Caracterização da Rede Bitcoin: Uma Visão sobre a Evolução de Blocos, Transações, Endereços e Saldos de 2009 até 2017

Cristiano M. Silva[1], **Bruna V. Ramos**[1], **Sérgio de Oliveira**[1], **Rogério Piccoli**[2]

[1]Departamento de Tecnologia – Universidade Federal de São João Del-Rei – Brasil

[2]Departamento de Sociologia – Universidade Federal de São João Del-Rei – Brasil

cristiano@ufsj.edu.br, brunavilarino21@gmail.com,

{sergiool, rogerpicoli}@ufsj.edu.br

Abstract. *Bitcoin is the most popular crypto-currency nowadays. It runs on a decentralized P2P network. The Bitcoin operation is accomplished by means of a distributed ledger. The notoriety of this network motivates the development of this work. Here, we investigate the evolution of the network in terms of blocks, transactions, addresses, and balances. More than 500 thousand data blocks are analyzed, corresponding to 1.54 billion transactions involving 368 million addresses worldwide. The results demonstrate that the volume of data stored in the blockchain is currently growing at the rate of 5GB monthly, with 10 million transactions being processed each month. The number of addresses created per month grows in quadratic proportion, although 74% of them have a life time of only one day. More than 85% of addresses carry out only two transactions, and 1.7% of addresses received 90% of the Bitcoins transacted throughout 2017.*

Resumo. *Bitcoin é a criptomoeda de maior popularidade na atualidade. Sua operação se dá a partir de uma rede P2P descentralizada que busca manter um livro razão de transações distribuído pela rede. A notoriedade dessa rede motiva o desenvolvimento desse trabalho, onde investiga-se a evolução da rede em termos de blocos, transações, endereços e saldos. São analisados mais de 500 mil blocos de dados correspondendo à 1,54 bilhões de transações que envolveram 368 milhões de endereços Bitcoin distribuídos pelo mundo. Os resultados demonstram que o volume de dados armazenado no blockchain cresce, atualmente, à taxa de 5GB ao mês, sendo processados 10 milhões de transações mensais. A quantidade de endereços criados por mês cresce em proporção quadrática, embora 74% deles tenha o tempo de vida de apenas um dia. Mais de 85% dos endereços realizam apenas duas transações e 1,7% dos endereços receberam 90% dos Bitcoins transacionados ao longo de 2017.*

1. Introdução

Bitcoin é a criptomoeda de maior popularidade na atualidade. Sua operação se dá numa rede P2P (par-a-par) descentralizada, composta por milhares de computadores, capaz de processar centenas de transações por minuto [Yermack, 2015]. No núcleo da rede está um mecanismo de consenso em que os pares concordam com a ordem das transações através de um processo chamado de ”prova de trabalho”, semelhante ao voto por maioria computacional. Embora todos os pares possam participar desse mecanismo de consenso,

essa atividade acabou tornando-se típica de mineradores com *hardwares* especializados, que buscam auferir lucro através das recompesas obtidas no processo de mineração.

De fato, a rede Bitcoin funciona com base na estruturação de uma sequência de registros de transações distribuídos na rede de usuários da moeda virtual; usuários que, em princípio, tem o anonimato de suas identidades assegurados pelo sistema. Os registros referem-se a transações realizadas entre os usuários da rede e são constantemente atualizados numa estrutura que espelha um livro razão distribuído (do inglês, *ledger*). A atualização de informações sobre as transações na rede contendo os novos registros de lançamentos, é feita por meio da adição de um novo bloco sequencial, contendo, dentro de si, o identificador do bloco imediatamente anterior; daí o termo *blockchain* (literalmente, corrente de blocos) [Narayanan et al., 2016].

Dada a importância que esta rede vem ganhando, e do fato da tecnologia *blockchain* ter potencial de servir a inúmeros tipos de contextos que envolvam transações, e não somente transações financeiras, esse trabalho apresenta uma caracterização da rede Bitcoin desde o início de sua operação em 03/01/2009. Foram coletados mais de 500 mil blocos de dados correspondendo à 1,54 bilhões de transações que envolvem mais de 368 milhões de endereços Bitcoin distribuídos pelo mundo.

As análises indicam que o volume de dados armazenado no *blockchain* cresce, atualmente, à taxa de 5GB ao mês, o que corresponde à 10 milhões de transações. A quantidade de endereços criados por mês cresce em proporção quadrática, embora 74% deles tenha o tempo de vida de apenas um dia. Apenas 0,6% dos endereços possui transações em intervalos maiores do que um ano. Pouco mais de 85% dos endereços realizam apenas duas transações e 1,7% dos endereços receberam 90% dos Bitcoins transacionados ao longo de 2017. Mais de 95% dos endereços possuem saldos inferiores à 1 Bitcoin. Finalmente, já foram movimentados mais de 4,4 bilhões de Bitcoins, sendo 932 milhões apenas no ano de 2017.

Esse artigo encontra-se organizado da seguinte forma: A seção 2 apresenta os trabalhos relacionados. A seção 3 apresenta a operação básica da rede Bitcoin. A seção 4 introduz a metodologia usada para a coleta e elaboração do estudo. A seção 5 caracteriza os blocos da rede Bitcoin. A seção 6 estuda o tempo de vida dos endereços. A seção 7 discute o volume de transações por endereço. A seção 8 apresenta a distribuição de saldos por endereço. A seção 9 volta sua atenção para as transações registradas na rede. Finalmente, a seção 10 conclui o trabalho.

2. Trabalhos Relacionados

A rede Bitcoin vêm sendo estudada sobre diversas perspectivas. Em termos de estudos de caracterização, Pappalardo et al. [2017] utilizam um cliente Bitcoin personalizado para monitorar a atividade da rede por 7 dias, conectando-se em mais de doze mil pares únicos para medir o tempo necessário para explorar os *hashes* de blocos válidos, sua variação e percentil. Os autores também investigam a dinâmica de transações e blocos. Ron and Shamir [2013] derivam propriedades estatísticas do grafo de transações entre os anos de 2009 até 2012, apresentando respostas para o comportamento típico dos usuários, como adquirem e gastam seus Bitcoins, e como esses Bitcoins são movimentados entre diversas contas. Os autores também isolam um conjunto de grandes transações e descobrem que elas possuem estreita relação entre si, provavelmente fruto de um usuário tentando

esconder uma grande carteira a partir de sua complexa divisão em uma cadeia de longas transações que acabam convergindo para uma carteira final do mesmo usuário.

Ricci et al. [2016] apresentam uma caracterização quantitativa da rede Bitcoin em termos de métricas operacionais, como a probabilidade uma transação ser confirmada e o tempo decorrido para essa confirmação. O trabalho mostra que transações Bitcoin geralmente são confirmadas em curtos períodos de tempo (30 minutos). Ainda assim, há uma quantidade significativa dessas transações que aguardam mais de 24 horas por confirmação. Os autores destacam a correlação entre a taxa de remuneração de uma transação e seu tempo de processamento.

Kondor et al. [2014] usam a lista de transações para reconstruir o tempo e o montante de cada pagamento. Eles analisam as transações medindo características da rede ao longo do tempo, como a distribuição de graus, correlações de graus e agrupamentos, bem como o fluxo de dinheiro. Já, Meiklejohn et al. [2013] observam a interessante característica de anonimato dos detentores de Bitcoins em contraste com o fluxo de moedas público e implementam heurísticas para realizar o agrupamento de carteiras baseando-se em evidências como padrões de compras, buscando caracterizar o mercado de Bitcoins e as tensões que estas mudanças podem gerar na rede.

Mineradores Bitcoin também são estudados na literatura. Wang and Liu [2015] estudam a evolução dos mineradores analisando a cadeia de transações. Caracterizam como a produtividade, o poder de computação e a atividade de transação dos mineradores evoluem ao longo do tempo. Os autores mostram como o poder de computação é distribuído entre os mineradores, além de construir um modelo econômico simples para explicar sua evolução.

Eyal and Sirer [2014] mostram que o protocolo de mineração Bitcoin possui pontos passíveis de melhoria quando se trata do mecanismo de incentivos. Os autores apresentam um tipo de ataque baseado em conluio em que os mineradores obtêm maiores lucros do que pares que atuam corretamente. Em termos gerais, mineradores egoístas retêm, estrategicamente, blocos para enganar o sistema de incentivo à mineração. Mineradores racionais preferem se juntar aos egoístas, e o grupo de conluio cresce em tamanho até se tornar maioria. Neste ponto, o Bitcoin deixa de ser uma moeda descentralizada.

Cabe notar que a mineração de Bitcoins é um processo aleatório com grande variação, fazendo com que mineradores interessados em rendimentos constantes participem de *pools* de mineração que dividem as recompensas obtidas entre seus membros. Nesse contexto, Lewenberg et al. [2015] estudam a dinâmica da mineração agrupada e as recompensas que os *pools* conseguem fornecer. Os autores também aplicam ferramentas teóricas cooperativas de jogos para analisar como os membros do *pool* podem compartilhar essas recompensas. Mostram que, para alguns parâmetros de rede, especialmente sob altas cargas de transação, é difícil, ou mesmo impossível, distribuir recompensas de forma estável: alguns participantes sempre são incentivados a alternar entre *pools*.

3. Rede Bitcoin

As criptomoedas (também chamadas de moedas virtuais ou digitais) buscam prover um meio de trocas que envolva apenas as duas partes interessadas (comprador e vendedor), retirando a instituição financeira da mediação da transação com a justificativa de que

isso torna o processo mais barato, inclusivo e seguro. O barateamento do serviço seria consequência do fim da intermediação de transações por instituições financeiras, e suas consequentes taxas de serviços. O caráter inclusivo surge do fato de que não há como saber a identidade da outra parte, garantida por um processo de anonimato e criptografia. Por fim, os defensores das criptomoedas argumentam que um sistema financeiro centralizado (como existe hoje) representa um risco a toda a sociedade. Um ataque à esse sistema pode desbalancear toda a economia de um país.

Com essa motivação, a rede Bitcoin foi apresentada no artigo [Nakamoto, 2008] publicado na *criptography mailing list* da `metzdowd.com`. Possivelmente, a contribuição mais interessante do artigo foi apresentar uma estratégia para prevenir o problema de gasto duplicado (do inglês, *double-spend*). O gasto duplicado ocorre quando um usuário usa a mesma unidade de moeda como pagamento em mais de uma transação. Ou seja, um usuário mal-intencionado pode realizar mais de uma compra ao mesmo tempo e pagá-las com a mesma moeda digital. Bitcoin resolve esse problema a partir da chamada cadeia de blocos. Um servidor de *timestamp* distribuído atribui carimbos de horários a blocos de transações. Cada carimbo inclui no bloco, também, o código *hash*[1] do bloco anterior. Dessa forma, o cálculo do *hash* do bloco atual é alterado pelo *hash* do bloco imediatamente anterior (predecessor). Assim, cada novo bloco solidifica os blocos anteriores, pois alterar uma transação de um bloco anterior demanda mudar o *hash* de todos os blocos após ele.

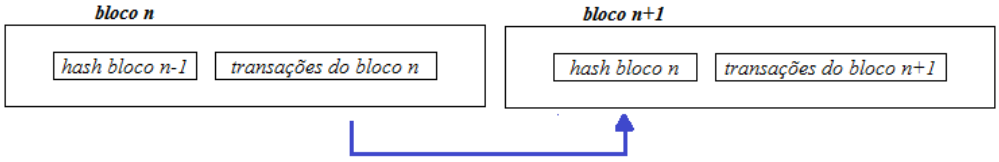


Figura 1. Figura apresenta o encadeamento de blocos no *blockchain*. Cada bloco contém dentro de si o *hash* do bloco anterior. Assim, o valor do *hash* do bloco atual é alterado pelo *hash* do bloco anterior.

Para implementar um servidor de *timestamp* distribuído num modelo P2P, Bitcoin usa um sistema de prova de trabalho (do inglês, *proof-of-work*) semelhante ao *Hashcash*[Back, 2002]. Essa prova consiste em encontrar um valor que inserido no campo *nonce* do bloco faz com que o *hash* do bloco inicie com uma dada quantidade de *bits* zero. O trabalho médio requerido é exponencial no número de *bits* zero necessários. Após encontrado um valor que satisfaça à prova de trabalho, o bloco não pode ser alterado sem se refazer o trabalho. À medida que blocos são acorrentados após ele, o trabalho para mudar uma transação incluiria refazer todos os blocos depois dele.

Na rede, novas transações são transmitidas para todos os nós. Cada nó recolhe novas transações para um bloco e trabalha para resolver sua prova de trabalho para o bloco de transações ainda não confirmadas. Quando um nó encontra uma prova de trabalho, ele transmite o bloco para todos os nós, que devem validar todas as transações, verificando se todas as transações não foram anteriormente gastas. Esses nós expressam a aceitação desse bloco trabalhando na criação do próximo bloco para o *blockchain* usando o *hash* do bloco recém descoberto. Os nós sempre consideram que a cadeia mais longa é a correta

[1] *hash* é o resultado de uma operação matemática sobre os *bytes* do bloco.

e continuam trabalhando para estendê-la. Se dois nós transmitem diferentes versões do próximo bloco simultaneamente, alguns nós podem receber um ou outro primeiro.

Nesse caso, eles trabalham no primeiro que recebem, mas salvam o outro ramo no caso desse se confirmar como ramo aceito. Isso só será descoberto quando a próxima prova de trabalho for encontrada e um ramo se provar como aceito; os nós que estavam trabalhando no outro ramo mudam para o mais longo. Por convenção, a primeira transação em um bloco é uma transação especial que inicia uma nova moeda de propriedade do criador do bloco. Isso é um mecanismo de incentivo para nós suportarem a rede, bem como distribuir moedas, uma vez que não há autoridade central para isso.

Cada transação pode envolver diversas entradas que direcionam a um conjunto de saídas. As entradas são especificadas pelo identificador das transações onde o comprador recebeu as moedas que pretende repassar. Já as saídas indicam os destinatários das moedas (vendedor). A rede não permite que se trabalhe com frações de uma transação. Assim, quando o valor das entradas ultrapassa o valor a ser repassado ao destinatário,pode-se incluir uma saída que redirecione o excedente para o endereço que está repassando os Bitcoins, simulando o fornecimento de troco. Por fim, é interessante ressaltar que a rede comporta 21 milhões de Bitcoins. A menor unidade monetária é chamada Satoshi, e corresponde à 1.0×10^{-8} Bitcoins (ou seja, 1 Bitcoin equivale à 100 milhões de Satoshis).

4. Metodologia

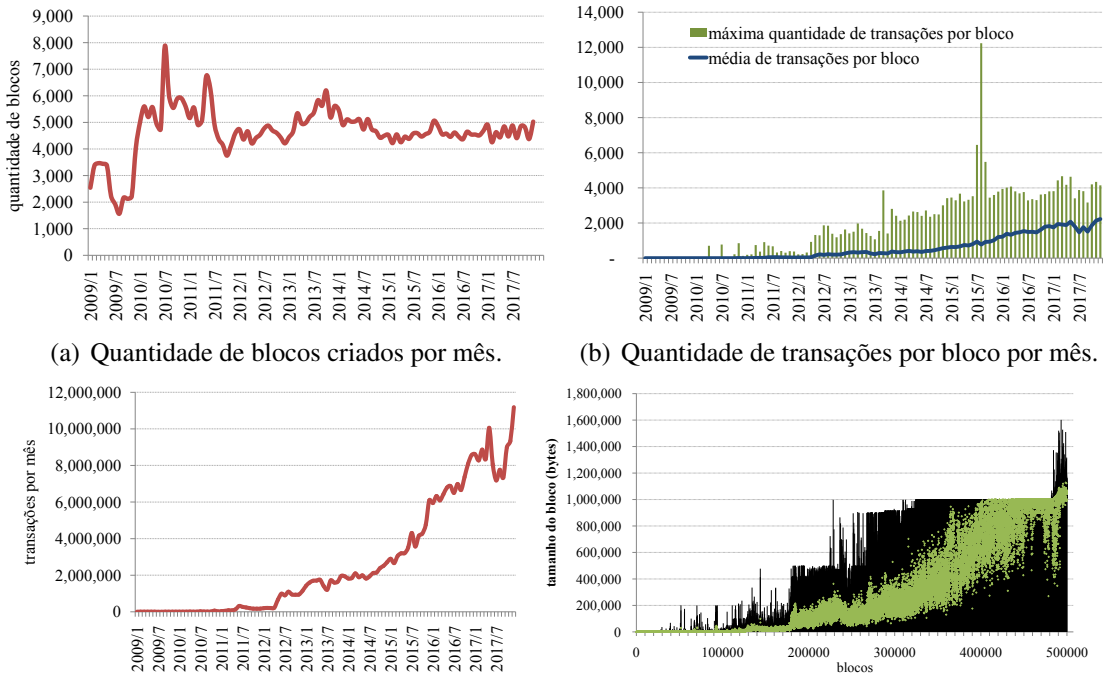
Esse estudo de caracterização baseia-se em 500 mil blocos de transações coletados no site `https://blockchain.info/`, correspondendo à todo o período de Jan/2009 até meados de Jan/2018. O site disponibiliza uma API para desenvolvedores Bitcoin, através da qual pode-se obter o conjunto de blocos. O processamento dos dados foi realizado por uma série de programas desenvolvidos pela equipe de pesquisa. Os experimentos são planejados para oferecer uma visão generalista sobre a evolução da rede ao longo dos anos, buscando sumarizar os principais aspectos relativos à disseminação da moeda virtual, seu padrão de uso e distribuição de riqueza.

5. Blocos de Transações

Na rede Bitcoin, as transações são agrupadas em blocos, gerando-se a chamada corrente de blocos ou *blockchain*. Aqui, caracteriza-se os blocos gerados na rede ao longo dos anos de 2009 até 2017. Pela figura 2(a), percebe-se que foram criados (aproximadamente), 2,5 mil blocos em Jan/2009, enquanto que, atualmente, são gerados em torno de 5 mil blocos por mês, o que representa uma variação pequena quando compara-se a quantidade de usuários naquela época com a atual.

De fato, a quantidade de blocos é apenas uma dimensão de análise (blocos são meros agrupamentos lógicos de transações). A figura 2(b) apresenta a quantidade de transações armazenadas em cada bloco ao longo desse período. Enquanto que, no início da rede, blocos eram gerados com umas poucas unidades de transações, agora comportam mais de 2 mil transações, não raramente ultrapassando 4 mil. Para complementar esse estudo, a figura 2(c) apresenta a evolução da quantidade de transações processadas por mês pela rede, dando a dimensão adequada do crescimento de sua utilização.

Enquanto que, no seu primeiro mês de operação, a rede processou pouco mais de 2 mil transações, em Dez/2017 ela processa mais de 10 milhões. O aumento da quantidade



(a) Quantidade de blocos criados por mês.

(b) Quantidade de transações por bloco por mês.

(c) Quantidade de transações por mês.

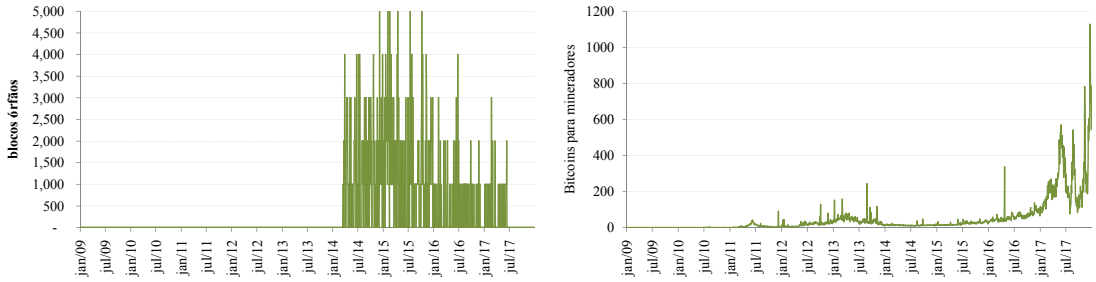
(d) Evolução do tamanho dos blocos (bytes).

Figura 2. A figura (a) indica a quantidade de blocos minerados por mês. A figura (b) indica a quantidade de transações nos blocos. A figura (c) apresenta a quantidade de transações por mês. A figura (d) indica a evolução do tamanho dos blocos (bytes).

de transações armazenadas por bloco tem implicações diretas no crescimento do tamanho dos novos blocos. A figura 2(d) apresenta a evolução do tamanho dos blocos. Os pontos em cor verde indicam o tamanho médio dos blocos (esses pontos podem não estar visíveis numa impressão em preto e branco), enquanto que os pontos em cor negra indicam o tamanho dos maiores blocos encontrados. Pode-se perceber que o tamanho dos blocos já ultrapassa 1MB. Como são gerados em torno de 5 mil blocos por mês, pode-se inferir que o *blockchain* cresce em torno de 5GB mensais.

É interessante notar que a corrida dos mineradores por gerar novos blocos faz com que o tamanho dos blocos cresça na forma de degraus. Esse comportamento resulta do mecanismo de aceitação de novos blocos. Quando dois ou mais blocos são minerados ao mesmo tempo, o bloco de maior tamanho acaba sendo escolhido pela rede, e a remuneração pela montagem do bloco vai apenas para o minerador responsável pelo bloco selecionado. Com isso, os mineradores acabam tendo que gerar blocos de tamanho competitivo para obterem a remuneração. Por outro lado, não podem gerar blocos muito grandes, sob pena de não completarem a tarefa em tempo hábil.

Conforme observado por alguns autores, a mineração Bitcoin pode incorrer em efeitos negativos para o sistema. Um desses efeitos é destacado na figura 3(a), que apresenta a quantidade de transações órfãs obtida a partir de série de dados disponibilizada no sítio Web `https://blockchain.info/` (transações ainda não incorporadas à *blockchain*). Tal comportamento gera insegurança, pois não há um controle ativo por parte da rede para que essas transações sejam validadas e incorporadas. Naturalmente, essa é



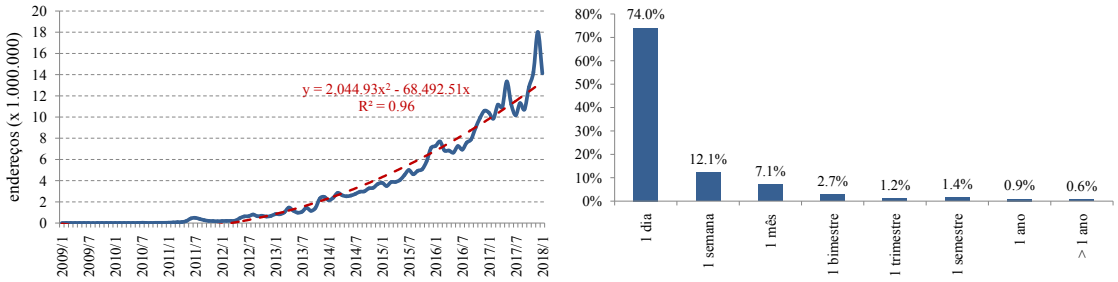
(a) Blocos órfãos. (b) Receita de mineradores.

Figura 3. Caracterização do processo de mineração. A figura (a) apresenta a quantidade de blocos órfãos (ainda não anexados ao *blockchain*. A figura (b) apresenta o total pago aos mineradores. Figuras geradas a partir da série de dados disponível no sítio Web https://blockchain.info/.

uma questão que pode ser endereçada a partir de uma pequena modificação no mecanismo de incentivos para privilegiar transações mais antigas. Basta aumentar a remuneração por bloco minerado que privilegia transações antigas. Já a figura 3(b), também gerada a partir de série de dados baixada do sítio `https://blockchain.info/`, apresenta a remuneração paga aos mineradores que, em Dez/2017, ultrapassa 1 mil Bitcoins.

6. Tempo de Vida dos Endereços Bitcoin

Foram encontrados mais de 368 milhões de endereços Bitcoin (368,584,449). A figura 4(a) apresenta o momento em cada endereço foi visto pela primeira vez em uma transação. A curva azul indica a quantidade de endereços (x 1 milhão), enquanto que a curva vermelha apresenta a linha de tendência que segue um padrão polinomial de segunda ordem (novos blocos surgem em proporção quadrática). O último ponto (Jan/2018) apresenta uma queda pois a coleta de dados terminou na primeira quinzena.



(a) Quantidade de endereços criados por mês. (b) Tempo de vida dos endereços.

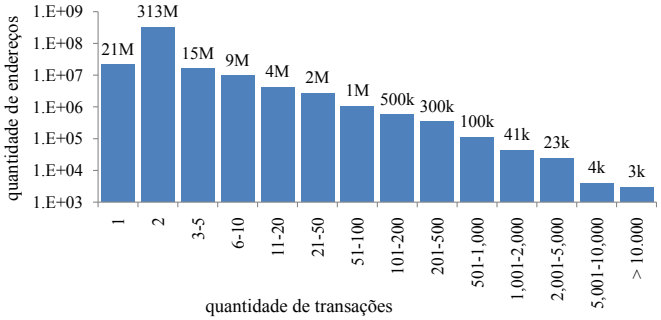
Figura 4. Caracterização de endereços Bitcoin. A figura (a) indica a quantidade de novos endereços vistos em transações por mês. O eixo x indica o mês, e o eixo y indica a quantidade de milhões de endereços criados. A figura (b) indica o tempo de vida dos endereços em termos percentuais.

A figura 4(b) analisa o tempo de vida dos endereços usando como base o intervalo entre a primeira e a última transação registrada. Mais de 74% dos endereços tiveram tempo de vida igual a um dia (todas as transações realizadas pelo endereço concentram-se no mesmo dia). Apenas 0,6% dos endereços possuem intervalo entre transações maior do que um ano. As razões desse comportamento podem estar relacionadas à troca constante

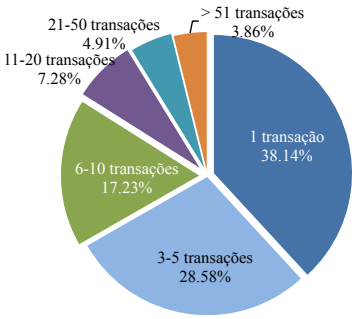
de endereços por parte dos usuários para reduzir riscos de segurança, bem como o comportamento especulativo de compra de Bitcoins aguardando por sua valorização futura.

7. Quantidade de Transações por Endereço

A figura 5(a) apresenta a distribuição de endereços por quantidade de transações. Repare que o eixo y encontra-se em escala logarítmica. Mais de 85% dos endereços realizaram apenas duas transações (313 milhões de endereços), enquanto que outros 21 milhões de endereços realizaram apenas uma transação. A figura 5(b) apresenta a distribuição dos endereços por quantidade de transações, agora excluindo aqueles endereços que praticaram apenas duas transações (mais de 85%). Considerando os endereços restantes, mais de 28% realizou entre 3 e 5 transações, enquanto que apenas 3,86% realizou mais de 51 transações, o que pode indicar que usuários migram seus Bitcoins entre endereços.



(a) Quantidade de transações por endereço.



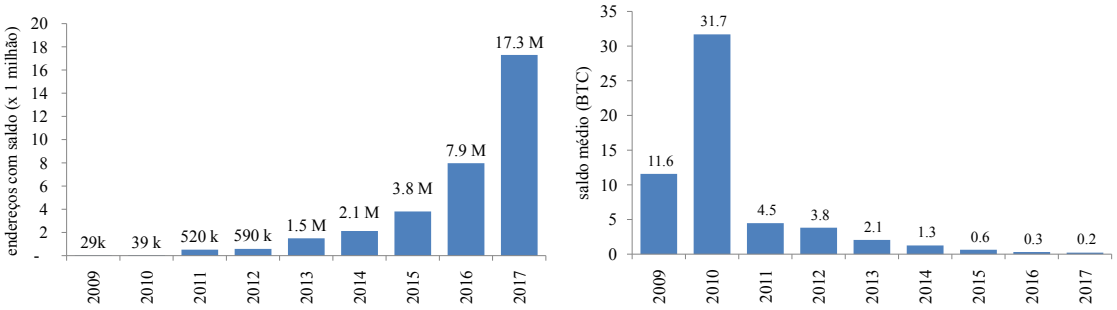
(b) Distribuição de endereços.

Figura 5. Caracterização de transações por endereço. A figura (a) apresenta a quantidade de transações por endereço. O eixo x indica a quantidade de transações, enquanto que o eixo y indica a quantidade de endereços (em escala logarítmica). A figura (b) apresenta a distribuição de endereços por transação desconsiderando endereços com apenas duas transações (que representam mais de 85% da amostra).

8. Saldos dos Endereços Bitcoin

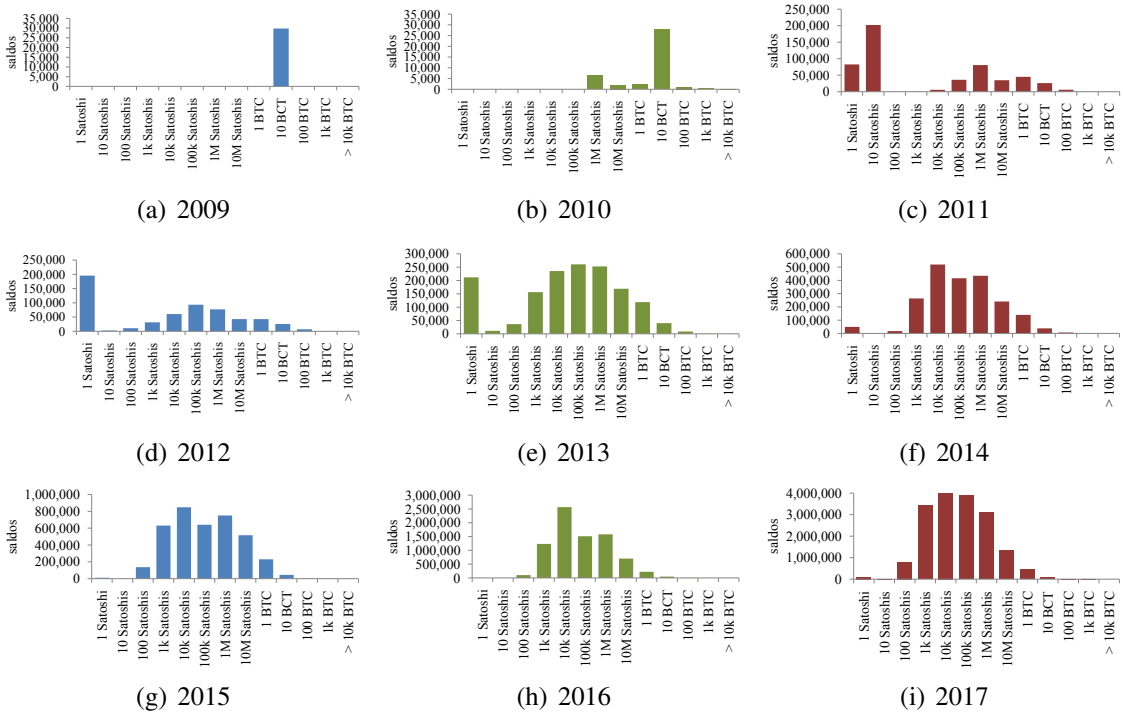
Agora avalia-se como a riqueza está distribuída na rede Bitcoin. Para tanto, realiza-se um estudo da evolução dos saldos ao longo do tempo. Esse saldo é computado levando-se em conta todas (e apenas) as transações que ocorrem dentro do ano em questão. O crescimento da quantidade de endereços com saldos positivos considerando **apenas** as transações ocorridas dentro de cada ano é apresentado na figura 6(a).

A rede fecha o ano de 2009 com pouco mais de 29 mil endereços com saldo. Em 2010 esse número cresce para mais de 39 mil. No ano seguinte (2011), ultrapassa 520 mil endereços. Após 5 anos (2016), essa quantidade é multiplicada por 20, atingindo mais de 7,9 milhões de endereços. O ano de 2017 contabiliza 17,3 milhões de endereços fechando o ano com saldo. A figura 6(b) apresenta a evolução do saldo médio apurado nas operações de cada ano. Em 2009, cada endereço recebeu, em média, 11,6 Bitcoins. Em 2010, percebe-se que esse valor triplica para 31,7 Bitcoins como transação média no ano. A partir de 2011, esse valor demonstra um movimento de redução gradativa, aingindo 0,2 Bitcoins em 2017.



(a) Endereços com saldo ao final de cada ano. (b) Saldo médio.

Figura 6. A figura (a) apresenta a quantidade de endereços que recebeu 90% dos Bitcoins transacionados em cada ano. A figura (b) indica o saldo médio por endereço.



(a) 2009 (b) 2010 (c) 2011

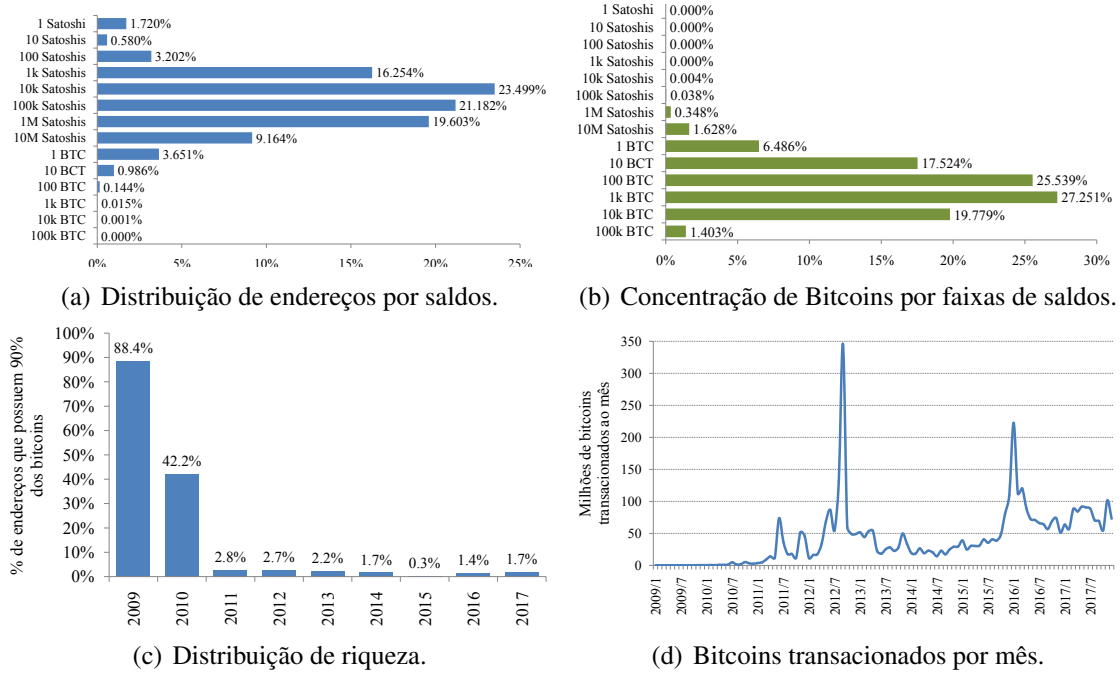
(d) 2012 (e) 2013 (f) 2014

(g) 2015 (h) 2016 (i) 2017

Figura 7. Figura apresenta a distribuição de saldos apurada no final de cada ano. O eixo x apresenta faixas de saldos a partir de 1 Satoshi em intervalos múltiplos de 10. O eixo y apresenta a quantidade de endereços cujo saldo encontra-se na faixa determinada pelo eixo x.

Considerando todo o conjunto de dados analisados, são encontrados mais de 368 milhões de endereços com saldo em Jan/2018. As figuras 7(a)-7(i) apresentam a quantidade de endereços (eixo y) pela faixa de saldo (eixo x). As faixas de saldos iniciam a partir de 1 Satoshi e seguem em múltiplos de 10 até 10 mil (10k) Bitcoins. Ao longo de 2009 e 2010, o saldo típico de um endereço era 10 Bitcoins. Conforme a rede se populariza e o câmbio do Bitcoin se altera, o perfil de saldos acompanha essas movimentações. De 2011 até 2013 percebe-se um grande volume de endereços com saldos inferiores à 10 Satoshis. A partir de 2014, os saldos passam a se concentrar entre 100 Satoshis e 10

milhões de Satoshis. Ainda assim, ao final de 2017 percebe-se 21 endereços com saldos acima de 10 mil Bitcoins, um valor considerável visto que 1 Bitcoin está na casa de US$ 4 mil. Considerando todo o período analisado, a distribuição de saldos dos endereços é apresentada na figura 8(a). O saldo mais popular está na faixa de 1.001 até 10.000 Satoshis (23,499%), seguido por endereços com saldos entre 10.001 até 100.000 Satoshis (21,182%). Mais de 95% dos endereços possuem saldos inferiores à 1 Bitcoin.



(a) Distribuição de endereços por saldos.

(b) Concentração de Bitcoins por faixas de saldos.

(c) Distribuição de riqueza.

(d) Bitcoins transacionados por mês.

Figura 8. A figura (a) apresenta a distribuição de endereços por faixas de saldo. A figura (b) apresenta a distribuição da riqueza por faixas de saldos. A figura (c) apresenta a quantidade de endereços que recebeu 90% dos Bitcoins ao longo do ano em questão. A figura (d) indica o montante de Bitcoins transacionados por mês ao longo dos anos.

Em contrapartida, a figura 8(b) apresenta como o dinheiro está distribuído na rede. Essa figura indica, por exemplo, que os endereços na faixa de 10.001 até 100.000 Bitcoins concentram 1,403% de toda a moeda disponível. No entanto, apenas dez endereços possuem esse montante. Ou seja, 1,403% da moeda em circulação é propriedade de 0,00003% dos endereços. De forma similar, endereços contendo entre 1.001 até 10.000 Bitcoins concentram 19,779% da moeda disponível, mas apenas 423 endereços (0.0011%) possuem tal montante.

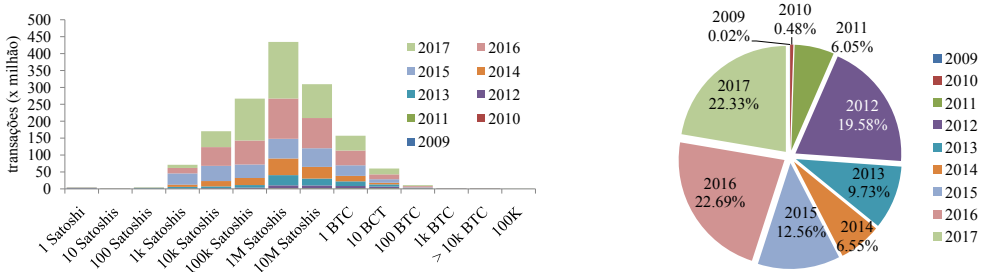
Assim, ao se contrastar as figuras 8(a) e 8(b) percebe-se que a distribuição de riquezas é desigual. Para complementar esse resultado, a figura 8(c) apresenta o fluxo de Bitcoins ao longo dos anos. Para cada ano, apresenta-se a quantidade de endereços que recebeu 90% dos Bitcoins transacionados. Em 2009, 90% dos Bitcoins transacionados foram distribuídos entre 88,4% dos endereços que mais acumularam Bitcoins. Em 2010, o fluxo convergiu para apenas 42,2% dos endereços. A partir de 2011, a rede passa a apresentar um alto fluxo de Bitcoins em direção aos endereços mais ricos. Nesse ano, 90% dos Bitcoins convergiram para os 2,8% endereços de maior posse. Em 2017, o

fluxo convergiu para os 1,7% endereços mais ricos (que receberam 90% dos Bitcoins transacionados na rede).

A figura 8(d) apresenta o volume de Bitcoins transacionados por mês. Ao longo do ano de 2017 são movimentados entre 50 e 100 milhões de Bitcoins mensalmente, um montante expressivo considerando-se o valor atual da moeda. Por outro lado, há a possibilidade de que algumas dessas movimentações ocorram entre endereços de um mesmo usuário sem estarem, necessariamente, atreladas à aquisição de um produto ou serviço, uma ação de mera migração de moedas entre contas.

9. Caracterização das Transações na rede Bitcoin

A rede completou mais de 1,54 bilhões de transações entre 2009 e 2017. Naturalmente, os valores típicos de transações mudam ao longo do tempo. A figura 9(a) apresenta a distribuição de transações ao longo dos anos por faixa de valor. Novamente, as faixas de valores seguem de 1 Satoshi até transações com valores superiores aos 100 mil (100k) Bitcoins. As transações mais frequentes encontram-se entre os valores de 1 milhão de Satoshis (0,01 Bitcoins) até 10 milhões de Satoshis (0,1 Bitcoins). Algumas poucas transações (da ordem de centenas ao longo de toda a existência da rede) ultrapassam o valor de 100 mil Bitcoins.



(a) Distribuição de transações por faixa de valor.

(b) Volumes transacionados por ano.

Figura 9. A figura (a) apresenta a distribuição de transações ao longo dos anos por faixa de valor transacionado. A figura (b) apresenta a distribuição percentual por ano de todo o montante já transacionado pela rede.

A figura 9(b) concentra-se nos montantes transacionados por ano. O ano de 2017 é responsável pela movimentação de 22,33% do montante de Bitcoins transacionado durante toda a existência da rede. Em 2016, esse valor é 22,69%, enquanto que apenas 0,02% para o ano de 2009.

10. Conclusão

Esse trabalho apresenta um estudo de caracterização da rede Bitcoin conduzido com dados completos de Jan/2009 (início de operação da rede) até Jan/2018. Em termos gerais, observa-se que a rede apresenta grande concentração de riqueza. Considerando-se todas as transações do ano de 2017, 90% dos Bitcoins convergiram para apenas 1,7% dos endereços. Tamanha concentração de riquezas parece ser contraditória com a motivação inicial de criação da criptomoeda para servir como um meio de pagamento inclusivo.

Também infere-se desse estudo uma certa preocupação dos usuários com a segurança da rede, motivo pelo qual 85% dos endereços apresentam apenas duas

transações. Esse fato é um indicador de que uma parcela considerável de usuários têm por hábito migrar seus Bitcoins entre contas, um comportamento que, certamente, destoa do mercado financeiro tradicional. O comportamento especulativo também pode ser percebido. Quando desconsidera-se esses endereços de apenas duas transações, percebe-se que 38% dos demais endereços realiza apenas uma única transação (de compra). Apenas 0,29% dos endereços realizaram mais de 100 transações, o que é um indicativo de que o Bitcoin não vêm sendo muito usado para transações comerciais cotidianas.

Por outro lado, embora a quantidade de transações por endereço seja baixa, é notável perceber que foram movimentados entre 50 e 100 milhões de Bitcoins por mês ao longo de 2017. O destino dessas movimentações merece ser investigada com mais detalhes à luz dos achados reportados por Ron and Shamir [2013], que descobrem um conjunto de grandes transações em que a moeda partia e retornava ao mesmo endereço após uma intricada rede de transações.

Como trabalhos futuros, pretende-se seguir esse estudo de caracterização para compreender a dinâmica dessa rede. Um ponto de particular interesse é compreender com qual frequência usuários migram Bitcoins entre contas, e qual seu impacto na rede.

Agradecimentos

Este trabalho foi parcialmente financiado por recursos do CNPq, CAPES e FAPEMIG.

Referências

Back, A. (2002). Hashcash-a denial of service counter-measure. *[Online]. Available: http://www.hashcash.org/papers/hashcash.pdf*.

Eyal, I. and Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In Christin, N. and Safavi-Naini, R., editors, *Financial Cryptography and Data Security*, pages 436–454, Berlin, Heidelberg. Springer Berlin Heidelberg.

Kondor, Pósfai, Csabai, and Vattay (2014). Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network. *PLoS ONE*, e86197.

Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., and Rosenschein, J. S. (2015). Bitcoin mining pools: A cooperative game theoretic analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, AAMAS '15, pages 919–927, Richland, SC. International Foundation for Autonomous Agents and Multiagent Systems.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2013). A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 127–140, New York, NY, USA. ACM.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *[Online]. Available: http://www.bitcoin.org/bitcoin.pdf*.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

Pappalardo, G., Di Matteo, T., Caldarelli, G., and Aste, T. (2017). Blockchain inefficiency in the bitcoin peers network. *arXiv preprint arXiv:1704.01414*.

Ricci, S., Borges, A., Luiz, H., Menasché, D. S., and Ferreira, E. (2016). Dinâmica das transações do Bitcoin: uma abordagem quantitativa. In *Anais do WPerformance 2016 (Workshop em Desempenho de Sistemas Computacionais e de Comunicação)*, WPerformance '16.

Ron, D. and Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. In *International Conference on Financial Cryptography and Data Security*, pages 6–24. Springer.

Wang, L. and Liu, Y. (2015). Exploring miner evolution in bitcoin network. In Mirkovic, J. and Liu, Y., editors, *Passive and Active Measurement*, pages 290–302, Cham. Springer International Publishing.

Yermack, D. (2015). Chapter 2 - is bitcoin a real currency? an economic appraisal. In Chuen, D. L. K., editor, *Handbook of Digital Currency*, pages 31 – 43. Academic Press, San Diego.