Algoritmos como "máquinas de cultura": Notas sobre política e produção de consenso no sistema *peer-to-peer* Bitcoin

Bruno Campos Cardoso[1]

Resumo: Em operação desde 2009, o Bitcoin é a primeira criptomoeda em circulação e implementa um protocolo para trocas de valores eletrônicos por meio de métodos criptográficos em uma rede distribuída (*peer-to-peer*). O sistema Bitcoin consiste em um complexo global de máquinas, técnicas computacionais e atores humanos associados em comunidades e mercados de tipo descentralizado. A produção coletiva do "consenso distribuído" sobre as movimentações e balanços da rede se baseia em algoritmos, no emprego de máquinas de alto poder computacional, e na atuação de programadores e usuários em uma rede de trocas transnacionais que dispensa autoridades reguladoras centrais. Neste artigo trago alguns apontamentos sobre a política e a produção de consenso no sistema *peer-to-peer* Bitcoin. Para isso, inicio com uma descrição geral do funcionamento do sistema, enfatizando sua topologia descentralizada/distribuída e parte do aparato tecnológico que o constitui. Pretendo trazer à tona alguns elementos da "produção de consenso" entre as máquinas desse sistema de dinheiro eletrônico para descrevê-los sob a perspectiva dos algoritmos como "máquinas de cultura", isto é, procuro pensar os algoritmos não como artefatos *da* cultura, mas sim *como* cultura, como arranjos sociotécnicos, múltiplos e instáveis, entre humanos e não-humanos, efetuados por séries de práticas computacionais e, no caso do Bitcoin, por meio da implementação de políticas econômicas muito específicas.

Palavras-chave: algoritmos; redes distribuídas; mercados; antropologia; economia.

[1] Doutorando em Antropologia Social (PPGAS-UFSCar) e mestre em Antropologia (PPGA-UFPR). Participa do Laboratório de Experimentações Etnográficas (LE-E) e do Grupo de Estudo e Pesquisa sobre Relações de Poder, Conflitos, Socialidades (HYBRIS). E-mail: cardoso.bc@gmail.com

Introdução

Os apontamentos aqui presentes fazem parte da minha pesquisa de doutorado sobre o que venho chamando de "política dos algoritmos" a partir de uma etnografia dessas formas de dinheiro eletrônico que ficaram conhecidas como *criptomoedas*.[2] Em especial, tenho voltado minha atenção para o sistema *peer-to-peer* Bitcoin, que é a primeira e a maior criptomoeda em operação. O Bitcoin e as criptomoedas começaram a aparecer na mídia há alguns anos, principalmente ao longo do segundo semestre do ano retrasado, por conta da oscilação de preço que fez 1 bitcoin valer quase 20 mil dólares em meados de dezembro de 2017. A grande volatilidade do preço é uma das características dos mercados de criptomoedas, que têm sido descritas tanto como *formas de dinheiro digital* quanto como uma *nova classe de ativos financeiros*.

Em minha pesquisa, tenho abordado o Bitcoin e as outras criptomoedas a partir de uma perspectiva dupla: por um lado, tenho pensado as criptomoedas como um *objeto técnico*, como um software livre que é produzido coletivamente em plataformas públicas de desenvolvimento e que envolve o trabalho coletivo de muitos programadores de várias partes do mundo, sejam eles anônimos ou não. Há também todo o ecossistema de desenvolvimento de softwares, aplicativos e serviços que se conectam de alguma maneira com esses sistemas, bem como uma indústria especializada na produção de *hardware* dedicado às exigências computacionais dessas redes.

Por outro lado, tenho pensado as criptomoedas como um *objeto financeiro*, que circula em comércios, mercados digitais, corretoras, e que é muitas vezes objeto de especulação e outras atividades nem sempre lícitas, além de possuir um *status* legal bastante ambíguo na maioria dos países. *Grosso modo*, as criptomoedas têm sido enquadradas pelas agências reguladoras como uma *nova classe de ativos financeiros*. O que costuma escapar aos modelos regulatórios tradicionais é que esses novos objetos financeiros circulam em redes de tipo distribuído (P2P), em que a politica de emissão monetária e os protocolos de comunicação entre os pares da rede são definidos por algoritmos criptográficos e pela produção maquínica do que é chamado de "consenso emergente" sobre o estado de uma rede que opera sem intermediários e sem autoridades centrais. Tudo isso

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

torna mais difícil e virtualmente até impossibilita a regulação tal como se faz com outros ativos e *commodities*. Mas essa é uma questão que segue sob disputa e tem sido motivo de intensas controvérsias.

Nos últimos meses eu tenho feito um levantamento bibliográfico do que tem sido produzido sobre criptografia e criptomoedas – livros, artigos acadêmicos, artigos não-acadêmicos – e também tenho pesquisado os arquivos de e-mails de listas públicas de desenvolvedores e fóruns de discussão. Mais recentemente eu tenho voltado minha atenção para o repositório de código da implementação de referência do Bitcoin, que está hospedada na plataforma pública Github[3]. Como se trata de uma plataforma de controle de versão, é possível acompanhar os processos de desenvolvimento e o histórico de todas as alterações, bem como os debates sobre correções de *bugs* e implementações de melhorias no sistema. Com isso procuro entender melhor o funcionamento desses procedimentos técnicos e os arranjos inovadores que culminaram na montagem – e constante transformação – do *software* Bitcoin.

Pretendo, nas páginas que seguem, chamar a atenção para os imbricamentos da dimensão técnica com a dimensão financeira nesse sistema de dinheiro eletrônico. Para isso trago como exemplo um dos algoritmos que é responsável, ao mesmo tempo, pela política de emissão deflacionária do Bitcoin e pelos subsídios ou incentivos econômicos que estão atrelados ao processo de validação de transações, que é chamado de *mineração*. Além de ser o procedimento responsável pela validação de transações e pela emissão de novas moedas, a *mineração* tem como objetivo assegurar e fazer cumprir as "regras de consenso"[4] do sistema por meio do investimento de poder computacional na produção de "provas criptográficas".

Panorama: *Genesis,* estruturas de dados & topologias de rede

3 de janeiro de 2009. O jornal britânico *The Times* estampava a seguinte manchete: "Chanceler à beira do segundo resgate aos bancos". O nome do jornal, a data e o título

[3] https://github.com/bitcoin/bitcoin/

[4] Por "regras de consenso" me refiro às definições elementares das estruturas de dados e dos protocolos de comunicação implementados. São essas regras que definem o comportamento do sistema. Se um software implementa regras diferentes ou contraditórias, a comunicação é invalidada pelos demais pares da rede, ou pode ocasionar o surgimento de uma rede paralela, onde essas novas regras são "consensuais".

estão inscritos no primeiro bloco de transações do sistema Bitcoin, que passou a ser chamado de bloco *Genesis*. A referência à manchete do jornal é tanto uma prova de que este bloco não podia ter sido criado antes dessa data, quanto uma referência crítica à crise financeira internacional de 2008 e seus desdobramentos.

O bloco *Genesis* é diferente de todos os blocos subsequentes da *blockchain*, ou corrente de blocos, que é a principal estrutura de dados do sistema, responsável pelo registro sequencial de todas as transações realizadas. Logo abaixo da manchete do *The Times*, o bloco *Genesis* registra a primeira transação: as primeiras 50 moedas são criadas *ex nihilo* e são então movidas para um endereço que se supõe pertencer a Satoshi Nakamoto.

Satoshi Nakamoto é o criador da primeira implementação do Bitcoin, anunciada por ele dois meses antes, em novembro de 2008, numa lista de e-mails sobre criptografia, onde ele publica um *paper* de nove páginas descrevendo como viria a funcionar seu sistema de dinheiro eletrônico (NAKAMOTO, 2008)[5]. No dia 9 de janeiro de 2009, seis dias após o *Genesis*, ele anuncia nessa mesma lista de e-mails a primeira versão funcional do software e publica também seu código-fonte[6]. Vários dos usuários da lista começam a rodar o software em suas máquinas e passam a discutir sobre ele.

A rede segue em operação desde então. Satoshi Nakamoto desaparece no final de 2010, sem deixar rastros e sem nunca ter movido nenhuma das outras centenas de milhares de moedas que se supõe pertencer a ele (ou a eles, ou a elas), tendo legado sua criação à comunidade de desenvolvedores.

O que nos primeiros anos era uma rede distribuída e experimental, mantida apenas por computadores domésticos e pequenas instalações de entusiastas, *hackers*, cientistas da computação e *cypherpunks*, tornou-se uma indústria bilionária em escala global. O *ecossistema* do Bitcoin – como muitos dos participantes costumam se referir às redes sociotécnicas que o constituem – diz respeito não somente aos programadores e desenvolvedores que contribuem com a elaboração coletiva deste projeto de software livre, mas também com a formação de mercados em torno desse fenômeno: serviços e sistemas de pagamento, corretoras (*exchanges*), lojas e comunidades virtuais, associações jurídicas[7],

[5] A primeira mensagem de Satoshi Nakamoto pode ser lida em: https://www.mail-archive.com/ cryptography@metzdowd.com/msg09959.html.

[6] A mensagem pode ser lida em: https://www.mail-archive.com/cryptography@metzdowd.com /msg10142.html.

[7] Há, no Brasil, duas associações, criadas ao longo do ano de 2018, voltadas para o setor de criptomoedas: a Associação Brasileira de Criptomoedas e Blockchain (ABCB) e a ABCripto, que reúnem, em sua maioria, representantes

e toda uma indústria multinacional especializada na produção de *hardware* dedicado ao processo de *mineração* de criptomoedas.

A rede conta hoje com mais de 10 mil nós completos (*full nodes*) espalhados pelo mundo, que são máquinas que replicam e atualizam cópias locais de todo registro de transações, a *blockchain*[8]. Além dos *full nodes*, há uma variedade de outros pares que não possuem cópias completas da *blockchain* (chamados *light nodes*), mas que se utilizam dessas cópias como referência em suas operações (como aplicativos de celular, carteiras digitais, corretoras e serviços de pagamento). O sistema Bitcoin comporta hoje algo em torno de 200 mil a 350 mil transações diárias (ou de 2 a 4 transações por segundo)[9], que são anunciadas na rede e, a cada dez minutos, são agrupadas e validadas em novos blocos de transação. Esses novos blocos são replicados e anexados às cópias locais da *blockchain*. Tudo o que está registrado na *blockchain* é considerado pelos pares como um fato consolidado e irreversível. Portanto, a *blockchain* é o registro consensual distribuído sobre todas as transações que já aconteceram no sistema. Do ponto de vista das máquinas da rede, tudo o que está na *blockchain* é verdadeiro e imutável – e o que está fora dela, não existe[10].

Essa estrutura de dados compartilhada só pode ser modificada pela constante adição de novos blocos ao final da corrente – nenhum bloco anterior pode ser modificado sem que se rompa a integridade corrente, o que é verificável por uma série encadeada de provas criptográficas. Mais ainda, "escrever" na *blockchain*, ou seja, agrupar e validar novas transações em blocos, é um procedimento extremamente custoso, tanto computacionalmente, quanto energeticamente, pois os incontáveis ciclos computacionais exigidos

de corretoras nacionais e outros "players do mundo dos criptoativos", em diálogo com setores do mercado financeiro e instituições reguladoras, como o Banco Central do Brasil (BACEN), a Comissão de Valores Mobiliários (CVM), e o Conselho Administrativo de Defesa Econômica (CADE).

8 Tal registro, chamado *ledger* ou *blockchain* (corrente de blocos), é a estrutura de dados que funciona como um livro-caixa de todas as transações do sistema. Sua principal característica é ser imutável (nenhum registro anterior pode ser editado) e *append-only* (os novos dados são inseridos em série, mas nunca removidos ou alterados), isto é, as novas entradas (blocos de transações) são sempre adicionadas ao final da corrente e têm como referência os valores registrados anteriormente. A consistência dos dados é frequentemente verificada por procedimentos criptográficos e replicação assíncrona da informação.

9 Essa é uma estimativa baseada na densidade de transações por bloco nos últimos meses. Melhorias de software introduzidas nos últimos anos têm aumentado a capacidade dos blocos, que possuem um tamanho máximo preestabelecido, por meio de otimizações e flexibilizações das estruturas de dados das transações. Dados e gráficos sobre o estado atual do sistema podem consultados em https://statoshi.info.

10 Uma exceção é a *mempool*: antes de serem validadas (ou rejeitadas), agrupadas em blocos e encadeadas de modo definitivo à *blockchain*, as transações anunciadas pelos pares da rede são acumuladas numa *memory pool*, outra estrutura de dados que reúne todas as transações pendentes (isto é, à espera de validação e confirmação), ordenadas em função das taxas de transação – transações que pagam taxas maiores ganham prioridade na composição dos próximos blocos.

dependem do constante consumo de energia elétrica. É somente por meio desse procedimento técnico, chamado "prova de trabalho" (*proof of work*), que os participantes que dispõem de vastos recursos computacionais, conhecidos como *mineradores*, competem entre si para, a cada dez minutos, criar um bloco de transações por meio da resolução adequada de um enigma criptográfico.

Esse enigma criptográfico só pode ser resolvido pelo método da força bruta, testando diferentes possibilidades numéricas uma a uma. Os *mineradores*, portanto, estão sempre competindo entre si para encontrar essa solução antes dos outros – quanto mais poder computacional investido, maiores as chances de encontrar uma solução em tempo hábil. Esse procedimento tem como objetivo assegurar a validade do registro, pois é inviável tentar alterá-lo ou adulterá-lo (o que implicaria a alteração, computacionalmente custosa, de toda uma série de dados encadeados), e também institui um sistema de incentivo econômico para os *mineradores* que criam blocos válidos, uma vez que as novas moedas que são criadas a cada bloco, bem como a soma de todas as taxas das transações validadas naquele bloco, são transferidas para o *minerador* que o criou.

A dificuldade dos métodos de validação aumenta em função do tamanho da rede e do volume de transações que são realizadas. Um algoritmo de "ajuste de dificuldade", a cada duas semanas, regula a oferta de poder computacional (chamada *hash rate*) para que os novos blocos sejam produzidos, em média, a cada 10 minutos. Dado o incentivo econômico a esse esforço coletivo de validação (de transações e das regras de consenso), os *mineradores* tornaram-se, nos últimos anos, agrupamentos altamente especializados. Atualmente, o aparato tecnológico necessário (máquinas ASIC) e os custos com energia elétrica e manutenção das máquinas e instalações tornou inviável, tanto computacional quanto economicamente, a participação de usuários domésticos nesse processo, o que era comum nos primeiros anos do sistema. Empresas especializadas na produção industrial de ASICs e instalações conhecidas como *mining farms* (galpões com centenas ou milhares dessas máquinas rodando ininterruptamente) têm se instalado em países da América do Sul (Paraguai e Venezuela), no sudeste asiático e principalmente na China (que também produz a maioria componentes de *hardware* necessários), onde os custos energéticos e operacionais possibilitam uma margem de lucro razoável.

A superespecialização dos *mineradores* é motivo de controvérsias entre os diferentes agrupamentos da rede[11]. Ainda que o sistema Bitcoin opere sob uma lógica distribuída,

[11] Em trabalho apresentado na 31ª Reunião Brasileira de Antropologia (2018), descrevo alguns dos aspectos relativos à produção desses componentes conhecidos como ASICs (*Application-Specific Integrated Circuits*), bem como

nota-se a formação de adensamentos ou regiões de centralização, tanto por conta da concentração de poder computacional nas mãos de poucas empresas, quanto pelo domínio da oferta de serviços, como é o caso das grandes *exchanges* (corretoras digitais), que são a porta de entrada para a maioria dos usuários e, por isso, responsáveis pela operação de parte significativa das transações efetuadas na rede. No âmbito do desenvolvimento de software, a *expertise*, o prestígio e o envolvimento com a comunidade de desenvolvedores são também fatores que favorecem a especialização de grupos de programadores e influenciam decisões sobre a implementação de melhorias ou alterações nas regras de consenso do sistema. Novamente, embora as máquinas operem de acordo com protocolos de comunicação distribuída, as topologias das redes de relações do ecossistema são maleáveis e parecem oscilar entre configurações mais ou menos descentralizadas, de modo que "centralização" e "descentralização" são metáforas ou adjetivos que podem ser aplicáveis em muitas partes diferentes do sistema (GOLUMBIA, 2016).[12]

Ao definir estruturas de dados específicas – modalidades de transação, blocos de transação, a corrente de blocos – e protocolos estritos de comunicação entre os pares da rede, essas estruturas de dados são mobilizadas em função de procedimentos sociotécnicos complexos e possibilitam modalidades de comunicação, transação e cálculo que são aceitas por todos os participantes. "The result", explica Satoshi Nakamoto em uma mensagem, "is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending"[13]. A principal invenção de Satoshi Nakamoto, de acordo com Andreas Antonopoulos, é esse mecanismo descentralizado de *consenso emergente*: "Emergent, because consensus is not achieved explicitly – there is no election or fixed moment when consensus occurs. Instead, consensus is an emergent artifact of the asynchronous interaction of thousands of independent nodes, all following simple rules" (ANTONOPOULOS, 2015: 177).

as controvérsias sobre centralização, disputas de patentes e os debates de desenvolvedores da implementação de referência do Bitcoin sobre possíveis alterações nos protocolos de consenso que poderiam inviabilizar sua utilização.

[12] Baseio-me, aqui, na divisão clássica proposta por Paul Baran (1964) dos três tipos topológicos de redes computacionais: centralizadas (um servidor, vários clientes), descentralizadas (vários servidores, vários clientes) e distribuídas (todos os pares da rede são simultaneamente servidores e clientes), a que posteriormente se convencionou chamar *peer-to-peer* (P2P), um tipo de topologia planificada e *ad hoc*. Em uma topologia *peer-to-peer*, a partir das conexões circunstanciais estabelecidas entre os pares, forma-se uma ampla rede de múltiplos caminhos comunicação e replicação de informação. Uma vez que não há servidores centrais, essa topologia é notadamente mais robusta e flexível que as demais, ao custo de um aumento de complexidade dos protocolos de comunicação.

[13] Mensagem de 11 de fevereiro de 2009. Disponível em: http://p2pfoundation.ning.com/forum/topics/ bitcoin-open-source.

Algoritmos como "máquinas de cultura": implicações políticas e econômicas de configurações algorítmicas

Michel Callon e Fabian Muniesa (2005) desenvolvem a ideia de "configurações algorítmicas" para descrever mercados econômicos como dispositivos coletivos de cálculo. A noção de cálculo não se restringe ao cálculo matemático ou numérico, mas se refere ao estabelecimento de distinções entre coisas e estados do mundo, bem como à imaginação, ao estabelecimento de cursos de ação sobre essas coisas e estados, e suas consequências (ou seja, o cálculo é entendido como *calculação*). Dispositivos de cálculo podem coabitar um mesmo espaço de cálculo, podem ser superpostos ou podem entrar em oposição. O "poder calculativo" de um dispositivo (ou sua calculabilidade) diz respeito à sua capacidade de mobilizar e listar o maior número possível de entidades, relações entre entidades, variações dessas relações e suas configurações, bem como dispor de ferramentas classificatórias efetivas e flexíveis. Isto é, sua calculabilidade depende dos arranjos qualitativos ou quantitativos que possibilitam ou impossibilitam o cálculo. Callon e Muniesa argumentam que a noção de "cálculo econômico" não seria uma "ficção antropológica" precisamente por que *não é* puramente uma competência humana, mecânica ou mental: a *calculação* está distribuída entre atores humanos e dispositivos materiais. Portanto, algoritmos não podem ser descritos ou definidos apenas de modo abstrato, uma vez que dependem de condições e limites materiais de execução.

Sob essa perspectiva, configurações algorítmicas são arranjos sociotécnicos dos quais dependem os mercados, uma vez que circunscrevem, identificam e enumeram grupos de "agências calculativas". Elas organizam encontros e conexões entre pares, e estabelecem regras, convenções e protocolos sobre essas conexões. Cada mercado corresponde, então, a um modo particular de organização, conexão e *calculação*. Assim como argumenta Philip Mirowski (2002; MIROWSKI; SOMEFUN, 1998), os objetos de estudo da economia não são (apenas) seres humanos, mas principalmente máquinas econômicas ou "máquinas algorítmicas" que operam como dispositivos coletivos de cálculo. De acordo com Mirowski, é no interior de um ecossistema diverso, de múltiplas formas de agentes e culturas, que os mercados calculam e evoluem em complexidade (1998: 343). E cada vez mais, como também argumenta Donald MacKenzie, os próprios mercados financeiros e a maioria de seus atores *são* algoritmos (MACKENZIE, 2014).

Para ilustrar esse ponto, trago o exemplo do algoritmo responsável pela *política de emissão deflacionária de moedas* do sistema Bitcoin, que está atrelada aos subsídios

da *mineração*. Esse procedimento faz parte de um conjunto de outros procedimentos que implementam e asseguram o cumprimento das "regras de consenso" do sistema. A política monetária de emissão de moedas e de subsídios está definida, no código-fonte, por um algoritmo de apenas 11 linhas[14]. Como todo bom algoritmo, sumário e explícito (KNUTH, 1997: 4-6), enuncia que a quantidade de moedas criadas por bloco (o *subsídio* da *mineração*) é inicialmente de 50 moedas, e que a cada 210000 blocos (aproximadamente quatro anos), essa quantidade deve ser reduzida pela metade. Assim, nos primeiros quatro anos de funcionamento do sistema, foram criadas 50 moedas a cada dez minutos (10,5 milhões de moedas). Nos quatro anos seguintes, 25 moedas a cada dez minutos (5,25 milhões). Atualmente, a cada dez minutos são criadas 12,5 moedas por bloco. Eventualmente, por volta do ano 2140 e muito próximo do teto preestabelecido de 21 milhões de moedas, o subsídio dos blocos será igual a zero, restando apenas a soma das taxas das transações validadas por bloco como incentivo econômico aos *mineradores*. Esta é a principal regra de consenso do sistema.

Tomando o algoritmo apenas como a descrição abstrata de um processo de emissão de moedas, vemos que ele descreve uma curva assintótica que tende a um limite finito, o que também poderia ser descrito como um processo de *escassez*: ao longo do tempo, a quantidade que é produzida (ou extraída) diminui (daí, portanto, a origem da analogia do procedimento técnico da *mineração* com a mineração de metais)[15]. Tal performatividade do sistema é percebida por usuários e entusiastas como *deflacionária*. No entanto, essa percepção não está restrita à descrição formal do algoritmo enquanto *código-fonte*, mas aos efeitos da sua implementação enquanto um dispositivo distribuído de cálculo ("o sistema P2P Bitcoin"). Trata-se de perguntar, então, qual é performatividade de um objeto *tecnofinanceiro* percebido como "deflacionário" e "distribuído", em função de sucessivos procedimentos de escrita (transações e provas criptográficas) e procedimentos de propagação de estruturas de dados em um espaço que não se pretende um mercado *per se*, mas sim um sistema de dinheiro eletrônico em um arranjo de múltiplos mercados (locais e globais), máquinas (virtuais e materiais), plataformas, algoritmos e pessoas.

[14] O algoritmo está definido em um dos vários arquivos do código-fonte da implementação de referência do Bitcoin: https://github.com/bitcoin/bitcoin/blob/cbe7efe9ea6c14a3649d3e10f5f18d2097ebef74/src/validation.cpp#L1152-L1163.

[15] Satoshi Nakamoto explicita essa analogia em seu *paper*: "The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended" (NAKAMOTO, 2008: 4).

A noção de "máquinas de cultura" é desenvolvida por Ed Finn (2017) para descrever como algoritmos – arranjos complexos de abstrações, processos e pessoas – implementam conceitos do "espaço idealizado da computação" na realidade material do cotidiano (: 2). Para ele, algoritmos executam ideias teóricas em instruções pragmáticas, mantendo sempre uma lacuna entre ambos nos detalhes da implementação (*idem*). Ao contrário de formulações que estabelecem uma distinção entre técnica e cultura, onde algoritmos *modelam* a cultura e, por sua vez, são modelados por ela – o que Nick Seaver (2017) denomina de abordagem "algoritmos *na* cultura" – as noções de "máquinas de cultura" e de "configurações algorítmicas" não reificam divisões entre dimensões técnicas e não-técnicas, pois as combinam. Nesse sentido, algoritmos não são objetos técnicos singulares em diferentes interações culturais, mas sim objetos instáveis culturalmente executados pelas práticas das pessoas que se engajam com eles: algoritmos *são* cultura porque são compostos de práticas humanas coletivas (: 5).

Mas se algoritmos implementam ideias teóricas em instruções pragmáticas, de onde vêm as ideias acerca da política de emissão deflacionária que são implementadas no sistema Bitcoin?

Para o cientista e filósofo da computação David Golumbia (2016), as ideias que embasam a estrutura do Bitcoin e de outras criptomoedas têm origens em ideologias políticas e econômicas tradicionalmente veiculadas pela extrema direita, como o neoliberalismo e, mais especificamente, o *ciberlibertarianismo*. De acordo com Langdon Winner (1997), em uma das primeiras formulações do termo, o ciberlibertarianismo consiste em uma coleção de ideias que unem o entusiamo por formas de vida mediadas pela tecnologia com definições neoliberais de liberdade, vida social, economia e política, e que culminam em um determinismo tecnológico – quanto mais rápido o desenvolvimento de "coisas artificiais", mais elas passam a ser explicadas em termos "quase biológicos" de evolução. Para Winner, outros dois pontos centrais dessa ideologia são o individualismo radical (a autorrealização do indivíduo no ciberespaço e a necessidade de liberação das amarras que constrangem a realização de seus interesses racionais), e o conceito de "livre mercado", tal como formulado por Milton Friedman e a escola de Chicago. Há também, nesse modo de pensamento, uma tendência em amalgamar as atividades dos indivíduos com as operações de grandes corporações capitalistas, que visam a maximização de lucros e a defesa da propriedade privada. A liberdade, em termos muito gerais, emergiria então do crescente desenvolvimento tecnológico e, portanto, esforços de interferência

ou regulação desse desenvolvimento seriam "antiéticos". Tanto para Winner quanto para Golumbia, o ciberlibertarianismo ganha força em meados dos anos 1990, em movimentos contra a regulação da Internet, e passa, desde então, a ser amplamente difundido por empresários, investidores e entusiastas da tecnologia do Vale do Silício e além. Mais ainda, conjuntos de *slogans* e crenças associadas à difusão de tecnologias digitais costumam incorporar partes importantes dessa ideologia, mesmo sob a superfície retórica do compromisso com valores que não parecem estar imediatamente associados à direita (como é o caso nos próprios debates sobre a regulação da Internet ou de objetos financeiros).

Golumbia argumenta que o Bitcoin – em debates, na literatura e nos tropos narrativos mobilizados por seus entusiastas – leva adiante um sutil argumento extremista que diz que "inflação" e "deflação" são causadas por políticas monetárias, em vez de serem causadas por outros aspectos da economia, como preços de consumo, preços de ativos e *commodities*, produtividade e outros aspectos do trabalho. De acordo com Golumbia, é uma característica central do pensamento financeiro de direita promover a ideia de que inflação e deflação são o resultado das ações de bancos centrais, em vez da visão, segundo ele, bem mais comum entre economistas, de que os bancos centrais agem para controlar a inflação ou a deflação em resposta a pressões econômicas externas. Nesse sentido, o Bitcoin, esse artefato técnico constituído de regras aparentemente arbitrárias (pois mais econômicas do que computacionais), foi, segundo ele, deliberadamente construído pra se comportar de modo muito semelhante às formulações de políticas monetárias postuladas pela economia neoclássica – a partir de autores como Carl Menger, Friedrich Hayek, Ludwig von Mises, precursores da chamada Escola Austríaca de Economia, e dos neoliberais da Escola de Chicago, como Milton Friedman, que estabelece expressamente essa correlação entre inflação e as políticas de emissão monetária[16]. Do modo com que estão configurados, argumenta Golumbia, o Bitcoin e a "tecnologia blockchain" que o embasa satisfazem necessidades que só podem fazer sentido no contexto de uma política neoliberal, uma vez que esses valores políticos e econômicos estão literalmente codificados no próprio *software*.

[16] Notadamente, Satoshi Nakamoto, na mesma mensagem citada anteriormente, em que divulga o código-fonte da versão 0.1 do Bitcoin, compara seu sistema aos bancos: "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible."

Não me interessa, aqui, reduzir o fenômeno das criptomoedas ao posicionamento estrito, do Bitcoin e das pessoas, no espectro da direita, como faz Golumbia, embora, em minha pesquisa, eu também venha observando a prevalência de variações do ciberlibertarianismo na maioria dos discursos a respeito desses sistemas. Em especial, a disposição bastante difundida de que "problemas sociais" podem ter soluções tecnológicas ou podem ser reduzidos a problemas computacionais (disposição essa também conhecida como *computacionalismo*, cf. GOLUMBIA, 2009); ou, ainda, de que todos os fenômenos sociais, em última instância, podem ser explicados como fenômenos econômicos (em termos como oferta e demanda, livre mercado, individualismo, empreendedorismo, financeirização). Isso que não significa, contudo, que essas pessoas se identifiquem como "conservadoras" ou necessariamente se posicionem politicamente dessa maneira. Com a crescente difusão e apropriação desses sistemas em novos contextos, há muitos outros fatores que devem ser levados em consideração (ainda que, segundo os autores, o aspecto difuso dessas proposições políticas e econômicas seja também uma das características do ciberlibertarianismo).

Nesse momento da minha pesquisa, tem me interessado mais pensar como os algoritmos, esses aglomerados de processos, abstrações, implementações e diferentes imaginações de mundo, não apenas executam certas "ideias teóricas" em certas "instruções pragmáticas", mas também os modos com que essas configurações algorítmicas efetuam sistemas de troca e constituem objetos financeiros que circulam em mercados locais e globais. Por meio de uma multiplicidade de práticas humanas e maquínicas, desde o desenvolvimento de software à produção do consenso distribuído, esses algoritmos e sistemas, entidades executáveis e muitas vezes impenetráveis, rodando e constituindo amplas redes sociotécnicas de vários tipos e escalas, implicam (e impõem) consensos, mas também uma série de dissensos e modalidades específicas de governança digital sobre esses mesmos processos, abstrações e outras tecnologias da imaginação.

Referências

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

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

CALLON, Michel; MUNIESA, Fabian. Economic Markets as Calculative Collective Devices. **Organization Studies**, v. 26, n. 8, p. 1229–1250, ago. 2005.

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

GOLUMBIA, David. **The Cultural Logic of Computation**. Cambridge, Mass.: Harvard University Press, 2009. Disponível em: <http://public.eblib.com/choice/publicfullrecord.aspx?p=3300785>. Acesso em: 30 dez. 2018.

GOLUMBIA, David. **The Politics of Bitcoin: Software as Right-Wing Extremism**. Minneapolis: University of Minnesota Press, 2016. (Forerunners: ideas first).

KNUTH, Donald E. **The Art of Computer Programming. Volume 1: Fundamental Algorithms**. 3ed. ed. [S.l.]: Addison-Wesley Professional, 1997.

MACKENZIE, Donald. A Sociology of Algorithms: High-Frequency Trading and the Shaping of Markets. **Preprint**, p. 1–67, 2014.

MIROWSKI, Philip. **Machine Dreams: Economics Becomes a Cyborg Science**. Cambridge ; New York: Cambridge University Press, 2002.

MIROWSKI, Philip; SOMEFUN, Koye. Markets as Evolving Computational Entities. **Journal of Evolutionary Economics**, v. 8, n. 4, p. 329–356, 1998.

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

SEAVER, Nick. Algorithms as culture: Some tactics for the ethnography of algorithmic systems. **Big Data & Society**, v. 4, n. 2, p. 12, dez. 2017.

WINNER, Langdon. Cyberlibertarian myths and the prospects for community. **ACM SIGCAS Computers and Society**, v. 27, n. 3, p. 14–19, 1 set. 1997.