Análise da Rede de Transações do Ethereum

Juliana Z. G. Mascarenhas[1], **Alex B. Vieira**[2] **e Artur Ziviani**[1]

[1]Laboratório Nacional de Computação Científica (LNCC)
Av. Getúlio Vargas – 333 – 25651-075 – Quitandinha – Petrópolis – RJ – Brasil

[2]Universidade Federal de Juiz de Fora (UFJF)
Rua José Lourenço Kelmer, S/N - Martelos – Juiz de Fora – MG – Brazil

{julianam,ziviani}@lncc.br, alex.borges@ufjf.edu.br

Abstract. *The use of blockchain-based cryptocurrencies increases every year, while Bitcoin is the most notorious example. Nevertheless, another more recent platform, called Ethereum, is on a consistent rise in this scenario. Despite the growing interest both in industry and in academy, there are few network characterizations of blockchain-based applications, in particular of Ethereum. The goal of this work is then to perform a preliminary analysis of the transaction network of Ethereum, an emergent plataform that is not well studied in the literature, obtaining different interesting characteristics about the behavior of the users of this network.*

Resumo. *O uso de criptomoedas baseadas em blockchain cresce a cada ano, sendo Bitcoin o exemplo mais notório. Entretanto, outra plataforma mais recente, denominada Ethereum, está em franca ascensão nesse cenário. Apesar do crescente interesse na indústria e academia, há pouca caracterização de redes das aplicações baseadas em blockchain, em particular de Ethereum. O objetivo deste trabalho consiste em uma análise preliminar da rede de transações do Ethereum, uma plataforma emergente e muito pouco estudada na literatura, obtendo diversas características interessantes acerca do comportamento dos participantes dessa rede.*

1. Introdução

Transações ou acordos são tipicamente realizadas por indivíduos que não necessariamente possuem conhecimento ou confiança mútua. Nesse contexto, é comum a existência um terceiro ente confiável ("*Trusted Third Party*"), tais como governos, bancos, cartórios, moeda (dinheiro) ou autoridades centralizadoras para prover confiabilidade em um acordo ou transação firmado entre as partes.

Em muitos casos, confiar em entidades centralizadoras não é atrativo. Há problemas nos custos que essas entidades impõem, na escalabilidade das aplicações que realizam transações e até mesmo, problemas de segurança inerentes aos sistemas centralizados. Por outro lado, realizar transações distribuídas, sem a presença de entes centralizados confiáveis, apresenta grandes desafios. De fato, prover consenso entre usuários que não possuem conhecimento prévio (nem confiança) dos demais, mantendo a segurança e corretude dos dados e de eventos criados dentro da rede, requer uma tecnologia robusta.

Atualmente, há um crescente interesse pela tecnologia de blockchains justamente por ela prover uma alternativa nesse contexto. Um blockchain opera como um livro-razão

que pode registrar transações entre entidades *sem um ente centralizador*, garantindo assim confiabilidade distribuída no sistema [Buterin 2014, Lin and Liao 2017]. Esses registros são realizados de forma eficiente, permanente e podem ser facilmente verificáveis. Normalmente, um blockchain é gerenciado por uma rede P2P, onde os participantes aderem ao protocolo da aplicação e validam os blocos que são criados ao longo da existência da cadeia [Xu et al. 2017]. Uma vez que um bloco é registrado pelo coletivo de usuários, seus dados não podem ser alterados sem a devida alteração de todos os blocos subsequentes a ele. A tecnologia de blockchain cria, portanto, uma base de inovação tecnológica que abre muitas perspectivas e oportunidades para uma nova geração de aplicações em diversas áreas que podem ser constituídas sobre essa tecnologia de base [Braga et al. 2017].

Entre as diversas aplicações de blockchain, criptomoedas, tal como Bitcoin, estão entre as que proporcionam maior notoriedade à tecnologia. Por exemplo, Ethereum [Buterin 2014, Wood 2014] é um sistema baseado em blockchain que permite, além da transferência de valores, criação e execução de programas auto-executáveis, que realizam ações baseadas em regras pré-definidas. Esses programas, denominados contratos inteligentes (*smart contracts*) (Seção 2.2), podem criar aplicações diversas, como a autenticação ou rastreio da origem de produtos em uma cadeia produtiva. Apesar do crescente interesse em blockchains e criptomoedas, indústria e academia sentem falta de análises quantitativas desses sistemas. Ainda são poucos os trabalhos que tratam de caracterizações desses sistemas e, quando o fazem, tipicamente focam no Bitcoin [Ricci et al. 2016, da Silva Rodrigues 2017]. Em especial, trabalhos sobre Ethereum são raros e focam na definição do sistema ou em discussão e tratamento de anonimidade e ataques a esse sistema [Meiklejohn et al. 2013, Payette et al. 2017].

Ethereum é, atualmente, a segunda moeda virtual mais utilizada. De fato, o Bitcoin era detentor de aproximadamente 91,3% do mercado, seguido por baixa participação de outras criptomoedas, até o surgimento do Ethereum em 2015. Desde então, o quadro mudou: a fatia do mercado relacionada ao Bitcoin foi reduzida para 39,8%, enquanto a do *ether* (criptomoeda referente ao Ethereum) subiu para 28,5%.[1]

Neste artigo, apresentamos uma caracterização do Ethereum, uma plataforma emergente e pouco estudada na literatura, modelando sua rede transações para encontrar nós com perfis específicos. Por exemplo, identificamos fontes e sorvedouros de transações, os níveis de atividade e importância de determinados nós da rede. Nossos resultados indicam que há uma pequena quantidade de nós possuem maior número de conexões, maior número de transações, se comparado ao restante da rede. Esses nós também possuem maior participação na economia da rede, movimentando um maior volume de valores. Por exemplo, esses nós apresentam grau 8 vezes maior que a média da rede, indicando uma centralização da rede Ethereum, ou domínio de suas atividades por poucos nós computacionalmente muito poderosos. Observou-se também que nós classificados como fontes, estavam relacionados a usuários mineradores do Ethereum. Observamos ainda que cerca de 90% realizam média de transações com valores mais baixos com máximo de 9 mil dólares. Por fim, acreditamos que as caracterizações apresentadas cobrem lacunas da literatura e são importantes para compreender o Ethereum, frente à grande demanda por utilização das moedas virtuais e blockchains.

[1] O que é o ether, nova moeda virtual que cresceu 4.000% em seis meses e ameaça o bitcoin: `http://www.bbc.com/portuguese/geral-40380808`

Este trabalho é organizado como segue. A Seção 5 apresenta os trabalhos relacionados da área. A Seção 2 discute os conceitos principais da plataforma Ethereum. A Seção 3 apresenta a metodologia de coleta de dados e as métricas avaliadas. A Seção 4 traz os resultados das caracterizações realizadas. Por fim, a Seção 6 conclui o artigo e aborda possíveis trabalhos futuros.

2. Tecnologia blockchain

O Bitcoin [Nakamoto 2008] foi a primeira aplicação baseada em blockchain a ganhar notoriedade. O blockchain utilizado pelo Bitcoin foi a primeira solução descentralizada confiável para o problema de gasto duplo (*double-spending*), ou seja, o risco do mesmo recurso em criptomoeda ser utilizado mais de uma vez [Buterin 2014]. Até então, evitar esse risco era somente garantido por entidades centralizadoras. Essa característica do blockchain foi um dos aspectos viabilizadores do Bitcoin como criptomoeda [Buterin 2014]. Como dito anteriormente, blockchain é um livro-razão de registros público distribuído, onde todos os eventos ocorridos (transações ou contratos) são armazenados [Crosby et al. 2016]. Os participantes possuem uma cópia exata desse livro-razão de registro de transações e contratos, garantindo a autenticidade dos dados inseridos e a grande dificuldade de alteração devido ao encadeamento de blocos.

Mais precisamente, as informações propagadas na rede blockchain são encapsuladas em transações e essas, em blocos, formando assim uma cadeia de blocos. Cada bloco dessa cadeia é composto por um conjunto de transações realizadas na rede e outros campos de identificação [Braga et al. 2017]. Etapas de validação de transações e blocos são necessárias para verificar a autenticidade das informações e realizar inserções no blockchain de forma segura [Braga et al. 2017].

O primeiro bloco do blockchain, o gênese, tem por identificador o resultado de uma função *hash* baseada no seu conteúdo. Cada bloco subsequente a ele possui um campo com o identificador do bloco anterior, cujo conteúdo é considerado no cálculo do seu identificador [Zheng et al. 2017]. O mecanismo utilizado para validação de blocos, ou mineração no caso do Bitcoin, é denominado *Proof-of-Work* (PoW) [Wood 2014]. A validação de um bloco, portanto, depende da validação de blocos anteriores, constituindo assim o encadeamento de blocos que dá origem ao blockchain.

2.1. Transações em aplicações de criptomoeda

Blockchain também adota criptografia assimétrica, com usuários possuindo chaves pública e privada. Cada transação é propagada na rede de usuários com o objetivo de ser inserida em um bloco a ser validado [Pilkington 2016]. Uma transação deve ser assinada digitalmente com a chave privada do usuário origem para prover autenticidade e corretude. Caso haja falha, esta transação é descartada pela rede. Além disso, caso ocorra o problema de gasto duplo, apenas uma das transações identificadas na rede é mantida. Após a validação de uma transação, essa é inserida em blocos que também devem ser validados, contribuindo por fim para a expansão da cadeia de blocos, i.e. o blockchain.

O mecanismo de consenso PoW utiliza trabalho computacional para determinar o identificador (via *hash*) de um bloco. No caso do PoW do Bitcoin, deve-se encontrar um *hash* com uma determinada quantidade de zeros inicias. O Ethereum utiliza o mecanismo PoW, mas não determina uma quantidade de zeros iniciais. Na verdade, o

Ethereum vem buscando formas de realizar consenso de maneira mais eficiente e assim, é possível que em breve haja uma alteração em seu mecanismo de validação. Por exemplo, [Buterin and Griffith 2017] apresentam o algoritmo Casper com base em *Proof-of-Stake (PoS)*. Esse algoritmo é, em realidade, um híbrido de PoS e PoW. PoS consiste na validação de blocos, acordos e inserções, onde qualquer usuário com crédito dentro do sistema pode participar como validador. Os valores que um usuário possui influenciam em sua escolha como um validador de blocos [Lin and Liao 2017]. Após a validação, os blocos são propagados pela rede de usuários e adicionados ao blockchain, expandindo-o de forma consistente e descentralizada. Após a inserção do bloco na blockchain, as informações e valores podem ser resgatados pelo usuário destinatário da transação.

2.2. Contratos inteligentes

Um contrato inteligente (*smart contract*) se assemelha a um contrato legal tradicional, regulamentando a interação entre partes interessadas no objeto comum do contrato. Entretanto, o conceito de contrato inteligente define que as cláusulas de um contrato são codificadas e podem ser incorporadas a um hardware ou software com auto-execução [Christidis and Devetsikiotis 2016]. Assim, sistemas de contratos inteligentes podem mover recursos digitais de acordo com regras e comandos pré-estabelecidos na sua criação. A partir desse conceito básico, contratos inteligentes podem ser usados em uma grande variedade de aplicações, tais como liquidação de transações e testamentos inteligentes criptografados [Buterin 2014].

Segundo [Braga et al. 2017], blockchain passou por uma grande evolução com o uso de contratos inteligentes. Em aplicações baseadas em blockchain, contratos inteligentes são *scripts* inseridos nas transações que executam ações baseadas nas regras do contrato. O programa do contrato inteligente é executado por todos os nós da rede do blockchain, sendo sua execução correta e consistente garantida pelo mecanismo de consenso distribuído [Braga et al. 2017]. Em aplicações de criptomoedas construídas em contratos inteligentes, primeiro as entradas das transações são verificadas pelas assinaturas digitais. Em seguida, verifica-se se o saldo dos endereços de saída coincidem com os de entrada. Por fim, aplica-se a mudança de estado, ou seja, os recursos são efetivamente transferidos. Em aplicações de criptomoedas, tal como Ethereum, usuários podem criar transações de acionamento (*call*) e criação (*create*) de contratos inteligentes [Wood 2014].

2.3. Plataforma Ethereum

A plataforma Ethereum é um sistema de contratos inteligentes baseado em blockchain. A plataforma é composta por máquinas virtuais descentralizadas denominadas de Ethereum Virtual Machines (EVM), que executam os contratos inteligentes [Braga et al. 2017]. Um contrato é identificado por um endereço e, é acionado quando seu endereço é referenciando como destino por uma transação. A partir de seu acionamento, o contrato é executado automaticamente em cada nó da rede [Christidis and Devetsikiotis 2016].

Ethereum pode ser visto como uma máquina de estados baseada em transações [Wood 2014]. A partir de um estado inicial, a cada transação, o estado se modifica até se transformar em estado final. Estados podem incluir informações como balanço de contas, reputação, arranjos confiáveis, ou qualquer informação que possa ser representada por um computador [Wood 2014]. Além disso, outras aplicações podem utilizar o blockchain do Ethereum [Buterin 2014]. Segundo [Wood 2014], essa plataforma

descentralizada executa aplicações exatamente como foram programadas, sem a possibilidade de *downtime*, fraude ou interferência de terceiros. Esses aplicativos são executados em um blockchain de compilação customizada, em uma rede de infraestrutura compartilhada global que pode mover valores e representar o dono da propriedade.

Na rede do Ethereum, os endereços de carteira pertencentes a usuários podem ser associados a nós de uma rede, onde os usuários trocam informações através desses nós. A comunicação é feita com o objetivo de transferir informações entre carteiras, sejam valores, ou parâmetros de um contrato [Wood 2014]. Essas informações são inseridas dentro de transações, que podem ser representadas por arestas interconectando os nós da rede Ethereum envolvidos em cada transação. Usuários da plataforma Ethereum podem ser classificados como mineradores, usuários ou pertencer as duas categorias. O usuário comum apenas realiza transações, enquanto o minerador valida os blocos dentro da rede.

3. Metodologia e coleta de dados

Nesta seção, apresentamos o método de representação de redes complexas utilizado para modelar a rede de transações do Ethereum, definimos as métricas de ciência de redes adotadas na análise e decrevemos os dados coletados.

3.1. Representação de redes complexas por grafos multiaspecto (MAG)

Grafo multiaspecto é uma generalização de grafos capaz de representar redes de qualquer ordem (finita), na qual as relações expressadas entre nós nesse contexto são binárias [Wehmuth et al. 2016]. Utilizando-se de MAGs, podem ser representadas, através de um único objeto matemático, redes multi-camadas, redes variantes no tempo, ou redes composta por ambos os tipos, bem como redes de ordem ainda superior.

Um grafo tradicional é dado por $G = (V, E)$ onde V é um conjunto de vértices e E é um conjunto de arestas representando ligações entre pares de vértices. Em MAG, por sua vez, têm-se $H = (A, E)$, onde E é um conjunto finito de arestas e A é composto por uma lista de *aspectos*. Um aspecto é um conjunto finito de características independentes (vértices, instantes de tempo, camadas, e assim por diante). Uma aresta no MAG é um tupla de elementos de aspectos, indicando uma relação binária entre grupos de aspectos. O número de aspectos p determina a ordem do MAG. Uma propriedade fundamental de MAGs é que o grafo representante da rede complexa de alta ordem é *isomorfo* a um grafo direcionado comum, permitindo assim a aplicação de métricas tradicionais de ciência de redes, com a devida interpretação contextualizada do resultado. O MAG cria um grafo direcionado entre vértices compostos, onde os vértices são formados por aspectos.

A Figura 1 apresenta um pequeno exemplo ilustrativo de aplicação de MAG na representação de uma rede hipotética de transporte. Nesse caso, a rede é composta pelos seguintes aspectos: camadas como modal de transporte (ônibus e metrô), instantes de tempo e vértices como locais (paradas de ônibus e estações de metrô), que podem ter representações em mais de modal, sendo pontos de baldeação entre esses modais. Existem três tipos de arestas na representação MAG: espacial, temporal e mista. A aresta espacial é restrita ao mesmo instante de tempo; a aresta temporal conecta o mesmo nó em instantes de tempo distintos; e a aresta mista conecta nós diferentes em instantes de tempo distintos. Caso seja necessário retirar um determinado aspecto do MAG, é utilizada uma subdeterminação. Por exemplo, se a camada referente ao modal de transporte na Figura 1

for subdeterminada, têm-se uma rede sem a diferenciação do tipo de transporte. Neste caso, obtêm-se uma visão integrada do sistema de transporte como um todo.

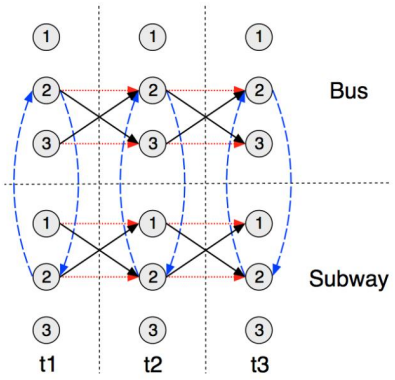


Figura 1. Exemplo de uma rede de transporte em MAG [Wehmuth et al. 2017].

3.2. Modelagem da rede de transações do Ethereum

Como o modelo adotado busca representar uma rede de transações Ethereum, esta não possui periodicidade de eventos, como horários de sistema de transporte, por exemplo. Nesse caso, o tempo é contínuo e não-cíclico. Dentro do Ethereum uma transação é considerada válida após o bloco que a contem ser inserido no blockchain. Entretanto, uma transação pode ser considerada inválida por problemas de autenticação ou gasto duplo antes de ser inserida em um bloco. Portanto, foi considerado como instante em que a transação ocorreu o mesmo instante de tempo em que seu bloco foi minerado (validado).

A Figura 2 apresenta os elementos da rede de transações Ethereum representada por um MAG de dois aspectos: (i) os nós que representam os endereços de carteiras e (i) os instantes de tempo (T1, T2 e T3), sendo que as arestas representam as ligações entre esses nós. Uma transação, nesse contexto, caracteriza a transferência na rede de *ether* de um nó origem a um nó destino, sendo uma transferência como essa representada por uma aresta espacial (setas claras). Uma aresta temporal (setas escuras) representa a continuidade de um nó no decorrer do tempo da rede. Por exemplo, o nó A existe no instante T1 e T3, logo existe uma aresta temporal interligando a instância do nó A em T1 e a instância do nó A em T2. A transação do nó A para o nó B no instante T1 caracteriza uma aresta espacial. O sentido da aresta determina os nós origem e destino da transação.

Nas análises realizadas, foram consideradas duas representações da rede: (i) a de transações do Ethereum e (ii) a representação subdeterminando o aspecto tempo, ambas usando MAG. Pela subdeterminação do MAG é possível analisar a rede de forma estática, verificando todas as transações já realizadas independentemente do tempo.

3.3. Métricas de ciência de redes

No que segue, definimos as métricas adotas para análise da rede de transações Ethereum.

3.3.1. Centralidade de grau

O número de arestas incidentes a um nó i é denominado grau k_i. Em redes direcionadas, considera-se para um nó i o grau de entrada k_i^{in}, de saída k_i^{out} ou total k_i. Para redes

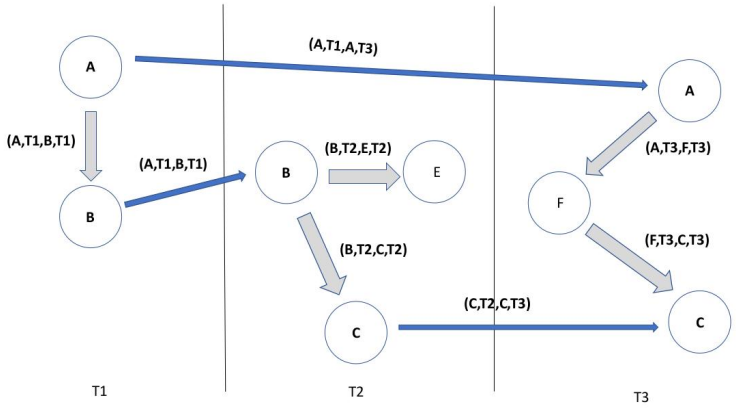


Figura 2. Representação da rede de transações em um MAG de 2 aspectos.

não-direcionadas, o grau médio $< k >$ é dado por: $< k >= \frac{1}{N}\sum_{i=1}^{N} k_i = \frac{2L}{N}$. Para redes direcionadas: $< k^{in} >= \frac{1}{N}\sum_{i=1}^{N} k_i^{in}; < k^{out} >= \frac{1}{N}\sum_{i=1}^{N} k_i^{out}, < k >= \frac{L}{N}$.

A centralidade de grau mede a importância relativa de um nó na rede de acordo com seu número de conexões. O valor da centralidade de grau para um nó i é equivalente ao seu grau k_i para redes não-direcionadas. Para redes direcionadas, considera-se a centralidade de grau de entrada k_i^{in} e de saída k_i^{out}. Em nossa análise, o grau k_i do nó i representa o número de transações realizadas pela carteira associada ao nó i. Por sua vez, os grau de entrada k_i^{in} e de saída k_i^{out} representam as transações iniciadas pelo nó i e as transações recebidas pelo nó i, respectivamente.

3.3.2. Centralidade de betweenness

A centralidade de betweenness utiliza os caminhos mínimos do grafo para determinar o poder de intermediação que um nó possui perante a rede na qual está inserido [Barabasi 2016]. Assim, um nó é importante se este pertence a vários caminhos mínimos entre pares de outros nós, ou seja, este nó é essencial na passagem de informação. A centralidade de betweenness do nó i é formalmente definida por: $betweennesscentrality(i) = \sum_{j<k} {}^{g_{jk}(i)}/_{g_{jk}}$. onde g_{jk} é o número total de caminhos mínimos entre os nós j e k; e $g_{jk}(i)$ é o número desses caminhos mínimos que passam pelo nó i [Barabasi 2016]. Um nó com alto betweenness em uma rede de transações indica um ponto da rede crucial para o fluxo de recursos na plataforma Ethereum. Em redes direcionadas o sentido do enlace é considerado no caminho mínimo.

3.3.3. Métrica nonce por intervalo de tempo

Toda transação realizada por um usuário (nó) dentro da plataforma Ethereum possui um campo incrementador denominado *nonce*. Esse campo determina o número de sequência da transação realizada. Dessa forma, a primeira transação realizada por um nó tem seu nonce com valor zero. O nonce então vai sendo incrementado a cada nova transação realizada pelo nó. Formalmente, o nonce é um valor escalar igual ao número de transações já enviadas pelo remetente [Wood 2014]. Transações recebidas não afetam o nonce.

Portanto, ao se verificar o nonce de uma transação é possível conhecer o total de transações realizadas por um determinado nó até aquela transação. Analisar a rede de transações utilizando o parâmetro nonce possibilita então obter alguns resultados independentemente dos dados armazenados no conjunto de dados. Assim, com o nível de atividade de um nó na rede (número de transações realizadas) pode-se avaliar o tipo desse nó. Um nó da rede pode ser recente, antigo, ou ter realizados poucas transações e se tornar inativo. Utilizar a métrica nonce por intervalo de tempo possibilita obter uma noção de *vazão* de transações que um nó realiza. Mais formalmente, definimos η como a métrica referente à quantidade de nonces por intervalo de tempo, i.e. a vazão de transações, como: $\eta(i) = \frac{(n^i_{max} - n^i_{min}) + 1}{\Delta t}$, onde n^i_{max} e n^i_{min} são os valores do nonce máximo e mínimo das transações de um nó i no intervalo de tempo Δt, respectivamente. O total de transações no intervalo Δt é dado por $(n^i_{max} - n^i_{min}) + 1$.[2] Tipicamente, para nossa análise, vamos adotar Δt equivalente a 1 dia, resultando para fins deste artigo em uma métrica de vazão de transações medida em nonce por dia.

3.4. Dados utilizados

Neste trabalho, foram coletadas todas as transações de 10 endereços de carteiras distintos, durante um período de 7 meses entre os dias 06/05/2017 e 02/12/2017. Essas 10 carteiras monitoradas se relacionaram com 22 outras carteiras no período, totalizando uma rede de 32 nós observados com 607 transações. Desses 32 nós, 20 nós iniciaram transações, os demais apenas receberam. As informações das transações são de domínio público, podendo ser acessadas pela API da plataforma etherscan que realiza o acesso aos dados do Ethereum. As carteiras cujas transações foram coletadas foram escolhidas aleatoriamente dentre as carteiras que possuíam histórico minimamente ativo desde a criação do sistema.

No Ethereum, existem dois tipos de transações: transações internas e transações normais [Wood 2014]. As transações normais resultam em transferências de valores, enquanto as transações internas envolvem acionamentos e criação de contratos. Neste trabalho, focamos nas transações normais.

A rede de transações foi construída partir dos dados coletados sob uma perspectiva espacial e temporal. Os nós da rede representam os endereços de carteiras. As arestas, que conectam as carteiras envolvidas, por sua vez, representam a operação de transferência de valores de uma carteira à outra, i.e., uma transação. Os tipos de arestas utilizados na modelagem da rede de transações do Ethereum por MAG estão descritos na Seção 3.2.

As arestas espaciais, que representam a transferência de valores em *ether*, são representadas pela tupla $\underline{(end.origem, data}, \underline{end.destino, data}) < valor > < nonce >$ onde end.origem e end.destino são, respectivamente, as carteiras de onde um valor é debitado/creditado; valor representa o total de ether transacionado e nonce é o valor incrementado a cada nova transação realizada (ver Seção 3.3). A maioria das transações são feitas em Wei, a menor unidade de ether, onde 1 ether equivale a 10^{18} Wei [Wood 2014].

Por fim, ressaltamos que a subrede criada permite avaliação das características básicas da rede de transações do Ethereum. Além disso, a metodologia empregada é extensível a redes maiores, dependendo apenas do conjunto de dados e dos recursos computacionais disponíveis.

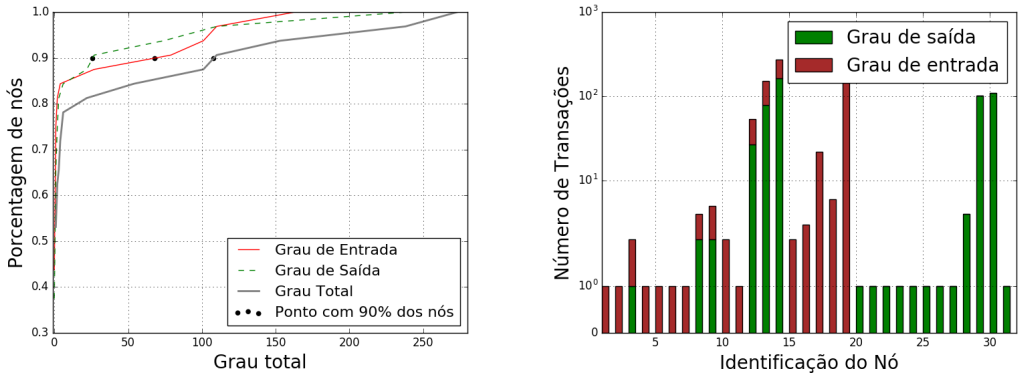
[2]É necessário adicionar uma unidade uma vez que o campo nonce é iniciado com valor zero.

4. Análise e resultados

Nesta seção, apresentamos as avaliações conduzidas sobre a rede de transações da aplicação Ethereum.

4.1. Resultados para centralidade de grau

As carteiras avaliadas, em geral, possuem baixo grau. Apenas algumas delas tem um grau nitidamente superior à moda da rede. Mais precisamente, a Figura 3(a) apresenta a CDF do grau das carteiras encontradas no subgrafo avaliado. Foi possível avaliar o grau de um total de 32 carteiras, envolvidas com transações entre as 10 carteiras iniciais. De acordo com essa figura, cerca de 80% da rede tem grau total inferior a 20. Porém, cerca de 10% das carteiras tem grau total acima de 110 e, algumas carteiras, chegam a ter grau superior a 200. A rede de forma geral possui poucos nós com alto grau e muitos nós com baixo grau com uma variação brusca no valor de grau como apresenta a curva CDF na Figura 3. A maior parte da concentração da rede se encontra abaixo do grau total de 108.



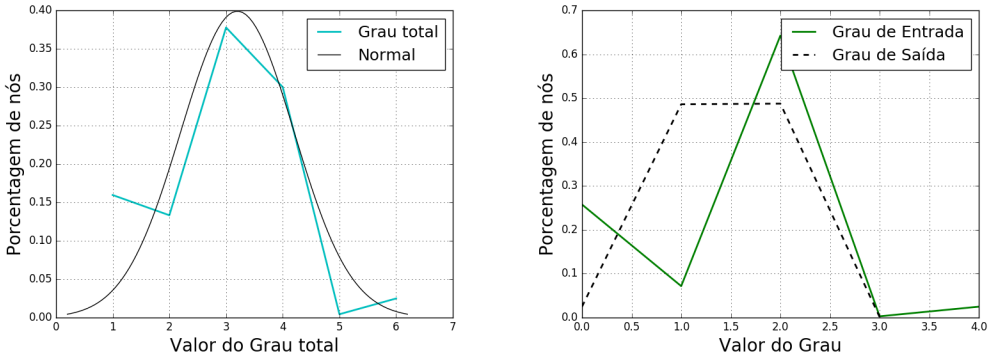
(a) CDF da distribuição de grau

(b) Distribuição de transações por nó

Figura 3. Distribuição de grau e de transações por nó.

Com base na Figura 3(b), percebemos também que, na rede avaliada, há nós que atuam primordialmente como fontes de transações e outros apenas como sorvedouros. Os endereços de nós fontes do grafo avaliado foram contrastados com endereços da plataforma *ethersecan.io* e, de acordo com as informações obtidas, podemos inferir que esses nós são mineradores da plataforma Ethereum. De fato, os nós mineradores recebem as recompensas por mineração de blocos por transações especiais. Essas transações não aparecem nas transações normais, o que é consistente com o resultado. Observou-se ainda que nós com altos valores de grau de entrada e saída estão associados a aplicações externas. Os dados relativos a esses nós, na plataforma *ethersecan.io*, indicam que essas aplicações utilizam o blockchain do Ethereum para fornecer serviços e receber pagamentos, como por exemplo: Monaco card. Alguns desses nós possuem conexões com nós sorvedouro, o que pode indicar que eles pertencem a um mesmo usuário que concentra toda sua rentabilidade em um único ponto. Mais ainda, isso pode indicar a existência de algum relacionamento profissional (prestação de serviços) entre usuários distintos. Para determinar qual cenário realmente ocorre, são necessários mais dados para análise. Por fim, observamos que nós que caracterizam usuários comuns possuem valores menos expressivos de grau de entrada e saída.

O grau composto, ou seja, a quantidade de transações de uma carteira em determinada data, tem valores baixos. Por exemplo, o máximo de transações para esta rede em um determinado dia são 6 transações. A Figura 4(a) apresenta a distribuição de grau composto e a Figura 4(b) traz a distribuição de grau de entrada/saída. Note que a distribuição do grau composto total se aproxima grosseiramente de uma distribuição normal, com média 3, sendo necessárias mais amostras para um refino e melhor constatação. O valor mais comum para grau de entrada e grau de saída é 2.



(a) Distribuição do grau composto (b) Distribuição do grau entrada/saída

Figura 4. Distribuição do grau composto e de grau entrada/saída.

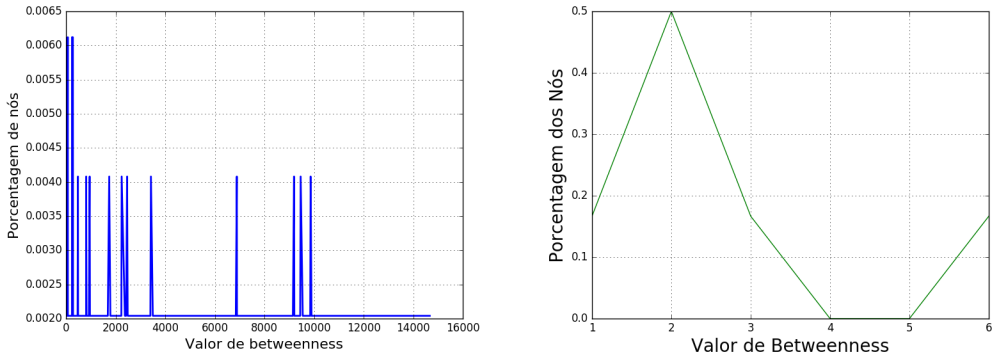
Por fim, ressaltamos que as duas representações da rede apresentam diferenças relacionadas à métrica grau. Inclusive, o *ranking* de grau (ordem das carteiras de acordo com a métrica grau) difere substancialmente entre as duas representações. Isso ocorre, pois a representação de rede por MAG diferencia nós que tenham o mesmo número de transações concentradas num curto período de tempo ou diluídas ao longo de um período mais prolongado. Nesse caso, nós com atividade concentrada acabam tendo uma centralidade de grau maior do que os nós com a mesma atividade diluída no tempo. Essa distinção não ocorre na rede em que o aspecto tempo é subdeterminado.

4.2. Resultados para centralidade de betweenness

A influência de um nó dentro da rede depende do contexto no qual este nó está inserido. A centralidade de betweenness ordena os nós da rede de acordo com seu nível de intermediação com relação ao restante da rede (ver Seção 3.3.2). Essa métrica auxilia a definir o papel de cada nó na economia do sistema. Quanto maior o valor de betweenness, maior o poder de intermediação ou seja, mais um nó é capaz de intermediar fluxos de recursos. Em nossas análises, foram desconsiderados os nós que possuem valor de betweenness igual a zero (60% da rede).

A Figura 5(a) apresenta a centralidade de betweenness para a representação MAG da rede de transações do Ethereum. Por essa figura, é possível verificar a existência de *hubs* na rede de transações. *Hubs* são nós que possuem maior conectividade (i.e., alto grau) e pode haver uma tendência de concentrarem um maior número de caminhos mínimos atravessando-os, dependendo da topologia da rede. De todo modo, na rede de transações do Ethereum analisada, os resultados indicam ser este o caso.

A distribuição de centralidade de betweenness, da rede subdeterminada pelo aspecto tempo, mostra que há poucos *hubs* na rede. Nesse caso, verificamos pequenos



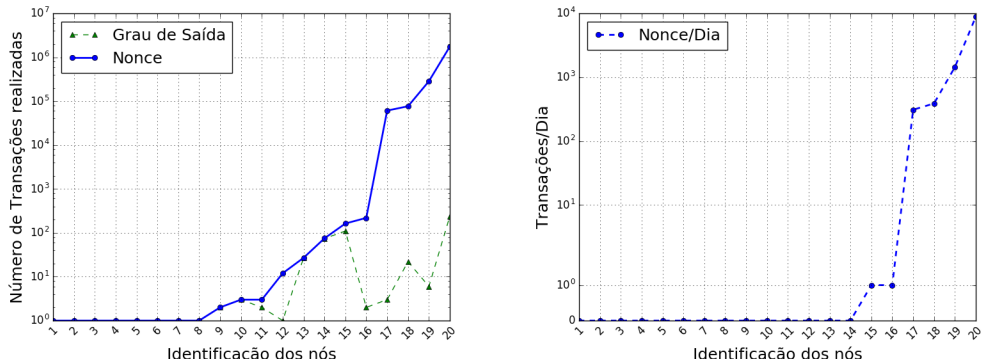
(a) MAG (b) MAG subdeterminado

Figura 5. Distribuição do valor da centralidade de betweenness.

grupos de nós conectados entre si e isolados do restante da rede. Isso condiz com o comportamento dos indivíduos que tendem a se relacionarem com outros de um mesmo grupo. Há também alguns nós com alto valor de betweenness por pertencerem a uma rede isolada. Todos os demais membros do mesmo grupo realizam transações com esse, e assim, ele se torna um *hub*. Além disso, a maioria dos nós possui conexões em seu próprio grupo e poucos são os nós com maior diversificação de interações. Essa menor parcela de nós movimenta a maior quantidade de valores na rede, interligando grupos distintos.

4.3. Resultados para a métrica nonce por intervalo de tempo

Nonce por dia retorna a quantidade de transações que um nó realizou por dia, ou seja, a vazão de transações por dia. Pode-se inferir o total de transações realizadas por nó através do parâmetro *nonce* das transações do Ethereum.



(a) Total de transações realizadas (b) Transações por dia (Nonce/Dia)

Figura 6. Transações realizadas.

A Figura 6(a) apresenta o histograma dessa métrica, para os 20 nós avaliados que iniciaram transações na subrede MAG e sua subdeterminação no tempo. Note que, pela Figura 6(a), nós com maiores valores de nonce tendem a não ter o mesmo número de grau de saída. Isso ocorre por que o nonce é incrementado a qualquer transação realizada pelo usuário, seja essa transação interna ou normal (Seção 3.4). Por exemplo: o nó 16 possui grau de saída igual a 2, mas o total de transações são de 219 (utilizando nonce).

A diferença corresponde às transações internas realizadas pelo nó. Por outro lado, o nó 13 possui o grau de saída e o total de transações realizadas iguais a 27. Esse nó realizou durante o período estipulado apenas transações normais.

A subdeterminação agrega a atividade dos nós por todo o período de 7 meses, como apresenta a Figura 6(b). Em todo o período, grande parte dos nós apresentam baixa quantidade de transações e assim, $nonce/dia \rightarrow 0$. Pôde-se perceber que uma pequena parcela dos nós possui um nível de atividade superior ao restante da rede. Uma parte desses nós são os que possuem maior centralidade de grau. Esse resultado pode indicar concentração de transações em poucos nós da rede.

O nonce igual a zero indica que a primeira transação foi realizada. Pode-se determinar se o nó é novo na rede e quando este se tornou ativo. Foram encontrados nós com valores de nonce mínimo e máximo (Seção 3.3) iguais a zero. Isso descreve o comportamento de um nó novo e não ativo na rede. Nós com número baixo de transações realizadas, porém com número de sequência (nonce) alto podem ser considerados inativos por um período. Valores altos de nonce identificam alto nível de atividade, como alguns nós da rede demostram na Figura 6(b). Esses resultados em conjunto com a centralidade de grau, auxiliam a determinar a importância de um nó na rede.

4.4. Classificação de carteiras (nós) por transações versus valor

Os nós foram classificados de acordo com seu número de transações e a média de valores transferidos desconsiderando valores pagos aos mineradores. A Tabela 1 apresenta as classes em que cada carteira (nó) pode ser classificado conforme o número de transações e o valor médio dessas transações em ether. Por sua vez, a Tabela 2 mostra a classificação das carteiras (nós) pelo seu volume de transações e pelo valor médio dessas transações. A grande maioria das transações é composta de valores baixos ou médios. Essas transações podem indicar comportamentos característicos de pessoa física. Além disso, há uma pequena porcentagem de transações com valores muito acima do gasto rotineiro de pessoas comuns. Essas transações podem indicar a utilização da aplicação por empresas ou pessoas jurídicas, onde essas transações possuem valores de algumas centenas de ether (centenas de milhares de dólares americanos),[3] contabilizando 1.5% das transações.

Tabela 1. Classes conforme número de transações e valor médio das transações.

Classificação	Número de transações	Intervalo de valor (em ether)
Baixo	0 a 10	[0,5]
Médio	11 a 100	]5,30]
Alto	101 a 300	]30,200]
Muito Alto	—	]200,900]

5. Trabalhos relacionados

Trabalhos de análise de plataformas de criptomoeda em sua imensa maioria são voltados para Bitcoin. Em [Ricci et al. 2016], realizou-se a modelagem do tempo de validação de transações da rede Bitcoin, incluindo a verificação dos parâmetros que

[3] 1 ether = 491 dólares americanos em 26/03/2018 (Fonte: `https://coinmarketcap.com/pt-br/currencies/ethereum/`).

Tabela 2. Classificação das carteiras (nós) por transações versus valor.

Transações \ Valor	Baixo	Médio	Alto	Muito Alto
Baixo	60%	15%	3%	1.5%
Médio	15%	0%	0%	0%
Alto	5.5%	0%	0%	0%

influenciam nas confirmações. Em [da Silva Rodrigues 2017] foi analisado o nível de segurança das transações do Bitcoin através de modelagem matemática. Os autores de [Meiklejohn et al. 2013] realizaram a caracterização da rede Bitcoin verificando o anonimato alcançado pelos usuários e o potencial de manutenção do anonimato. Em [Ron and Shamir 2013], os autores caracterizaram os gastos dos usuários Bitcoin. Através de técnicas estatísticas determinaram como os usuários movimentam e gastam seus bitcoins entre diversos endereços com o objetivo de garantir anonimidade. Em [Payette et al. 2017], houve a categorização dos endereços do Ethereum em quatro grupos de comportamentos.

O presente trabalho, em contraste, analisa uma rede de transações com objetivo de caracterizar um subconjunto de transações da plataforma Ethereum. A diferença deste trabalho para os demais supracitados está na caracterização das transações e usuários, além de ser aplicado à rede de transações no Ethereum, uma plataforma emergente e pouco estudada na literatura.

6. Considerações finais e trabalhos futuros

Neste artigo, analisamos a rede de transações do Ethereum, que tem sido pouco estudado na literatura relacionada apesar de sua adoção expressiva nos últimos anos. Através dos resultados obtidos, observou-se a existência de padrões de comportamento na rede de transações do Ethereum que auxiliam no melhor entendimento da dinâmica do sistema, como por exemplo nós fontes associados a nós mineradores. Foi também possível obter uma outra perspectiva das transações realizadas pelos nós, através da utilização do parâmetro nonce por intervalo de tempo. Os resultados de nossa análise auxiliam na caracterização da rede de transações do Ethereum por múltiplas perspectivas.

Esses resultados são preliminares, mas promissores, o que nos encoraja a expandir o estudo, sendo este o principal alvo para trabalhos futuros. Expansão que permitirá uma visão mais representativa e menos tendenciosa da rede. Assim, planejamos expandir a base de dados para a inclusão de transações desde bloco gênesis e realizar análises mais aprofundadas. Para enriquecer o modelo utilizado na representação da rede, consideramos também coletar dados relacionados ao *hash-pointer* da transação, ou seja, as informações utilizadas na prevenção de gasto duplo. Por fim, também consideramos coletar dados para analisar o tempo de confirmação de transações do Ethereum.

Agradecimentos

À CAPES, FAPERJ, FAPEMIG, FAPESP e ao CNPq, pelo apoio financeiro.

Referências

Barabasi, A.-L. (2016). Network science. `http://networksciencebook.com/`.

Braga, A. M., Marino, F. C. H., and dos Santos, R. R. (2017). Segurança de aplicações blockchain além das criptomoedas. pages 99–148. Livro-texto dos minicursos SBSeg.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper.

Buterin, V. and Griffith, V. (2017). Casper the friendly finality gadget. https://arxiv.org/pdf/1710.09437.

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303.

Crosby, M., Pattanayak, P., Verma, S., and Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2:6–10.

da Silva Rodrigues, C. K. (2017). Sistema bitcoin: uma análise da segurança das transações. *iSys-Revista Brasileira de Sistemas de Informação*, 10(3):5–23.

Lin, I.-C. and Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *IJ Network Security*, 19(5):653–659.

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 *Proc of the ACM IMC*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

Payette, J., Schwager, S., and Murphy, J. (2017). Characterizing the ethereum address space. https://pdfs.semanticscholar.org/db53/a0281ea25f0041ca4aa812be5c9013f33f26.pdf.

Pilkington, M. (2016). *Blockchain technology: principles and applications*. Research handbook on digital transformations, Edward Elgar Publishing.

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*.

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

Wehmuth, K., Fleury, E., and Ziviani, A. (2016). On MultiAspect Graphs. *Theoretical Computer Science (TCS)*, 651:50–61.

Wehmuth, K., Fleury, E., and Ziviani, A. (2017). MultiAspect Graphs: Algebraic representation and algorithms. *Algorithms*, 10(1).

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151:1–32.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., and Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. In *Proc. of the IEEE International Conference on Software Architecture (ICSA)*.

Zheng, Z., Xie, S., Dai, H., 4, X. C., and Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Big Data (BigData Congress), IEEE International Congress*, pages 557–564. IEEE.