Dinâmica das transações do Bitcoin: uma abordagem quantitativa

Saulo Ricci[1,2], Alex Borges[3], Helder Luiz[4], Daniel S. Menasché[1], Eduardo Ferreira[1]

[1]Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, RJ – Brasil

[2]Skry, Palo Alto CA, USA

[3]Universidade Federal de Juiz de Fora (UFJF), Juiz de Fora, MG – Brasil

[4]Instituto Federal do Norte de Minas Gerais (IFNMG), Teófilo Otoni, MG – Brasil

Resumo. *Apesar do crescente interesse em cripto moedas, tanto indústria quanto a academia sentem falta de análises quantitativas desses sistemas. Neste trabalho, caracterizamos o Bitcoin, um dos mais populares sistemas de cripto moedas, sob a ótica quantitativa. Visamos métricas importantes relacionadas a transações, como a probabilidade uma transação ser confirmada e o tempo decorrido para essa confirmação. Nossos resultados mostram que há um número não negligenciável de transações que não são confirmadas 24 horas após serem postadas na rede. Nesse caso, nós observamos uma alta correlação entre a taxa de uma transação, seu volume e a suspeita de que a transação não será confirmada. O trabalho 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. Finalmente, nós provemos uma análise de nível de atividade simples, comparando um período importante na existência do sistema do Bitcoin –o fechamento do Silk Road– e um período subsequente. Em resumo, concluimos que a rede Bitcoin se apresenta resiliente e não é dependente de hubs altamente centralizados.*

Abstract. *Despite the growing interest in cryptocurrencies, both industry and academia lack on quantitative analysis of such systems. In this work, we have characterized the cryptocurrency system Bitcoin under a quantitative perspective. We have addressed important transaction metrics, such as the transaction confirmation probability and the time to confirmation, and found a non-negligible number of transactions that are not confirmed 24 hours after being issued. We also observed a high correlation between the transaction fee, value and probability of confirmation. Bitcoin transactions usually are confirmed in short periods, but still much larger than conventional credit card systems. Finally, we have provided a simple analysis of activity level on a specific period of Bitcoin life –the ending of Silk Road– and contrasted it against subsequent periods. In summary, our preliminary results indicate that the Bitcoin network is resilient and do not depend on main hubs.*

1. Introdução

Nos útimos anos o interesse por moedas virtuas tem aumentado e atraído a atenção de diversos setores da sociedade. Espeficamente, o Bitcoin atualmente se destaca como

solução *de facto* para comércio digital que envolve cripto moedas. Estima-se que milhares de dólares circulem diariamente na rede. Ainda assim, alguns elementos fundamentais do Bitcoin ainda não são plenamente compreendidos. Portanto, uma caracterização das propriedades das suas transações, levando em conta aspectos temporais, torna-se necessária.

Neste trabalho 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. Nossos 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 trabalho, 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?
2. qual a distribuição do tempo de confirmação das transações que são confirmadas?
3. o quão robusta é a rede Bitcoin com relação a remoção de nós da rede e/ou ataques que visem quebra de anonimidade?

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, nossas contribuições, com relação às perguntas anteriores são:

1. verificamos que várias das transações inválidas possuem propriedades que permitem prever, com alto grau de acurácia, que de fato tais transações não serão confirmadas;
2. caracterizamos a distribuição do tempo de confirmação das transações válidas, e parametrizamos distribuições clássicas a fim de que se possa utilizar nossas caracterizações de forma simples e conveniente em trabalhos futuros;
3. identificamos que a rede Bitcoin é robusta com relação a remoção de nós previamente considerados como centrais; mas que certas transações no Bitcoin não seguem os padrões recomendados pelo protocolo oficial, e apontamos potenciais formas de se explorar assimetrias na rede a fim de quebrar anonimidade de transações.

O trabalho segue com a definição de conceitos-chave na seção 2. Os *datasets* coletados para análise são descritos na seção 3. Na seção 4 são apresentados caracterizações de alguns aspectos orgânicos das transações, enquanto na seção 5 são abordados os aspectos que refletem o estado e dinâmica como um todo da rede do Bitcoin. É mostrado um caso específico sobre a robustez da rede na seção 6. Os trabalhos relacionados são levantados na seção 7 enquanto a seção 8 fecha o trabalho com a conclusão e oportunidades futuras de pesquisa nesta linha.

2. Fundamentos

Nesta seção são abordados os principais conceitos para o entendimento do Bitcoin [Narayanan et al. 2016]. Em particular, focamos nos conceitos relevantes para a compreensão do restante do artigo.

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.

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.

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]. O tempo para confirmação de transações e validação de blocos será discutido nas seções 4 e 5 deste trabalho.

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 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 minerados 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 5, prioridades afetam de forma significativa o tempo de confirmação

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

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*).

3. Dados Utilizados

Nesta seção, descrevemos os três *datasets* utilizados neste trabalho.

O primeiro conjunto de dados, usado na seção 4, 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[2] 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 5, 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, temos 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*.

O terceiro conjunto de dados, usado na seção 6, é proveniente de informações retiradas do *blockchain*. Foram avaliados os meses de outubro, novembro e dezembro de 2013, fevereiro de 2014, além de todos os meses de novembro do sistema Bitcoin, desde seu início de funcionamento. Após a extração dos dados, realizamos a modelagem das informações deste *dataset* em um banco de dados relacional, tal qual apresentado por [Spagnuolo 2013]

4. Prevendo Confirmações

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 de nossos monitores.

É de valia um modelo que faça previsão para confirmação de transações conforme elas são geradas. 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.

[2]No trabalho uma transação é considerada como não confirmada se não houve sua efetivação no *blockchain* em até 24 horas

Para construção do modelo de previsão, é necessária a caracterização prévia de aspectos que podem ser agrupados dentre aqueles orgânicos e inerentes à própria transação bem como aqueles referentes aos estado e dinâmica de todo o sistema de nós e mineradores. Assim, nesta seção concentramos nos fatores orgânicos 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 1 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, uma vez que as transações podem ser confirmadas em no máximo 30 minutos.

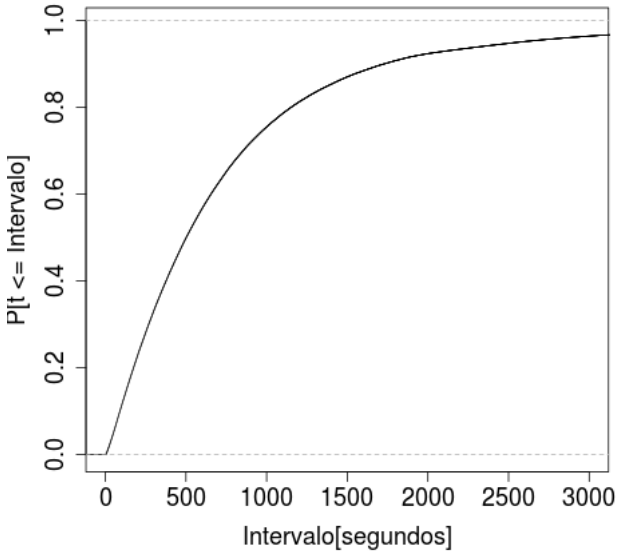


Figura 1. CDF do tempo de confirmação para as transações confirmadas

Por outro lado, no grupo de transações não confirmadas houve casos em que uma transação 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. 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 2016]). 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] A precisão do tempo de confirmação está atrelada à cobertura dos monitores que estão espalhado por todos os continentes. Assim temos uma visão da rede.

5. 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 propomos um modelo que relaciona tais aspectos com o tempo de confirmação das transações.

A linha de tempo na Figura 2 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 bloco B_j e a confirmação do bloco B_{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.

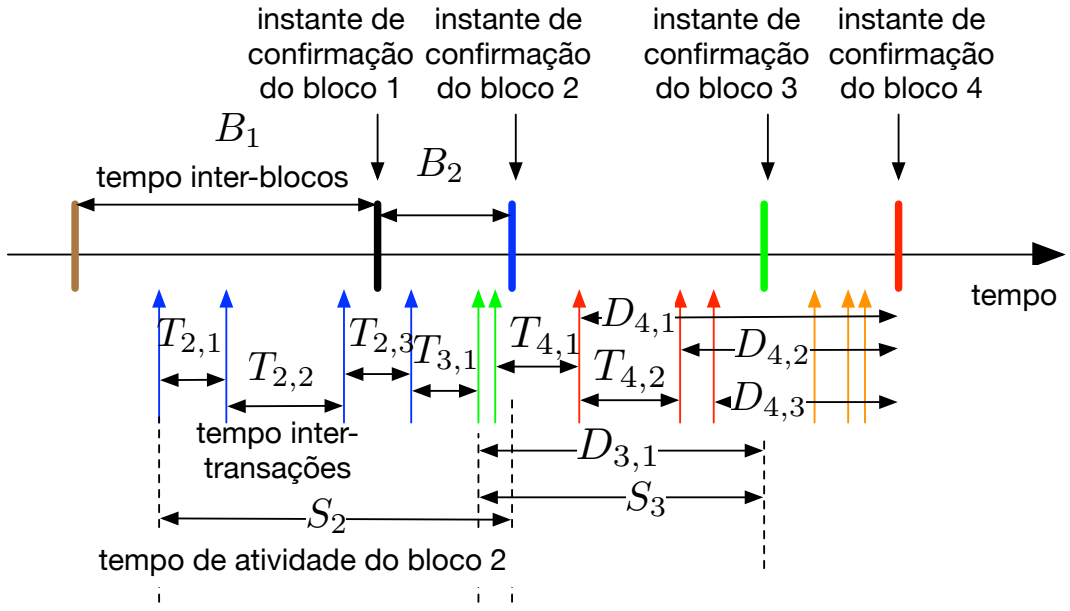
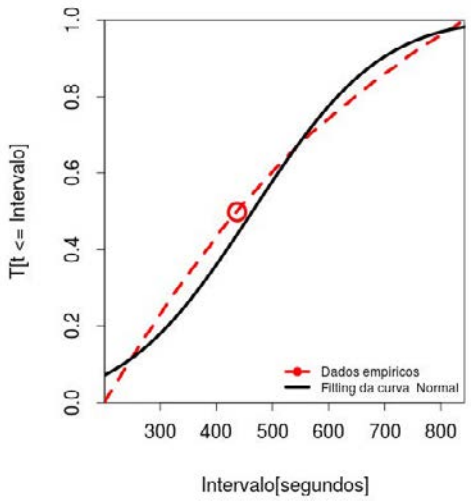


Figura 2. Caracterizaçao do tempo de confirmação.

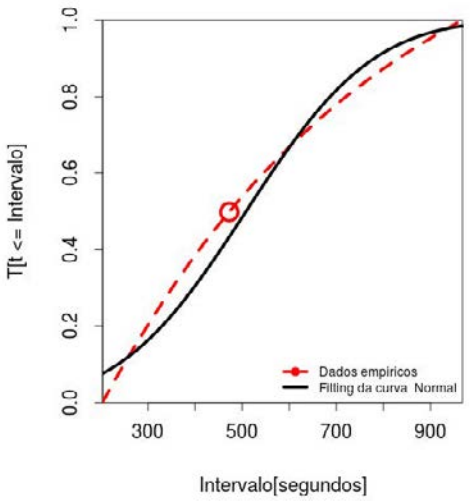
A fim de minimizar o efeito de ruídos gerados pelas ferramentas de coleta de dados executadas por nossos monitores, realizamos uma filtragem dos dados da série temporal de tempo entre transações, e consideramos apenas valores que estão entre o primeiro e terceiro quartis da distribuição. Após feita esta 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 3(a). Seja B a variável

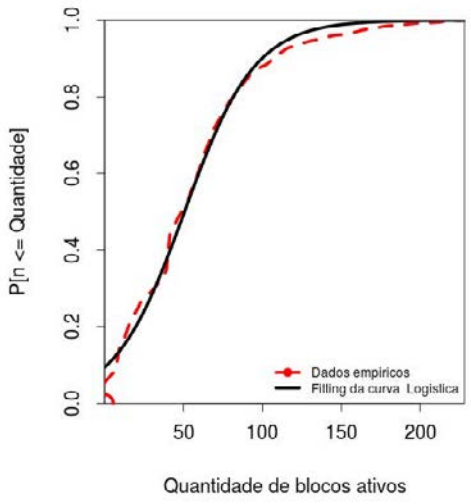
aleatória que caracteriza o tempo entre confirmação de blocos. A melhor distribuição que descreve o intervalo entre confirmação de blocos é a normal com parâmetros $E(B) = 464.30$ segundos e $V(B) = 179.57$. Desta forma temos um coeficiente de variação de 0.029. Em média os blocos gastam quase 8 minutos 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).



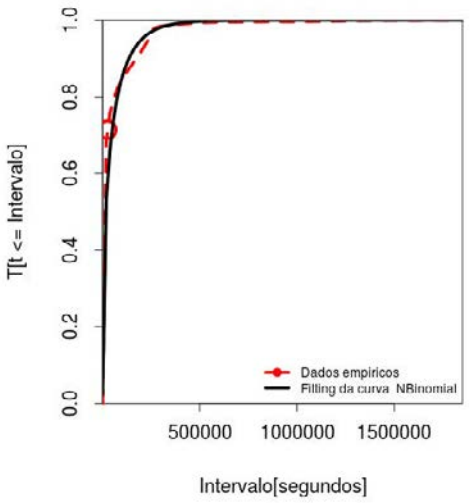
(a) Fitting da CDF do tempo entre blocos, B



(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 3. Fittings de métricas para a dinâmica de confirmação e tempos relacionados com transações e blocos

Já a CDF representada na Figura 3(b) 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. Percebemos 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,

$$E(B_r) = E(B^2)/(2E(B)) \tag{1}$$

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,

$$E(D) = \alpha E(B) + E(B_r) \tag{2}$$

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,

$$E(D) = 0.6(E(B) + E(B_r)) + 0.4E(B_r) \tag{3}$$

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.

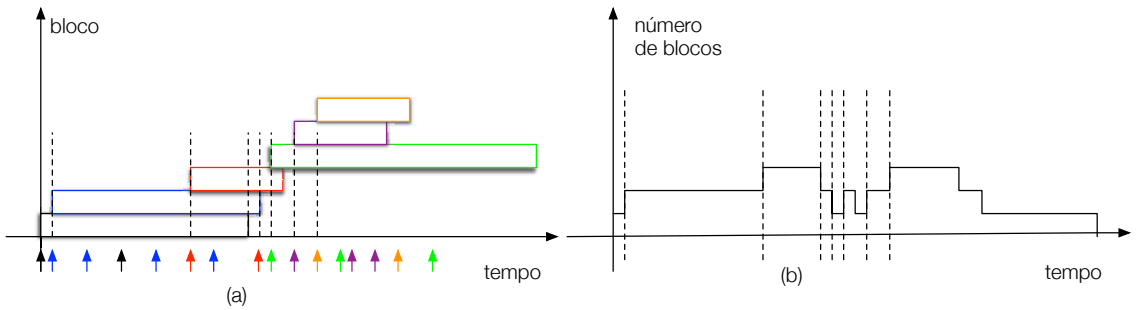


Figura 4. Blocos ativos: (a) cada barra inicia quando ocorre a primeira transação associada ao bloco, e termina quando o bloco é confirmado; (b) número de blocos ativos em função do tempo. A área embaixo desta curva divida pelo tempo produz o número médio de blocos ativos.

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 4 divida pelo tempo de observação.

A figura 3(c) 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 3(d) 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 3(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. Trabalho futuro consiste em melhor compreender a causa de tal disparidade.

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.

6. Robustez da Rede

Nesta seção, avaliamos o quanto que a rede Bitcoin é sensível a remoção de nós tidos como centrais, e estudamos alguns aspectos estruturais da rede.

6.1. Remoção de Nós

Em outubro e novembro de 2013 o FBI fechou o site denominado *Silk Road*. Este site da *DeepWeb* ficou amplamente conhecido por realizar vendas de produtos e serviços ilegais através da rede Bitcoin. A fim de capturar possíveis alterações no sistema Bitcoin decorrentes do fechamento, foram analisados os dados referentes à atividade da rede, durante e após o fechamento do *Silk Road*. É possível notar que a quantidade de transações após o fechamento do site praticamente se mantém, conforme as estatísticas sobre a atividade na rede reportadas na tabela 1. Estas estatísticas reforçam a hipótese de que há grande diversidade nas transações do Bitcoin, de forma que aquelas relacionadas com mercado negro correspondem apenas a uma pequena parcela de todas as transações na rede.

Mês	Transações	Mês	Transações	Mês	Transações
Outubro	1,645,153	Novembro	1,959,041	Dezembro	1,941,525

Tabela 1. Número de transações antes e após o fechamento do *Silk Road* (2013).

Além da aparente manutenção da atividade da rede Bitcoin, nota-se que não há sazonalidade desta atividade, como pode ser conferido na figura 5, referente aos dias entre os meses de outubro e dezembro de 2013.

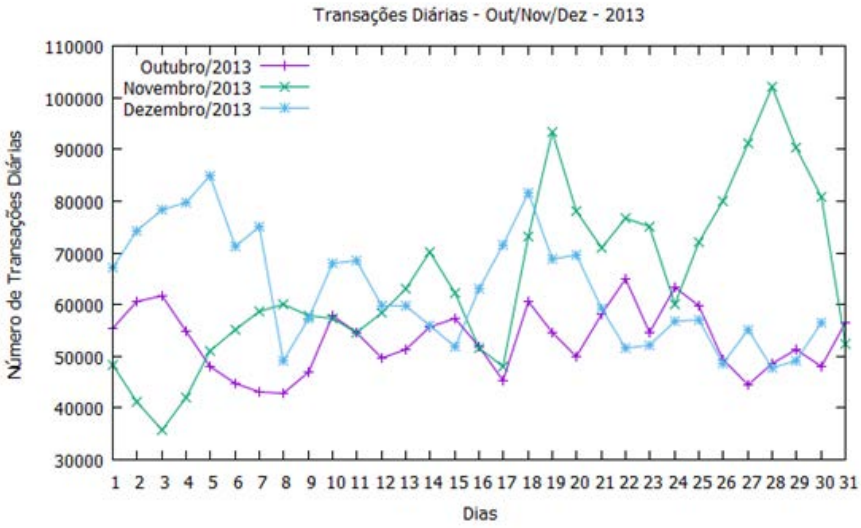


Figura 5. Diárias: outubro, novembro e dezembro de 2013

6.2. Transações de Grau Um e Transações de Grau Zero

Cada transação na rede Bitcoin está associada a um grau de entrada (número de transações que alimentam a transação em questão) e a um grau de saída (número de transações que recebem recursos da transação em questão, incluindo a transação referente ao troco). Uma análise das transações envolvendo graus altos é realizada em [Luiz 2016]. A seguir, em contrapartida, estudamos transações de baixo grau – ou seja, de grau 0 e grau 1. Em novembro de 2013 e fevereiro de 2014, contamos com 999,427 e 1,048,575 transações, respectivamente, e verificamos que existiu uma grande quantidade de transações com grau um e uma pequena parcela de transações com grau zero. Em janeiro e fevereiro, o número de transações de grau zero foi de 1,480 e 1,862, respectivamente. O número de transações de grau um foi de 123,875 e 82,092, respectivamente.

Apesar das transações de grau zero não serem recomendadas pelo protocolo padrão do Bitcoin, elas podem ser usadas para diferentes fins tais como a divulgação de chaves públicas. Entretanto, vislumbra-se que tais transações também possam ser usadas em ataques do tipo negação de serviço (“denial of service”), e por isso elas são desencorajadas. É interessante observar que o caráter descentralizado do protocolo Bitcoin admite que mesmo operações desencorajadas (e proibidas de acordo com o cliente padrão), acabem ocorrendo no *blockchain*.

Muitas das transações no Bitcoin envolvem o pagamento de uma certa quantia e um troco para o pagador. Por este motivo, elas possuem grau de saída maior ou igual

a dois. Entretanto, algumas transações possuem grau de saída igual a um. A maioria das transações de grau de saída igual a um configuram transações geradas pelo protocolo como recompensa por mineração. Estas transações, que possuem grau de entrada zero e grau de saída um, são denominadas de *coinbase*, e cada bloco possui ao menos uma transação deste tipo. Dentre os trabalhos futuros, pretendemos caracterizar todas as transações que possuem grau de saída igual a um (independente do seu grau de entrada), e buscar entender o seu papel na rede de transações.

7. Trabalhos Relacionados

O trabalho que originou o Bitcoin foi publicado na Internet em 2008 para que todos tivessem acesso a idealização do funcionamento do sistema [Nakamoto 2008]. O autor, com pseudonimo Satoshi Nakamoto, nunca foi identificado. Uma das principais contribuições do trabalho seminal consiste no uso do *proof of work* para evitar o problema do gasto duplo.

[Androulaki et al. 2013] e [Reid and 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.

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 and 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.

8. Conclusão

Neste trabalho, nós apresentamos uma caracterização acerca das transações do Bitcoin, o sistema de cripto moeda mais popular até o presente. Nós conduzimos nosso estudo

a partir dos dados públicos, disponíveis na rede a todos os clientes Bitcoin, bem como dados colhidos ao longo de um ano por centenas de monitores instrumentados executando na rede Bitcoin em diversos pontos do mundo.

Além de métricas importantes relacionadas com transações, como a probabilidade uma transação ser realmente confirmada e o tempo decorrido para essa confirmação, nós provemos uma análise temporal simples, comparando um período referente ao fechamento do Silk Road com períodos subsequentes.

Nossos resultados mostram que há um número não negligenciável de transações que não são confirmadas. Nesse caso, nós observamos uma alta correlação entre o *fee*, seu volume e a suspeita de que a transação não será confirmada. Mais ainda, transações do Bitcoin geralmente são confirmadas em períodos curtos, mas ainda assim, muito acima de tempos usuais de sistemas convencionais de cartão de crédito. Em mais de 90% dos casos, uma transação foi confirmada em até 30 minutos. Em resumo, nós acreditamos que a rede Bitcoin é resiliente e não é dependente de *hubs* altamente centralizados, e que o presente trabalho abre novas avenidas em direção ao melhor entendimento de características básicas do sistema, ao propor um modelo baseado em teoria de filas para inferir o tempo médio de confirmação das transações.

Referências

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

Bitcointalk (2016). Bitcoin talk forum. `https://bitcointalk.org/index.php?topic=1382996.0`.

Bitcoinwiki (2016). Transaction fees. `https://en.bitcoin.it/wiki/Transaction_fees`.

Luiz, H. (2016). Estudo da dinamicidade do sistema bitcoin. Master's thesis, UFJF, Juiz de Fora.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names.

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

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. `https://class.coursera.org/bitcointech-001/wiki/readings`.

Reid, F. and Harrigan, M. (2013). *An analysis of anonymity in the Bitcoin system*. Springer.

Ron, D. and Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph.

Spagnuolo, M. (2013). Bitiodine: extracting intelligence from the bitcoin network. *Politecnico di Milano*.