Governança digital e o processo de *mineração*:

Especialização e controvérsias no sistema *peer-to-peer* Bitcoin[1]

Bruno Campos Cardoso (PPGAS-UFSCar / SP)

Resumo

Considerado a primeira *criptomoeda* e em operação desde 2009, o Bitcoin é, por um lado, um protocolo para a troca de valores eletrônicos e, por outro, um sistema complexo de máquinas, técnicas e atores humanos, associados em comunidades e mercados de tipo descentralizado. A produção coletiva de um estado de consenso distribuído se dá por meio do emprego ostensivo de algoritmos criptográficos, da mobilização de aglomerados de máquinas com alto poder computacional e da atuação de programadores, investidores e usuários em uma rede de troca transnacional que opera sem a necessidade de autoridades reguladoras centrais. Nos últimos anos, para além da crescente adoção e da alta volatilidade de preço, o sistema *peer-to-peer* Bitcoin também tem sido palco de uma série de controvérsias em seu ecossistema de usuários, desenvolvedores, empresas, serviços e indústrias. Neste artigo tenho como foco uma dessas controvérsias, a que tem se dado por conta da superespecialização de certos atores da rede conhecidos como *mineradores*. A partir do desenvolvimento de *hardware* dedicado (ASICs) à *mineração* – um processo de validação de transações essencial ao funcionamento da criptomoeda – tal atividade, antes desempenhada por computadores domésticos e pequenos *rigs* (acoplamentos de componentes, como séries de placas de vídeo, para maximizar o poder computacional de uma instalação) é agora dominada por empresas que desenvolvem, produzem e empregam em larga escala o uso de máquinas ASIC (*Application-Specific Integrated Circuit*). Uma vez que a *mineração* é um processo que demanda grande quantidade de poder computacional e, por conseguinte, um alto consumo de energia elétrica, essa atividade tem passado por processos de *centralização* em torno desses atores e de suas instalações. Tais processos de *centralização* são motivo de intensas controvérsias sobre o funcionamento do sistema, uma vez que este se pretende *descentralizado* e autônomo. O fato da concentração de poder nas mãos de poucos atores, bem como suas implicações econômicas e técnicas, serão abordados a partir da interface da antropologia e da política, visando a descrição etnográfica da rede a partir do processo de *mineração* e dos seus desdobramentos mais recentes. A intenção é mostrar como uma rede *peer-to-peer* de tipo distribuído, como a do Bitcoin, é motivo de disputas técnicas, econômicas e políticas, bem como de processos específicos de centralização e descentralização que transformam a topologia e a governança desta rede sociotécnica.

Palavras-chave: política, algoritmos, Bitcoin.

---

1 Trabalho apresentado na 31a Reunião Brasileira de Antropologia, realizada entre os dias 09 e 12 de dezembro de 2018, Brasília/DF.

Introdução – o sistema Bitcoin e algumas controvérsias preliminares[2]

O sistema *peer-to-peer* Bitcoin está em operação desde janeiro de 2009 e pretende atuar como um tipo de "dinheiro eletrônico". Criado por uma (ou várias) pessoa(s) sob o pseudônimo Satoshi Nakamoto, teve seu funcionamento detalhado pela primeira vez em novembro de 2008, num *whitepaper* postado em uma lista de e-mails sobre criptografia (NAKAMOTO, 2008). Desde então, por ter sido lançado como um projeto de *software livre*, aos poucos congregou uma comunidade de programadores e desenvolvedores que, ao longo dos anos, introduziram mudanças, melhoramentos e novas funcionalidades em seu código-fonte, tornando o Bitcoin um projeto robusto, coletivo e global[3]. Satoshi Nakamoto, no entanto, desapareceu sem qualquer aviso em meados de 2010, sem nunca ter revelado sua identidade e legando sua criação ao domínio público.

Uma característica de projetos de código aberto, como o Bitcoin, é a gestão coletiva do desenvolvimento de *software* – auditoria do código-fonte, proposição de mudanças por meio de protocolos específicos e ritos estritos de modificação e implementação – que levanta, assim, questões relevantes sobre a governança de projetos descentralizados no âmbito digital (FINN, 2017; KELTY, 2009). Um *software* de código aberto pressupõe a possibilidade de replicações, transformações e derivações, como é o caso das centenas de outras criptomoedas que surgiram a partir do código-fonte do Bitcoin, bem como tantas outras centenas que se baseiam nas inovações trazidas por Nakamoto e demais programadores, combinadas em novos arranjos.

Dentre as várias inovações introduzidas pelo Bitcoin, destaco as duas principais. Em primeiro lugar, uma solução funcional para o problema do "gasto duplo" ou da "produção de escassez", problema característico do âmbito digital, visando evitar que uma informação possa ser copiada indefinidamente, e permitindo a circulação controlada por meio da aplicação de algoritmos criptográficos conhecidos. Embora soluções para o problema do "gasto duplo", mais conhecidas como algoritmos de "falha de tolerância", já fossem conhecidas no âmbito da computação, em especial sob a

2 O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

3 Mais de 600 pessoas de todo mundo, anonimamente ou não, já colaboraram com o projeto Bitcoin, cujo repositório principal está hospedado na plataforma Github: https://github.com/bitcoin/bitcoin

formulação original do “Problema dos Generais Bizantinos” (LAMPORT; SHOSTAK; PEASE, 1982) que visava minimizar ou neutralizar os efeitos de mal funcionamento ou ataques às máquinas de uma rede, não havia até então uma implementação desse algoritmo para redes de tipo distribuído (*peer-to-peer*), isto é, em uma rede autônoma e sem autoridade central. No caso do Bitcoin, esses métodos assumem a forma de uma política monetária de emissão e circulação da criptomoeda por meio de estritas “regras de consenso”[4]. E, em segundo lugar, a própria montagem inovadora desse sistema de produção de “consenso distribuído” como um sistema complexo de replicação e validação criptográfica de toda informação por meio de “provas de trabalho” (*proof-of-work*) que garantem a *emergência de consenso* entre pares que não se conhecem e não confiam uns nos outros por meio do emprego ostensivo de poder computacional. Essas duas inovações, devidamente implementadas desde o início pelo Bitcoin, abriram caminho para a consolidação de formas de “dinheiro eletrônico” que podem circular sem a necessidade de bancos, instituições financeiras ou outros intermediários reguladores (ANTONOPOULOS, 2015, 2016; NARAYANAN *et al.*, 2016).

A *mineração* (*mining*)[5] é um processo sociotécnico que articula a participação de diversos atores dentro e fora da rede. Em linhas gerais, a mineração diz respeito ao emprego de poder computacional (máquinas potentes com alto consumo de energia elétrica) para a realização da contínua validação das transações que ocorrem no sistema Bitcoin. Ou seja, cabe aos *mineradores* (*miners*) a tarefa de conferir se as transações que circulam pela rede são válidas (se há fundos, se os endereços batem, se a quantia em questão já não foi gasta em outra transação) e, a cada dez minutos, de acordo com as regras de consenso do sistema, ordená-las e escrevê-las em “blocos” que constituem o registro distribuído de todas as movimentações. Os blocos de transações são conectados uns aos outros em cadeia cronológica, onde cada bloco aponta para o “endereço” do

4 Algumas dessas regras dizem respeito à quantidade máxima de bitcoins que podem existir (21 milhões) e à curva deflacionária de emissão – a quantidade de novas criptomoedas criadas a cada ciclo da rede decresce pela metade a cada quatro anos, tendendo a zero conforme se aproxima do teto estipulado por Nakamoto na primeira versão do *software*. Essas e outras “regras de consenso”, em vigor desde o início do sistema, não podem ser alteradas sem provocar cisões e incompatibilidades na rede.

5 Para tornar a leitura mais fluida, este e outros termos, daqui em diante, aparecem pela primeira vez em itálico e depois serão grafados normalmente, a não ser quando a ênfase num dado termo ou conceito se faça necessária. Citações e analogias virão entre aspas.

bloco anterior, como em uma corrente (daí o termo *blockchain*), criando assim um histórico comum de transações semelhante às páginas numeradas de um "livro-caixa".

Os mineradores, para produzir um bloco válido a cada dez minutos, devem competir entre si: aquele que primeiro encontrar uma solução para um problema criptográfico, que tem como *input* as transações que serão validadas, anuncia para a rede a "descoberta do novo bloco" e recebe, como recompensa, uma quantidade de novos bitcoins recém-criados e a soma de todas as taxas das transações por ele validadas. Esse procedimento técnico de validação, inventado por Nakamoto, é chamado *proof-of-work* (PoW): os mineradores "provam" para a rede que, para tornar válido aquele bloco de transações, empregaram uma tal quantidade de poder computacional (*hash power*) na descoberta de uma solução cuja integridade pode ser facilmente verificável por meio de uma prova criptográfica – em outras palavras, a "prova de trabalho" envolve a produção de um número (*hash*) muito difícil de obter mas muito fácil de verificar. O *hash* produzido garante a integridade das informações de um bloco: qualquer alteração ou inconsistência nas transações ali contidas produziria um *hash* completamente diferente, algo que uma rápida verificação (feita a todo momento por todos os pares da rede), denunciaria o bloco como inválido. Os mineradores, tendo validado um feixe de transações, são por isso recompensados, e a cadeia de blocos com a maior quantidade de poder computacional acumulado é então considerada a "mais verdadeira", pois é o histórico do acumulo de mais recursos no esforço de validação.

Os "mineradores" são incentivados a agir "honestamente" tanto por que têm mais chances de coletar para si as recompensas dos blocos caso invistam mais máquinas e recursos nessa competição, quanto por que agir "maliciosamente" contra tamanha quantidade de poder computacional é economicamente inviável[6].

É, portanto, somente por meio do *proof-of-work* que as transações são registradas e replicadas em blocos e, assim, de fato *efetuadas*: a cada dez minutos,

6 É o "poder computacional acumulado" necessário para produzir a cadeia de provas criptográficas (em que a mais recente aponta para a anterior e assim sucessivamente até o primeiro bloco criado em 2009) que "prova" tanto a validade das transações ocorridas no sistema quanto sua inviolabilidade, uma vez que a alteração do registro de uma transação passada implicaria a alteração da prova criptográfica do bloco em que ela reside e de todos os blocos subsequentes. Para adulterar as "provas de trabalho" de todos esses blocos seria necessário mobilizar mais da metade de todo poder computacional da rede, o que, embora seja um cenário de ataque plausível, é hoje virtualmente impossível dada as dimensões do sistema e a pluralidade de atores envolvidos.

novos blocos de transação são incorporados à longa cadeia de blocos e propagados por toda rede, de modo que os demais pares "não-mineradores" (*full nodes* e *light nodes*) também conferem a integridade dos blocos recebidos por meio da rápida verificação da "prova de trabalho" e assim concatenam os novos blocos às suas respectivas cópias da *blockchain*. O estado coletivo da rede é a todo momento replicado, conferido, rejeitado ou validado por todos pares, sejam mineradores ou não, e é por meio desse contínuo encadeamento de procedimentos técnicos e algoritmos criptográficos que se dá a *emergência do consenso* na rede distribuída do Bitcoin.

A mineração é, assim, um processo sociotécnico lucrativo e, nos dias de hoje, altamente especializado. Empresas e desenvolvedores de *hardware* específico têm comercializado máquinas dedicadas (ASICs) e estabelecido conglomerados em diversos países para *minerar* Bitcoin e outras criptomoedas, o que levanta questões sobre os impactos desses grandes empreendimentos no ecossistema das criptomoedas. As controvérsias em torno da mineração envolvem também os efeitos colaterais da implementação em larga escala de instalações de ASICs e *mining rigs*. Por um lado, dado o alto consumo de energia, a produção e necessária exaustão do calor produzido pelas máquinas constituem parcela significativa dos custos de operação das "fazendas de mineração", que tem se concentrado em países ou regiões em que a energia elétrica é mais barata ou subsidiada pelo Estado. Por outro lado, a questão do alto consumo de energia e do *foot-print* ecológico do Bitcoin também têm acirrado a polêmica sobre a eficácia e utilidade de seu método de "prova de trabalho", uma vez que, no interior do sistema Bitcoin, a demanda por recursos energéticos e de *hardware* de alto desempenho cresce em função do crescimento da rede: conforme mais participantes adentram no sistema, a dificuldade do processo de mineração é ajustada para que o ritmo de produção dos blocos se mantenha mais ou menos regular (de dez em dez minutos); quanto mais máquinas participam da rede, mais difícil é a mineração de um bloco.

Embora os possíveis impactos ambientais do Bitcoin devam ser considerados com bastante atenção[7], neste artigo pretendo abordar o processo da mineração no

7 O sistema computacional global, somando computadores domésticos, empresariais e todos os *datacenters*, é responsável pelo consumo de 5% de toda energia elétrica produzida no planeta (WOLPERT, 2018). Estima-se que o sistema *peer-to-peer* Bitcoin consuma atualmente 0,5% da produção de energia global, ou cerca de 70 TWh por ano, o equivalente ao consumo anual de países como a Irlanda ou a República Tcheca (DE VRIES, 2018). Não há, no entanto, um consenso sobre a melhor maneira de calcular o consumo energético do Bitcoin, tampouco de estabelecer estimativas confiáveis de consumo

sistema Bitcoin como um jogo complexo de forças e expedientes técnicos que visam equalizar certos fluxos materiais (*hardwares*, instalações, energia elétrica, patentes) e procedimentos algorítmicos (*softwares*, algoritmos criptográficos e de rede) em uma operação que seja, do ponto de vista dos mineradores, economicamente vantajosa ou minimamente lucrativa.

Para tanto, apresento uma descrição da controvérsia em torno do *ASICBoost*, uma otimização que prometia reduzir em 20% os gastos dos mineradores com energia elétrica, maximizando os lucros de uma dada instalação de ASICs. Tomo por base etnográfica as mensagens trocadas na lista de e-mails *bitcoin-dev* (de 2016 a 2018), importante canal de debate dos desenvolvedores do Bitcoin, e documentos técnicos publicados na plataforma colaborativa Github, onde o software principal é desenvolvido, que detalham posicionamentos e perspectivas divergentes sobre essa questão. Pretendo mostrar como vários expedientes de comunicação e debates de propostas são articulados na constituição de processos de governança digital num ambiente descentralizado[8].

para os próximos anos. Embora o consumo de energia elétrica aumente substancialmente a cada ano, uma vez que a demanda por mais poder computacional também aumenta, inovações nas indústrias de *hardware* e energia renovável tendem a colocar essas previsões em perspectiva. Um estudo recente publicado pela revista Nature Climate Change, tomando de empréstimo a metodologia controversa de De Vries e supondo uma taxa de crescimento e consumo semelhante às atuais, aponta que o sistema Bitcoin produziria, em três décadas, emissões de CO2 suficientes para elevar em até 2ºC o aquecimento global (MORA *et al.*, 2018). O estudo, no entanto, não leva em conta a crescente utilização de fontes renováveis de energia, tampouco a curva de eficiência computacional na produção de componentes tecnológicos. Estas e outras considerações serão desenvolvidas em artigo futuro.

8 O levantamento aqui presente, inspirado pelo método do "mapeamento de controvérsias" (LATOUR, 2012; VENTURINI, 2010, 2012; VENTURINI; LATOUR, 2010), faz parte das primeiras etapas da minha pesquisa de doutorado (PPGAS/UFSCAR) sobre a "Política dos Algoritmos" a partir da etnografia do sistema *peer-to-peer* Bitcoin. A opção por uma descrição mais etnográfica e menos teórica se dá à luz da formulação mais ou menos recente de várias das ideias e leituras aqui apresentadas.

ASICBoost – um vetor de (des)centralização?

Em um *whitepaper* publicado em 31 de março de 2016 na lista *bitcoin-dev*[9], o pesquisador e matemático Timo Hanke anunciava, em parceria com o pesquisador Sergio Lerner, um "melhoramento algorítmico" para o processo de mineração do Bitcoin que ainda não havia sido discutido em público[10]. De acordo com seu artigo, que trazia especificações do processo, o chamado "*AsicBoost* is a method to speed up Bitcoin mining by a factor of approximately 20%. *AsicBoost* is an algorithmic optimization and therefore applicable to all types of mining hardware" (HANKE, 2016):

> The *AsicBoost* method is based on a new way to process work items inside and outside of the Bitcoin mining ASIC. It involves a new design of the SHA 256 hash-engines (inside the ASIC) and an additional pre-processing step as part of the mining software (outside the ASIC). The result is a performance improvement of up to 20% achieved through a reduction of gate count on the silicon. (...) Through gate count reduction on the silicon *AsicBoost* improves two essential Bitcoin mining cost metrics simultaneously and by a similar factor: the energy consumption (Joule per Gh) and the system cost ($ per Gh/s). With the system cost being proportional to the capital expenses of a Bitcoin mine and the energy consumption being proportional to its operating expenses, *AsicBoost* reduces the total cost per bitcoin mined by approximately 20%. For the Bitcoin mines of the future *AsicBoost* will make all the difference between a profitable and an unprofitable mine. (*ibid.*)

Por meio de pequenas alterações no *hardware* de um ASIC e com a implementação algorítmica descrita por Hanke e Lerner, a aplicação desta otimização poderia reduzir os custos de mineração de uma dada instalação em até 20% – o que num ambiente de disputas acirradas, pequenas margens de lucro e elevados custos de manutenção, é uma vantagem bastante expressiva. Também de acordo com o artigo, que trazia várias especificações técnicas, o *ASICBoost* era uma patente de registro pendente (*patent-pending*) em nome dos dois pesquisadores.

---

9 "Bitcoin Protocol Discussion": lista de e-mails para o desenvolvimento e discussão do protocolo do sistema Bitcoin, acessível em: https://lists.linuxfoundation.org/mailman/listinfo/bitcoin-dev

10 A mensagem original de Timo Hanke, e provável primeira ocorrência pública do termo *ASICBoost*, pode ser lida em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-April/012596.html

Já na mensagem seguinte ao anúncio de Hanke, o desenvolvedor Peter Todd questionava acerca dos riscos de centralização do processo de mineração por conta do uso de patentes e do possível favorecimento de um ou outro fabricante:

> "What steps are you going to take to make sure that this improvement is available to all ASIC designers/mfgs on a equal opportunity basis? The fact that you've chosen to patent this improvement could be a centralization concern depending on the licensing model used. For example, one could imagine a licensing model that gave one manufacture exclusive rights."[11]

Por outro lado, o hacker Mustafa Al-Bassam especulava que o ASICBoost poderia, ao contrário, ser um vetor de descentralização global:

> "Alternatively scenario: it will cause a sudden increase of Bitcoin mines in countries where the algorithm is not patented, possibly causing a geographical decentralization of miners from countries that already have a lot of miners like China (if it is patented in China)."[12]

Marek Palatinus, fundador da *pool* de mineração S*lush*[13], argumentava que a patente sobre uma inovação desse tipo não serviria de nada: "To my understanding it is purely software thing. It cannot be detected from outside if miner uses this improvement or not. So patenting it is worthless."[14]

Como veremos nas próximas páginas, ao longo dos meses seguintes e até o lançamento da implementação de código aberto do *ASICBoost* em outubro de 2018,

---

11 Peter Todd, "Re: [bitcoin-dev] AsicBoost", 1º de abril de 2016, disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-April/012597.html

12 Mustafa Al-Bassam, "Re: [bitcoin-dev] AsicBoost", 4 de abril de 2016, disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-April/012600.html

13 Em operação desde dezembro de 2010, a Slush Pool (https://slushpool.com) foi a primeira *pool* de mineração do Bitcoin. Em termos gerais, uma vez que a demanda por poder computacional – chamado *hash-rate* e calculado em *gigahashes* (Gh) ou *terahashes* (Th) por segundo – para a realização do processo de *proof-of-work* da mineração foi aumentando com a expansão do sistema, computadores pessoais e *rigs* domésticos logo se tornaram obsoletos, incapazes de produzir blocos dentro de uma margem de lucro desejável ou mesmo em tempo hábil, dada a crescente complexidade da computação necessária. A solução encontrada por Palatinus (e, depois dele, por outros tantos) foi reunir máquinas e usuários de várias partes do mundo em uma mesma *pool*, um aglomerado digital que, somando esforços computacionais numa mesma "força-tarefa", poderia rivalizar com mineradores profissionais e então repartir os dividendos de acordo com o *hash-rate* investido por usuário.

14 Marek Palatinus, "Re: [bitcoin-dev] AsicBoost", 6 de abril de 2016, disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-April/012601.html

todas as três perspectivas manifestadas acima, embora contraditórias, se mostraram mais ou menos acertadas.

Interlúdio – o grande debate da escalabilidade

O debate sobre o *ASICBoost* se inscreve numa longa série de disputas e controvérsias que, de modo amplo, é chamado "o debate da escalabilidade" (ou bem: *the great scaling debate*). Não convém aqui tentar resumi-lo. Todavia – e em suma – tornou-se um consenso, em especial a partir de meados de 2015, que a arquitetura do sistema Bitcoin seria incapaz comportar um grande volume de transações (acaso quisesse *mesmo* operar como uma forma viável de "dinheiro eletrônico") sem passar por alterações substanciais em seu protocolo. Porém, não havia qualquer consenso em como, nem quais alterações deveriam ser implementadas para solucionar os problemas identificados pelos participantes.

A política vigente de proposição de mudanças e melhorias fora proposta pelo hacker anglo-iraniano Amir Taaki em agosto de 2011, como parte de um esforço para organizar os processos decisórios de uma comunidade em expansão. O *Bitcoin Improvement Proposal*, ou *BIP*, pretendia formalizar e documentar as propostas feitas por membros da comunidade em uma estrutura comum. Um BIP, de acordo com o BIP 001, que define a si mesmo, é:

> "a design document providing information to the Bitcoin community, or describing a new feature for Bitcoin or its processes or environment. The BIP should provide a concise technical specification of the feature and a rationale for the feature. We intend BIPs to be the primary mechanisms for proposing new features, for collecting community input on an issue, and for documenting the design decisions that have gone into Bitcoin. The BIP author is responsible for building consensus within the community and documenting dissenting opinions. Because the BIPs are maintained as text files in a versioned repository, their revision history is the historical record of the feature proposal."[15]

15 BIP 001: "BIP Purpose and Guideline", disponível em https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki . O BIP 002, "BIP process, revised", de fevereiro de 2016, substitui e aprimora o processo definido pelo BIP 001. Vide: https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki

Por meio dos BIPs – documentos numerados com propostas ou informações sobre o sistema ou sobre a própria gestão de informação – as diversas propostas, muitas delas contraditórias entre si, visam a veiculação de ideias, documentação de rotinas, protótipos de implementação de uma correção ou melhoria, ou estímulo ao debate e colaboração dos participantes em torno das questões colocadas pelo autor do documento. Toda gestão coletiva dos documentos e, principalmente, do código-fonte, se dá na mesma plataforma e segue mesmos princípios de produção colaborativa de *software*: usuários escrevem correções ou melhorias que são submetidas para análise dos demais, podendo ser aceitas, rejeitadas ou vir a ser motivo de debates, num processo semelhante ao *peer-review* acadêmico (embora mais simples e muito mais rápido).

A partir do ano de 2015, quando o *grande debate* foi tomando as proporções que seu nome sugere, os BIPs tornaram-se instrumentos importantes nas disputas entre soluções conflitantes para o problema da escalabilidade, sendo profusamente mobilizados a favor e contra ideias ou grupos que as defendiam.

Tomo rapidamente – pois o caso envolve outros tantos atores e desdobramentos – as duas posições mais eloquentes: de um lado, desenvolvedores, mineradores e fabricantes que viam num *hardfork*[16] da rede, isto é, a introdução de funcionalidades por meio de uma cisão de compatibilidade, a solução para implementar uma série de melhorias substanciais, em especial o aumento do tamanho dos blocos de transações (de 1MB por bloco, para 2MB ou até 4MB, de acordo com as várias propostas nesse sentido). Essa posição passou a ganhar adesões a partir da publicação do BIP 101[17], de 22 de junho de 2015, em que o desenvolvedor Gavin Andresen propõe pela primeira vez um *harkfork* para estender de modo gradual o tamanho dos blocos, a fim de reduzir o impacto do limite de tamanho na adoção e no crescimento do sistema Bitcoin. Já no dia seguinte, em 23 de junho, o BIP 102[18], escrito por Jeff Garzik, propunha o aumento dos blocos de 1MB para exatos 2MB.

---

16 Chama-se *hardfork* uma modificação ou derivação do código que envolve alterações nas regras de consenso. Quando implementado, quebra a compatibilidade com as versões anteriores em operação, de modo que a rede se divide em duas: de um lado, os pares que estão rodando a versão “atualizada”, e de outro, os que estão rodando a versão “clássica”; a partir do momento da bifurcação da rede, não há comunicação ou intercâmbio possível entre os pares “atualizados” e os pares “clássicos” pois seus protocolos implementam regras contraditórias e, na maioria dos casos, mutuamente inválidas.

17 BIP 101: “Increase maximum block size”, disponível em: https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki

De outro lado, desenvolvedores que se mostravam mais preocupados com a compatibilidade com versões anteriores do *software*, argumentavam que as mudanças poderiam ser feitas de modo a evitar uma cisão entre versões possivelmente incompatíveis do *software* Bitcoin. Em dezembro de 2015, os desenvolvedores Eric Lombrozo, Johnson Lau e Peter Wuille, a partir de experimentos e propostas que vinham circulando em vários grupos de discussão, publicam o BIP 141[19], uma proposta de extensão por *softfork*[20] que ficou conhecida como *SegWit* e que operava uma reestruturação dos dados nos blocos de transação a fim de maximizar o volume de informação sem que o limite nominal precisasse ser alterado, mantendo assim uma solução de compatibilidade com pares antigos.

Essas duas posições mostraram-se, em grande medida, antagônicas. No entanto, em 21 de fevereiro de 2016, em um centro de convenções em Hong Kong, representantes da "indústria bitcoin" e alguns representantes da comunidade de desenvolvedores reuniram-se como signatários de um acordo cujo cronograma de desenvolvimento implementasse tanto o *SegWit* quanto o aumento dos blocos para 2MB por meio de um *hardfork*. O Acordo de Hong Kong, como ficou conhecido, previa que uma implementação do *SegWit* fosse lançada já em abril, e o código-fonte para o *hardfork* em junho de 2016. "Havendo forte apoio da comunidade," terminava o documento, "a ativação do *hardfork* deverá acontecer em meados de julho de 2017."[21]

---

18 BIP 102: "Block size increase to 2MB", disponível em: https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki

19 BIP 141: "Segregated Witness (Consensus layer)", disponível em: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

20 Um *softfork* implica uma alteração de código que mantém uma compatibilidade regressiva (*backwards compatible*), isto é, trata-se de uma atualização que não altera as regras de consenso: embora a(s) funcionalidade(s) introduzida(s) com a atualização do software só possam ser executadas e/ou compreendidas pelos pares que realizarem a atualização, todos os outros componentes permanecem compatíveis, de modo que os pares que estejam rodando versões "atualizadas" continuam capazes de "entender" a comunicação dos pares "clássicos" e, portanto, continuam a se comunicar numa mesma rede. Pares que estejam rodando versões "clássicas" (não atualizadas), ainda que não "entendam" o formato da nova comunicação (podendo rejeitá-la como inválida), continuam a se comunicar entre si, isto é, do ponto de vista deles, não há alteração na rede – para além, é claro, do fato da diminuição da quantidade de pares comunicáveis conforme estes forem atualizando seus *softwares* para as versões mais novas.

21 "Bitcoin Roundtable Consensus", disponível em: https://medium.com/@bitcoinroundtable/bitcoin-roundtable-consensus-266d475a61ff . Dos 38 os signatários, apenas 5 são indicados como "Bitcoin Core Contributors" (Cory Fields, Johnson Lau, Luke Dashjr, Matt Corallo e Peter Todd), e os demais, representantes de empresas de "mineração", *pools* de "mineração" e fabricantes de hardware.

ASICBoost – entre mineradores, fabricantes, desenvolvedores e patentes

No dia 10 de maio de 2016, o *ASICBoost* voltou à pauta da lista de discussão *bitcoin-dev* em uma mensagem de Peter Todd – "Making ASICBoost Irrelevant" – em alusão ao Acordo de Hong Kong: "As part of the hard-fork proposed in the HK agreement we'd like to make the patented AsicBoost optimisation useless, and hopefully make further similar optimizations useless as well. What's the best way to do this?"[22]

Nas mensagens e semanas por vir, seguiram-se especulações sobre como evitar, por meio de um *hardfork*, os impactos do *ASICBoost* e, mais ainda, sobre como patentes sobre as "tecnologias de consenso do Bitcoin" representavam uma ameaça à descentralização[23]. Propostas enviadas à lista por Hanke e Lerner passaram a ser vistas com alguma desconfiança[24], dada a suspeita de estarem associadas a interesses particulares ou atreladas a outras patentes do mesmo tipo. Também se especulava que o *ASICBoost* poderia ser uma "descoberta independente" de outras duas ou três partes, ao menos desde 2013, que também possuiriam patentes sobre ela em outros países[25]. Parte dos envolvidos sugeria que, como um gesto de confiança, a patente sobre o *ASICBoost* devia ser posta por Hanke e Lerner sob uma licença DPL[26].

É somente em abril de 2017 que várias dessas especulações e disputas convergem numa mesma narrativa. Embora se trate de um método matemático, para que

---

22 Peter Todd, "[bitcoin-dev] Making AsicBoost irrelevant", 10 de maio de 2016, disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-May/012652.html

23 Peter Todd, "Re: [bitcoin-dev] Drivechain proposal using OP_COUNT_ACKS", disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-October/013175.html

24 Btc Drak, "Re: [bitcoin-dev] About ASICBoost", 2 de outubro de 2016, disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-October/013184.html

25 Timo Hanke, "Re: [bitcoin-dev] Making AsicBoost irrelevant", 10 de maio de 2016, disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-May/012662.html ; e Sergio Demian Lerner, "[bitcoin-dev] About ASICBoost", 2 de outubro de 2016, disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-October/013178.html . A princípio Hanke e Lerner se referiam às patentes da antiga fabricante israelense de equipamentos de mineração Spondoolies-Tech (cf. https://patents.google.com/patent/WO2015077378A1/en registrada em 19 de novembro de 2013) e da fabricante chinesa Bitmain (cf. https://patents.google.com/patent/CN105245327A/en registrada em 21 de agosto de 2015).

26 A *Defensive Patent License*, uma licença livre de tipo *copyleft*, estipula que entidades que licenciem suas patentes sob a DPL o façam com todas as demais patentes que possuam, de modo que todas as entidades participantes do DPL gozem de acesso livre às patentes de mesmo tipo. Disponível em: https://defensivepatentlicense.org

o *ASICBoost* pudesse ser devidamente utilizado seria necessário que certos componentes de *hardware* fossem implementados junto aos processadores ASIC. A presença desses componentes podia ser constatada por meio da engenharia reversa de um *chip* de um certo fabricante (não especificado), segundo alegava o desenvolvedor Gregory Maxwell em uma mensagem enviada à lista *bitcoin-dev* na forma de um esboço de BIP (*BIP draft*). Identificado por ele como um tipo de "ataque" ou um método que explorava uma "vulnerabilidade" no protocolo do Bitcoin, Maxwell enfatizava os riscos que o *ASICBoost* poderia trazer para todo sistema – não apenas pelo método matemático que implementava, mas também por ser objeto de uma patente não licenciada para uso público, o que favoreceria a formação de monopólios:

> Exploitation of this vulnerability could result in payoff of as much as $100 million USD per year at the time this was written (Assuming at 50% hash-power miner was gaining a 30% power advantage and that mining was otherwise at profit equilibrium). This could have a phenomenal centralizing effect by pushing mining out of profitability for all other participants, and the income from secretly using this optimization could be abused to significantly distort the Bitcoin ecosystem in order to preserve the advantage.[27]

Dois dias depois, a empresa chinesa Bitmain, maior fabricante de ASICs para mineração, publicou em seu blog uma resposta às alegações de Maxwell, confirmando que sim, suas máquinas ASIC já traziam há algum tempo as modificações necessárias para implementar o *ASICBoost*, mas que, no entanto, eles não haviam comunicado seus clientes das modificações pois também eles não estariam utilizando o *ASICBoost* na *mainnet* do Bitcoin, apenas na *testenet*, por conta de questões legais com a patente:

> Our ASIC chips, like those of some other manufacturers, have a circuit design that supports ASICBOOST. However, the ASICBOOST method has not been used by us on the mainnet. We have not seen any evidence yet on the main net that anyone has used it in the patented way.[28]

---

27 Gregory Maxwell, "[bitcoin-dev] BIP proposal: Inhibiting a covert attack on the Bitcoin POW function", 05 de abril de 2017. Disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-April/013996.html

28 Bitmain, "Regarding Recent Allegations and Smear Campaigns", 07 de abril de 2017. Disponível em: https://blog.bitmain.com/en/regarding-recent-allegations-smear-campaigns

Ainda que os pesquisadores Timo Hanke e Sergio Lerner fossem os detentores da patente original[29], a patente chinesa equivalente ao método *ASICBoost* fora registrada pela própria Bitmain. Embora o *hardware* da Bitmain, utilizado em galpões próprios e vendido para clientes do mundo todo, estivesse habilitado para rodar o *ASICBoost*, a utilização deste método teria permanecido dormente por conta de questões legais e pelo "bem maior" do Bitcoin: "We can legally use it in our own mining farms in China to profit from it and sell the cloud mining contracts to the public. This, however profitable, is not something we would do for the greater good of Bitcoin."

Maxwell chamava atenção para os dois modos com que o *ASICBoost* podia ser empregado: um modo "evidente" (*overt*), facilmente identificável por outros pares da rede e motivo da maioria das discussões sobre o tema, e um modo "encoberto" (*covert*), que estaria, este sim, sendo utilizado por mineradores não só para maximizar seus lucros, como também para barrar implementações que viessem a eliminar essa possibilidade, como algumas daquelas que vinham sendo debatidas no âmbito da escalabilidade do sistema:

> "There are two major ways of exploiting the underlying vulnerability: One obvious way which is highly detectable and is not in use on the network today and a covert way which has significant interaction and potential interference with the Bitcoin protocol. The covert mechanism is not easily detected except through its interference with the protocol. In particular, the protocol interactions of *the covert method can block the implementation of virtuous improvements such as segregated witness* [*SegWit*]."[30]

Em seu comunicado, a Bitmain se defendia da acusação de promover um "ataque" ao Bitcoin dizendo que se tratava do uso de uma "otimização" com o intuito de reduzir o custo "J/GH" (joules por gigahash):

---

29 Como já apontado anteriormente, o nome *ASICBoost* e a menção à patente aparecem pela primeira vez na postagem pública de Timo Hanke, em 2016. Já a patente chinesa da Bitmain parece ter sido registrada em 2015 (vide nota 25). No entanto, de acordo com um artigo de maio de 2017 da Bitcoin Magazine, a requisição de Hanke junto ao PCT (International Patent System), que tem validade na China, dataria de 2013, o que lhe conferiria precedência e significaria que a Bitmain infringira a patente ao implementar os componentes necessários ao *ASICBoost* em seus *chips*. Vide: https://bitcoinmagazine.com/articles/bitmain-may-be-infringing-asicboost-patent-after-all

30 Gregory Maxwell, *cf.* nota 27. Ênfase minha.

> "There are better ways to resolve the issues that Gregory Maxwell's proposal seeks to address. Adversarial thinking is not the only way. We suggest working with the patent owners so that the patent could be used by the public. If all mining equipment could use ASICBOOST, it will lower the J/GH cost and the total network hash rate will increase, making the Bitcoin network even stronger. So, the ASICBOOST method is not a "covert attack" on the Bitcoin PoW function. It is an engineering optimization."[31]

Ao longo da série de disputas e acusações de cumplicidade com o esquema que favoreceria apenas algumas empresas e, na prática, constituiria um *lobby* para barrar "melhorias virtuosas", as posições do *grande debate* tornaram-se ainda mais polarizadas. Um mês antes da revelação de Maxwell, Sergio Lerner havia proposto na lista *bitcoin-dev* um novo cronograma de ativação do que chamou "SegWit2MB", combinando as propostas vigentes do Acordo de Hong Kong (um *hardfork* com aumento dos blocos) com a proposta de ativação do *SegWit* por meio de um *softfork*, ainda que distinta da proposta do *SegWit* original[32] Não por acaso, a nova proposta de Lerner é recebida com críticas, uma vez que a ativação do *SegWit* por esse método manteria possível o uso "encoberto" (*covert*) do *ASICBoost* – enquanto que a ativação por *softfork* da proposta original acabaria por eliminar essa possibilidade, permitindo apenas o uso "evidente" (*overt*) da otimização, entendido como "mais justo".

A proposta de Lerner, no entanto, é abraçada por vários representantes da "indústria bitcoin". Em maio de 2017, durante a conferência Consensus, realizada em Nova York, é estabelecido um novo acordo para a adoção do "*soft/hard-fork*" SegWit2MB nos próximos seis meses. Este acordo, também conhecido como "New York Agreement", é então assinado por "58 companhias de 22 países", que alegam ser responsáveis por mais de 4/5 de todo poder computacional do sistema Bitcoin ("83.28% of hashing power"), 5,1 bilhões de dólares em volume de transações e 20,5 milhões de carteiras Bitcoin[33]. Numa clara demonstração de força e, ironicamente, de centralização

31 Bitmain, *cf.* nota 28.

32 Sergio Lerner, "[bitcoin-dev] Segwit2Mb - combined soft/hard fork - Request For Comments", 31 de março de 2017, disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-March/013921.html

33 "Bitcoin Scaling Agreement at Consensus 2017", de 25 de maio de 2017, disponível em: https://medium.com/@DCGco/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77

de recursos, as partes envolvidas mobilizavam todo seu aparato de mineração para "sinalizar" a concordância com essa posição[34].

Novamente, a complexidade dos eventos excede o escopo deste artigo. Para manter o foco nos desdobramentos da controvérsia do *ASICBoost*, cabe dizer apenas que o Acordo de Nova York não foi levado a cabo: em julho de 2017, diante da iminente ativação do *SegWit* via *softfork* e sem que a contraproposta de extensão dos blocos para 2MB obtivesse a mesma adesão consensual, parte da comunidade e representantes da "indústria bitcoin", em especial a gigante Bitmain, decidiram apoiar um *hardfork* que deliberadamente criaria uma nova criptomoeda (e, portanto, uma nova rede) com blocos de 8MB antes da ativação do *SegWit*. A divisão ocorreu em 1º de agosto de 2017, dando origem à criptomoeda "Bitcoin Cash", fazendo com que parte do "hashing power" migrasse da rede Bitcoin e produzindo uma série de outras repercussões no ecossistema. Finalmente, em novembro, o *hardfork* que implementaria o aumento dos blocos previsto no novo acordo foi então cancelado por conta da "falta de consenso".

Se, até então, a grande preocupação de parte da comunidade era com os "riscos de centralização" que uma otimização como o *ASICBoost* oferecia para o sistema, ao longo do ano de 2018 um "cenário alternativo de descentralização", como aquele imaginado por Mustafa Al-Bassam, começa a se desenhar. Em março de 2018, em vez de insistir na patente "exclusiva" do *ASICBoost*, a Little Dragon LLC, empresa para quem Hanke havia vendido sua patente ainda em 2017, opta por licenciar a otimização nos termos da patente "defensiva" BDPL[35] e "abrir o *ASICBoost* para uso defensivo", condenando o método *covert* e defendendo a viabilidade do método *overt* na redução de custos e na promoção da "descentralização":

> We have strong reason to believe that some manufacturers of mining equipment have been secretly using this covert method to evade detection by the patent holder and gain unfair advantage over others

34 Definido pelo BIP 009 ("Version bits with timeout and delay", de outubro de 2015), a noção de *signaling* parte da ideia de que mineradores podem utilizar determinados *bits* dos blocos que produzem para sinalizar a concordância ou não com uma dada proposição, como um "voto", ou como uma forma de expressar maioria por contraste sobre determinada posição num dado intervalo de tempo.

35 A *Blockchain Defensive Patent Licence* (BDPL) – https://blockchaindpl.org – surge como uma especificação da DPL para "tecnologias *blockchain*" *copyleft*, isto é, adaptada para os usos da indústria das criptomoedas. A ideia de "defesa" se expressa tanto contra disputas empresariais, quanto contra a crescente ofensiva de "*patent trolls*", pessoas ou instituições que buscam registrar patentes sobre tecnologias de domínio público para obter lucro ou provocar interferências.

> but not revealing what they were doing, and without making it known to the patent holders. Conversely, version-rolling [*overt*] method of AsicBoost is completely transparent in the blockheader of each boosted Bitcoin block. (…) We believe AsicBoost is such an important an innovative patent that, if licensed defensively, can become a force for good to protect decentralization in Bitcoin. At this point, it is clear that covert AsicBoost does not serve the interests of Bitcoin due to the negative incentives outlined, however, version-rolling AsicBoost has none of these drawbacks, and is additionally more efficient than covert merkle grinding. No matter how efficient a mining machine is made at hardware level, version-rolling AsicBoost will always deliver more efficiency when done correctly. If this method of version-rolling is used by a large portion of the hash-rate, there may be no escaping the need for all mining equipment manufacturers to use it to remain competitive.[36]

Com a mudança de licenciamento, fabricantes concorrentes, como a chinesa Halong Mining, passaram a aderir à "comunidade BDPL"[37], licenciando sua propriedade intelectual nos mesmos termos. Outras empresas, como a Braiins, associada à Slush Pool, anunciaram em outubro de 2018 um sistema operacional livre, baseado em Linux, que pode ser instalado nos ASICs da maioria dos fabricantes (Bitmain, Halong Mining e outros), substituindo o software padrão e permitindo a ativação irrestrita da modalidade *overt* do ASICBoost em qualquer máquina suportada a fim de aumentar sua produtividade[38].

Com isso, o paradoxo do *ASICBoost*, por enquanto, se estabiliza: inicialmente anunciado como uma melhoria a ser implementada para a redução de custos, mas também objeto de uma patente controversa, foi encarado como um vetor de centralização que poria em risco a participação no sistema Bitcoin e favoreceria o surgimento de monopólios com o poder de influenciar decisões técnicas e alterações substanciais nas regras de consenso. Por outro lado, e ao longo de uma série de

---

36 "Opening AsicBoost for Defensive Use", 1º de março de 2018, disponível em: https://www.asicboost.com/single-post/2018/03/01/opening-asicboost-for-defensive-use/

37 Halong Mining, "BDPL Offering Announcement", 6 de março de 2018, disponível em: https://halongmining.com/blog/2018/03/06/bdpl-offering-announcement/

38 Braiins, "Introducing Braiins OS, open-source system for cryptocurrency devices", 22 de setembro de 2018, disponível em: https://medium.com/@braiins_systems/braiins-os-introduction-45c545d13d51 . Ver tambem: https://braiins-os.org

complexas disputas, conforme se encaminhava para um licenciamento público em termos “copyleft”, a possibilidade de utilização do *ASICBoost* passou a operar como um vetor de descentralização, abrindo espaço para outras iniciativas e novos participantes.

Tensões topológicas – considerações futuras sobre especialização e disputas

Os mineradores têm se tornado, nos últimos anos, um grupo cada vez mais especializado tecnologicamente, posto que a dificuldade dos métodos de validação aumenta em função do tamanho da rede e do volume de transações, exigindo maiores investimentos em energia e *hardware* dedicado. As implicações geopolíticas da formação desses aglomerados especializados – a maior parte deles localizados na China, sudeste asiático e em países da América do Sul, como o Paraguai e a Venezuela – vão desde a questão da regulação estatal desses empreendimentos, do *status* legal das criptomoedas sob a jurisdição de cada país, até os efeitos práticos dessa polarização na criação de mercados especializados para produção e comercialização de *hardware* dedicado (ASICs).

Há, assim, uma constante tensão entre os diferentes grupos de atores da rede sobre os direcionamentos e mudanças que intentam implementar. Uma noção de “governança distribuída” parece então imanente: embora a rede de computadores seja descentralizada, isso não evita os efeitos diretos de adensamentos de poder computacional, como é o caso dos conglomerados de mineradores, e de outros pontos centralizadores, como as grandes *exchanges* (casas de câmbio digital), “baleias” (usuários com enorme quantidade de moedas ou recursos, capazes de influenciar diretamente os preços de mercado), veículos de mídia e políticas de estado[39]. Também dentro dos círculos de desenvolvimento e implementação de software, a tendência de

39 A questão da regulamentação estatal das criptomoedas e seu *status* legal é um assunto delicado e ainda nebuloso na maioria dos países. Na maioria dos casos, as criptomoedas são definidas não como “moeda”, mas como um tipo especial de “ativos” financeiros. No Brasil, tramita desde 2015 o projeto de lei 2303/2015 que visa criar uma legislação específica para a negociação de criptomoedas. Em 2014, um parecer do Banco Central (BC) reforçava o *status* de “ativo digital” e alertava sobre os altos riscos de investimentos em um mercado sem regulamentação central. Já a Comissão de Valores Mobiliários (CVM), em Ofício Circular nº 1/2018/CVM/SIN, instada por “diversos participantes de mercado”, interpreta que “as criptomoedas não podem ser qualificadas como ativos financeiros” e, portanto, não têm a aquisição direta permitida por fundos de investimentos regulados. O ofício da CVM ressalta, tal como o parecer do BC, os riscos de segurança digital e a possível restrição e criminalização previstas no PL 2303/2015.

centralização, se não do comando das atividades, se dá pela especialização técnica necessária, o prestígio e o envolvimento com a comunidade.

A tensão que atravessa todo ecossistema, presente nas narrativas, preocupações e motivações dos diversos atores, se dá principalmente entre vetores identificados por eles como *centralizadores* e *descentralizadores*. Parece haver uma imbricação entre duas dimensões de um mesmo fenômeno: do ponto de vista das máquinas e dos pares (*nodes*) que constituem a rede, o sistema Bitcoin opera numa rede distribuída que assegura a viabilidade de transações nos termos de um rígido protocolo de comunicação. Porém, do ponto de vista dos demais atores – usuários, desenvolvedores, mineradores, fabricantes, analistas, prestadores de serviços, etc. – que constituem o chamado *ecossistema*, a rede é percebida a partir de uma topologia maleável que parece oscilar entre o ideal de distribuição (uma rede *peer-to-peer* totalmente planificada) e um acoplamento de associações hierarquizadas que se assemelham a uma organização mais ou menos descentralizada. Essas percepções favorecem organizações políticas distintas e concorrentes, sujeitas à correlação de forças que operam como vetores de transformação topológica nos termos das topologias clássicas da ciência da computação: redes "centralizadas", "descentralizadas" e "distribuídas" (BARAN, 1964).

Ao longo da descrição, procurei evidenciar os meios de comunicação e construção de consenso utilizados no desenvolvimento do Bitcoin: as listas de e-mails e a plataforma colaborativa Github, que hospeda toda a base de código do projeto. Além destes, ressalto os meios de produção coletiva, de proposição e de deliberação, em especial o uso de documentos no formato nativo BIP e a lógica da submissão de correções e melhorias empregadas no âmbito do desenvolvimento de projetos de *software*. Por fim, uma série de expedientes controversos favorecem associações e rupturas, como os acordos firmados entre diferentes atores e grupos, a mobilização de recursos computacionais na sinalização de posicionamentos ou maximização de dividendos, *lobbies*, as patentes "defensivas" e o artifício dos *softforks* e *hardforks* para implementação de mudanças substanciais no protocolo. Estas e outras relações constituem os meios e processos específicos com que se articulam os procedimentos sociotécnicos de produção de consenso e governança digital de um projeto colaborativo tão heterogêneo como o Bitcoin.

Referências bibliográficas

ANTONOPOULOS, Andreas M. *Mastering Bitcoin: Unloking digital cryptocurrencies*. Sebastopol, CA: O'Reilly, 2015.

ANTONOPOULOS, Andreas M. *The Internet of Money*. [S.l.]: Merkle Bloom LLC, 2016.

BARAN, Paul. On Distributed Communications Networks. *IEEE Transactions of the Professional Technical Group on Communications Systems*, jan. 1964.

DE VRIES, Alex. Bitcoin's Growing Energy Problem. *Joule*, v. 2, n. 5, p. 801–805, maio 2018.

FINN, Ed. *What Algorithms Want: Imagination in the Age of Computing*. [S.l.]: The MIT Press, 2017.

HANKE, Timo. AsicBoost - A Speedup for Bitcoin Mining. *arXiv:1604.00575 [cs]*, arXiv: 1604.00575, 2 abr. 2016. Disponível em: <http://arxiv.org/abs/1604.00575>. Acesso em: 30 out. 2018.

KELTY, Christopher. Collaboration, Coordination, and Composition: Fieldwork after the Internet. *Fieldwork Is Not What It Used to Be: Learning Anthropology's Method in a Time of Transition*. [S.l.]: Cornell University Press, 2009. . Disponível em: <http://www.jstor.org/stable/10.7591/j.ctt7zfjh.13>.

LAMPORT, Leslie; SHOSTAK, Robert; PEASE, Marshall. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, v. 4/3, p. 382–401, 1982.

LATOUR, Bruno. *Reagregando o Social: uma introdução a Teoria do Ator-Rede*. Tradução Gilson César Cardoso De Sousa. Salvador/Bauru: Edufba/Edusc, 2012.

MORA, Camilo *et al.* Bitcoin emissions alone could push global warming above 2°C. *Nature Climate Change*, v. 8, n. 11, p. 931–933, 1 nov. 2018.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>.

NARAYANAN, Arvind *et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. [S.l.]: Princeton University Press, 2016.

VENTURINI, Tommaso. Building on faults: How to represent controversies with digital methods. *Public Understanding of Science*, v. 21, n. 7, p. 796–812, out. 2012.

VENTURINI, Tommaso. Diving in magma: how to explore controversies with actor-network theory. *Public Understanding of Science*, v. 19, n. 3, p. 258–273, maio 2010.

VENTURINI, Tommaso; LATOUR, Bruno. *The Social Fabric: Digital Traces and Quali-Quantitative Methods*. [S.l: s.n.], 2010.

WOLPERT, David. *Why Do Computers Use So Much Energy?* Disponível em: <https://blogs.scientificamerican.com/observations/why-do-computers-use-so-much-energy/>. Acesso em: 13 out. 2018.