou inválidas). Em cada *bin*, usamos 3 tons de cinza para distinguir diferentes tipos de transações. Na Figura 8, distinguimos entre transações que possuem tamanho maior do que $20KB$ (preto), de $10KB$ a $19KB$ (cinza escuro) e de 0 a $9KB$ (cinza claro). Na Figura 9, distinguimos entre transações que possuem quantidade de saída maior do que 548 (preto), de 274 a 547 (cinza escuro) e de 0 a 273 (cinza claro). Na Figura 10, distinguimos entre transações que possuem a razão entre o *fee* e *valor da transacão* maior do que 13740.0 (preto), de 10.0 a 13739.99 (cinza escuro) e de 0 a 9.99 (cinza claro).

4.4 ANÁLISE E FILTRAGEM

O *dataset* considerado possui algumas características peculiares. A primeira se refere a distribuição dos tamanhos das transações como mostrado no histograma da Figura 8. Necessariamente todas as transações com mais de 9KB não foram confirmadas em 24 horas desde o seu recebimento em um dos nodos da rede.

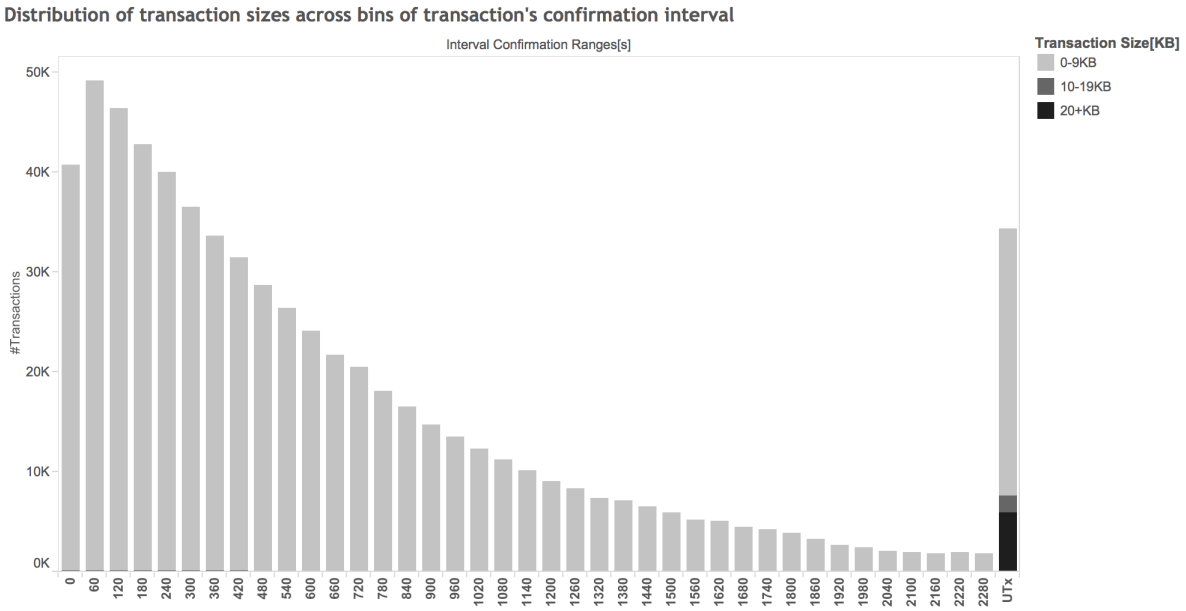


Figura 8 – Histograma da distribuição dos tamanhos das transações que estão representados via escala de cinza entre os bins de intervalos de tempo de confirmação. O último bin se refere as transações que não foram confirmadas em 24 horas

Todas as transações desta base de dados que possuem mais de 273 endereços de saída não foram confirmadas em até 24 horas pela rede de mineradores como mostrado na Figura 9.

Já uma outra característica retratada na Figura 10 aponta que todas as transações cuja razão entre seu *fee* e valor transacionado é superior a 10 também não foram confirmadas.

4.5 ÁRVORE DE DECISÃO

Considerando todas as características apontadas, o problema de classificação pode, em parte, ser facilmente mapeado para uma árvore de decisão. Assim a aplicação da *WiSARD* se destina a tarefa de classificar aquele grupo de transações que não podem ser consideradas não confirmadas considerando apenas algumas destas características apontadas.

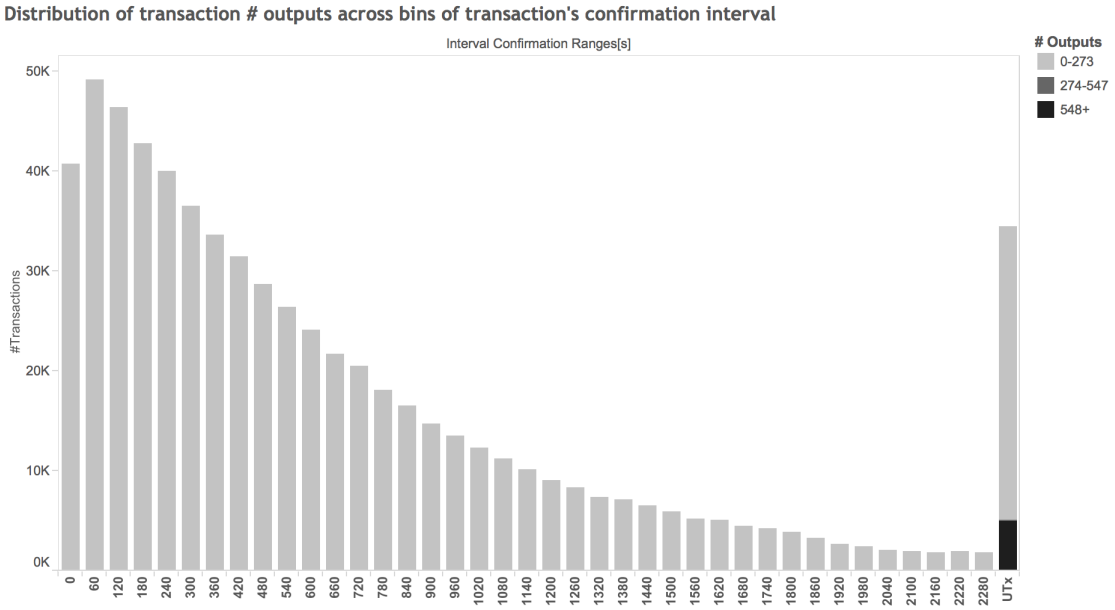


Figura 9 – Histograma da distribuição da quantidade de endereços de saída que estão representados via escala de cinza entre os bins de intervalos de tempo de confirmação. O último bin se refere as transações que não foram confirmadas em 24 horas

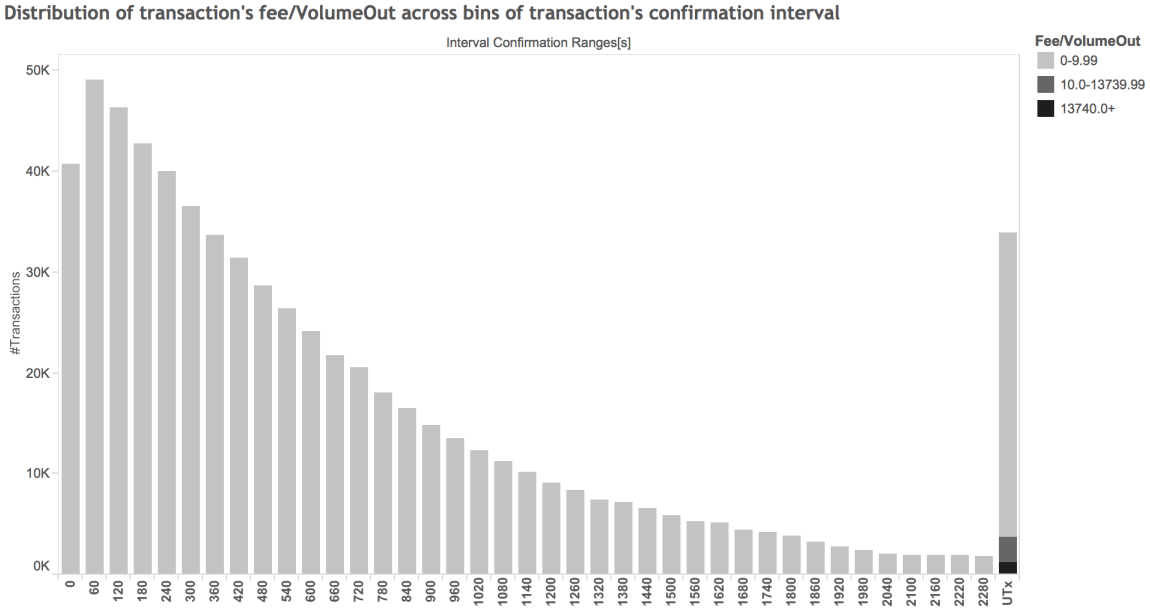


Figura 10 – Histograma da distribuição da razão entre o fee pelo valor transacionado que estão representados via escala de cinza entre os bins de intervalos de tempo de confirmação. O último bin se refere as transações que não foram confirmadas em 24 horas

A Figura 11 ilustra a árvore de decisão usada no modelo em conjunção com a *WiSARD*.

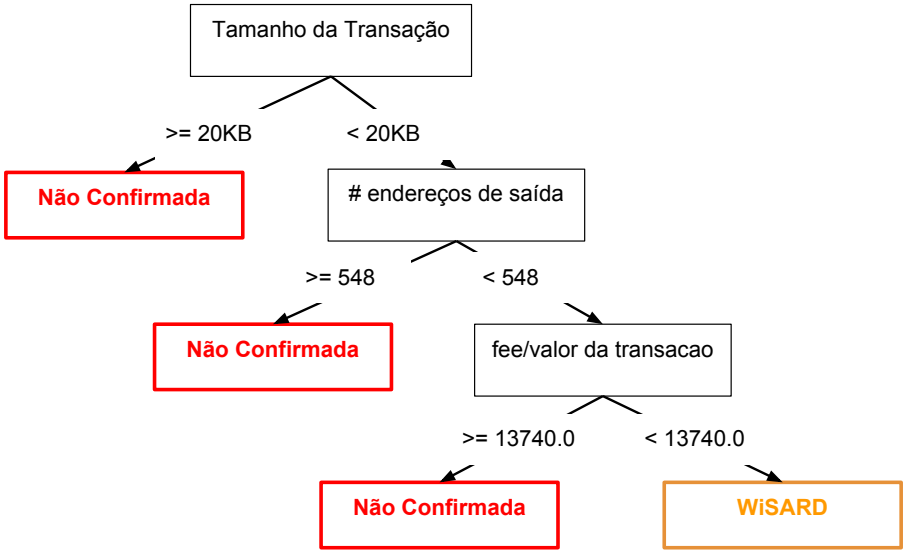


Figura 11 – Árvore de Decisão usada para classificar transações em confirmadas e não confirmadas. Baseada em algumas *features*, a árvore classifica preliminarmente as transações que não serão confirmadas. O conjunto que não tem-se certeza é verificado junto a *WiSARD* proposta no modelo.

4.6 CONJUNTOS DE TREINO E TESTE

Contamos com um total de 680800 transações para serem consideradas pelo classificador *WiSARD*. Deste conjunto aproximadamente 20000 estão rotuladas como não confirmadas e o restante como confirmadas. Portanto para evitar o desbalanceamento entre rótulos no momento do treinamento, foram selecionados aleatoriamente 500 exemplos de cada uma das duas classes de transações. Desta forma a base de treino possui 1000 exemplos.

4.7 MAPEAMENTO PARA RETINA

Como a *WiSARD*[1] lida somente com entradas binárias, fizemos um pré-processamento na base de dados de treino incluindo discretização e binarização para cada *feature* considerada.

[1] A implementação utilizada para a Rede Neural sem pesos está disponível em <http://github.com/firmino/PyWANN>

Para a discretização foram considerados os algoritmos de discretização supervisionados *Chi2* e *ChiMerge* abordados respectivamente em (LIU; SETIONO, 1995) e (KERBER, 1992). Na seção 4.8 há o comparativo dos resultados para as duas discretizações utilizadas.

O segundo passo consiste em binarizar os dados discretizados. Assim foi descoberto o tamanho mínimo da palavra binária para representar cada *feature*. Para a codificação foi utilizado o *Gray Code* onde valores sucessivos diferem de apenas um *bit*, assim favorecendo uma melhor classificação pela rede neural. Após a codificação, os valores codificados são concatenados para formar uma única palavra binária. Tal palavra será considerada a retina que é lida pela *WiSARD*. Para a discretização usando o algoritmo *Chi2*, o tamanho resultante da retina é de 36 bits, enquanto para a discretização usando *ChiMerge* é de 42 bits.

4.8 RESULTADOS

Para os experimentos realizados foram utilizados duas versões da *WiSARD*. A primeira versão consiste na rede básica, apenas decidindo qual o tamanho da memória RAM para cada um dos discriminadores. Já a segunda versão inclui *bleaching*, como tentativa para melhorar os resultados obtidos.

Os experimentos foram realizados usando *10-fold cross validation*. Desta forma a base de treino foi dividida, igualmente, em 10 partições, das quais uma escolhida para treino e as outras 9 são utilizadas para os testes. Assim, os resultados obtidos são as médias de cada um dos 10 cenários realizados.

Cada avaliação consiste em verificar a porcentagem de acertos e erros na classificação. Cada classificação é decidida em função da quantidade de RAMs ativadas para cada discriminador. Logo, aquela classe do classificador cuja quantidade de ativações é a maior entre as duas classes consideradas (transação confirmada e transação não confirmada) é considerada como a resultante na classificação da transação. A tabela 1 mostra que o melhor resultado nas classificações foi obtido quando o tamanho da palavra da RAM é de 6 para a discretização usando o método *Chi2*, enquanto para o *ChiMerge* a maior percentagem de acertos na classificação foi para palavras de 7 bits de RAM.

As Figuras 12 e 13 mostram *scatter plots* das percentagens de erros e de acertos para as duas discretizações utilizadas. Cada ponto simboliza uma combinação diferente da quantidade de bits da memória RAM usada, do fator de *bleaching*, bem como para o fator de confiança na classificação.

Tabela 1 – *WiSARD* sem *bleaching*

Discretização	#bits RAM	%Acertos	%Erros
Chi2	2	51.11	48.88
	3	51.41	48.58
	4	52.94	47.05
	6	53.21	46.78
	9	52.92	47.07
ChiMerge	2	49.70	50.30
	3	49.77	50.22
	6	49.85	50.14
	7	50.31	49.68
	14	49.51	50.48

Para a discretização *Chi2* o tamanho da memória RAM de 3 bits foi a que obteve melhor resultados com o fator de *bleaching* igual a 3 e fator de confiança na classificação de 0.05, como apontado na Figura 12. Já para a discretização *ChiMerge*, o melhor resultado em que a porcentagem de acertos foi maximizado e porcentagem de erros minimizada foi ao utilizar memória RAM de 7 bits com fato de *bleaching* de 5 e confiança na classificação de 0.05

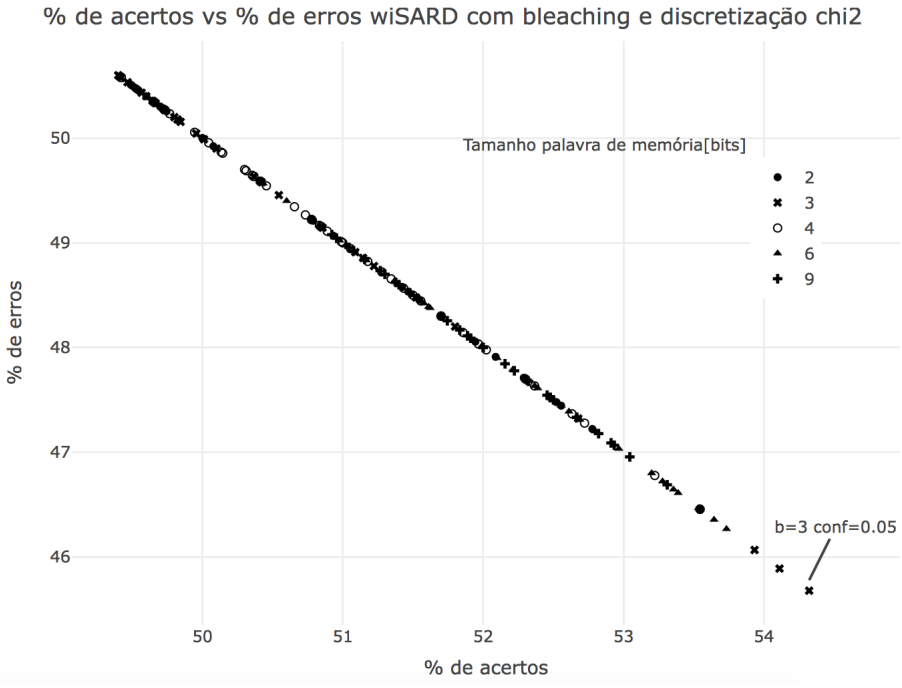


Figura 12 – *Scatter plot* das percentagens de acertos e erros considerando a discretização *Chi2*.

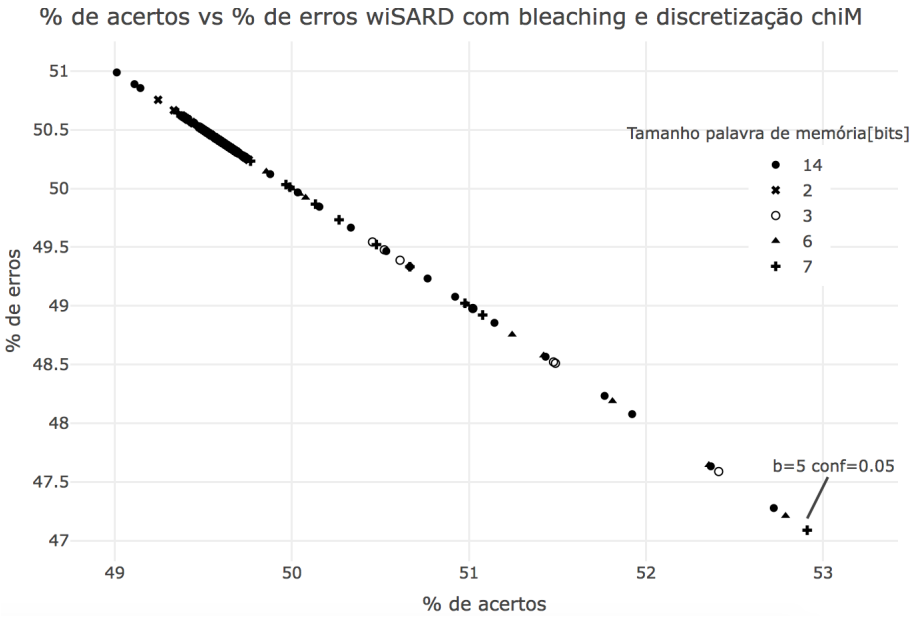


Figura 13 – *Scatter plot* das percentagens de acertos e erros considerando a discretização *ChiMerge*.

5 DETECÇÃO DE ANOMALIAS NA REDE BITCOIN

Este capítulo trata da detecção de transações consideradas como anômalas em relação àquelas transações mais recentes.[1] Neste âmbito é feito a aproximação da detecção de transações *outliers*, consideradas anômalas, com base no quão nova a informação associada a elas estão em relação ao histórico de recência de transações no *Bitcoin*.

A proposta do capítulo é abordar dois métodos para detecção de transações anômalas. Tais abordagens são úteis no monitoramento de transações e automatizam a indicação de ocorrência de *outliers* que podem ser discriminados, a fim de análises mais detalhadas.

Os dois métodos são estatísticos e fazem aproximação da distribuição gaussiana (BISHOP, 2006; GOODMAN, 1963) para cada *feature* usada em uma transação. O primeiro método, univariado, considera como distribuição conjunta das *features* o produto de gaussianas, enquanto segundo considera a mistura de gaussianas.

5.1 DADOS E PRÉ-PROCESSAMENTO

Os dados se referem aos grafo de fluxo de bitcoins onde a transação a ser analisada recebe o fluxo de dinheiro resultante provenientes das transações anteriores. Em específico é considerado para cada transação uma profundidade de 5 *hops* anteriores no seu grafo de fluxos.

A Figura do 14, ilustra um grafo de fluxos de bitcoins. A transação **Tx1** é a transação para a qual será calculado o seu *score* de anomalia. Nota-se que no grafo, que é um subgrafo do grafo de transações da rede Bitcoin, as arestas refletem a movimentação de bitcoins do endereço de saída da transação anterior para uma das entradas da transação subsequente. Neste caso, a ilustração mostra a construção do grafo até o terceiro *hop* de profundidade a partir da transação a ser analisada, **Tx1**.

Cada grafo é modelado como um vetor de *features* que traduzem aspectos quantitativos do grafo de transações. Os seguintes termos são usados para definição das

[1] As análises dos modelos de detecção de anomalias foram realizadas usando o *Google Cloud Datalab*, bem como os *frameworks* e bibliotecas desenvolvidas em *Python* e *Python Notebook*

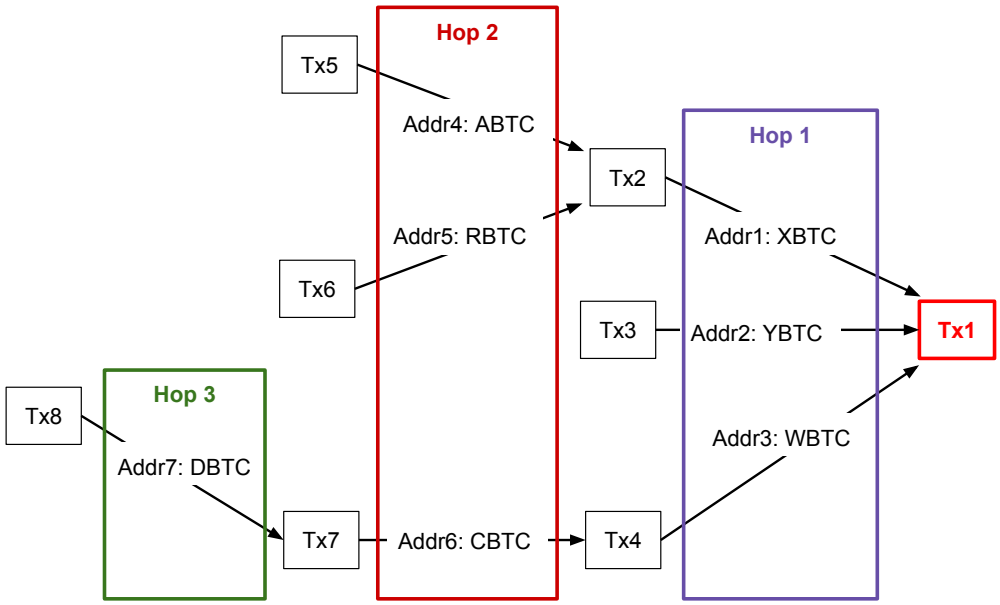


Figura 14 – Grafo de fluxos de 3 *hops* de profundidade para cálculo de anomalia da transação Tx1

features:

- **intervalo de blocos:** é o intervalo do espaço temporal, onde a unidade de tempo é o número do bloco. Portanto o intervalo de bloco entre o bloco 10 e bloco 15 é 5. O número do bloco é gerado para cada bloco minerado e de forma incremental é atribuído um novo número a cada bloco criado.
- **volume transacionado por bloco:** o somatório de todas as transações que pertencem a um mesmo bloco e que estão presentes no grafo de fluxos construído.
- **quantidade de saídas por bloco:** quantidade de arestas de um bloco e que estão presentes no grafo de fluxos.
- **caminho:** a sequencia mais longa de arestas delimitadas por nós (transações).
- **entradas:** são os valores associados a cada endereço usado como pagador em cada uma das transações.
- **saídas:** são os valores associados a cada endereço para o qual *bitcoins* são destinados.

- ***fee*:** a diferença entre os somatórios de valores da entrada e da saída. Esse valor é destinado para os mineradores.

A seguinte lista mostra as *features* utilizadas:

- **média, mínimo, máximo e variância** da quantidade de entradas nas transações do grafo;
- **média, mínimo, máximo e variância** da quantidade de saídas nas transações do grafo;
- **média, mínimo, máximo e variância** do volume de entrada nas transações do grafo;
- **média, mínimo, máximo e variância** do volume de saída nas transações do grafo;
- **média, mínimo, máximo e variância** do *fee* nas transações do grafo;
- **média** do intervalo de blocos em cada caminho de fluxos do grafo;
- **média** do volume transacionado por bloco em cada caminho de fluxos do grafo;
- **média** da quantidade de saídas por bloco em cada caminho de fluxos do grafo.

Para ilustrar o cálculo de cada uma das *features* temos os seguintes valores para o grafo mostrado na Figura 15, obtida a partir da Figura 14 :

- **média, mínimo, máximo e variância das métricas das transações:** a tabela 2 mostra os valores calculados das métricas relacionadas com quantidade de entradas e saídas, volumes de entrada e saída e *fee* para o grafo analisado.

Tabela 2 – Tabela das estatísticas descritivas das métricas das transações do grafo de fluxos

Feature	**média**	**mínimo**	**máximo**	**variância**
# saídas	1.5	0	3	0.86
# entradas	0.875	0	3	1.27
volume de entrada	16.75	0	60	494.5
volume de saída	16.75	0	32	177.36
fee	0.3	0.01	0.3	0.0092

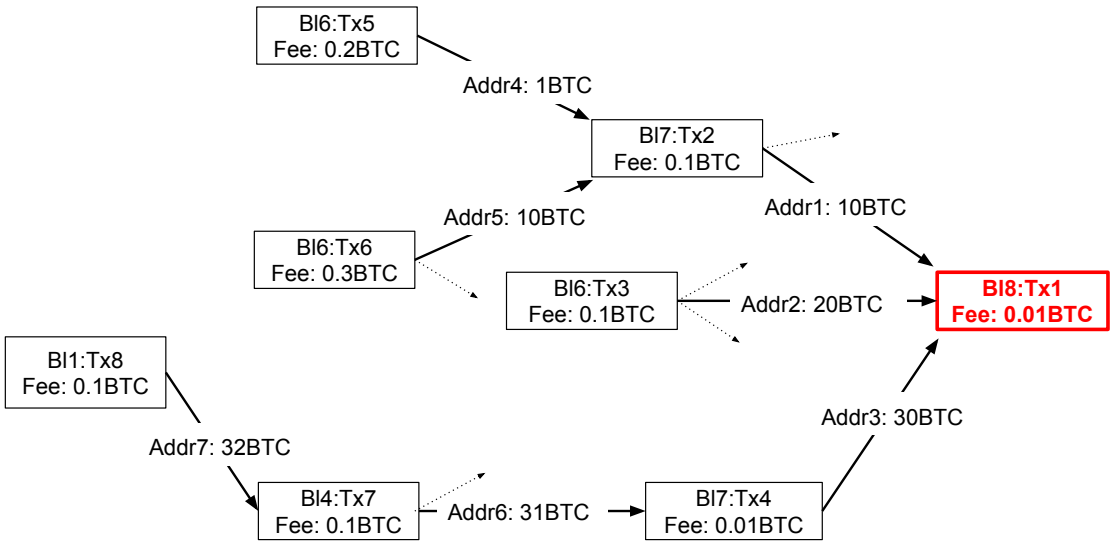


Figura 15 – Exemplo do grafo de fluxos de 3 *hops* de profundidade para cálculo de anomalia da transação Tx1

Tabela 3 – Cálculo das métricas relacionadas com os caminhos do grafo de fluxos

	Intervalo Blocos	**Volume bloco**	**#saídas por blocos**
Tx1->Tx2->Tx5	2	1/3	3/3
Tx1->Tx3	2	20/2	3/2
Tx1->Tx2->Tx6	2	10/3	4/3
Tx1->Tx4->Tx7->Tx8	7	30/4	4/4
Média	3.25	5.29	1.21

- **média do intervalo de blocos, do volume transacionado e da quantidade de saídas em cada caminho:** seja um definido como uma cadeia entre o nó *sink* e nó folha do grafo de fluxos, temos como exemplo o caminho $Tx1 -> Tx2 -> Tx5$ no grafo da Figura 15. Portanto a tabela 3 mostra o cálculo das métricas relacionadas com as médias entre os caminhos.

Desta forma o conjunto de *features* procura refletir estatísticas descritivas dos componentes principais e básicos de cada transação contida num grafo de fluxos, bem como aproximação da velocidade do fluxo de moedas em cada caminho do grafo.

O primeiro passo do pré-processamento é transformar todas as *features* em escala logarítmica na base neperiana. Desta forma cada valor é considerado como valor modular e somado com uma constante c, onde $c = 100.0$. Após essa modificação é calculado o valor do logaritmo na base neperiana:

$$n = \log(|o| + c) \tag{5.1}$$

onde,

- n é o valor resultante da *feature*
- o é o valor bruto e original da *feature*

O próximo procedimento é realizar a normalização pela média e desvio-padrão de cada uma das *features*, cujo objetivo é aproximar cada distribuição como normal com média 0 e desvio-padrão 1:

$$\hat{v} = (v - \mu)/\sigma \tag{5.2}$$

onde,

- $\hat{v}$ é o valor resultante da normalização
- v é o valor original
- μ corresponde a média dos valores da população para a *feature*
- σ se refere ao desvio-padrão da *feature* na população

O *boxplot* na Figura 16 mostra a média, valores máximo e mínimos para cada uma das *features* consideradas.

Com o objetivo de eliminar redundância de informação, foi calculada a correlação das *features* e todas aquelas cuja correlação com outra *feature* resultou em coeficiente de *Spearman* acima de 0.99 foram eliminadas. No caso específico, foram eliminadas as *features* relacionadas com o volume de saída, já que estão com correlação acima de 0.99 com todas *features* correspondentes e que descrevem ao volume de entrada. No total são 4 *features* eliminadas (média, máximo, mínimo e variância do volume de saída). A matriz de correlações é apresentada na Figura 17.

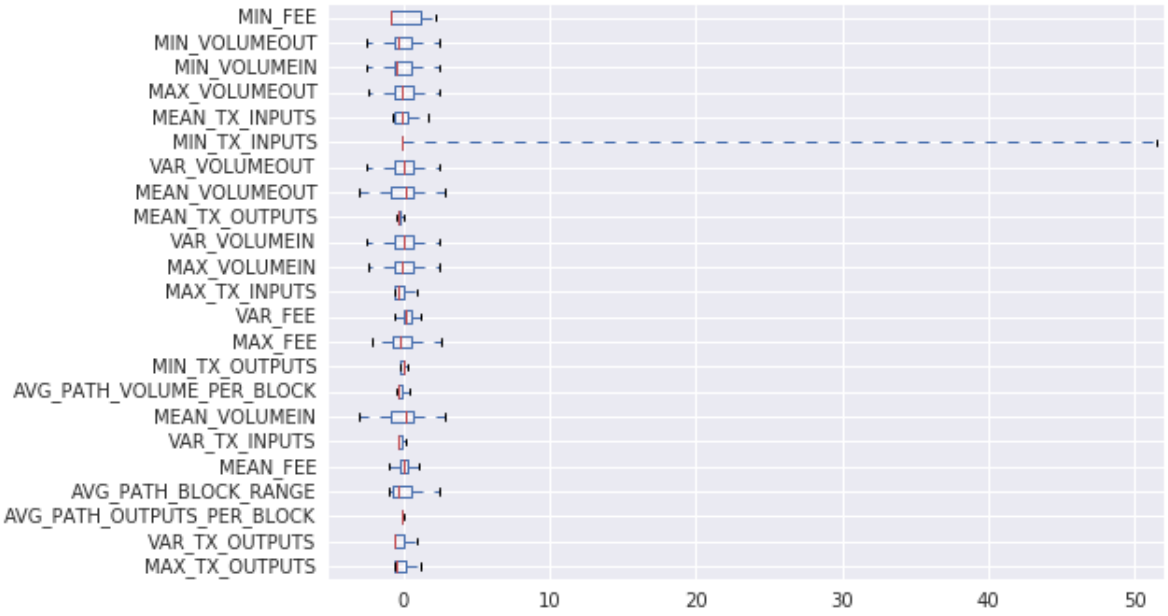


Figura 16 – *Boxplot* para cada uma das *features* normalizadas

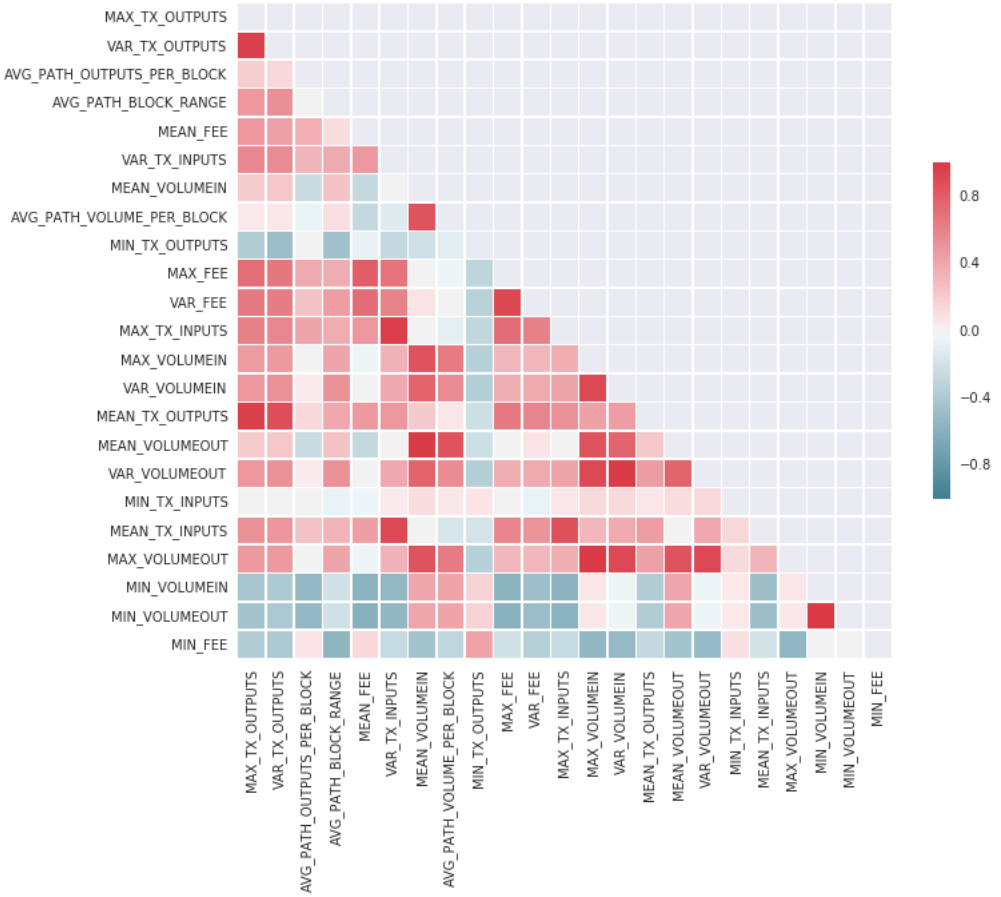


Figura 17 – Matriz de correlação entre as features do grafo de fluxos. A escala de cor representa o valor das correlações calculadas.

5.2 MODELO GAUSSIANO

Cada *feature* é considerada como normalmente distribuída. Dada a média μ_i e desvio-padrão σ_i associados à i-ésima *feature*, seja $f_i(x)$ a função de densidade de probabilidade desta *feature*. $f_i(x)$ é dada por:

$$f_i(x; \mu, \sigma) = \frac{1}{\sqrt{2\sigma^2\pi}} e^{-\frac{(x-\mu)}{2\sigma^2}} \tag{5.3}$$

Seja $x_{i,t}$ o valor da i-ésima *feature* na transação t. Seja r_t o *score* de anomalia associado à transação t. Assumimos que cada *feature* contribui de forma independente para o *score* final de anomalia da transação t, de forma que r_t é dado pelo produtório das funções de densidade de probabilidade (5.4),

$$r_t = \prod_{i=0}^{n} f_i(x_{i,t}) \tag{5.4}$$

Para ajustar os valores r_t no intervalo $[0.0, 1.0]$ aplicamos a seguinte transformação, de forma a obter s_t:

$$s_t = \frac{\left(1 - \sqrt[n]{r_t}\right) - 0.5}{0.5} \tag{5.5}$$

O histograma 18 mostra a distribuição dos *scores* de anomalia para cada grafo de fluxos de teste analisado.

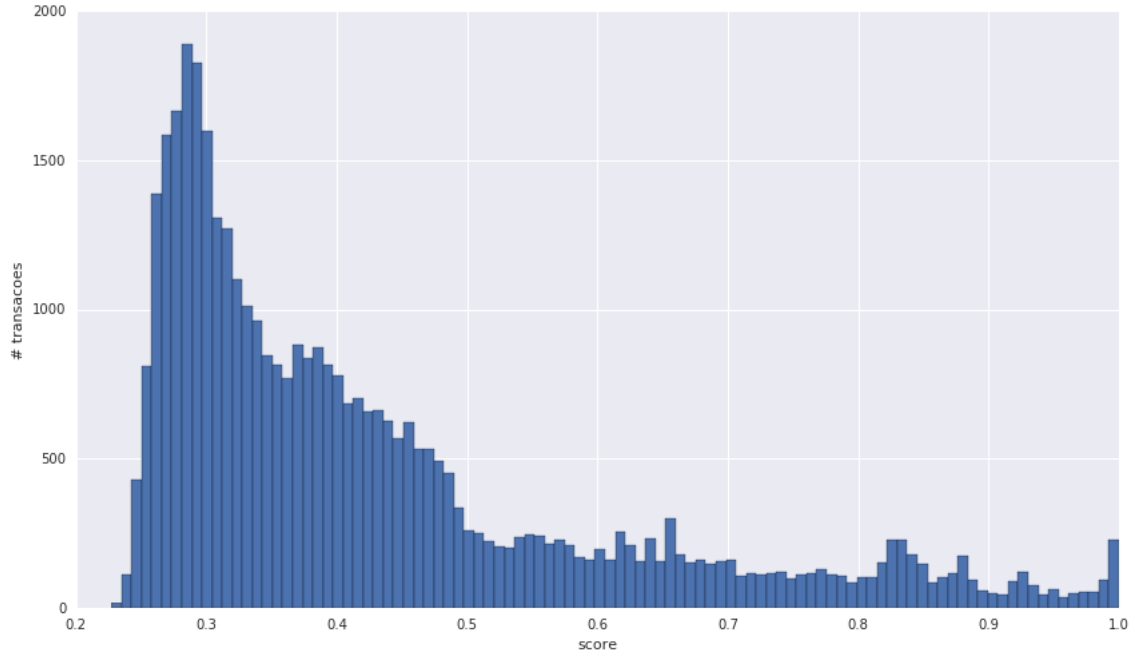


Figura 18 – Histograma dos scores de anomalia finais para o modelo univariado

O histograma 18 mostra que a maioria das entidades possuem *scores* de anomalia entre 0.2 e 0.5. Visualmente a distribuição dos *scores* sugere ser uma curva *long tail*.

5.3 MODELO DE MISTURA GAUSSIANA

O modelo de mistura gaussiana considera o *score* final de anomalia como uma composição de funções de probabilidade de cada *feature* no espaço n dimensional, onde n é a quantidade de *features*.

Em geral, o modelo de mistura gaussiana considera as correlações entre todas as *features*. Nesta seção, entretanto, nos atemos ao caso particular em que as *features* são consideradas independentes, e associamos um peso w_i à i-ésima *feature* para capturar a sua importância em relação às demais *features*.

Seja x o vetor de *features* da transação t. Dada a matriz de covariância Σ, vetor de pesos peso w e de médias μ de cada *feature* i, tem-se que o *score* de anomalia r_t para a transação t é dado por:

$$r_t = \sum_{i=1}^{n} w_i f_i(x_i; \mu_i, \Sigma_i) \tag{5.6}$$

onde $f_i(x_i; \mu_i, \Sigma_i)$ é a função de densidade de probabilidade marginal da *feature* i, dada por (5.3).

O histograma da Figura 19 mostra a distribuição dos *scores* de anomalia para as transações de teste normalizados no intervalo $[0.0, 1.0]$

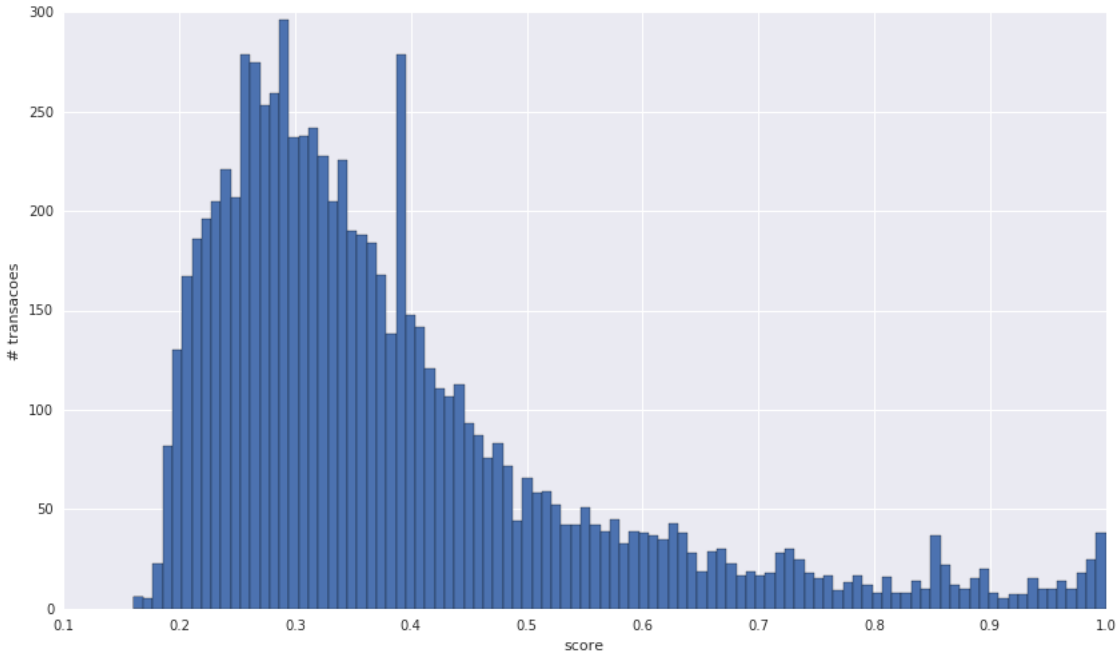


Figura 19 – Histograma dos scores de anomalia finais para o modelo multivariado

A maioria das transações obtiveram score entre 0.1 e 0.5, o que sugere que o limite the decisão do modelo seja superior a 0.5. O histograma da Figura 19, os *scores* do modelo gaussiano multivariado visualmente aparentam estar distribuídos conforme uma distribuição de calda longa.

5.4 CONCLUSÕES

Através dos modelos estatísticos gaussianos, foi possível treinar e verificar os *scores* de anomalias nas transações do *Bitcoin*, atráves da modelagem de seu grafo de fluxos e de forma não computacionalmente cara.

Seguindo as práticas adotadas em metodologias tradicionais de aprendizado de máquina, foram efetuadas transformações nas *features* de forma que elas se aproximassem de distribuições normais normalizadas, bem como remoção de informações que estão altamente correlacionados.

Visualmente, as distribuições dos *scores* sugerem ser regidos por distribuição estatística de cauda longa e adequadas para o cenário de detecção de anomalias. Neste cenário uma anomalia deve ser considerado uma exceção e não comum estatisticamente. Tanto para o modelo gaussiano univariado quanto para o multivariado, a maioria das transações obtiveram *scores* com no máximo 0.5 e portanto os limites de decisão de ambos modelos deveriam ter seus *thresholds* acima de 0.5.

6 DETECÇÃO DE ANOMALIAS NA REDE ETHEREUM

6.1 INTRODUÇÃO

Ethereum, assim como *Bitcoin*, é desenvolvido sob o princípio de descentralização e consenso global (WOOD, 2016). Desta forma, de maneira similar ao *Bitcoin*, o *Ethereum* adota o *blockchain* como a estrutura básica de dados onde todas as informações da rede são armazenadas, tais como transações e blocos.

No *Ethereum*, todos que participam da rede devem primeiramente sincronizar seus clientes com o *blockchain*, de forma que, localmente, todo o histórico e consenso global desde o bloco de gênese (bloco 0) estejam presentes antes de se efetuar qualquer transação.

A principal divergência entre *Bitcoin* e *Ethereum* é na camada adicional que este último adiciona ao primeiro. *Ethereum* por definição é uma plataforma descentralizada p2p, baseada no conceito de *blockchain*, para *smart contracts* ao invés de uma simples moeda.

Smart contracts são um dos conceitos fundamentais do *Ethereum*. Contratos inteligentes são códigos que podem ser encapsulados em transações para que tal código seja rodado e portanto efetivado na rede *Ethereum*. Um contrato pode conter chamadas para outros contratos e desta forma cada chamada é associada com um gasto em *ether* que é a unidade monetária do *Ethereum*.

Existem diversos usos do *Ethereum*:

- ***Tokens***: *tokens* são representações no *Ethereum* para qualquer bem virtual/digital. Contratos envolvendo tais bens podem ser criados e manipulados na estrutura *blockchain* do *Ethereum* (XIE, 2016). Assim não há necessidade de criar novos *blockchains* para novos *tokens*. *Tokens* têm muitas aplicações tais como implementação de novas moedas (vide seção 6.1.1 a seguir) ou estabelecimento de contratos envolvendo qualquer bem que possa ser representado neste ambiente (papéis de ações de uma empresa, ouro ou até mesmo outras entidades sem nenhum valor agregado).

- **Sistemas de identidade e reputação**: contratos podem desenvolver um papel de registro de nomes. O banco de dados está na própria arquitetura do *blockchain* e desta forma o contrato pode conter funções para gerenciar tal registro.

- **DAOs**: conceituamente uma organização descentralizada autônoma, do inglês *Decentralized Autonomous Organization* é uma entidade virtual com certos membros que possuem mais de 2/3 das ações e bens da organização e, portanto, possuem o poder de decisão sobre a entidade, tais como alocar e transferir os bens. O exemplo mais simples de DAO no *Ethereum* é um contrato que se auto modifica se pelo menos 2/3 dos membros concordam em uma eventual mudança do código.

6.1.1 Por que criar novas moedas virtuais?

O *Ethereum* serve, dentre outras finalidades, para se criar novas moedas virtuais. Enquanto que o *Bitcoin* é uma moeda virtual, o *Ethereum* é uma plataforma para a criação de tais moedas. Cabe então a pergunta: por que alguma instituição iria querer criar uma nova moeda virtual, se já temos o *Bitcoin*? Existem inúmeras respostas para tal pergunta. Dentre elas, destacamos o fato de que uma organização pode querer ter o controle sobre a geração de novos *tokens* (inflação) ou sobre outros aspectos da moeda. Na rede *Ethereum*, pode-se implementar tais funcionalidades, destacando-se que a criação de novas moedas virtuais é apenas uma dentre as várias aplicações que se pode executar sobre o *Ethereum*.

6.1.2 Estrutura deste capítulo

Particularmente, este trabalho é focado no problema de detecção de anomalias já definido no capítulo 5. Desta forma os dois métodos estatísticos para detecção de anomalias são usados nas transações e blocos do *Ethereum*, conforme tratado nas próximas seções.

A seção 6.2 define o problema de detecção de anomalias para o contexto abordado. Logo em seguida, a seção 6.3 descreve os dados utilizados para o problema proposto e a seção 6.4 aponta os resultados obtidos nos experimentos com os modelos de detecção de anomalias aplicados aos blocos e transações do *Ethereum*.

6.2 DETECÇÃO DE ANOMALIAS

Uma anomalia se refere à possibilidade de uma transação ou bloco fazerem parte de uma série de ataques já reportados na literatura, alguns dos quais descritos à seguir. Desta forma, para cada transação e bloco é atribuído um índice(*score*) entre 0 e

1 conforme o quão anômala tal entidade se apresenta dadas as *features* modeladas e o modelo treinado.

Em (BOK, 2016a; BOK, 2016b) foram reportados uma série de ataques na rede *Ethereum*, como por exemplo ataques DoS com criação de contas vazias que são fundamentalmente executadas por transações que invocam contratos maliciosos.

Os ataques tratados em (BOK, 2016a; BOK, 2016b) são os seguintes:

- **DoS**: conforme analisado em (FORUM, 2016) foi possível discriminar transações relacionados com ataques DoS onde os contratos maliciosos *0xd6a64D7...* e *0x0c40cF6...* estavam presentes. Tais contratos têm recebido atenção devido ao seu caráter disruptivo: eles podem gerar um atraso de até uma hora na mineração desde o começo do ataque.
- **Corrupção de memória**: o contrato *0xb284e6a...* contém código que levou clientes *Ethereum* à corrupção de memória.
- **Criação massiva de contratos SUICIDE e CREATE**: o atacante envia transações de baixo custo com contratos que criam pelo menos milhões de contas vazias com apenas códigos **SUICIDE** ou **CREATE**. O contrato *0x6a0a0fc...* criou contas vazias SUICIDE, enquanto o contrato *0x7c20218...* criou contas vazias CREATE.

6.3 DADOS UTILIZADOS

Os dados para os experimentos foram extraídos diretamente do *blockchain* do *Ethereum* e contém informações sobre transações e blocos que foram confirmados. Os dados foram coletados por um *crawler* que requisitava informações de um cliente *Ethereum* local através da API JSON-RPC. Todos os dados coletados foram armazenados no cluster onde os experimentos foram feitos.

A cada transação e a cada bloco é associado um vetor de *features*. Cada *feature* é entendida como uma medida de um determinado aspecto da entidade em questão. As *features* podem ser classificadas em atômicas e inerentes à um dado bloco ou transação ou agregadas, como por exemplo, a quantidade de transações por bloco.

Para transações são usadas as seguintes *features*:

- **taxa (*fee*)**: valor colocado na transação por quem a gerou (cliente) a fim de recompensar o minerador.
- **valor da transação**: valor em *Ether* referente a quantidade monetária a ser transferida.
- **combustível (*gas*)**: valor colocado na transação como crédito para rodar o código presente na transação. Quem gerou a transação deve provisionar o valor do combustível.
- **combustível usado (*used gas*)**: a quantidade de combustível usada para rodar o contrato inteligente (código).
- **preço do combustível**: valor unitário do gás em *Ether* no momento em que a transação foi criada.

Para cada bloco as *features* usadas são:

- quantidade de transações dentro do bloco onde quantidade de combustível oferecido é igual a quantidade de combustível usado
- quantidade de transações dentro do bloco
- soma dos valores das transações dentro do bloco
- média dos valores das transações dentro do bloco
- soma de *gas* usado nas transações dentro do bloco
- média de *gas* usado nas transações dentro do bloco
- soma de *gas* nas transações dentro do bloco
- média de *gas* nas transações dentro do bloco
- média do preço do *gas* estipulados nas transações dentro do bloco
- preço máximo do *gas* nas transações dentro do bloco
- preço mínimo do *gas* nas transações dentro do bloco
- soma das taxas das transações dentro do bloco
- média das taxas das transações dentro do bloco

- fator de espalhamento (*spread factor*): proporção de endereços destinatários diferentes das transações dentro do bloco
- fator de concentração (*join factor*): proporção de endereços iguais que criaram diferentes transações dentro do bloco

Foram construídos os conjuntos de treino, de validação e de teste para transações e blocos. Cada modelo de detecção de anomalias foi treinado considerando o conjunto de treino. Em seguida fizemos o ajuste dos parâmetros do modelo usando o conjunto de validação e por último o modelo foi testado com os dados de teste a fim de simular dados nunca vistos antes.

Tanto a validação como teste consideram a curva ROC onde é possível visualizar precisão versus revocação para o algoritmo de detecção de anomalias. Estes dois critérios são utilizados para decidir o melhor compromisso entre prever corretamente com o custo de alguns falsos positivos.

6.4 METODOLOGIA E EXPERIMENTOS

A criação do modelo de detecção de anomalias envolve as duas variações do modelo gaussiano como tratado no capítulo 5 (univariado e multivariado). O primeiro passo consiste em treinar os modelos, para em seguida validá-los para seleção dos melhores parâmetros de decisão de anomalia. Para treinar os modelos, primeiro são extraídas as *features* desejadas para todas as transações e blocos que estavam presentes no momento dos experimentos.[1] Todas as transações e blocos foram divididos em dois grupos:

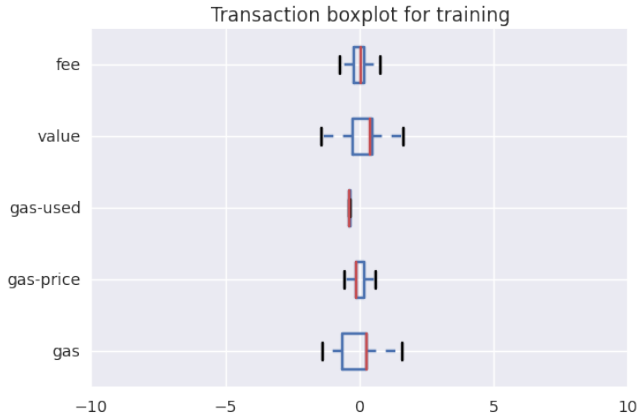
- Transações maliciosas e blocos com transações maliciosas: todas as transações que contém algum dos contratos reportados nos ataques são consideradas como maliciosas. Consequentemente todos os blocos que continham pelo menos uma transação considerada maliciosa foram automaticamente considerados como maliciosos.
- Transações não maliciosas e blocos sem transações maliciosas: todas as transação não consideradas maliciosas e consequentemente todos os blocos que não estão no conjunto daqueles maliciosos.

Os dados foram particionados em 2 conjuntos:

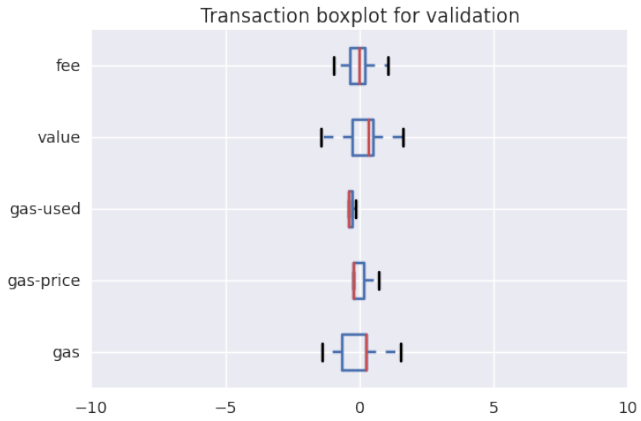
[1] no momento do experimento, em 11/2016, o banco de dados continha 3 milhões de blocos desde o bloco de gênese 0

- **Treino**: tanto para blocos como para transações são considerados 6000 exemplos não maliciosos selecionados de maneira uniforme aleatória.
- **Validação/teste**: contém 2000 transações ou blocos não maliciosos e 10 transações ou blocos maliciosos

Foram aplicadas, assim como no capítulo 5, transformações nas *features* de forma que elas se aproximassem de distribuições normais. Cada *feature* foi transformada usando a função logaritmo na base 10, em seguida deslocada com o valor de 100.0 e normalizada com sua média e desvio padrão. Desta forma temos cada *feature* seguindo distribuições normais com média 0 e desvio-padrão de 1. As Figuras 20 e 21 mostram os *boxplots* respectivamente para as transações e blocos utilizados nos experimentos.

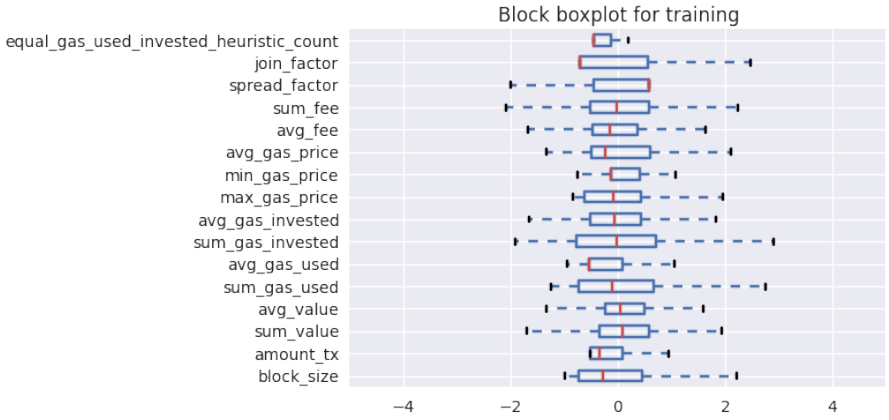


(a) Boxplot das features das transações utilizadas no conjunto de treino

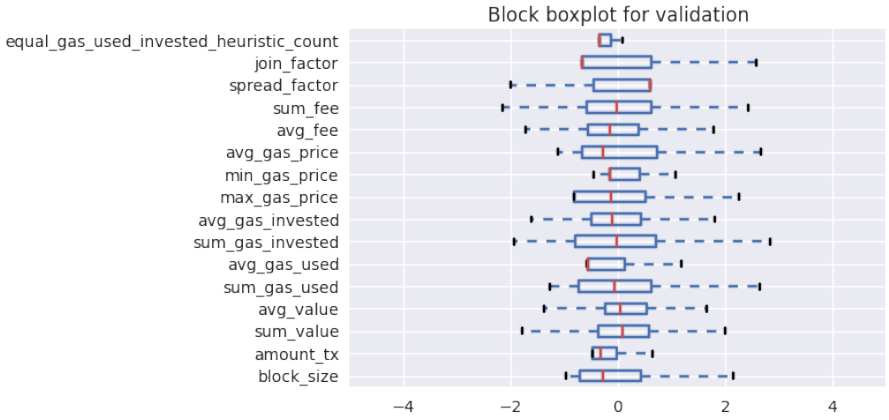


(b) Boxplot das features das transações utilizadas no conjunto de validação

Figura 20 – Boxplot das *features* para as transações de cada conjunto de dados utilizado



(a) Boxplot das features dos blocos utilizadas no conjunto de treino



(b) Boxplot das features dos blocos utilizadas no conjunto de validação

Figura 21 – Boxplot das *features* para os blocos de cada conjunto de dados utilizado

A fim de eliminar informações redundantes as *features* foram pareadas e então eliminamos uma *feature* de cada par cuja correlação fosse maior do que 0.99 ou menor do que -0.99. As Figuras 22 e 23 ilustram as matrizes de correlações das features para os blocos e transações consideradas nos dados de treino dos modelos gaussianos. Não foi eliminada nenhuma *feature* dos blocos. Já para as transações foram eliminadas:

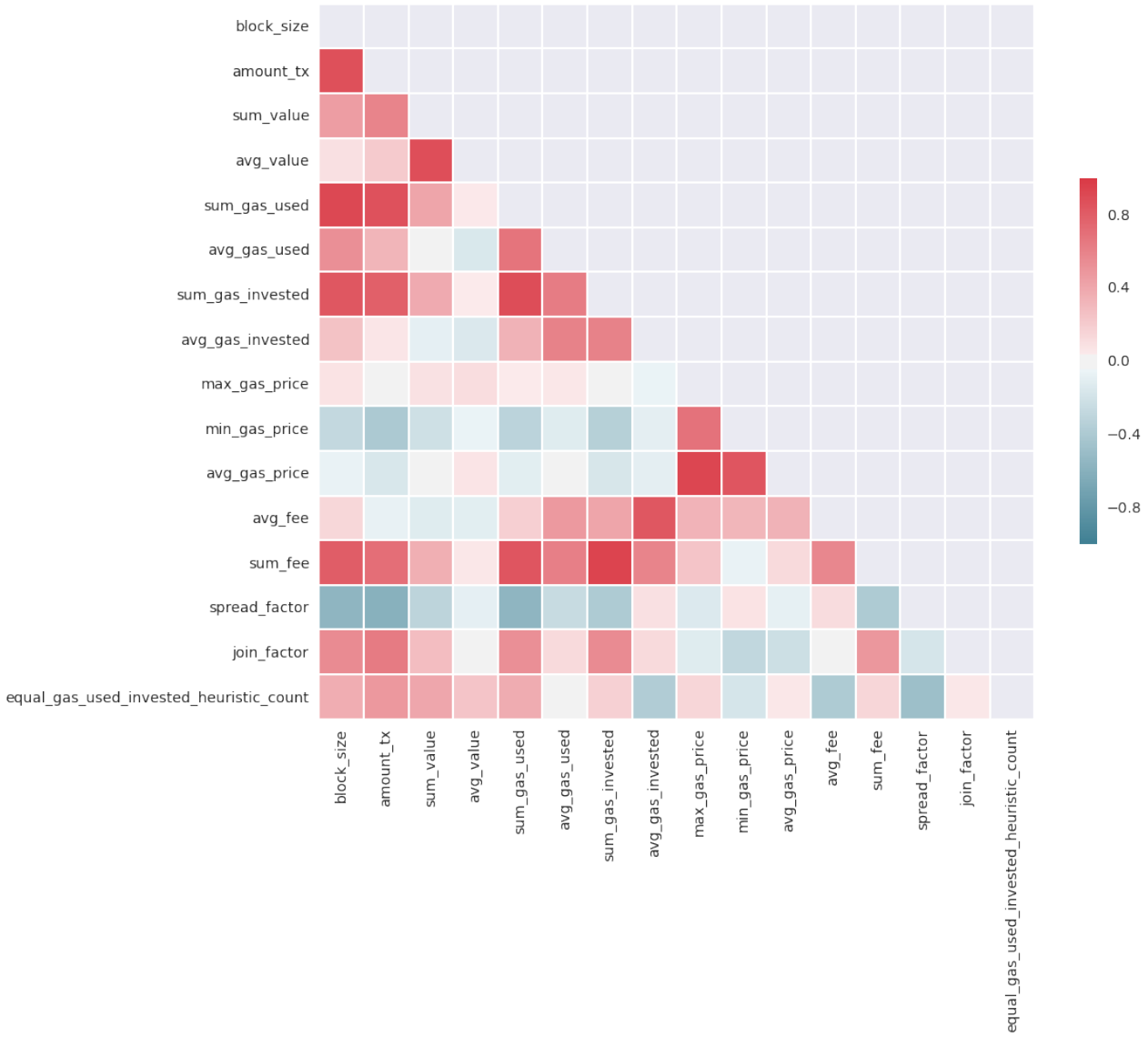


Figura 22 – Matriz de correlação entre as *features* para blocos

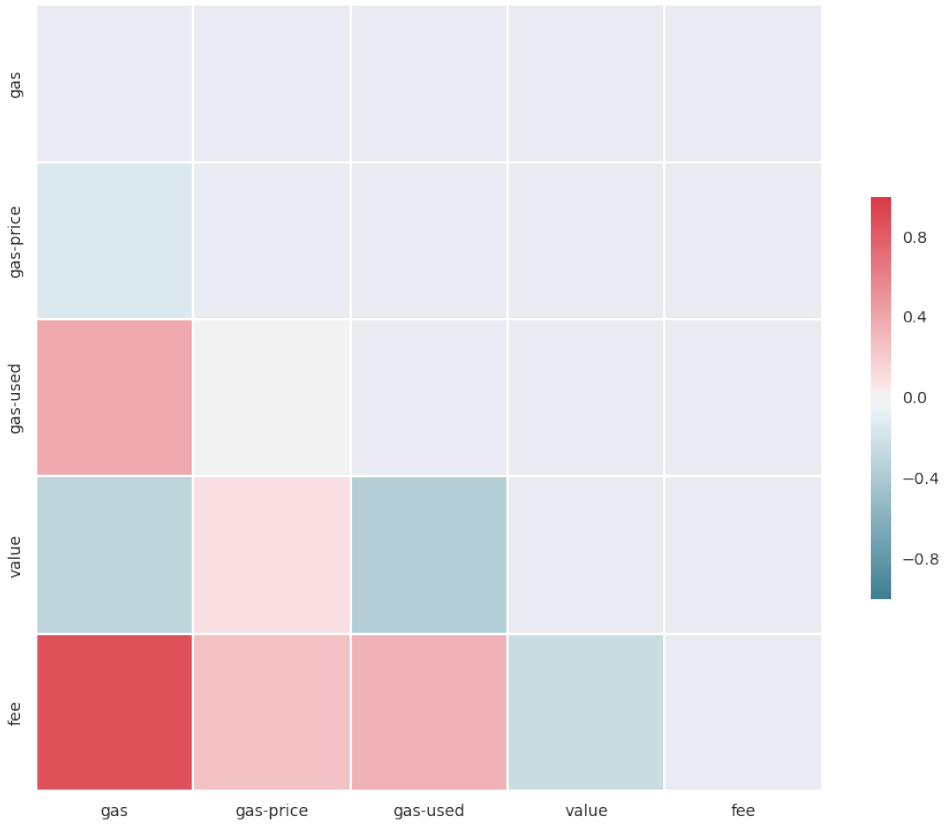


Figura 23 – Matriz de correlação entre as *features* para transações

- a soma das *taxas* pois estava altamente correlacionada com a soma de combustível no bloco (0.9978)
- média do preço do combustível no bloco pois estava com alto valor positivo de correlação com o valor máximo de combustível no bloco(0.9940)
- soma de combustível usado no bloco pois continha alta correlação positiva com o tamanho do bloco (0.9951)

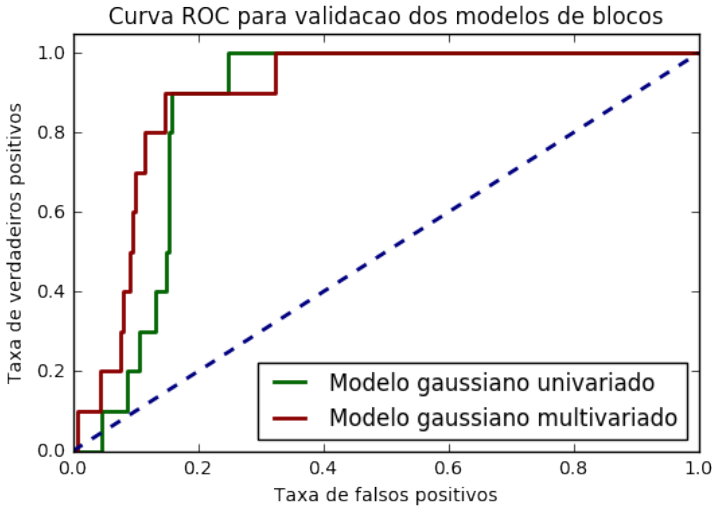
Neste trabalho usamos as curvas ROC no processo de validação. A curva ROC (curva de operação do receptor, do inglês *receiver operating characteristic*), ilustra o comportamento de um classificador binário, em termos do quanto ele consegue detectar uma determinada classe face aos falsos alarmes para um determinado *threshold* de decisão. Portanto a curva ROC mostra a taxa de verdadeiros positivos contra a taxa de falsos positivos variando-se o *threshold* de decisão do classificador. Outra função das curvas ROC é avaliar visualmente classificadores de forma que aquele classificador cuja curva

apresenta maior área tende a ter menos falsos alarmes para o mesmo nível de detecção ou descoberta (verdadeiros positivos).[2]

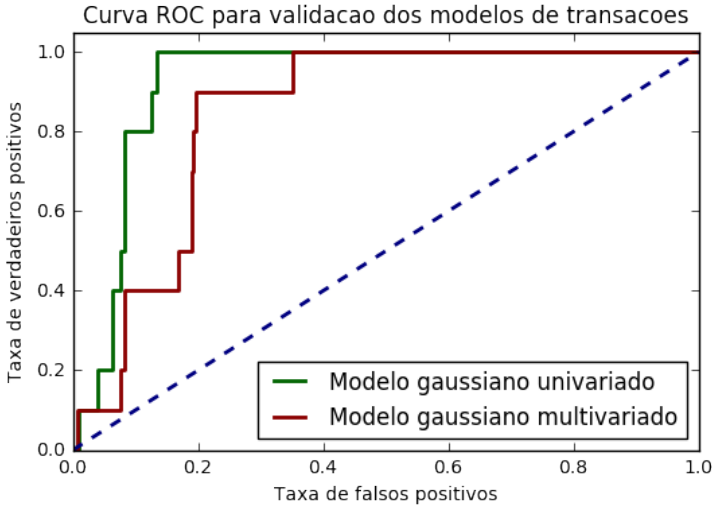
No contexto do presente trabalho, as curvas ROC mostram os níveis de acerto na classificação se a transação ou bloco é entendido como anômalo com o compromisso de errar algumas entidades ao classificá-las como anômalas ou não. O *threshold* de decisão neste âmbito é o valor da probabilidade da transação ou bloco ser anômalo. O modelo selecionado no passo de validação é aquele que apresenta a maior área da curva ROC.

Desta forma as curvas ROC apresentadas em 24 mostra visualmente como é a variação do nível de detecção com o custo de falsos positivos, variando-se o *threshold* de decisão dos modelos.

[2] De forma alternativa, em (VENKATAKRISHNAN; FANTI; VISWANATH, 2017) os autores utlizaram a curva PR (precisão *versus* revocação) para avaliarem os seus modelos.



(a) Curva ROC para blocos do conjunto de validação



(b) Curva ROC para transações do conjunto de validação

Figura 24 – Curva ROC para os dados de validação

As seguintes decisões foram aplicadas considerando a validação dos modelos através do critério das curvas ROC:

- para transações, o modelo gaussiano univariado apresentou maior área sob a curva ROC (0.93, contra 0.89 do gaussiano multivariado). Portando o modelo gaussiano univariado é o escolhido em detrimento do multivariado para detecção de anomalias em transações.
- para blocos, o modelo gaussiano multivariado apresentou maior área sob a curva ROC (0.94, contra 0.87 do gaussiano univariado). Portando o modelo gaussiano

multivariado é o escolhido em detrimento do univariado para detecção de anomalias em blocos.

6.5 CONCLUSÕES

O presente capítulo explorou os dados do *Ethereum* sob a ótica de detecção de anomalias, dados certos ataques relacionados com comportamentos maliciosos.

Tais modelos são simples de serem implementados e são úteis para automaticamente detectar blocos e transações que podem estar relacionados com os ataques reportados, expressando assim um comportamento anômalo.

Baseado nas métricas de recuperação de informação precisão e revocação, chegou-se a seguinte conclusão para a escolha do melhor modelo para cada contexto:

- para transações, o melhor modelo para caracterizar as *features* é modelo gaussiano univariado. Para transações, o modelo gaussiano univariado foi capaz de produzir o compromisso precisão-revocação de 100% e 13% com o *threshold* de decisão de 0.5879. Consistentemente, ele foi capaz de manter tais níveis para o conjunto de teste.
- para blocos, o melhor modelo para caracterizar as *features* é o gaussiano multivariado. Para blocos, o modelo gaussiano multivariado obteve o compromisso precisão-revocação de 100% dos blocos maliciosos recuperados com o custo de quase 9% de falsos positivos para o *threshold* de decisão no valor de 0.5866.

7 CONCLUSÃO

Neste trabalho apresentamos medições, modelos e algoritmos para caracterizar transações na rede *Bitcoin*. Nossas medições indicaram que algumas transações na rede *Bitcoin* levam até 30 minutos para serem confirmadas. Este alto tempo de espera nos motivou ao desenvolvimento de mecanismos de predição para confirmação de transações.

Primeiramente, adotamos uma abordagem empírica, e fizemos o *fitting* de várias distribuições de probabilidades à diferentes *features* associadas à rede *Bitcoin*. Em seguida, utilizando um modelo de filas, capturamos como diferentes fatores influenciam no tempo de confirmação das transações.

A fim de prever a confirmação de uma transação, foi adotada a rede neural sem pesos *WiSARD*. Ela foi capaz de acertar em torno de 60% das transações que não foram facilmente detectadas como confirmadas ou não confirmadas via uma árvore de decisão.

Finalmente, o trabalho contribui com a aplicação de dois modelos estatísticos e que usam misturas de gaussianas. Tais modelos visam detectar o quão anômala é uma transação em relação a aquelas mais recentes. Aplicando a mesma metodologia para transações e blocos das redes *Bitcoin* e *Ethereum*, identificamos os modelos gaussiano univariado e gaussiano multivariado como adequados para caracterizar *scores* de anomalias de transações e blocos.

Como continuação do trabalho é de importância para o âmbito investigativo analisar se as transações consideradas anômalas podem ser considerados casos de comportamento maliciosos, tais como roubos e lavagem de dinheiro. Devem ser consideradas outras informações como aquelas relacionadas a cada uma das partes relacionadas nas transações, tais como tipos de entidades associada a cada um dos endereços envolvidos nas transações. Vislumbramos também que os resultados apresentados neste trabalho sirvam como precursores para análises de risco visando, por exemplo, a identificação de esquemas fraudulentos.

REFERÊNCIAS

ALEKSANDER, I. et al. A brief introduction to weightless neural systems. ***ESANN***, p. 299–305, 2009.

ANDROULAKI, E. et al. ***Evaluating user privacy in Bitcoin***. [S.l.]: Springer, 2013.

BISHOP, C. M. ***Pattern recognition and machine learning***. [S.l.]: Springer, 2006.

BITCOINTALK. ***Can someone explain the high-fee spam attack now?*** 2016. <https://bitcointalk.org/index.php?topic=1382996.0>. [Online, acessado 24 de junho 2017].

BITCOINWIKI. ***Transaction Fees***. 2015. <https://en.bitcoin.it/wiki/Transaction_fees>. [Online, acessado 24 de junho 2017].

BOK. ***Ethereum Network Attacker's IP Address Is Traceable***. 2016. <https://www.bokconsulting.com.au/blog/ethereum-network-attackers-ip-address-is-traceable/>. [Online; acessado 10 de agosto 2017].

BOK. ***The DAO Hacker's Booty Is On The Move***. 2016. <https://www.bokconsulting.com.au/blog/the-dao-hackers-booty-is-on-the-move/>. [Online; acessado 10 de agosto 2017].

BONNEAU, J. ***How long does it take for a Bitcoin transaction to be confirmed?*** 2015. <https://coincenter.org/entry/how-long-does-it-take-for-a-bitcoin-transaction-to-be-confirmed>. [Online, acessado 24 de junho 2017].

BUNTIX, J. ***It appears another spam attack is taking place on the bitcoin network***. 2017. <http://www.newsbtc.com/2017/03/20/appears-another-spam-attack-taking-place-bitcoin-network>. [Online; acessado 24 de junho 2017].

CARVALHO, D. S. et al. B-bleaching agile overtraining avoidance in the wisard weightless neural classifier. ***ESANN***, 2013.

FERRIN, D. ***A Preliminary Field Guide for Bitcoin Transaction Patterns***. 2013. <http://diyhpl.us/~bryan/papers2/bitcoin/Apreliminaryfieldguideforbitcointransactionpatterns.pdf>. [Online; acessado 10 de agosto 2017].

FORUM. ***Some blockchain analysis of the current DOS***. 2016. <https://www.reddit.com/r/ethereum/comments/544y1p/some_blockchain_analysis_of_the_current_dos/>. [Online; acessado 10 de agosto 2017].

GOODMAN, N. Statistical analysis based on a certain multivariate complex gaussian distribution (an introduction). ***The Annals of mathematical statistics***, JSTOR, v. 34, n. 1, p. 152–177, 1963.

KERBER, R. Chimerge discretization of numeric attributes. ***Proceedings of the tenth national conference on Artificial intelligence***, p. 123–128, 1992.

KHAC, N. A. L. et al. An investigation into data mining approaches for anti money laundering. ***Proceedings of International Conference on Computer Engineering and Applications (ICCEA 2009)***, v. 2, 2011.

LIU, H.; SETIONO, R. Chi2 feature selection and discretization of numeric attributes. ***ICTAI***, p. 388–391, 1995.

LUO, X. Suspicious transaction detection for anti-money laundering. ***International Journal of Security and Its Applications***, v. 8, n. 2, p. 157– 166, 2014.

MEIKLEJOHN, S. et al. A fistful of bitcoins: characterizing payments among men with no names. *In: IMC'13*, 2013.

MÖSER, M.; BÖHME, R. Trends, tips, tolls a longitudinal study of bitcoin transaction fees. ***International Conference on Financial Cryptography and Data Security***, p. 19–33, 2015.

MÖSER, M.; BÖHME, R.; BREUKER, D. An inquiry into money laundering tools in the bitcoin ecosystem. ***eCrime Researchers Summit (eCRS), 2013***, p. 1–14, 2013.

MÖSER, M.; BÖHME, R.; BREUKER, D. Towards risk scoring of bitcoin transactions. ***International Conference on Financial Cryptography and Data Security***, p. 16–32, 2014.

MOUGAYAR, W. ***Understanding the blockchain***. 2016. <https://www.oreilly.com/ideas/understanding-the-blockchain>. [Online, acessado 20 de outubro de 2017].

NAKAMOTO, S. ***Bitcoin A peer-to-peer electronic cash system***. 2008. <https://bitcoin.org/bitcoin.pdf>. [Online; acessado 10 de agosto 2017].

NARAYANAN, A. et al. ***Bitcoin and Cryptocurrency Technologies***. 2015. <https://class.coursera.org/bitcointech-001/wiki/readings>. [Online, acessado 24 de junho 2017].

PEREZ, Y. B. ***Bitnet Launches 'Instant Approval' Tool for Bitcoin Merchants***. 2014. <http://www.coindesk.com/bitnet-launches-instant-approval-tool-for-bitcoin-merchants/>. [Online, acessado 24 de junho 2017].

REID, F.; HARRIGAN, M. ***An analysis of anonymity in the Bitcoin system***. [S.l.]: Springer, 2013.

RICCI, S. et al. Dinâmica das transações do bitcoin: uma abordagem quantitativa. *In: Workshop em Desempenho de Sistemas Computacionais e de Comunicação*, 2016.

RON, D.; SHAMIR, A. Quantitative analysis of the full bitcoin transaction graph. *In: Sadeghi AR. (eds) Financial Cryptography and Data Security*, v. 7859, 2013.

VENKATAKRISHNAN, S. B.; FANTI, G.; VISWANATH, P. Dandelion: Redesigning the bitcoin network for anonymity. *In: Proceedings of the ACM on Measurement and Analysis of Computing Systems*, **ACM**, v. 1, n. 1, p. 22, 2017.

WOOD, G. ***Ethereum: A secure decentralised generalised transaction ledger***. 2016. <https://bravenewcoin.com/assets/Whitepapers/Ethereum-A-Secure-Decentralised-Generalised-Transaction-Ledger-Yellow-Paper.pdf>. [Online; acessado 10 de agosto 2017].

XIE, L. ***A beginner's guide to Ethereum tokens***. 2016. <https://blog.coinbase.com/a-beginners-guide-to-ethereum-tokens-fbd5611fe30b>. [Online; acessado 10 de agosto 2017].