UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE EDUCAÇÃO E CIÊNCIAS HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ANTROPOLOGIA SOCIAL

BRUNO CAMPOS CARDOSO

A POLÍTICA DOS ALGORITMOS E A ECONOMIA DAS MÁQUINAS

UMA ETNOGRAFIA SOBRE O SISTEMA *PEER-TO-PEER* BITCOIN

São Carlos
2024

BRUNO CAMPOS CARDOSO

A POLÍTICA DOS ALGORITMOS E A ECONOMIA DAS MÁQUINAS

UMA ETNOGRAFIA SOBRE O SISTEMA *PEER-TO-PEER* BITCOIN

Tese apresentada ao Programa de Pós-Graduação em Antropologia Social da Universidade Federal de São Carlos, para obtenção do título de Doutor em Antropologia Social.

Orientadora: Profa. Dra. Anna Catarina Morawska Vianna

Banca Examinadora:

Profa. Dra. Jessica Sklair (QMUL)

Profa. Dra. Magda dos Santos Ribeiro (UFMG)

Prof. Dr. Marko Synésio Alves Monteiro (UNICAMP)

Prof. Dr. Piero de Camargo Leirner (UFSCar)

Suplentes:

Profa. Dra. Vanessa Parreira Perin (UFSCar)

Prof. Dr. Kauê Barreiros Corrêa Pessoa Guimarães (UFPR)

São Carlos

2024

Bruno Campos, Cardoso

A política dos algoritmos e a economia das máquinas: uma etnografia sobre o sistema peer-to-peer Bitcoin / Cardoso Bruno Campos -- 2024.
138f.

Tese de Doutorado - Universidade Federal de São Carlos, campus São Carlos, São Carlos
Orientador (a): Anna Catarina Morawska Vianna
Banca Examinadora: Jessica Sklair, Magda dos Santos Ribeiro, Marko Synésio Alves Monteiro, Piero de Camargo Leirner
Bibliografia

1. Ativos digitais. 2. Algoritmos. 3. Bitcoin. I. Bruno Campos, Cardoso. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Ronildo Santos Prado - CRB/8 7325

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Educação e Ciências Humanas
Programa de Pós-Graduação em Antropologia Social

Folha de Aprovação

Defesa de Tese de Doutorado do candidato Bruno Campos Cardoso, realizada em 02/04/2024.

Comissão Julgadora:

Profa. Dra. Anna Catarina Morawska Vianna (UFSCar)

Profa. Dra. Jessica Beth Sadie Sklair Correa (QMUL)

Prof. Dr. Marko Synésio Alves Monteiro (UNICAMP)

Prof. Dr. Piero de Camargo Leirner (UFSCar)

Profa. Dra. Magda dos Santos Ribeiro (UFMG)

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Antropologia Social.

AGRADECIMENTOS

À minha família, Diva e Ronald, Aline e Pablo, Maria e Ana Cristina, pelo amor e apoio incondicional.

À Karina Coelho, pelo afeto e parceria de muitos anos.

À Catarina Morawska, orientadora e amiga, que sempre me incentivou e acreditou no meu trabalho.

Aos meus amigos e colegas da UFPR, UFSCar e de outros caminhos da vida, pelas amizades e aprendizados.

Aos membros titulares da banca, Jessica Sklair, Marko Monteiro, Piero Leirner e Magda Ribeiro, e aos suplentes, Vanessa Perin e Kauê Pessoa, pelo aceite e pelas valiosas trocas durante meu doutorado.

Ao Laboratório de Experimentações Etnográficas (LE-E), pelos importantes debates e contribuições.

Ao Programa de Pós-Graduação em Antropologia Social da Universidade Federal de São Carlos e à CAPES, pela possibilidade de desenvolvimento desta pesquisa e pelo auxílio financeiro para sua realização.

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

RESUMO

Esta tese descreve relações sociotécnicas que constituem os sistemas digitais das criptomoedas a partir das interfaces da antropologia das finanças e da antropologia da ciência e tecnologia. Com base no material etnográfico coletado e elaborado entre 2017 e 2020, como documentos e artefatos digitais, em grupos de discussão, fóruns, listas de e-mails, plataformas públicas de desenvolvimento de software e entrevistas, o trabalho descreve os principais procedimentos algorítmicos e as economias político-materiais que fundamentam as criptomoedas enquanto sistemas de dinheiro eletrônico de tipo distribuído ou descentralizado. Tendo como principal objeto de análise a primeira destas criptomoedas, o sistema *peer-to-peer* Bitcoin, reflito sobre as relações tecnofinanceiras dos chamados *players* – humanos e máquinas envolvidos no estabelecimento de sistemas de transação de propriedades digitais, especulação de valores e estruturas de dados de registro distribuído. A tese visa oferecer uma descrição das relações, atores e sistemas sociotécnicos em torno do Bitcoin a fim de evidenciar os efeitos político-econômicos da circulação de criptomoedas na formação de mercados e infraestruturas sobre as quais se estabelecem os ativos digitais. Também exploro as imaginações de futuro que decorrem da elaboração de instrumentos financeiros, novas modalidades de transação e as ideologias tecnocráticas e neoliberais cujos princípios estão, de modo mais ou menos explícito, codificados em software.

Palavras-chave: Bitcoin; criptomoedas; ativos digitais; algoritmos; antropologia econômica.

ABSTRACT

This thesis describes the socio-technical relationships that constitute the digital systems of cryptocurrencies from the interfaces of the anthropology of finance and the anthropology of science and technology. Based on ethnographic material collected and elaborated between 2017 and 2020, such as documents and digital artifacts, in discussion groups, forums, email lists, public software development platforms and interviews, the present work describes the main algorithmic procedures and political-material economies that underpin cryptocurrencies as distributed or decentralized electronic cash systems. By taking the first of these cryptocurrencies, the peer-to-peer Bitcoin system, as the main object of analysis, I reflect on the techno-financial relations of the so-called *players* – humans and machines involved in establishing digital property transaction systems, value speculation and distributed ledger data structures. The thesis aims to offer a description of the relationships, actors and socio-technical systems surrounding Bitcoin in order to highlight the political-economic effects of the circulation of cryptocurrencies on the formation of markets and infrastructures on which digital assets are established. I also explore the imaginations of the future that arise from the development of financial instruments, new modes of transaction and the technocratic and neoliberal ideologies whose principles are, more or less explicitly, encoded in software.

Keywords: Bitcoin; cryptocurrencies; digital assets; algorithms; economic anthropology.

SUMÁRIO

INTRODUÇÃO

Esta tese apresenta uma etnografia de trocas digitais em redes descentralizadas a partir do campo das criptomoedas e das transações e operações favorecidas por implementações de algoritmos criptográficos e sistemas do tipo *blockchain*, levando em conta o caráter processual e relacional das transações realizadas nesses sistemas. Tomo como objeto o sistema *peer-to-peer* Bitcoin, que teve suas primeiras transações registradas em janeiro de 2009. Desde então, sua rede de usuários aumentou de modo tímido nos primeiros anos, e de modo exponencial a partir de 2013, quando se tornou a principal moeda de troca dos usuários do *Silk Road*, um portal de compra e venda de produtos, em geral ilícitos (como drogas e armas, por exemplo), e com usuários anônimos de diversos países do hemisfério norte. Com a popularidade, ainda que negativa, garantida pela grande mídia[1], o Bitcoin passou então a ser utilizado em uma série de transações online – compra e venda de bens e serviços, transferências pessoais e reserva de valores – e a acumular um valor de mercado que hoje, após 15 anos de operação, oscila na casa das dezenas de milhares dólares por moeda, sendo, desde então, a maior e mais difundida criptomoeda em operação[2].

Uma rede *peer-to-peer* diz respeito a um paradigma de construção de redes em que as conexões não são estabelecidas ou determinadas a partir de um ponto central, nem a partir de pontos privilegiados: redes *peer-to-peer* ou *distribuídas* são constituídas a partir de conexões "ponto a ponto", de modo que cada máquina ou participante se conecta contingencialmente a alguns outros *nós* (e estes, por sua vez, se conectam a outros), formando assim uma ampla rede de comunicação.

---

1 Há incontáveis matérias e reportagens sobre o *Silk Road* com variáveis níveis de desinformação, como também ocorre com boa parte da cobertura sobre criptomoedas e segurança digital. O jornal The Guardian, entretanto, fez à época uma cobertura bem detalhada: https://theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace. Acesso em: 23 fev. 2024.

2 O código-fonte do Bitcoin, assim como todo seu histórico de desenvolvimento, está disponível na plataforma colaborativa Github: https://github.com/bitcoin/bitcoin. Há, entretanto, uma verdadeira constelação de outras criptomoedas, surgidas por derivação (*fork*) do código-fonte do Bitcoin e de criptomoedas derivadas deste. O site *Map of Coins* traça a genealogia de 667 criptomoedas, que pode ser visualizada no site http://mapofcoins.com/bitcoin. Acesso em: 23 fev. 2024.

Notório por suas oscilações, um bitcoin chegou a ser cotado em quase 20 mil dólares em dezembro de 2017, acumulando uma capitalização de mercado (preço unitário multiplicado pela quantidade de moedas em circulação) de cerca de 150 bilhões de dólares, contribuindo para que todo ecossistema de criptomoedas somasse, à época, uma capitalização de quase 400 bilhões dólares. Em novembro de 2021, um bitcoin chegou a ser negociado por 69 mil dólares, o topo histórico de negociação até então, e hoje, no início de 2024, segue cotado em 44 mil dólares, com uma capitalização de mercado de 865 bilhões de dólares – sendo, portanto, parte majoritária da capitalização global do *ecossistema cripto*, que é estimada em 1,6 trilhões de dólares[3].

O sistema *peer-to-peer* Bitcoin é, assim, um fenômeno duplo: por um lado, é um protocolo para a troca de valores eletrônicos e, por outro, um sistema complexo de máquinas (computadores, *mining rigs*, *bots*, serviços online), técnicas (de programação, criptografia, engenharia) e atores humanos (usuários, *traders*, grupos de desenvolvedores) associados em comunidades virtuais e mercados econômicos que se pretendem descentralizados, uma vez que a operação deste arranjo sociotécnico prescinde de autoridades centrais ou intermediários financeiros tradicionais. No entanto, embora o sistema crie as condições de possibilidade para a comunicação e a troca sem intermediários, um grande volume de transações desta e de outras criptomoedas ocorre por meio de *exchanges*, plataformas centralizadas para troca de ativos baseadas na oferta e demanda. Há, entretanto, iniciativas de implementação de plataformas autônomas de troca, como a rede Bisq[4], que visam criar alternativas livres para esses mercados.

A principal inovação do sistema Bitcoin está em assegurar, por meio de uma série de algoritmos criptográficos, a produção coletiva de um *consenso distribuído* – um "regime de verdade" matematicamente verificável, sem a necessidade de um mediador ou intermediários "confiáveis" – que garanta a integridade dos valores e das transações efetuadas na rede (ANTONOPOULOS, 2015, 2016a).

---

3 Dados provenientes do site https://coinmarketcap.com, que oferece um monitor dos preços de mais de 2 mil criptomoedas, negociadas em quase 700 exchanges digitais ao redor do mundo. Acesso em: 23 fev. 2024.

4 Bisq - A decentralized bitcoin exchange network: https://bisq.network. Acesso em: 23 fev. 2024.

O consenso distribuído era um dos problemas que Satoshi Nakamoto, pseudônimo de uma ou mais pessoas cuja identidade permanece desconhecida, procurava resolver no célebre *whitepaper* intitulado "Bitcoin: A Peer-to-Peer Electronic Cash System", publicado em novembro de 2008 em uma lista de discussão sobre criptografia[5]. Nakamoto descreve as bases conceituais de um sistema descentralizado de trocas eletrônicas baseado em provas criptográficas e em um registro distribuído de transações, que passou a ser chamado *blockchain*. Unindo essas duas ideias, implementadas por ele na primeira versão do software Bitcoin, Nakamoto argumentava ter resolvido o antigo problema econômico do *double-spending* – ou, como também é conhecido na matemática, o problema do consenso distribuído ou "o problema dos generais bizantinos".

Os modos de produção do consenso distribuído, como se verá adiante, estão no cerne da questão antropológica tratada neste trabalho. O problema dos generais bizantinos, tal como formulado por Lamport, Shostak e Pease (1982), é a expressão abstrata de um modelo algorítmico de "tolerância de falha" em sistemas computacionais: como garantir a consistência da informação em rede quando uma parte de seus componentes apresenta falhas de comunicação? – seja por mal funcionamento, por conta de elementos não-confiáveis que possam ter sido comprometidos por agentes externos, ou por "traição", isto é, por ações maliciosas deliberadas. Desde então, embora haja diferentes implementações conhecidas para dar conta deste problema, a proposta por Nakamoto é inovadora ao instituir um registro criptográfico público como parte de sua solução.

Se o sistema monetário, por exemplo, para assegurar a validade de uma troca entre pares, depende de uma "terceira parte confiável", isto é, de um banco ou uma instituição financeira que possa assegurar a identidade e a consistência das informações, o sistema de registro distribuído proposto por Nakamoto, por sua vez, elimina esse intermediário por meio do uso ostensivo de métodos criptográficos e de uma "prova de trabalho" (*proof-of-work*) computacional a que devem ser submetidos todos os blocos de transações para que sejam validados e então acrescentados à cadeia de blocos de transações anteriores (MORABITO, 2017; NARAYANAN *et al.*,

5 A mensagem original pode ser lida nos arquivos da lista de discussão *Cryptography*. Disponível em: https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html. Acesso em: 23 fev. 2024.

2016). Conforme argumentam os cientistas da computação Arvind Narayanan e Jeremy Clark, a cadeia de blocos de transações (*blockchain*) é uma estrutura distribuída de dados mantida coletivamente por pares que não se conhecem e que, por esse motivo, não podem confiar uns nos outros: "unlike a regular data structure that's stored on a single machine, the ledger is a *global* data structure collectively maintained by a mutually untrusting set of participants" (NARAYANAN; CLARK, 2017, p. 4).

Ao contrário das redes de troca interpessoais a que normalmente a antropologia dá atenção, o sistema de registro distribuído proposto por Nakamoto implica a possibilidade de trocas entre um conjunto de participantes em "desconfiança mútua". O foco das preocupações dos programadores – como superar falhas de comunicação em um sistema informacional descentralizado – aponta, assim, para um problema antropológico de outra ordem: como implementar a troca em meio a relações marcadas pelo anonimato e impessoalidade[6]. Com efeito, uma das inovações do sistema Bitcoin é justamente a implementação de uma nova forma de "arbitragem computacional" (FINN, 2017), que cria as condições de possibilidade de troca por meio da emergência de um consenso sobre o estado atual do registro global de transações (*blockchain*).

Como descreve Andreas Antonopoulos (2015), o consenso emerge do entrelaçamento de diferentes processos de verificação, agregação e seleção das cadeias de blocos com a maior quantidade de poder computacional empregado em sua geração (*proof-of-work*). A noção de um "consenso emergente" deriva de sua natureza não-explícita: "consensus is not achieved explicitly – there is no election or fixed moment when consensus occurs. Instead, consensus is an emergent artifact of

6 De um ponto de vista técnico, as transações do sistema Bitcoin não são completamente anônimas. Ainda que não seja necessário qualquer tipo de cadastro ou identificação pessoal para se efetuar uma transação, os endereços digitais (entendidos na rede como *carteiras*) e os valores transferidos entre eles são sempre anunciados publicamente para todos os pares da rede, para que estes possam então atestar sua validade e garantir o registro na cadeia de blocos. Assim, o Bitcoin é mais precisamente uma rede "pseudoanônima", uma vez que é teoricamente possível, por meio de análise heurística, traçar correlações entre as movimentações de um dado conjunto de endereços e suas supostas "identidades reais". Para considerações técnicas específicas sobre este tema, ver: https://en.bitcoin.it/wiki/Anonymity. Acesso em: 23 fev. 2024.

the asynchronous interaction of thousands of independent nodes, all following simple rules." (p. 177). Nas palavras de Nakamoto:

> We propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes (NAKAMOTO, 2008, p. 1).

Assim, cada novo bloco de transações, produzido em média a cada dez minutos, está ligado ao bloco anterior, como em uma corrente, de modo permanente e imutável, o que garante a confiabilidade do registro e a integridade de todo o histórico de transações. O emprego de métodos criptográficos garante a consistência e validade da informação trocada em rede:

> As the word suggests, cryptocurrencies make heavy use of cryptography. Cryptography provides a mechanism for securely encoding the rules of a cryptocurrency system in the system itself. We can use it to prevent tampering and equivocation, as well as to encode, in a mathematical protocol, the rules for creation of new units of the currency (NARAYANAN *et al.*, 2016, p. 33).

Sendo a primeira e mais difundida criptomoeda em operação, o sistema *peer-to-peer* Bitcoin constitui um campo complexo de investigação antropológica sobre troca de valores, implementação técnica e os modos de governança de uma criptomoeda que, em oposição às moedas fiduciárias nacionais, pretende-se global, transnacional e descentralizada. Uma vez que prescinde de uma autoridade central (grupo restrito, empresa, instituição ou país) para a regulação de seus fluxos, o sistema tem como características o pseudoanonimato e a resistência à censura: todas as transações são públicas e independem da identificação dos usuários, de modo que nenhum participante pode evitar que a transação de outrem seja realizada ou, posteriormente, alterá-la. A contínua produção de consenso sobre o estado global do sistema, desse modo, se dá por meio de agenciamentos complexos entre humanos, computadores e algoritmos, que operam como "máquinas culturais" (FINN, 2017). Os efeitos desses processos e o desenvolvimento de modos de governança coletiva, produção de software e troca de valores digitais são o objeto desta tese, que busca mostrar como as dimensões ideológica e técnica se entrelaçam na produção do sistema *peer-to-peer* Bitcoin.

ALGORITMOS E MATERIALIDADE

Mas o que é um algoritmo? Talvez a analogia mais simples seja com uma receita de bolo: por meio de uma série de procedimentos (ações encadeadas de maneira correta) e abstrações (valores, quantidades e tempos), uma receita ou um algoritmo traçam métodos para a realização de uma determinada tarefa de modo efetivo. De acordo com Donald Knuth, no primeiro volume do clássico "The Art of Computer Programming" (KNUTH, 1997), um algoritmo tem ao menos cinco características importantes: 1. *finitude* (um algoritmo deve sempre *terminar* após um número finito de passos); 2. *definição* (cada um dos passos deve ser definido com precisão e sem ambiguidades); 3. *input(s)* (tanto zero quanto um conjunto de parâmetros ou quantidades dadas de início ou de modo dinâmico ao longo da sua execução); 4. *output(s)* (aquilo que é produzido pelo algoritmo, isto é, quantidades que possuem uma relação específica com os *inputs*); e 5. *efetividade* (um algoritmo precisa ser efetivo, ou seja, suas operações devem ser executadas em um tempo finito ou razoável para dada tarefa).

Enquanto Donald Knuth enfatiza o aspecto determinante dos algoritmos, o pesquisador da ciência e tecnologia Ed Finn (2017) chama atenção para a sua indeterminação. Para ele, o algoritmo, componente necessário de qualquer implementação computacional, parece habitar uma zona ambígua entre a linguagem e a produção material – ou, em suas palavras, "the algorithm is not a space where the material and symbolic orders are contested, but rather a magical or alchemical realm where they operate in productive indeterminacy" (p. 34). Operando nesse espaço entre o código (o espaço computacional) e a cultura, Finn argumenta que os algoritmos são como "máquinas culturais" cuja principal característica é a sua implementação – uma forma de materialidade, baseada no *hardware* e no *software*, que constitui a fundação da expressão computacional:

> By occupying and defining that awkward middle ground, algorithms and their human collaborators enact new roles as culture machines that unite ideology and practice, pure mathematics and impure humanity, logic and desire. To discuss implementation is thus to join a conversation about materiality and the embodied subjects that enact, transmit, and receive information (FINN, 2017, p. 47).

Há também, segundo o autor, uma dimensão mágica[7] acaso consideremos que os algoritmos funcionam como compósitos complexos de abstração, encantamento, matemática e memória tecnológica:

> They are material implementations of the cathedral of computation. When we interact with them, we are speaking to oracles, gods, and minor demons, hashing out a pidgin or trade language filled with command words, Boolean conjunctions, and quite often, deeply personal information (FINN, 2017, p. 51).

A efetividade e a magia do código-fonte (*source code*) – ou, nos termos da pesquisadora Wendy Chun (2008), *sourcery*, "a fetishism that obfuscates the vicissitudes of execution and makes our machines demonic" (p. 300) – dependem de uma rede imaginada de humanos e máquinas. De acordo com Lucas Introna,

> to keep the code running "as code" is a significant sociomaterial accomplishment, requiring the circulation of action in a complex sociomaterial heterogeneous assemblage, even if it may be seen as routine. What has been suggested about the performativity of algorithms is true for all sociomaterial assemblages. Why then is there a particular concern with algorithms? Why do they need particular scrutiny? (INTRONA, 2016, p. 25)

Como peças de "magia tecnológica cotidiana" (FINN, 2017), os algoritmos podem também nos parecer perigosos. Por um lado, eles podem ser *inescrutáveis*: uma vez que operam sob a superfície como caixas-pretas (FLUSSER, 2002; INTRONA, 2016), seu extenso código-fonte, sempre sujeito a alterações, revisões e transformações, pode se tornar incompreensível até mesmo para quem o escreveu[8]. De outro lado, os algoritmos são *executáveis*: sob as condições constitutivas necessárias, são sempre capazes de executar sua programação com eficácia, no mais das vezes à revelia do que está *fora* do sistema. Como uma ferramenta ou "procedimento efetivo", escreve Finn, "the algorithm is an implement that is coded into existence through a framework of forensic and formal analogies, assumptions, and declarative frameworks" (FINN, 2017, p. 48).

---

7 Ou o que, nos termos do escritor de ficção científica Arthur C. Clarke (1973), poderia também ser enunciado como a 3ª lei de Clarke; "any sufficiently advanced technology is indistinguishable from magic".

8 Um adágio conhecido entre programadores como *Eagleson's Law* ressalta a importância de manter o código-fonte bem documentado: "Any code of your own that you haven't looked at for six or more months, might as well have been written by someone else."

Dado este panorama, são crescentes os trabalhos na antropologia que abordam a questão das redes computacionais sob o viés dos algoritmos e das suas redes de desenvolvimento – isto é, da perspectiva de uma ontologia digital, mais interessada em como esses agenciamentos efetivamente funcionam do que em perguntar o que eles "são" ou apenas quais são suas consequências[9]. Ainda que uma antropologia da cibercultura tenha se consolidado como um importante campo de pesquisa no contexto das novas tecnologias, das comunicações e das relações em redes digitais (FORSYTHE; HESS, 2002; KURBALIJA, 2017; MASSUMI; FISH; JAMESON, 2002; SEGATA; RIFIOTIS, 2016; SOUZA; SOLAGNA; LEAL, 2014), uma antropologia dos algoritmos desponta no horizonte das imbricações da cibercultura com a biopolítica, com os estudos da ciência e tecnologia e com as ontologias materiais (CADENA *et al.*, 2015; CLARK, 2003; FOUCAULT, 1979; HELMREICH, 1998; HU, 2015; INGOLD, 2011; 2015).

Este trabalho pretende se juntar ao debate ao refletir sobre sistemas descentralizados a partir da perspectiva dos algoritmos, dos seus participantes e das interfaces da antropologia da economia, da técnica e da ciência, de modo a descrever os movimentos, fluxos e as paisagens sociotécnicas que constituem o sistema Bitcoin e os campos associados às demais criptomoedas, marcados por articulações dinâmicas em torno de mercados e comunidades virtuais.

TROCA E VALOR EM REDES DESCENTRALIZADAS

Uma criptomoeda emerge como uma espécie de corolário do sistema de registro distribuído nos termos de uma *blockchain*: não é que seja necessário criar uma criptomoeda e nem que esta seja a única aplicação de um *blockchain*, mas para que um mecanismo do sistema de registro distribuído funcione, algo *precisa* ser trocado. Aquilo que é trocado como informação é entendido como uma unidade ou um *token*. No caso do Bitcoin, ainda que se pense em "um bitcoin" como uma unidade, do ponto de vista dos algoritmos envolvidos, a menor unidade possível de troca corresponde a um "satoshi" ou 0,00000001 bitcoin, o que permite a realização

9 Sobre esse tema cabe mencionar a coleção sobre ontologia digital publicada pela revista online Cultural Anthropology, cujos ensaios, de modo geral, têm nos "modos de funcionamento" uma via privilegiada para compreender as relações entre o mundo digital e material (KNOX; WALFORD, 2016).

de "micropagamentos" ou a movimentação de grandes somas de modo indistinto pela rede.

Nas redes de criptomoedas, aquilo que é trocado tem valor na medida em que a maioria dos pares da rede se dispõe a "jogar o jogo" das trocas e dos registros das transações sob as mesmas regras e nos termos impostos pelo sistema *blockchain* do qual fazem parte. Satoshi Nakamoto, em uma postagem na lista de discussão sobre criptografia, poucos dias após dar início ao funcionamento da rede do Bitcoin, descreveu a apreciação coletiva do valor de sua moeda digital como uma possível "profecia autorrealizável": "It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self-fulfilling prophecy"[10]. Ou seja, quanto maior a rede, ou quanto mais pessoas dela participam, maior o valor (ou valores) que ela movimenta em uma rede computacional coletiva.

Tal como enuncia a conhecida "Lei de [Robert] Metcalfe" – e como demonstram Zhang, Liu e Xu (2015) ao aplicar tais formulações sobre dados de rede sociais como Facebook e Tencent, bem como Alabi (2017) em seu argumento sobre as evoluções de preço do Bitcoin e outras duas criptomoedas (Ethereum e Dash) –, o valor de uma rede de comunicação é proporcional ao quadrado do número de usuários conectados ao sistema (n^2). O valor da rede cresce de modo exponencial em função do número de participantes, o que, portanto, também torna o inverso verdadeiro: em uma rede ou moeda utilizada por poucas ou apenas uma pessoa, não há valor, pois não há troca nem conexões significativas a serem estabelecidas[11].

Tanto a escala (número de participantes) quanto a capacidade computacional por participante contribuem para o valor geral de uma dada rede de computação coletiva. Consequentemente, a promoção do crescimento em qualquer uma das dimensões tende a maximizar o valor e os retornos produzidos. No caso do Bitcoin e outras criptomoedas, o aumento exponencial do valor se daria por meio de

---

10 A mensagem de 16 de janeiro de 2009. Disponível em: http://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html. Acesso em: 23 fev. 2024.

11 Sobre as aproximações da Lei de Metcalfe com a rede do Bitcoin e da criptomoeada Ethereum, ver também o artigo "Valuing Bitcoin and Ethereum with Metcalfe's Law". Disponível em https://medium.com/@clearblocks/valuing-bitcoin-and-ethereum-with-metcalfes-law-aaa743f469f6. Acesso em: 23 fev. 2024.

um número cada vez maior de nós envolvidos, mas também por meio do aproveitamento de recursos antes subutilizados (máquinas ociosas e/ou excedentes de contratos de energia), ou pela abertura de janelas de oportunidade para o desenvolvimento de tecnologias específicas e especialização dos atores econômicos na direção da implementação de soluções eficientes que, por sua vez, resultam em retornos expressivos para os investidores. Isto é, para Nakamoto, o tamanho da rede – em número de nós, máquinas, pessoas – é tão importante quanto aquilo que é trocado, pois é o que confere valor ao conjunto finito de *tokens* em circulação. Por este mesmo motivo, Finn argumenta que a computação coletiva seria uma forma de valor intrínseca: "Bitcoin's true radicalism stems from the fact that the blockchain grounds its authority on *collective computation as an intrinsic form of value*" (FINN, 2017, p. 165, grifos do autor).

Por outro lado, a noção de "profecia autorrealizável", como apontam Donald MacKenzie, Fabian Muniesa e Lucia Siu (2007), embasa também uma noção de performatividade na descrição de objetos econômicos:

> "The diverse fields that have adopted Robert K. Merton's (1949) notion of the "self-fulfilling prophecy" – in which the release and social circulation of a description or prediction enhances its validity – can be seen as investigating a version of performativity" (p. 3).

Para os autores, a questão do valor se dá nos termos da performatividade, da legitimidade daquilo que "faz fazer", e, assim, "quanto maior a rede", no sentido latouriano de *actantes* mobilizado pelos autores (que envolve nós, máquinas, pessoas, *exchanges*, gráficos, etc.), maior seu poder performativo. Portanto, para além de pensar no valor monetário da rede, é preciso pensar no problema antropológico do valor a partir da ideia de troca (*exchange*).

Alguns programadores e analistas do sistema Bitcoin teorizam sobre o funcionamento da rede a partir de certa literatura antropológica sobre a troca. Ao refletir sobre as origens do dinheiro, o *cypherpunk* Nick Szabo, criador do *Bitgold*[12] (uma proposta de moeda digital, precursora do Bitcoin, porém nunca implementada),

12 Postulado no final da década de 1990, o *Bitgold* pretendia resolver o mesmo problema que, mais tarde, o Bitcoin veio a abordar – isto é, o da troca digital sem intermediários, tendo como base a noção de escassez e custo de produção de metais preciosos e objetos colecionáveis, como conchas. Vide artigo de Szabo sobre o Bitgold, disponível em https://unenumerated.blogspot.com/2005/12/bit-gold.html. Acesso em: 23 fev. 2024.

estabelece aproximações entre "formas primitivas de dinheiro", objetos sem uma "utilidade concreta", com o entendimento moderno de moeda, como meio de troca, reserva de valor e unidade de conta. Em "Shelling Out: The Origins of Money", Szabo (2005) faz uma analogia entre moedas contemporâneas e "formas de dinheiro colecionáveis", tal qual os objetos trocados no circuito do Kula, descrito por Malinowski:

> by solving the double-coincidence problem an armshell or necklace would prove more valuable than its cost after only a few trades, but could circulate for decades. Gossip and stories that about prior owners of the collectibles further provided information about upstream credit and liquidity (SZABO, 2005, n.p).

À semelhança dos circuitos de troca bem conhecidos na literatura antropológica, como é o caso do círculo do Kula (MALINOWSKI, 1978), aquilo que é trocado não possui necessariamente um valor em si – isto é, os braceletes e colares não possuem valor inerente, mas expressam e representam os valores movimentados por toda rede de trocas, prestígio e relações anteriores, como demonstram estudos clássicos sobre a troca na teoria antropológica (MAUSS, 2003; MUNN, 1992; WEINER, 1992). Os trabalhos de David Graeber (2001, 2009), em especial, são frequentemente citados em debates entre *bitcoiners* sobre a "natureza" do Bitcoin como moeda e meio de troca, no mais das vezes para defini-lo como uma "forma superior de dinheiro" em relação às formas "primitivas" e às moedas fiduciárias contemporâneas. Essa alegada "superioridade" seria, portanto, um resultado direto de sua natureza descentralizada, e em especial por conta do rígido controle algorítmico sobre a quantidade máxima de moedas em circulação.

Nas redes de trocas digitais, o valor não é dado por uma autoridade central, mas pelo volume e consistência dos seus fluxos – muito embora o preço relativo de uma criptomoeda seja "descoberto" por meio das movimentações ocorridas em plataformas centralizadas, como *exchanges* virtuais. A ausência de um centro regulador é talvez a principal característica das redes de tipo descentralizado, ainda que certos agrupamentos exerçam influência sobre decisões técnicas e operacionais, como alterações nos algoritmos principais e nas dinâmicas da rede. Esse é o caso dos programadores e desenvolvedores do software principal (*Bitcoin core*) utilizado pelos usuários, dos *mineradores* e dos grupos de pessoas engajadas

filosófica e politicamente em fóruns de discussão e comunidades virtuais (BOELLSTORFF, 2008; HORST; MILLER, 2012). No caso específico das comunidades de criptomoedas, esses agrupamentos são definidos em função de um alto nível de especialização de seus participantes.

Um desses agrupamentos é o dos mineradores (*miners*), que são usuários, empresas ou grandes aglomerados da rede distribuída que dispõem de muitos recursos, como acesso à energia elétrica abundante ou barata, conexões de alta velocidade e imensa capacidade computacional. Conseguem, assim, realizar a contínua validação de blocos de transações, competindo entre si por recompensas (novas moedas e a soma das taxas de transação) a cada bloco que conseguem validar antes dos demais. 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 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 *hardwares* dedicados a essa atividade.

Há, assim, uma constante tensão entre os diferentes grupos de atores da rede sobre os direcionamentos e mudanças que intentam implementar[13]. 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

13 Um caso expressivo dessas disputas e divergências econômicas e políticas culminou, em agosto de 2017, numa divisão (*hardfork*) do Bitcoin e de parte da comunidade, uma vez que as partes envolvidas não puderam chegar a um acordo, mesmo depois de mais de dois anos de discussão sobre alterações no tamanho dos blocos de transação e outras "melhorias" da rede. A divisão, liderada por um grupo de empresas mineradoras e algumas figuras expressivas da comunidade, resultou na criação do *Bitcoin Cash*, uma criptomoeda derivada do Bitcoin e que compartilha com ela um mesmo histórico de transações até a data da divisão, sendo contudo incompatíveis a partir de então, pois implementam suas regras e redes de modo diferente e, por isso, não se comunicam.

influenciar diretamente os preços de mercado), veículos de mídia e políticas de estado[14]. Também dentro dos círculos de desenvolvimento e implementação de software, a tendência de centralização, se não do comando das atividades, se dá pela especialização técnica necessária e o envolvimento com a comunidade.

Contudo, a aplicação das regras impostas pelos algoritmos e a especialização dos diferentes atores procuram efetivar, no imaginário de grande parte dos participantes, o desejo da construção social de um "mercado perfeito" digital. Algo similar é descrito por Marie-France Garcia-Parpet em relação à construção de um mercado de morangos nos anos 1980, em que vendedores, compradores e os responsáveis pelo galpão de leilões operam um pregão eletrônico de preços imaginado como um "mercado ideal" da teoria econômica clássica (in MACKENZIE; MUNIESA; SIU, 2007, cap. 2). Isso em larga medida se assemelha ao funcionamento das *exchanges* virtuais de criptomoedas, onde por meio dos fluxos de oferta e demanda seus preços relativos são "descobertos". Como argumentam Callon (1998) e, em particular, Muniesa (2014) acerca do mercado financeiro, em especial no âmbito da fabricação eletrônica dos preços em mercados de ações,

> "prices are not discovered. They are made, they are fabricated. They are artefacts which are immanent to trading practice and to the exchange architecture within which trading takes place. So-called ’price discovery’ is, as a matter of fact, an object of tinkering, an object of engineering in the most sophisticated cases" (MUNIESA, 2014, p. 61).

Desse modo, as redes sociotécnicas que constituem o Bitcoin fazem aplicar regras e limitações a que os participantes devem se submeter para participar "honestamente", de modo que não seja necessário (nem aconselhável) confiar em

14 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.

qualquer outro par da rede, e tampouco em autoridades centrais, incluindo *exchanges*, que são pontos notórios de fragilidade e insegurança (SZABO, 2001). Para os entusiastas do Bitcoin, deve-se confiar no código-fonte, na robustez dos algoritmos criptográficos implementados e no poder de processamento e comunicação mobilizados por todo sistema em escala global.

As considerações de Fabian Muniesa (2014) sobre as imbricações sociais dos mercados apontam para a necessidade de um mapeamento tanto das redes de trocas e de seus atores, quanto das formas de efetuação de uma economia performativa que constitui redes e fluxos materiais. Muniesa atenta para os modos como essas trocas ou transações econômicas são descritas, performadas e, no mais das vezes, motivo de intensas controvérsias: "markets are socially embedded – embedded in interpersonal networks, geographical territories and physical spaces, in social institutions, political structures and cultural forms" (2014, p. 64).

Tendo por base esse debate mais amplo, esta tese enfatiza alguns dos procedimentos de colaboração, coordenação e composição com que programadores, investidores, entusiastas e ativistas orientam seu trabalho e atuação em comunidades virtuais, bem como nos modos de desenvolvimento de mercados descentralizados e políticas de governança em sistemas de consenso distribuído, como o Bitcoin.

Pretende-se, assim, descrever as relações *tecnofinanceiras* que constituem as criptomoedas enquanto sistemas sociotécnicos de dinheiro eletrônico, a partir das interfaces da antropologia das finanças e da antropologia da ciência e tecnologia. Por "relações tecnofinanceiras" entende-se aqui o conjunto de procedimentos técnicos, aglomerados materiais e configurações algorítmicas, agenciados por *players* humanos e máquinas, no estabelecimento de sistemas de transação de propriedades digitais, especulação de valores e registro de dados em redes de tipo distribuído (*peer-to-peer*).

Nesta tese, descrevo as criptomoedas – em especial, o Bitcoin – a partir dos principais procedimentos algorítmicos que as constituem enquanto sistemas sociotécnicos de dinheiro eletrônico e, ao mesmo tempo, enquanto redes *peer-to-peer* de registro distribuído para a transação desses valores digitais. Ao longo da

descrição, procuro pensar os efeitos político-econômicos da circulação de criptomoedas na formação de mercados e infraestruturas sobre as quais se estabelecem os ativos digitais, bem como as imaginações de futuro que decorrem da elaboração de instrumentos financeiros, novas modalidades de transação e ideologias tecnocráticas e neoliberais cujos princípios estão, de modo mais ou menos explícito, codificados em software.

NOTA METODOLÓGICA E APRESENTAÇÃO DOS CAPÍTULOS

A pesquisa teve como proposta inicial realizar uma etnografia do sistema *peer-to-peer* Bitcoin a partir da descrição das redes sociotécnicas que embasam a criação de objetos financeiros por meio de algoritmos e dos processos técnicos que constituem suas implementações. Tendo por base tal delimitação do objeto, e com o intuito de organizar o material e sua apresentação, estabeleci dois principais métodos de pesquisa. O primeiro se deu a partir da pesquisa documental em livros, textos, notícias, postagens em redes sociais, grupos de e-mail, fóruns de discussão e os debates acerca da implementação de referência do Bitcoin[15]. O segundo, conversas e entrevistas com participantes do mercado de criptomoedas: usuários do sistema, programadores, investidores, entusiastas. Esse acompanhamento e documentação foram feitos, principalmente, desde meados de 2017 até agosto de 2020. Nos últimos meses de 2019 e no início de 2020, realizei também algumas entrevistas formais com investidores e diversas conversas informais, principalmente online, com usuários e participantes desses mercados no Brasil. Assim, o material etnográfico aqui mobilizado é resultado da observação de debates em comunidades virtuais, grupos, fóruns, listas de e-mails e plataformas públicas de desenvolvimento de software.

15 A implementação de referência do Bitcoin é o repositório de código-fonte hospedado na plataforma pública GitHub: https://github.com/bitcoin/bitcoin. Embora haja outras implementações e repositórios menos conhecidos, este é o que reúne o maior número de contribuidores e sobre o qual são discutidas, testadas e implementadas a maioria das funcionalidades e melhorias a serem introduzidas no sistema. Esse repositório e os canais de comunicação dos desenvolvedores – o fórum de discussão do próprio repositório, o repositório dos BIPs, listas de e-mail e um canal no IRC – são o principal locus dos debates e disputas acerca do sistema, como veremos no capítulo 2. Postagens em blogs, páginas pessoais e no Twitter, bem como os portais de notícias, comunidades virtuais e grupos no WhatsApp e Telegram constituem um círculo mais amplo e difuso do desenvolvimento de narrativas, controvérsias e memes, como veremos no capítulo 3.

Nesses ambientes, as interações, os debates tecnofinanceiros e as disputas de narrativas se dão muitas vezes em função dos modos de produção e articulação de uma série de documentos e artefatos digitais como códigos-fonte, estruturas de dados, assinaturas criptográficas, notícias, gráficos de preço (e suas interpretações), previsões sobre preços e o futuro do dinheiro, e outros futuros imaginados.

Destaca-se uma modalidade de artefatos digitais específica a esse campo, os *whitepapers*, que dizem respeito ao uso de documentos para a descrição do funcionamento técnico de uma dada criptomoeda. *Whitepapers*, no contexto acadêmico inglês, são tipos de "position papers", artigos científicos que se propõem a resolver uma questão ou um determinado problema técnico, um formato relativamente comum no campo da ciência da computação e das engenharias. No entanto, no contexto das criptomoedas, os *whitepapers* são documentos elaborados por indivíduos ou grupos de desenvolvedores, ou mesmo investidores (anônimos ou não) com o intuito de apresentar os objetivos e o funcionamento de uma determinada criptomoeda ou projeto. De acordo com Koray Çalışkan (2018), o uso desse tipo de documentos faz das criptomoedas "a primeira forma de dinheiro criada por cientistas ou por pessoas que utilizam ferramentas e competências científicas sem a necessária participação de bancos ou Estados" (2018, p. 3).

Esses documentos podem ser artigos de orientação mais técnica, como o próprio *whitepaper* do Bitcoin (NAKAMOTO, 2008), que de certo modo inaugura, ainda em 2008, essa modalidade de apresentação nesse campo (embora seja também o formato do anteiriormente citado Bitgold, por exemplo), ou podem ser artigos de orientação abertamente panfletária, num formato que muitas vezes os tornam indistinguíveis de peças publicitárias ou apresentações criadas no PowerPoint. Tal como os *flyers* de edifícios que ainda não foram construídos, mas que servem para seduzir potenciais moradores a comprarem um "apartamento na planta", os *whitepapers* muitas vezes se referem a criptomoedas que sequer foram – e que muitas vezes sequer serão – devidamente implementadas, o que, entretanto, não impede que possam ser negociadas em certas corretoras digitais (*exchanges*). Dentre as milhares de criptomoedas que existem atualmente, muitas das quais não

são utilizadas de fato, a grande maioria possui um *whitepaper* que descreve seu potencial "inovador", "disruptivo" ou embasa seu (suposto) funcionamento técnico.[16]

Outra importante modalidade de documentos são aqueles destinados a formalização de "propostas de melhoria" ou introdução de funcionalidades específicas que, no caso do Bitcoin, são chamados BIPs, ou *Bitcoin Improvement Proposals*. Trata-se de um formato aberto de documentos numerados que visam padronizar e formalizar proposições de mudanças ou introdução de novas funcionalidades no sistema Bitcoin. Um BIP, à semelhança de um *paper* acadêmico, deve conter uma apresentação do problema que pretende resolver, uma metodologia ou código-fonte que embase a proposta e uma indicação dos desenvolvimentos subsequentes necessários[17]. Essa modalidade de documentos, criada a partir da necessidade de organizar os debates na comunidade de desenvolvedores do sistema, é o que motiva a maioria das discussões em listas de e-mail e nas comunidades virtuais de programadores.

A constante tensão em meio aos agrupamentos virtuais (os repositórios de código, listas de discussão, comunidades virtuais) e seus modos de governança mais ou menos descentralizados, reflete a instabilidade da topologia desses mesmos grupos e dos sistemas *peer-to-peer* criados e mantidos a partir deles.

Em função do seu caráter circunstancial (*ad hoc*), da sua maleabilidade, da diversidade dos participantes online, e à semelhança da comunicação "boca a boca", redes *peer-to-peer* muitas vezes oscilam entre dois tipos ideais: o distribuído, em que as conexões tendem à horizontalidade, e o descentralizado, em que

16 O site https://coinmarketcap.com lista essas criptomoedas em função do seu valor por unidade e da "capitalização de mercado", que é o produto do preço unitário pela quantidade unidades em circulação. Nem todas as criptomoedas listadas possuem um sistema ou uma rede própria, sendo muitas delas *tokens* programados com características específicas que rodam sobre o sistema de uma outra criptomoeda, notadamente o Ethereum. Das "Top 100" criptomoedas, que são aquelas com preços e usos mais relevantes, o Bitcoin sempre esteve na primeira posição, com atualmente quase 19,5 milhões bitcoins em circulação e uma capitalização de mercado de quase 865 bilhões de dólares. Estima-se que o valor total de mercado de todas as criptomoedas listadas esteja próximo dos 1,6 trilhões de dólares, de modo que o somente o Bitcoin é responsável por cerca de 60% de todos os valores negociados nas cerca de 700 exchanges listadas pelo site.

17 Os BIPs constituem um corpus de centenas de documentos reunidos num repositório paralelo ao do código-fonte do Bitcoin. Disponível em https://github.com/bitcoin/bips. Acesso em: 23 fev. 2024.

determinados pontos tendem a concentrar um número maior de conexões (BARAN, 1964). Em muitos contextos discursivos, no entanto, esses dois tipos ideias são mobilizados como sinônimos ou como termos intercambiáveis. Isto é, embora seja impossível determinar quaisquer agrupamentos citados de modo coeso, suas similaridades afetivas e ideológicas tendem a convergir sobre os mesmos pontos de oposição: oposição à tendências identificadas como "centralizadoras" ou *contra* "redes centralizadas" de modo geral, cujo exemplo mais comum, por sua vez, costuma ser o das instituições financeiras tradicionais e os aparatos estatais.

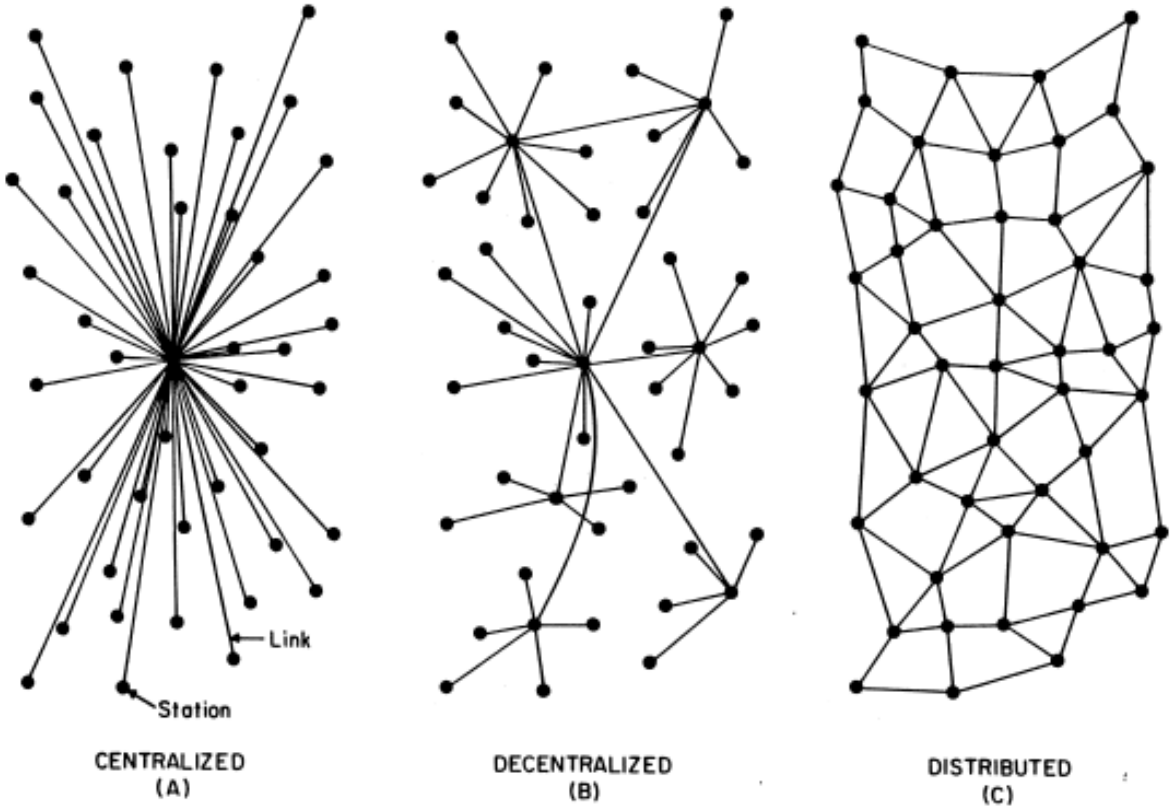

FIG. 1 — Centralized, Decentralized and Distributed Networks

Figura 1: Diagrama clássico mostrando as topologias de rede a partir de diferentes paradigmas de conexão entre "estações" (nós) de uma rede – na época, a ARPANET (BARAN, 1964).

Como será descrito em mais detalhes adiante, as conexões "centralizadas", baseadas no paradigma cliente-servidor, são entendidas pelos entusiastas das criptomoedas como "problemáticas" por conta da concentração de poder decisório num ponto central (o "servidor"). Assim, as ações do "centro de controle" costumam

ser consideradas pelos participantes (os "clientes") como arbitrárias ou autoritárias, e a própria topologia de uma rede centralizada – as relações materiais que orientam as conexões nesse tipo rede – evidencia o ponto central como um notório "ponto de falha" (SZABO, 2001). Alternativamente, por meio da recusa de um único "nó central", configurações de rede de tipo distribuído e descentralizado são consideradas mais resilientes, uma vez que suas topologias de rede se constituem em torno de múltiplos servidores (no caso das redes descentralizadas) ou a partir de um protocolo de comunicação que determina que cada nó da rede opere simultaneamente como cliente-e-servidor (no caso das redes distribuídas ou *peer-to-peer*), assim reduzindo ou eliminando "pontos de falha" centrais.

Em contrapartida, os protocolos de comunicação e, no caso das criptomoedas, os protocolos para o registro distribuído de dados e transações, adquirem maior complexidade em função do problema do estabelecimento de um "consenso" sobre o estado atual da rede. Uma vez que não há um servidor central e nem servidores privilegiados de referência, e uma vez que todos os pares da rede também podem atuar como "servidores", os algoritmos e protocolos de comunicação precisam assegurar que haja consistência nas informações que são armazenadas pelos nós e que são por eles propagadas pela rede. A circulação de informação e o estabelecimento de redes de confiança entre pares são questões caras à antropologia clássica, de modo geral, e à antropologia econômica, em particular, e que aqui se evidenciam no emprego de métodos técnicos de aferição da confiança atribuída às partes nas transações.

Como veremos no capítulo 1, esse é o principal problema que o sistema Bitcoin pretende resolver por meio de um sofisticado arranjo de algoritmos e métodos criptográficos para a manutenção de um consenso sobre os balanços e o histórico das transações efetuadas pelos participantes da rede. E, como veremos no capítulo 2, esse problema, imediato para as máquinas mas comumente insolúvel para os humanos, constitui a paisagem e o motivo da maioria das controvérsias sobre o desenvolvimento do protocolo e do software Bitcoin.

Se os protocolos de consenso estabelecem os conjuntos de regras e limitações que os participantes e suas máquinas devem seguir e observar, o

consenso sobre as especificidades dos protocolos e as diferentes visões sobre o sistema é um "artefato emergente" cuja resistência é posta a prova ao longo de intermináveis cadeias de debates sobre viabilidade e pertinência de novas estruturas de dados e regras que devem (ou não) ser implementadas no sistema.

O levantamento de alguns desses debates me permitiu observar, portanto, a dinâmica agonística dos discursos dos participantes, seja de modo mais "estruturado", como nas listas de discussão de programadores e na plataforma de desenvolvimento coletivo de software, seja de modo mais difuso, como na proliferação de grupos de discussão em aplicativos de mensagens instantâneas e em redes sociais, como o Twitter, Facebook, Reddit e Telegram.

Tais tensões, portanto, colocavam um problema para descrição etnográfica do Bitcoin: como descrever um sistema computacional como o que está aqui em questão? Para tanto, o corpo teórico a ser mobilizado é majoritariamente aquele da antropologia e sociologia econômica contemporânea – Michel Callon (1998; 2007), Fabian Muniesa (2014; 2017), Donald MacKenzie (2006; 2009), Juan Pablo Pardo-Guerra (2019), Philip Mirowski (2002, 2013; 2017) – e, de modo mais geral, dos estudos sociais de ciência e tecnologia e dos estudos de mídia e comunicação digital sobre algoritmos, capitalismo, neoliberalismo e mercado financeiro. O livro de Edemilson Paraná, "Bitcoin: a utopia tecnocrática do dinheiro apolítico" (2020), é uma importante referência em língua portuguesa para discussão sobre o conceito de moeda a partir de uma análise marxiana da teoria do valor.

Cabe ressaltar, no entanto, que os entusiastas das criptomoedas, eles próprios, mobilizam teorias, especialmente a partir de trabalhos da área de economia e sociologia, que costumam ser referidas de modo geral sob o termo *criptoeconomia*. Nesse sentido, uma separação entre, de um lado, um *corpus* etnográfico e, de outro, um *corpus* teórico é sobretudo arbitrária. Os elementos da teoria econômica neoclássica, por exemplo, são performados pelos participantes e, no caso do Bitcoin, estão imbricados em seu código-fonte. Da mesma forma, algoritmos, documentos e artefatos digitais que circulam por incontáveis comunidades virtuais e canais de comunicação fazem emergir objetos *tecnofinanceiros* que produzem efeitos sobre mercados locais e globais por meio de complexos mecanismos de *feedback*.

O conceito de *feedback* é uma noção central para o campo de estudos da Cibernética e diz respeito, *grosso modo*, aos vários mecanismos de "retroalimentação" (ou "alças de repetição") que podem servir à regulação (*feedback* negativo) ou à intensificação (*feedback* positivo) de um dado comportamento ou dos fluxos de energia em um sistema (WIENER, 2019). No caso do exemplo acima mencionado sobre as relações entre a teoria neoclássica e a produção de objetos *tecnofinanceiros*, esses mecanismos são efetuados na elaboração de modelos econômicos e implementados como software e sistemas que pretendem se comportar como "modelos ideais". Os vários mecanismos de feedback não apenas condicionam a leitura de fenômenos econômicos programados como "profecias autorrealizáveis", mas também condicionam o comportamento dos *players* humanos como agentes de mercado muitas vezes limitados ao escopo de atuação das máquinas e algoritmos que majoritariamente constituem esses próprios mercados. Dito de outro modo, assim como softwares, sistemas e mercados são programados para funcionar de acordo com "modelos ideais", *traders* humanos são (auto)condicionados a operar, por meio de estratégias operacionais e "análises técnicas" sobre gráficos (esses modelos de modelos), com a frieza e determinação dos *trading bots* que executam séries de regras simples em alta velocidade, capitalizando sobre pequenas e efêmeras diferenças de preço (MACKENZIE, 2014, 2017).

Creio que uma abordagem dos fundamentos ideológicos da criptoeconomia orientada pela noção cibernética de *feedback* permite uma descrição sobre como essas ideologias influenciam o próprio aparato sociotécnico que dá corpo às criptomoedas por meio de implementações técnicas e efeitos de rede específicos.

Ainda de acordo com uma abordagem cibernética, "o propósito de um sistema é aquilo que ele faz" (BEER, 2002, p. 217). De modo análogo, poderíamos dizer o mesmo sobre algoritmos – um algoritmo é aquilo que ele faz. E isso tanto de um ponto de vista mais abstrato, como uma série de procedimentos técnicos que executam instruções pragmáticas, quanto do ponto de vista da materialidade das suas implementações: séries de máquinas, cabos e operadores humanos trocando dados em redes mais ou menos descentralizadas, de acordo com as regras impostas por várias camadas de protocolos de comunicação.

Pretende-se aqui abordar o sistema Bitcoin como um tipo especial de caixa-preta, tal como poderíamos fazê-lo com a "Internet" ou com "a nuvem" onde somos constantemente pressionados a guardar nossos arquivos digitais. De acordo com Latour, no livro Ciência em Ação, "a expressão caixa-preta é usada em cibernética sempre que uma máquina ou um conjunto de comandos se revela complexo demais. Em seu lugar, é desenhada uma caixinha preta, a respeito da qual não é preciso saber nada, senão o que nela entra e o que dela sai" (LATOUR, 2012, p. 14). Essas complexas infraestruturas de comunicação e armazenamento podem ser cotidianamente abstraídas como ícones discretos no canto de uma tela, das quais nos lembramos apenas quando deixam de funcionar corretamente. Ou, por outro lado, podem ser pensadas como complexos sistemas sociotécnicos globais, de origem militar, sob o controle de multinacionais e sob a supervisão intrusiva e cotidiana de agências de vigilância.

A "caixa-preta" da Internet, por exemplo, foi muito bem descrita por Benjamin Bratton, no livro *The Stack: On Software and Sovereignty* (BRATTON, 2015), como uma "pilha" de infraestruturas materiais, protocolos de comunicação e camadas de aplicações. De modo semelhante, a "caixa-preta" da "nuvem" é esmiuçada por Tung-Hui Hu em *A Prehistory of the Cloud* (HU, 2015). Trata-se de um levantamento histórico em que o autor demonstra como a própria ideia de "nuvem" emerge como um artifício descritivo para englobar e abstrair a complexidade dos sistemas que constituíam a ARPANET/Internet ainda na década de 1970 (ou seja, nesse caso, a ideia de "nuvem" surge literalmente como esse artifício "caixa-preta", que depois passa a englobar outros tantos processos e complexidades). Ambos os trabalhos são referências importantes para reflexões sobre a constituição das infraestruturas desses sistemas digitais de comunicação, pois descrevem sistemas cuja extensão e complexidade transcendem as circunscrições localizadas, e cuja historicidade remete à transformação de estruturas de paradigmas anteriores.

Esses e outros trabalhos descrevem, com maior ou menor grau de detalhe, as especificidades e características de infraestruturas de comunicação *sobre as quais* têm se desenvolvido uma infinidade de outras aplicações, redes e sistemas, dentre as quais as redes *peer-to-peer* das criptomoedas. Tais leituras inspiraram a estrutura deste texto, que não pretende repeti-las, mas sim tomá-las como base para

a descrição de outras estruturas complexas que delas dependem. Assim, não se trata de elaborar uma explicação exclusivamente sistêmica dos fenômenos, mas de mobilizar séries de descrições parciais em que a ideia de sistema, em suas várias iterações, opera como um artifício descritivo.

Ao abordar o Bitcoin como uma espécie de caixa-preta, pretendemos não apenas descrevê-lo em função das suas relações com outras "caixas" e sistemas afins, por vezes abstraindo a complexidade do seu funcionamento, mas também pretendemos investigar seu interior, a complexidade técnica e os referentes ideológicos que embasam as abstrações de algoritmos e que determinam os ritmos e os movimentos de informação pela rede. Esta tese, assim, visa oferecer uma descrição das relações entre atores e sistemas a partir das questões político-econômicas suscitadas pelo sistema Bitcoin e pelo *ecossistema* de criptomoedas e ativos digitais.

No capítulo 1, o sistema Bitcoin é descrito a partir de suas dimensões técnica e ideológica, de modo a evidenciar os procedimentos que o constituem enquanto uma moeda percebida por seus usuários como "deflacionária". Por meio de uma descrição do mecanismo de redução gradual dos subsídios da mineração, chamado *halving*, vemos como a diagramática do gráfico de emissão monetária do Bitcoin produz uma imagem comum desse sistema tecnofinanceiro, bem como de ecossistemas derivados. Abordamos, assim, a questão do consenso distribuído em sistemas descentralizados como um problema antropológico, a partir das interfaces da antropologia da técnica e da ciência, de modo a descrever os movimentos, fluxos e as paisagens sociotécnicas que constituem o sistema Bitcoin e os campos associados às demais criptomoedas, marcados por articulações dinâmicas em torno de mercados e comunidades virtuais[18].

No capítulo 2, tratamos especificamente sobre as controvérsias inerentes à descentralização em sistemas digitais. Este capítulo tem por objetivo apresentar o sistema do Bitcoin do ponto de vista de disputas que acontecem nas comunidades de desenvolvedores do Bitcoin enquanto um projeto de software, evidenciando a

18 Parte da discussão apresenta no capítulo foi inicialmente desenvolvida e apresentada no seminário temático "Antropologia, tecnologias digitais e cibercultura" da VII Reunião de Antropologia da Ciência e da Tecnologia (ReACT) (CARDOSO, 2019).

multiplicidade de atores e partes interessadas nessas disputas[19]. Destacamos também como a especialização e radicalização desses grupos tem fomentado a hipótese da *hiperbitcoinização* enquanto uma estrutura de aglomeração por meio da qual os *maximalistas* do Bitcoin se envolvem e desenvolvem suas utopias coletivas e ficções especulativas sociais. De certa forma, esse mito funcional deriva das temporalidades específicas do sistema e das materialidades algorítmicas do Bitcoin, informadas por agendas políticas, econômicas e ideológicas específicas, como os movimentos ciberlibertários e de direita.

No capítulo 3, abordamos o problema da troca como propagação de informação a partir de diferentes perspectivas sobre os fundamentos do sistema Bitcoin e da chamada *criptoeconomia*, suas concepções subjacentes de política e economia, e como os *dashboards*, gráficos e outros dispositivos de mercado são indispensáveis para a produção de totalidades parciais do sistema. Por fim, mostramos como narrativas tomadas de empréstimo da antropologia e da economia servem como pano de fundo para a produção de sentido e de futuros imaginados sobre esses sistemas de dinheiro digital. O objetivo é descrever como essas variações de ideologias neoliberais e *ciberlibertárias* constituem as narrativas e as imaginações de futuro de programadores, entusiastas e investidores acerca de previsões sobre o "futuro da economia" e de profecias sobre o "futuro do dinheiro", do Estado e do próprio Capitalismo.

Esta tese pretende, portanto, evidenciar as imbricações entre os processos de desenvolvimento, governança coletiva e e o estabelecimento de infraestruturas materiais voltadas para a produção de valores digitais em sistemas descentralizados e comunidades virtuais. Uma das principais contribuições deste trabalho é demonstrar alguns dos modos como a justaposição de paradigmas tecnológicos e ideologias político-econômicas estabelecem os fundamentos para implementações de sistemas de trocas e imaginações de futuro particulares. Mais do que uma suposta "alternativa revolucionária" ao sistema financeiro, como costumam alegar os

19 Parte do capítulo 2 foi apresentada como um artigo na 31ª Reunião Brasileira de Antropologia (CARDOSO, 2018). Além disso, diversas considerações presentes neste capítulo e nas seções seguintes foram desenvolvidas anteriormente em Cardoso (2024), publicado em coletânea organizada por Matan Shapiro, intitulada "Crypto Crowds: Singularities and Multiplicities on the Blockchain" (SHAPIRO, 2024).

participantes mais engajados dessas redes, o que se verifica, em larga medida, são os diferentes modos com que esses sistemas acabam por favorer e até mesmo acelerar os processos de acumulação em curso, implementando no próprio código e nas plataformas digitais as modalidades de transação e os modelos econômicos que à primeira vista esses sistemas parecem confrontar.

Ao longo do texto, palavras grafadas em itálico referem-se aos termos utilizados no campo de discussões sobre criptomoedas e, de modo mais geral, no âmbito da ciência da computação e das redes sociotécnicas que o constituem. Embora muitos termos aqui mencionados possam ter uma tradução direta para o português, eles são frequentemente mobilizados em língua inglesa mesmo entre participantes brasileiros, dada a prevalência deste idioma como *língua franca* do campo digital. Sendo assim, uma vez que o campo do debate se articula majoritariamente por meio da língua inglesa, a maioria dos termos e citações foram mantidas no idioma original.

CAPÍTULO 1. O BITCOIN COMO UMA CORRENTE DE ACONTECIMENTOS

O contexto da crise financeira global, do *crash* de 2008 à pandemia da Covid-19, e as especificidades dos mercados nacionais locais são mencionados pelos entusiastas das criptomoedas como fundamentais para compreender as diferentes formas de apreensão das materialidades do sistema Bitcoin e das demais criptomoedas. Ainda que o sonho *cypherpunk*, denominação utilizada por hackers e ativistas, de um dinheiro digital totalmente anônimo e autônomo em relação aos Estados e ao sistema bancário tenha começado a ser imaginado ao longo dos anos 1980, em especulações tecnofinanceiras e experimentos práticos com algoritmos e sistemas criptográficos, é somente com o surgimento do Bitcoin e com o desenrolar da crise de 2008 que, de fato, ele passa a se concretizar. A coincidência de ambos acontecimentos, a disrupção imposta pela crise econômica e a implementação deliberada de uma alternativa *disruptiva* ao sistema financeiro tradicional, não poderia ter sido mais oportuna para o estabelecimento do Bitcoin enquanto uma rede global e distribuída de transações.

De lá para cá, o sistema proposto por Satoshi Nakamoto no *whitepaper* do Bitcoin (NAKAMOTO, 2008) passou por uma série de adaptações, melhorias e transformações, e sua estrutura técnica e teórica vem sendo efetuada em infraestruturas descentralizadas em diversas regiões do planeta. Acoplamentos técnicos e composições digitais, políticas econômicas imaginadas e as economias politico-materiais da produção de hardware e energia são fatores decisivos para o estabelecimento dos procedimentos que viabilizam transações *peer-to-peer*, consensos distribuídos, precificações, reservas de valor, custódias de propriedades digitais e os (pseudo)anonimatos promovidos pela rede.

Tais procedimentos, enquanto características ou funcionalidades do sistema Bitcoin, por exemplo, vêm sendo desenvolvidos, aprimorados e implementados ao longo da última década. Esses desenvolvimentos mobilizam os esforços de dezenas de desenvolvedores de diversos países, seja em função das próprias limitações da arquitetura do Bitcoin, em que certos procedimentos criptográficos e modalidades de transação constituem o "núcleo duro" do funcionamento do sistema, seja em função das demandas, inovações e disputas sobre a introdução de novas funcionalidades, correções de problemas e especulações sobre o futuro da rede. Tais debates se

inscrevem em um contexto histórico mais amplo, desde a criação do sistema de criptografia de chaves públicas nos anos 1970, os experimentos dos *cypherpunks* ao longo dos anos 1980 e 1990 com protótipos de moedas digitais, até o surgimento do Bitcoin.

A prática da criptografia e as implementações de algoritmos criptográficos têm sido, desde meados dos anos 1980, utilizadas e defendidas por *cypherpunks* como uma forma de ação política contra a vigilância digital exercida pelos Estados e agências de inteligência no mundo todo. A criptografia, segundo Julian Assange, "é a derradeira forma de ação direta não violenta" (ASSANGE *et al.*, 2013, p. 28). Muitas das ideias desenvolvidas por programadores, ativistas e pesquisadores, discutidas e compartilhadas em circuitos acadêmicos, fóruns e listas de e-mail, mostram como essas comunidades, também de modo descentralizado e assíncrono, articulam conhecimentos produzidos por diferentes pessoas e grupos para a implementação ou aperfeiçoamento de algoritmos e *softwares* associados, como bem mostram Arvind Narayanan e Jeremy Clark ao traçar uma genealogia das ideias e invenções das últimas décadas por trás da montagem inovadora do Bitcoin (NARAYANAN; CLARK, 2017). Tanto quanto no âmbito da produção do conhecimento científico, a produção do conhecimento tecnológico e computacional – em especial no campo do *software livre*[20] – se dá por meio da articulação (nem sempre harmoniosa) de modos de governança e cooperação em plataformas abertas de comunicação e colaboração digital (KELTY, 2009).

Desde o advento da criptografia assimétrica, também conhecida como "criptografia de chaves públicas", um procedimento descrito pela primeira vez por Whitfield Diffie e Martin Hellman (1976), a possibilidade de comunicações mais seguras e potencialmente anônimas abriu espaço para a imaginação de sistemas de comunicação descentralizada; dentre eles, a implementação de formas de dinheiro que pudessem ser trocadas diretamente entre pares, sem a necessidade de intermediários ou instituições financeiras. Já em 1989, David Chaum, cientista da

20 Os movimentos de *software livre* (ou FOSS: *Free and Open-Source Software*), iniciados na década de 1980 contra a produção e apropriação empresarial de "software fechado" (em que não se tem acesso ao código-fonte), advogam em favor da liberdade dos usuários em rodar, copiar, distribuir, estudar, alterar e melhorar o software que utilizam, vide: https://www.gnu.org/philosophy/free-sw.en.html. Acesso em: 23 fev. 2024.

computação e criptólogo bastante interessado nessas questões, cria o primeiro sistema de dinheiro eletrônico (*e-cash*) que permitia transações anônimas, instantâneas e completamente digitais, ainda que dependente de um servidor central (a sua empresa Digicash) para operacionalizar essas transações[21]. O empreendimento de Chaum obteve relativo sucesso por quase uma década, fazendo do *e-cash* um dos sistemas de pagamento mais utilizados nos anos que antecederam o *boom* do *e-commerce* e das *dotcom* na virada milênio, pois oferecia um mecanismo para bancos transformarem moedas correntes em dinheiro digital e este de volta em moedas nacionais (BRUNTON, 2019, p. 55).[22]

Ao longo dos anos 1990, quase uma dezena de outras tentativas – apenas teóricas ou implementações mais ou menos bem-sucedidas – tinham como objetivo transpor para o universo digital as principais características do dinheiro em espécie (*cash*): anônimo, instantâneo e irrastreável, com transações irreversíveis e sem intermediários. É o caso, por exemplo, do *b-money*, imaginado por Wei Dai em 1998, cujas características básicas em muito se assemelham e antecipam os mecanismos que viriam a ser implementados no Bitcoin dez anos depois[23]. Outro exemplo notável por suas semelhanças é o *Bitgold*, imaginado por Nick Szabo em uma igualmente breve postagem feita em seu blog, em 2005[24]. Motivado, do mesmo modo, pelo problema da criação de uma forma de dinheiro em uma rede sem intermediários centrais, o Bitgold deveria ter propriedades análogas às do ouro – escasso, não-forjável e circulável sem depender de bancos ou terceiros. Szabo descreve um

21 O sistema de pagamentos eletrônicos *e-cash*, implementado pela empresa Digicash, fundada por David Chaum, decorre diretamente de sua pesquisa acerca do que ficou conhecido como "blind signatures technology", que permitia o anonimato dos participantes por meio do emprego de métodos criptográficos de chaves públicas, conforme descrito em seu artigo "Blind Signatures for Untraceable Payments" (CHAUM, 1983). A importância do anonimato dos participantes como aspecto central da garantia da "liberdade" em um mundo crescentemente dominado pelas tecnologias da informação é descrita em mais detalhes no artigo "Security Without Identification: Transaction Systems to Make Big Brother Obsolete" (CHAUM, 1985).

22 E, de fato, anteceder a consolidação dos mercados de *e-commerce* na internet, bem como problemas de gestão diante da demanda dos usuários, foram alguns dos motivos que levaram a Digicash a declarar falência em 1998.

23 Vide o breve documento em que Wei Dai descreve o funcionamento do *b-money*, um projeto que nunca foi implementado: http://www.weidai.com/bmoney.txt. Acesso em: 23 fev. 2024.

24 Uma cópia do texto Bitgold, uma ideia também sem implementação efetiva, está disponível em https://nakamotoinstitute.org/bit-gold/. Acesso em: 23 fev. 2024.

sistema de verificação baseado em um sistema de "prova de trabalho" desenvolvido anos antes por Adam Back e, posteriormente, aprimorado por Hal Finney, chamado *Hashcash*[25]. Em comum, esses projetos e seus autores circulavam e compartilhavam ideias em listas de e-mails dedicadas ao tema da tecnologia, criptografia, criptoanarquismo e ciberlibertarianismo, muitos dos quais também participavam desde as primeiras reuniões dos *cypherpunks* do final dos anos 1980.

Apesar do relativo entusiasmo da década de 1990, e em grande parte devido ao fracasso da maioria dessas implementações, os primeiros anos do século XXI trouxeram poucas inovações nesse sentido. Até que, em novembro de 2008, numa lista de e-mails sobre criptografia, um certo Satashi Nakamoto envia sua primeira mensagem contendo um resumo de seu projeto de dinheiro eletrônico, ainda sem uma implementação consistente, e o link para um *paper* em que descreve os principais componentes de um sistema batizado por ele de *Bitcoin*[26]. Lá, já no título, está a sua primeira definição, sintética e precisa: "Bitcoin: um sistema *peer-to-peer* de dinheiro eletrônico" (*Bitcoin: a peer-to-peer electronic cash system*).

Nas nove páginas que seguem, Nakamoto (2008) descreve um sistema que se baseia em uma rede distribuída (*peer-to-peer*) e em um mecanismo destinado a evitar o "gasto duplo" de moedas. Esta configuração algorítmica define e atrela os procedimentos de validação, de registro de transações e de emissão de novas moedas baseados em um sistema de "prova de trabalho" computacional: a adição constante de novas moedas ao sistema, segundo Nakamoto, deve ser análoga ao gasto de recursos materiais e energéticos que os mineradores de ouro, por exemplo, devem incorrer para aumentar a quantidade de ouro em circulação. Porém, no caso do Bitcoin, os recursos gastos são ciclos computacionais e energia elétrica. Esse procedimento técnico, que consiste na execução intensiva de um conjunto de algoritmos criptográficos, por analogia, passou a ser chamado de *mineração*.

---

25 Tanto o *Hashcash* quanto o *b-money* são citados diretamente como referências no *whitepaper* do Bitcoin (NAKAMOTO, 2008). Vide o *whitepaper* escrito por Adam Back em 2002, em que apresenta e descreve o funcionamento do *Hashcash*: http://www.hashcash.org/papers/hashcash.pdf. Acesso em: 23 fev. 2024.

26 O e-mail original de Satoshi Nakamoto e as primeiras discussões sobre seu projeto, estão disponíveis em "Bitcoin P2P e-cash paper": https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html. Acesso em: 23 fev. 2024.

Todas as transações efetuadas no sistema são anunciadas na rede e replicadas pelos pares, de modo que, a cada dez minutos, elas são agrupadas e validadas em novos blocos de transação. Esses novos blocos, gerados a partir das provas de trabalho computacional, são replicados pela rede e encadeados às várias cópias locais da *blockchain*, uma corrente de blocos, que é a principal estrutura de dados do sistema. Tudo o que está registrado na *blockchain* é considerado pelos participantes como um fato consolidado e irreversível, uma vez que é virtualmente impossível alterar transações já realizadas e validadas.

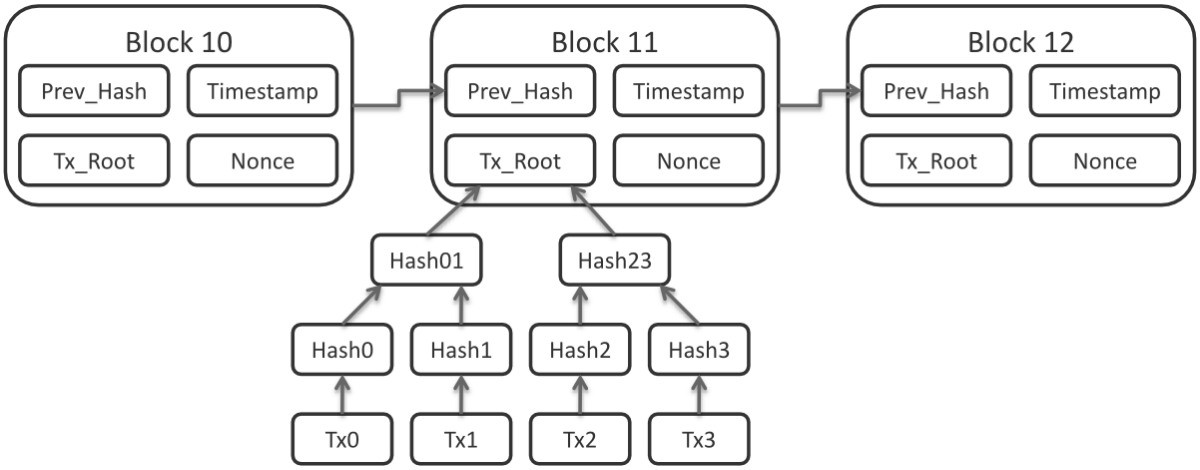

Figura 2: Diagrama de um bloco a partir de um segmento da blockchain. As transações (Tx) são armazenadas em uma estrutura de dados (árvore de Merkle) no interior de cada bloco, que contém também a identificação (hash) do bloco anterior e a prova de trabalho (nonce).

O objetivo deste capítulo é tomar alguns eventos históricos do Bitcoin como acontecimentos relevantes para uma descrição das próprias estruturas e mecanismos do sistema, que produz uma moeda entendida por seus participantes como *deflacionária*. Uma vez que o Bitcoin é constituído por estruturas de dados que definem e compõem seu sistema de registro distribuído de transações, neste capítulo tomo de empréstimo o mecanismo de encadeamento de blocos sequenciais de transações, a *blockchain*, tanto como imagem que orientará a descrição dos componentes que determinam o funcionamento do sistema, quanto como um registro histórico e contábil de acontecimentos desde o *bloco Gênesis*. Os detalhes sobre o funcionamento destes e de outros procedimentos serão abordados adiante e, tal como os próprios procedimentos algorítmicos a que se referem, serão

reiterados sempre que necessário (ainda que, à diferença dos laços de repetição de código, nunca do mesmo modo).

Sendo o sistema Bitcoin um arranjo inovador de ideias já conhecidas – como as redes *peer-to-peer*, a criptografia assimétrica e o mecanismo de "prova de trabalho", que está no cerne do processo de *mineração* – pretendo mostrar, a partir da descrição das estruturas de dados que o constituem, como esta configuração algorítmica produz, no interior do sistema, uma modalidade particular de *escassez digital* caracterizada por um procedimento técnico arbitrário denominado *halving*.

Mais precisamente, na seção seguinte, tomo como referências temporais quatro períodos específicos, que marcam a passagem de diferentes *eras* bem definidas do sistema. Busco argumentar aqui que o *halving* é provavelmente a temporalidade mais significativa do sistema Bitcoin.[27] É por causa desse mecanismo de *halving*, que estabelece uma redução gradual da taxa de emissão monetária do sistema, que o Bitcoin costuma ser descrito como uma moeda deflacionária. As seções seguintes tomam como referente, portanto, essas quatro *eras* para descrever elementos importantes do sistema e de sua história, bem como certas características do procedimento técnico da *mineração*. Tais especificidades da implementação evidenciam como certos aspectos da política econômica neoliberal, especialmente abarcadas aqui pela questão da deflação, estão codificadas e implementadas no próprio *software*.

1.1 IMPLEMENTAÇÃO DE UM SISTEMA DEFLACIONÁRIO

O chamado *bloco Gênesis*, o bloco número zero da *blockchain* do Bitcoin, foi gerado por Satoshi Nakamoto no dia 3 de janeiro 2009. Este bloco cria *ex nihilo* as primeiras 50 moedas (*bitcoins*) do sistema, destinando-as a um endereço específico e, por definição, posteriormente inacessível. À diferença de todos os blocos subsequentes, este bloco traz em seu código, além da cunhagem inicial, uma referência à manchete daquele mesmo dia do jornal britânico *The Times*, sobre as

27 Os principais mecanismos do sistema Bitcoin indicam um sistema que tem pulso (blocos), ritmo (intervalo entre blocos), épocas (cada intervalo de ajuste de dificuldade de mineração, a cada duas semanas, é chamado *epoch*), e uma temporalidade verificável (a *blockchain* como um registro histórico "autoconsistente", um "regime de verdade" matematicamente verificável). Neste capítulo, o foco, contudo, recai nas *eras* (os períodos de quatro anos entre os *halvings*).

políticas governamentais de *bailout* aos bancos nos primeiros meses da crise econômica de 2008. A primeira versão do *software*, junto com seu código-fonte, foi publicada seis dias depois, em 9 de janeiro, na mesma lista de e-mails em que foi inicialmente anunciado em novembro de 2008, criando em torno do projeto uma crescente comunidade de participantes e desenvolvedores.

```
00000000  f9 be b4 d9 1d 01 00 00  01 00 00 00 00 00 00 00  |................|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 3b a3 ed fd  |............;...|
00000030  7a 7b 12 b2 7a c7 2c 3e  67 76 8f 61 7f c8 1b c3  |z{..z.,>gv.a....|
00000040  88 8a 51 32 3a 9f b8 aa  4b 1e 5e 4a 29 ab 5f 49  |..Q2:...K.^J)._I|
00000050  ff ff 00 1d 1d ac 2b 7c  01 01 00 00 00 01 00 00  |......+|........|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 ff ff  |................|
00000080  ff ff 4d 04 ff ff 00 1d  01 04 45 54 68 65 20 54  |..M.......EThe T|
00000090  69 6d 65 73 20 30 33 2f  4a 61 6e 2f 32 30 30 39  |imes 03/Jan/2009|
000000a0  20 43 68 61 6e 63 65 6c  6c 6f 72 20 6f 6e 20 62  | Chancellor on b|
000000b0  72 69 6e 6b 20 6f 66 20  73 65 63 6f 6e 64 20 62  |rink of second b|
000000c0  61 69 6c 6f 75 74 20 66  6f 72 20 62 61 6e 6b 73  |ailout for banks|
000000d0  ff ff ff ff 01 00 f2 05  2a 01 00 00 00 43 41 04  |........*....CA.|
000000e0  67 8a fd b0 fe 55 48 27  19 67 f1 a6 71 30 b7 10  |g....UH'.g..q0..|
000000f0  5c d6 a8 28 e0 39 09 a6  79 62 e0 ea 1f 61 de     |\..(.9..yb...a.|
000000ff
```

Figura 3: Extrato hexadecimal do Bloco Gênesis, que contém a manchete do jornal The Times do dia 3 de janeiro de 2009 e a primeira transação das primeiras 50 moedas do sistema.

Tal como um eclipse, um evento astronômico periódico e sempre bastante aguardado como um acontecimento único e comumente auspicioso, o *halving* é um acontecimento cujos efeitos têm sido motivo de observações, estudos e especulações. Por conta de sua programação periódica, sempre a cada 210000 blocos, o *halving* produz efeitos sobre a produção diária de novos *bitcoins*, definindo diferentes "eras" na temporalidade do sistema. Ao determinar a redução deliberada do *subsídio da mineração* dos blocos de transações, ele atua como um *produtor de escassez*: é por meio deste ajuste programado sobre a cota de emissão monetária, definida no código-fonte, que se estabelece um regime decrescente de oferta de novas moedas ao longo do tempo.

Até o presente momento, desde a criação do sistema em 2009, ocorreram apenas três *halvings*: o primeiro, no bloco número 210000, que marca o fim da

"primeira era" e o início da "segunda era" da *mineração*, quando o subsídio dos blocos foi reduzido dos iniciais 50 *bitcoins* para 25 *bitcoins* por bloco; o segundo *halving* ou a "terceira era", na altura do bloco 420000, que reduziu o subsídio para 12,5 *bitcoins*; e, por fim, o terceiro halving ou a "quarta era", a era em que nos encontramos agora, em que o subsídio, a partir do bloco 630000 é de 6,25 bitcoins por bloco. Tais ciclos de redução estão programados para acontecer até que o subsídio chegue a zero.

A cada dez minutos, os mineradores da rede competem entre si para produzir um bloco válido de transações, ou seja, os mineradores reúnem um conjunto de transações consideradas "pendentes" e buscam agrupá-las em um bloco cujas características satisfaçam um "alvo de dificuldade" estabelecido pelo sistema naquele momento – este alvo estabelece o quão difícil deve ser produzir, por meio do algorítimo de prova de trabalho, um bloco que possa ser considerado "válido". Quando um bloco válido é "encontrado" por um minerador, as transações pendentes por ele agrupadas são consolidadas no *ledger* (a *blockchain*) e o minerador que produziu este bloco recebe como recompensa a soma das taxas das transações ali consolidadas e o subsídio da mineração, que são as moedas recém criadas naquele bloco.

Dado que a cada quatro anos esse subsídio cai pela metade, reduzindo portanto a quantidade de novas moedas que são introduzidas diariamente no sistema, o processo de mineração tende a ser tornar gradualmente mais custoso. O Bitcoin é, por isso, percebido por seus usuários e participantes do sistema como uma criptomoeda *deflacionária*, pois, se a quantidade de novas moedas produzidas sempre diminui ao longo do tempo, a oferta total de moedas em circulação tende portanto a um teto preestabelecido. Este teto, o número máximo de *bitcoins* que podem ser criados na rede, está definido no código-fonte em 21 milhões de unidades, e a redução periódica da cota de emissão de moedas por bloco tem como objetivo tornar a criação de novos *bitcoins* uma atividade cada vez mais onerosa. Supondo, por um momento, que não haja alteração na quantidade de máquinas mineradoras na rede, após um *halving* torna-se mais custoso produzir moedas e validar as transações do sistema, pois, em tese, a quantidade de energia e ciclos computacionais necessários para a criação de um bloco de transações passa a ser

recompensada com apenas a metade da quantidade de moedas dos blocos anteriores da era anterior. Cabe notar que cada bitcoin pode ser trocado "por inteiro" mas também em frações de até 8 dígitos decimais, sendo 0,00000001 a menor parte possível, que passou a ser denominada pela comunidade de usuários como um *satoshi*, em homenagem ao criador do Bitcoin, Satoshi Nakamoto.

```
1151
1152 CAmount GetBlockSubsidy(int nHeight, const Consensus::Params& consensusParams)
1153 {
1154     int halvings = nHeight / consensusParams.nSubsidyHalvingInterval;
1155     // Force block reward to zero when right shift is undefined.
1156     if (halvings >= 64)
1157         return 0;
1158
1159     CAmount nSubsidy = 50 * COIN;
1160     // Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years.
1161     nSubsidy >>= halvings;
1162     return nSubsidy;
1163 }
1164
```

Figura 4: Trecho do código-fonte da implementação de referência do Bitcoin em que está definida a política de subsídios do sistema (https://github.com/bitcoin/bitcoin).

A política monetária de emissão de moedas e de subsídios está definida, no código-fonte do Bitcoin, por um algoritmo de apenas 11 linhas (Figura 4). Como todo bom algoritmo, sumário e explícito (KNUTH, 1997, pp. 4–6), ele determina que a quantidade de moedas criadas por bloco, o chamado *subsídio* da *mineração*, é inicialmente de 50 moedas, e que, a cada 210000 blocos, o que equivale a aproximadamente quatro anos, essa quantidade deve ser reduzida pela metade[28].

Assim, nos primeiros quatro anos de funcionamento do sistema, entre 2009 e 2012, foram criadas 50 moedas a cada dez minutos, somando, neste período, 10,5 milhões de moedas – ou seja, metade da oferta total possível prevista pelo sistema. Nos quatro anos seguintes, foram criadas 25 moedas a cada dez minutos (somando assim 5,25 milhões de unidades). Posteriormente, a cada dez minutos, criadas 12,5 moedas por bloco (2,6 milhões). Atualmente, no início de 2024, e às vésperas de um

28 Os blocos de transações são criados, em média, a cada 10 minutos. Esta é uma regra do sistema, cuja verificação e observação deste intervalo cabe a um algoritmo de "ajuste de dificuldade", que será descrito adiante. Assim, um período de 210000 blocos criados a cada 10 minutos equivale a aproximadamente quatro anos.

novo *halving*, estão sendo criadas 6,25 moedas por bloco, totalizando assim cerca de 19,5 milhões de moedas em circulação. Com o próximo *halving* previsto para meados de abril de 2024, este número será reduzido para 3,125 moedas por bloco.

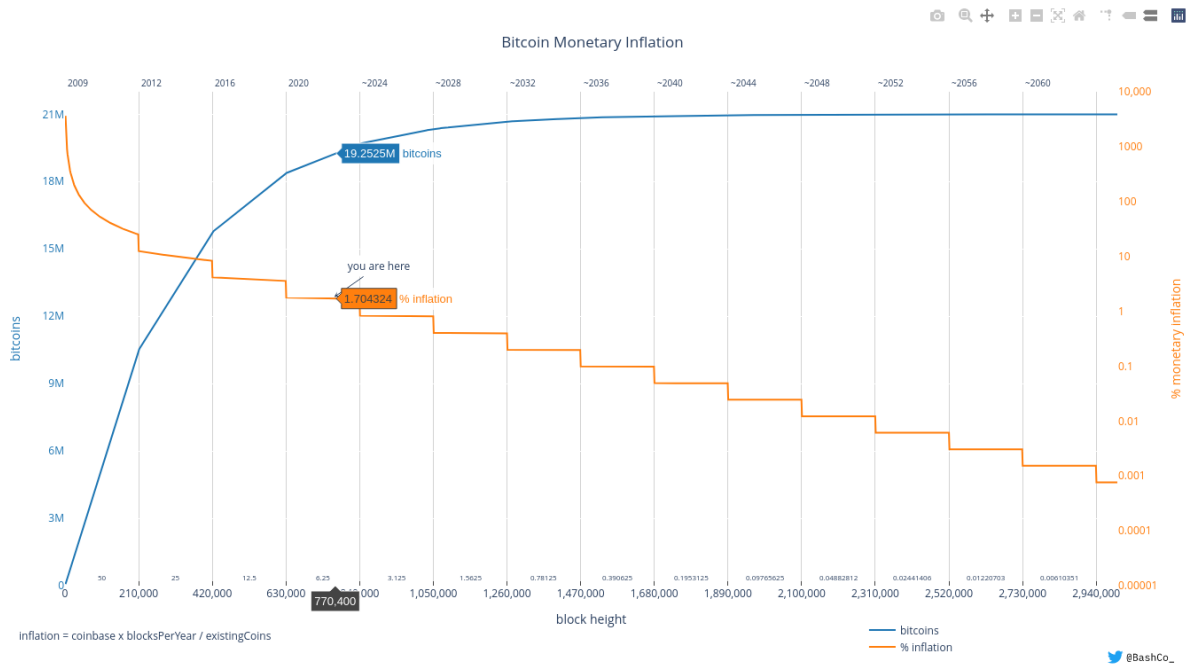

Figura 5: Gráfico da inflação monetária do Bitcoin. A linha azul representa a quantidade de moedas em circulação; a linha laranja, as diferentes "eras" de subsídio (os halvings). Fonte: https://bashco.github.io/Bitcoin_Monetary_Inflation

Tomando o algoritmo apenas como a descrição abstrata de um processo de emissão de moedas, vemos assim 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 (ZIMMER, 2017).

Satoshi Nakamoto explicita essa analogia em seu *whitepaper*: "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, p. 4). Peter Todd, um analista de sistemas e de segurança que já contribuiu com várias linhas de código para a implementação de referência do Bitcoin, foi perguntado em janeiro de 2019 pelo *host* de um *podcast*: "o

que é o Bitcoin?" A resposta de Todd, numa tradução livre, foi a seguinte: "Bitcoin é uma estrutura compartilhada de dados que nós tornamos artificialmente custosa de se modificar ao destruir [gastar] energia toda vez que nós a atualizamos."[29] Essa definição do Bitcoin em função da quantidade de energia e processamento explica também por quê Nakamoto estipula que o registro distribuído de transações deve ter como referência a maior cadeia de processamento computacional acumulado, evitando assim a proliferação de cadeias alternativas e garantindo a integridade da estrutura de dados.

A criptografia implica uma noção de temporalidade muito específica. Nenhum método criptográfico é totalmente "seguro" ou "inquebrável", mas os métodos comumente utilizados em sistemas digitais são considerados "seguros o bastante" em "tempo hábil", uma noção do campo da ciência da computação que estima o tempo necessário para que um computador muito potente seja capaz de "quebrar" a criptografia utilizada em uma mensagem. Essa temporalidade é geralmente calculada em anos, e um bom algoritmo de criptografia pode exigir centenas ou milhares de anos para ser quebrado por um computador que eventualmente iniciasse essa tarefa hoje.

No caso da *blockchain*, uma vez que as provas criptográficas de cada transação são assinadas por chaves criptográficas diferentes, e os blocos são "assinados" por um *hash* (uma função criptográfica unidirecional, isto é, não reversível) de todas as informações nele contidas, qualquer alteração em blocos anteriores (por exemplo, a adulteração de uma transação), implicaria uma necessária alteração de todos os blocos subsequentes. Uma vez que o poder computacional de toda rede é mobilizado na validação dessas transações, um "atacante" teria de dispor de, no mínimo, metade de todo poder computacional da rede para realizar uma alteração desse tipo.

29 No original: "Bitcoin is a shared data structure that we make artificially expensive to change by destroying energy every time we update it." O programa número 68 do podcast *What Bitcoin Did* foi publicado no dia 29 de janeiro de 2019 com o título "Peter Todd on the Essence of Bitcoin". A citação em questão está no minuto 11 deste programa, disponível em: https://www.whatbitcoindid.com/podcast/peter-todd-on-the-essence-of-bitcoin. Acesso em: 23 fev. 2024.

Na prática, de acordo com a "teoria dos jogos" no sentido mais corriqueiro utilizado em narrativas sobre o sistema, seria muito mais vantajoso que, em vez de "atacar" a rede, alguém com tamanho poder computacional trabalhasse para coletar para si todas as recompensas, criando assim apenas blocos válidos. Isso também significa que quanto mais antiga é uma transação, mas "segura" ela é. Ou, em outros termos, quanto mais antiga é uma transação, mais "verdadeira" (pois "mais consensual") ela é. É de praxe que, para que uma transação seja considerada de fato irreversível e imutável, se deva esperar por até seis "confirmações" – ou seja, é prudente esperar que seis blocos subsequentes sejam minerados (em cerca de uma hora), para que o poder computacional necessário para invalidar ou alterar a informação contida num bloco (e, portanto, alterar também todos os blocos seguintes) seja tão grande a ponto de que seja impossível fazê-lo em tempo hábil.

A rigidez das regras de emissão e a inviolabilidade das transações são tidas como o principal atrativo do sistema. Tal performatividade *deflacionária* difere deliberadamente do regime *inflacionário* de emissão das moedas emitidas por Bancos Centrais. Ou seja, ao contrário das moedas fiduciárias nacionais, caracterizadas pela progressiva expansão da sua base monetária, o Bitcoin tem uma taxa de emissão que é *programada*: dado que novos blocos de transações são gerados a cada 10 minutos, eventualmente, por volta do ano 2140, haverá um último *halving* e o subsídio dos blocos será igual a zero, restando apenas a soma das taxas das transações validadas por bloco como incentivo econômico aos *mineradores*. Nesse futuro, o sistema terá alcançado o teto preestabelecido de 21 milhões de moedas em circulação, tornando-se assim, de acordo com os *bitcoiners*, o ativo mais escasso e mais valioso do planeta. Esta é a principal regra de consenso do sistema.[30]

30 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 (trecho destacado na Figura 4). Nota-se no trecho destacado que "COIN" (linha 1159) é uma constante utilizada como base do cálculo, sendo definida em outro arquivo do código-fonte como o equivalente a "100000000", ou seja, algo que pode ser divisível em 100 milhões de partes inteiras, que são na prática as menores unidades possíveis do sistema. Como discutiremos adiante, a ideia de que *bitcoins* como "moedas" é uma abstração tanto do código-fonte, quanto dos modos de apreensão do sistema enquanto uma forma de "dinheiro eletrônico".

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.

Portanto, embora também existam outros mecanismos que compõem e ensejam as temporalidades específicas do sistema Bitcoin, como os ajustes do "alvo de dificuldade" da mineração, que ocorrem a cada duas semanas, o mecanismo de emissão monetária instituído pelos *halvings* dos subsídios de mineração, é, do meu ponto de vista, o que de forma mais eloquente caracteriza o Bitcoin como um sistema de dinheiro eletrônico bastante particular. É por causa desse mecanismo de produção de escassez digital que mais e mais mineradores têm cotidianamente conectado milhares de novas máquinas a essa rede, na expectativa de competir por esses subsídios e apostando que, ao longo do tempo, e por causa da emissão cada vez mais escassa, o valor do Bitcoin tenderia sempre a aumentar e, talvez, até aumentar indefinidamente.

Assim, a "primeira era" do Bitcoin é marcada pela "inicialização" do sistema, com a publicação do código-fonte da sua primeira versão, em torno do qual se constituiu uma comunidade restrita de especialistas – programadores, *hackers*, *early adopters* – e uma gradativa expansão da rede, sustentada, então, majoritariamente, por usuários domésticos e pequenas operações. É também nessa era, a partir de meados de 2010, que o Bitcoin passa ser negociado entre usuários de comunidades virtuais e nos primeiros mercados digitais (*exchanges* e mercados anônimos da "deep web", como o famoso *Silk Road*, por exemplo), assunto que voltaremos a abordar no capítulo 3.

O primeiro *halving* do sistema ocorreu em 28 de novembro de 2012. À época, um *bitcoin* era negociado por cerca de 13 dólares, metade do seu preço

recorde até então (26 dólares em outubro de 2011). A "segunda era", a partir deste evento, coincide com o início da precificação do Bitcoin em *exchanges* (corretoras e casas de câmbio digitais) e com a expansão da rede para além do nicho dos programadores e *cypherpunks*. Pode-se dizer, portanto, que os *halvings* são eventos que também exercem influência sobre o preço de negociação de *bitcoins* em mercados digitais. A despeito da alta volatilidade desta criptomoeda, os custos de operação (e, claro, especulação), ao longo de sua primeira década de existência, têm resultado numa valorização progressiva – dos preços inferiores a 1 dólar em 2010, aos vários milhares de dólares por moeda nos últimos anos. As frequentes oscilações no preço também podem alterar a composição da rede, produzindo efeitos às vezes inesperados – como, por exemplo, uma variação na quantidade de mineradores ativos que, diante de uma redução no subsídio de mineração ou desvalorização repentina, podem decidir por desligar suas máquinas por vários meses; ou, ao contrário, diante de uma alta no preço de negociação, podem voltar a ligá-las e, assim, encontrar a concorrência de novos mineradores.

O segundo *halving* acontece no dia 9 de julho de 2016, e traz no cabeçalho do bloco #420000 uma mensagem de amor: "#&#xfffd;h##七彩神仙鱼 Chandler Guo loves YangYang Jin.#🐟#Mined by zzhhzz"[31], dando início a uma "terceira era" em que a quantidade de usuários da rede passa a se tornar cada vez mais numerosa, extrapolando o nicho inicial dos programadores e entusiastas e ganhando novas proporções em relação ao seu potencial de valorização em mercados digitais então emergentes.

O bloco que antecede o do terceiro *halving* (ocorrido no dia 12 de maio de 2020) também traz em seu cabeçalho uma mensagem, dessa vez fazendo alusão ao *Bloco Gênesis* e à crise econômica de 2008, utilizando o mesmo expediente escolhido por Satoshi Nakamoto para criticar as políticas monetárias dos bancos

31 A mensagem de amor do minerador chinês, aqui reproduzida literalmente, pode ser visualizada em https://blockchair.com/bitcoin/block/420000. Os blocos são estruturas de dados com campos pré-definidos. Um desses campos, chamado OP_{RETURN}, foi introduzido na primeira versão com uma funcionalidade que se tornou obsoleta a partir de versões seguintes. Por comportar um número limitado de *bytes* de informação, que é ignorada pelo sistema, esse campo tem sido usado desde então para "assinaturas" dos criadores do bloco, ou mesmo para o armazenamento de pequenos arquivos ou fragmentos de arquivos. Sobre manifestações de amor e até mesmo casamentos consumados via *blockchain*, ver artigo "Love on the block", de Max Dovey (in GLOERICH; LOVINK; DE VRIES, 2018).

centrais: "NYTimes 09/Apr/2020 With $2.3T Injection, Fed's Plan Far Exceeds 2008 Rescue".[32] Esta mensagem explicita e reitera a crítica às economias nacionais e às "moedas fiduciárias" de modo geral, um tropo discursivo bastante recorrente em discussões nas comunidades de criptoativos. De certo modo, ela também reforça a proposição de que o Bitcoin, ao contrário de todas as demais moedas, seria "dinheiro de verdade" (*sound money*), pois deflacionário e "verdadeiramente apolítico". Tal proposição é corriqueira entre os entusiastas e vem, necessariamente, carregada de vieses ideológicos neoliberais e de um "utopismo tecnológico" (PARANÁ, 2020). A mensagem bíblica registrada no campo OP_RETURN de uma transação inserida no bloco #666.666, na noite do dia 18 de janeiro de 2021, também parece reforçar esse caráter utópico: "Do not be overcome by evil, but overcome evil with good - Romans 12:21".[33]

1.2 INFRAESTRUTURA DA MINERAÇÃO

Nesta seção, o sistema Bitcoin é descrito a partir da relação com outros sistemas sociotécnicos, por meio das relações e economias político-materiais que constituem diferentes interfaces materiais, a fim de evidenciar como a dinâmica da mineração, embora digital, reencena a lógica da mineração de metais, tanto como inspiração teórica, conforme descrita inicialmente por Nakamoto, quanto como um procedimento de extração e acumulação característico do capitalismo. Há, de certa maneira, dois sistemas sociotécnicos distintos implicados no Bitcoin: aquele que constitui uma infraestrutura que permite, literalmente, extrair energia da terra para criar, materialmente, uma série de maquinas acopladas entre si; e aquele que cria uma infraestrutura que pretende superar e suplantar o sistema financeiro tradicional.

A novidade introduzida pelas criptomoedas está em atrelar ao procedimento de mineração a atribuição de um regime de propriedade, por meio de um sistema de titularidade baseado em chaves criptográficas, sobre as novas moedas que entram em circulação, garantindo aos mineradores a possibilidade de obtenção de lucros

32 Os dados do bloco #629.999 podem ser visualizados em https://explorer.btc21.org/block/000000000000000000d656be18bb095db1b23bd797266b0ac3ba720b1962b1e. Acesso em: 23 fev. 2024.

33 A transação contida no bloco #666.666 pode ser visualizada em https://mempool.space/tx/057954bb28527ff9c7701c6fd2b7f770163718ded09745da56cc95e7606afe99. Acesso em: 23 fev. 2024.

sobre a tarefa de validação das transações efetuadas pelos pares da rede. A combinação dos procedimentos de validação e emissão monetária em um mesmo procedimento, que demanda o emprego de máquinas e alto consumo de energia, mostra como o sistema foi construído para incentivar a atuação "honesta" dos participantes, ainda que tenha como consequência a concentração de poder computacional em agrupamentos de usuários especializados – um efeito não antecipado na montagem inicial, mas decisivo no desenvolvimento do Bitcoin enquanto uma rede global de transações que veio a favorecer o desenvolvimento de indústrias de hardware dedicado (máquinas ASIC) e estratégias energéticas particulares.

Um ponto importante da transição da "primeira era" para a "segunda era" da mineração é justamente a transição do que se poderia denominar *mineração doméstica*, realizada por computadores comuns e instalações caseiras de séries de placas de vídeo (GPUs), para uma mineração em escala industrial, com o surgimento das primeiras máquinas e empresas especializadas na produção de *ASICs* (*Application-Specific Integrated Circuit*) dedicadas exclusivamente ao procedimento de mineração[34]. Os circuitos integrados de aplicação específica podem ser desenvolvidos para otimizar a execução de determinados algoritmos ou rotinas de programação, sendo assim considerados como tipos de hardware dedicados à tarefas particulares. No caso em questão, os ASICs são máquinas desenvolvidas com o intuito de otimizar o cálculo da função criptográfica unidirecional (*hash*) utilizada no procedimento de "prova de trabalho" do Bitcoin, definida pelo algoritmo criptográfico SHA-256. Enquanto um computador convencional pode realizar pouco mais de mil cálculos desse tipo por segundo, um ASIC moderno pode realizar alguns trilhões de cálculos por segundo, sendo, assim, e por várias ordens de grandeza,

34 Ao contrário, por exemplo, dos computadores domésticos, desenvolvidos para computação de propósito geral, essas máquinas possuem circuitos integrados desenvolvidos para um uso particular. Atualmente, a empresa chinesa Bitmain, que representa o maior aglomerado de mineração do sistema Bitcoin do mundo, detém também o monopólio do mercado de produção de ASICs especializadas no processamento do algoritmo criptográfico utilizado pelo Bitcoin e algumas outras criptomoedas (SHA-256). Devido à alta demanda de energia elétrica para alimentação e resfriamento das dessas máquinas, operações de mineração tendem a se instalar em localidades e países onde a energia e demais custos de operação são mais baratos, como China, Venezuela e Paraguai, e mais recentemente nos Estados Unidos, por exemplo.

muito mais eficiente em termos de poder computacional, porém com um custo energético também muito maior do que o de um computador pessoal.

O cerne do desafio de validação consiste em um procedimento de "prova de trabalho" (*proof-of-work*) que só pode ser solucionado por meio de um método de força bruta (*brute-force*): o minerador deve encontrar um número (*nonce*) que, quando combinado àquelas transações pendentes, produza um resultado satisfatório – isto é, o produto dessa combinação, quando introduzido em uma função criptográfica unidirecional (*hash function*), deve ter como resultado um número que esteja contido em um dado intervalo de resultados possíveis (MACKENZIE, 2019b). Assim, os mineradores devem proceder por tentativa e erro, executando muitos milhões de cálculos por segundo, até encontrar um número adequado, e é este número (*nonce*), quando encontrado ao acaso, que "prova" que uma certa quantidade de poder computacional foi empregada na validação de um bloco. Segundo Antonopoulos (2015), "a good way to describe mining is like a giant competitive game of *sudoku* that resets every time someone finds a solution and whose difficulty automatically adjusts so that it takes approximately 10 minutes to find a solution" (p. 26). Isso significa que quanto maior a quantidade de máquinas dedicadas que um minerador possa empregar nessa disputa, mais chances ele terá de produzir blocos válidos antes dos demais e, assim, acumular para si os *bitcoins* recém criados.

Na prática, o procedimento de *mineração*, governado por este algoritmo de *prova de trabalho*, consiste na contínua transformação de energia elétrica e processamento computacional em "unidades discretas digitais". É, portanto, em função desse procedimento que parte do aparato sociotécnico do Bitcoin vem se consolidando como uma indústria especializada na produção de máquinas dedicadas (ASICs) à conversão de energia elétrica e ciclos computacionais em *bitcoins*, e ao estabelecimento de *instalações de mineração* em localidades onde o custo energético é relativamente baixo, seja por conta de subsídios estatais, seja por conta da negociação de contratos de energia excedentes de outras indústrias.

Dado o incentivo econômico a esse esforço coletivo de validação (tanto das transações quanto das regras de consenso), a transição da "mineração doméstica"

para uma mineração em escala industrial, característica deste período, vai se consolidar na "terceira era", inviabilizando por completo as instalações domésticas e abrindo caminho para o domínio dos *mineradores* enquanto um agrupamento de participantes altamente especializados. Tal especialização catalisa o surgimento de empresas dedicadas à produção e comercialização de *ASICs* e às instalações conhecidas como *mining farms* – galpões com as proporções de grandes *datacenters*, repletos de máquinas mineradoras rodando de forma ininterrupta. Estima-se que pelo menos metade de todo processamento computacional do sistema Bitcoin, chamado *hashrate*, seja proveniente de instalações localizadas na China. Outros países, como o Irã, parecem estar ganhando proeminência nesse mercado de mineração, por conta de subsídios governamentais sobre contratos de energia. A dificuldade em estimar um número preciso advém da própria arquitetura do sistema, embora análises *off-chain* (ou seja, levando em conta informações externas ao sistema), embasem esses números[35].

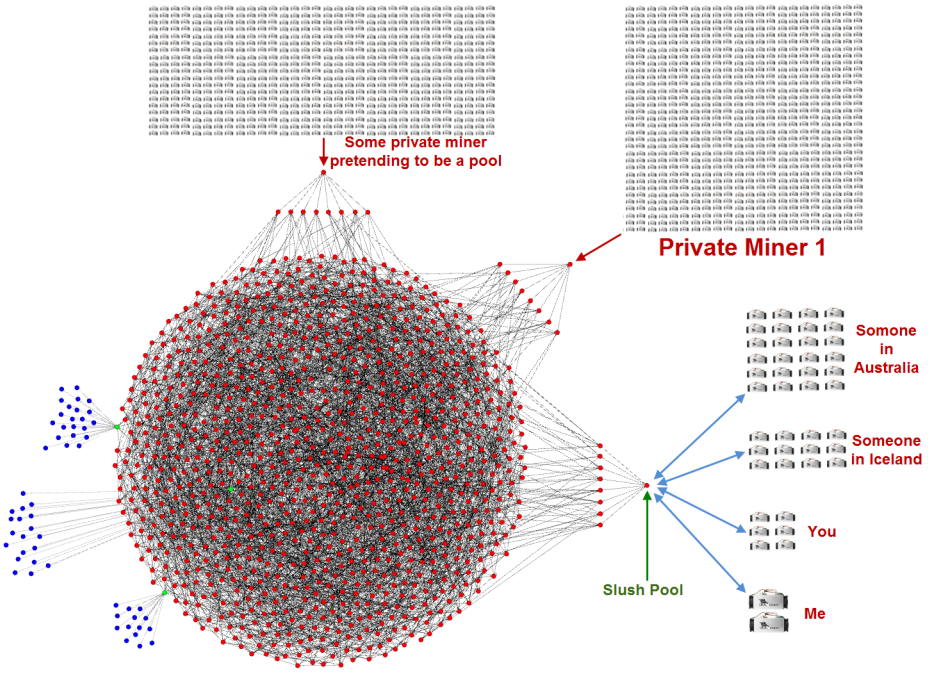

Figura 6: Diagrama evidenciando a rede P2P do Bitcoin como um emaranhado de pontos conectados; não há como aferir a quantidade de máquinas por traz de um ponto específico. os pontos em azul representam serviços que rodam a partir de nós particulares.

35 De acordo com o relatório "Bitcoin Mining Hashrate and Power Analysis" da BitOoda Research e do Fidelity Center for Applied Technology: https://bitooda.medium.com/bitcoin-mining-hashrate-and-power-analysis-bitooda-research-ebc25f5650bf. Acesso em: 23 fev. 2024.

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

É por meio do processo de mineração que os mineradores mobilizam grandes operações para a instalação de *clusters* de máquinas com o objetivo maximizar seus ganhos na validação das transações feitas na rede, coletando as taxas das transações e recompensas que obtêm a cada novo bloco minerado. Também é por meio deste processo que novas moedas são criadas e entram em circulação nos mercados digitais, exercendo uma determinada pressão de venda diária, em função da dificuldade da mineração e dos custos de operação e manutenção das máquinas.[36] Nesse sentido, a "variável flutuante" da equação dos mineradores, mais do que o preço e a vida útil das máquinas, costuma ser o preço da energia elétrica em uma determinada localidade. Os custos com energia – usada para alimentar as máquinas e o sistema de exaustão de calor de uma instalação –

36 Atualmente são criados 6,25 *bitcoins* por bloco a cada dez minutos. Somados, a taxa de emissão diária é de 900 bitcons, que, segundo alguns interlocutores, exercem uma "pressão de venda" no mercado por parte dos mineradores que precisam pagar por seus investimentos e resgatar lucros (o que não significa que essa quantidade de *bitcoins* seja necessariamente vendida todos os dias). O site https://coinmarketcap.com estima que, dos 19,5 milhões de *bitcoins* em circulação, o volume diário de negociação nos mercados digitais (*exchanges*) é de cerca 1,5 milhões *bitcoins*. No Brasil, o site https://cointradermonitor.com/preco-bitcoin-brasil estima que pouco mais de 1 mil bitcoins são negociados diariamente em *exchanges* nacionais. Em janeiro de 2021, foi movimentado um volume de 49 mil *bitcoins* https://valorinveste.globo.com/mercados/cripto/noticia/2021/02/03/brasileiros-movimentaram-mais-de-49-mil-bitcoins-em-janeiro.ghtml. Acesso em: 23 fev. 2024.

correspondem a cerca de 70% dos gastos mensais de uma operação de mineração, de acordo com interlocutores que pesquisam ou operam nesse mercado.

As operações podem ser montadas e desmontadas (máquinas são desligadas temporária ou permanentemente) em função dos custos de energia ou de um aumento da dificuldade da mineração. Segundo um interlocutor, mineradores poder minerar abaixo da sua faixa de lucro, na expectativa de que o valor do Bitcoin venha a subir no futuro (o que reflete uma crença na alta constante dos preços); desse modo, os *bitcoins* minerados passam a ser acumulados para um momento futuro, enquanto sua operação pode rodar por até vários meses no prejuízo. Uma alternativa, nesses casos, é conectar máquinas à *pools* de mineração, acoplamentos virtuais em que máquinas distribuídas em diversas localidades do planeta contribuem coletivamente em um mesmo esforço computacional para maximizar suas chances de produzir blocos válidos e dividir os lucros de modo proporcional.

A dificuldade de mineração é determinada por um algoritmo de "ajuste de dificuldade", um mecanismo de *feedback negativo* que ajusta automaticamente, a cada 2016 blocos (o equivalente a aproximadamente duas semanas), o quão difícil deve ser a criação de um bloco. É este mecanismo de autorregulação que garante que a taxa de emissão monetária se comporte de modo mais ou menos uniforme, pois a dificuldade da mineração está sujeita a esses ajustes periódicos em função da quantidade de máquinas conectadas à rede. Isso significa que quanto mais mineradores estão conectados à rede, isto é, quando há mais poder computacional disponível, mais difícil deve se tornar a mineração para que os novos blocos de transações sejam criados sempre em um intervalo de cerca de dez minutos; se a mineração estiver "fácil demais", os blocos podem ser criados com mais facilidade e em intervalos menores; se estiver "difícil demais", os blocos podem ser criados em intervalos muito grandes, prejudicando o funcionamento da rede. Historicamente, foram poucas as vezes em que a mineração ficou "mais fácil". É seguro dizer que o poder computacional agregado da rede (o chamado *hashrate*) é algo que tende sempre a aumentar, seja pela entrada de novos mineradores, seja pelo aumento da eficiência de novas máquinas, a despeito do subsídio dos blocos tender sempre a diminuir.

Esse é o jogo dos mineradores e a grande aposta dos investidores: buscar meios de maximizar suas estreitas margens de lucro montando operações mais ou menos itinerantes em função da "arbitragem" (comparação) dos preços e contratos de energia elétrica em diversas localidades do planeta – em alguns casos, indústrias de energia e indústrias pesadas com contratos já estabelecidos que vendem ou alugam seus próprios contratos de energia para que o excedente seja consumido na mineração de criptomoedas. Algumas empresas estão investindo no ramo de produção de energia para alimentar suas próprias operações de mineração.

Estimativas de economistas e pesquisadores colocam o consumo energético do sistema Bitcoin como equivalente a um país como a Áustria ou a Irlanda. Outros especulam que o Bitcoin, seguindo nesse ritmo de crescimento, virá a consumir toda a energia elétrica do planeta. Outros, ainda, dizem o mesmo, mas de modo entusiasmado: o Bitcoin consumirá toda energia do planeta pois toda energia ociosa será consumida na mineração de *bitcoins* para não ser "desperdiçada", fazendo com que essa criptomoeda funcione como uma "reserva de energia". Tal estágio, segundo algumas narrativas, é conhecido como "hiperbitcoinização" (*hiperbitcoinization*), quando o Bitcoin será então a única moeda global, como veremos no capítulo 2. Seja como for, o que importa notar é que a transformação de energia em unidades discretas digitais, atreladas a uma noção de propriedade digital constituída por algoritmos criptográficos, é um procedimento termodinâmico decisivo na implementação bem-sucedida desses aparatos sociotécnicos.

O sistema, com seus algoritmos, aspectos técnicos e infraestrutura material se constitui enquanto um artefato técnico autoconsistente, que, por vezes paradoxalmente, parece apartar-se da própria multidão de participantes por meio da contínua execução sumária de regras e rotinas virtualmente imutáveis[37]. Ainda que funcione como um relógio, não mede a passagem do tempo, mas instaura sua temporalidade em função de um intrincado arranjo sociotécnico de humanos, máquinas e infraestruturas dispersas já consolidadas, por meio da contínua extração e transformação de energia elétrica em um registro digital imutável: "It is a planetary-

37 Sobre o "núcleo duro" das regras de consenso do Bitcoin, Satashi Nakamoto escreveu no fórum BitcoinTalk em 2010: "The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime." https://bitcointalk.org/index.php?topic=195.msg1611#msg1611. Acesso em: 23 fev. 2024.

scale, thermodynamically-guaranteed, self-evident system of immutability" (ANTONOPOULOS, 2016b, n.p). Como um sistema cibernético, permite a troca descentralizada e distribuída de ativos digitais em um ambiente autorregulado, mas, como um sistema termodinâmico, também se caracteriza por outras séries de troca: trocas de energia, trocas de calor, trocas de valor.

A questão do consumo energético se inscreve em um debate ecológico mais amplo que não pode ser ignorado. Todo o sistema computacional global, somando todos os computadores domésticos, todos os sistemas empresariais e todos os *datacenters*, é responsável pelo consumo de cerca de 5% de toda energia elétrica produzida no planeta (WOLPERT, 2018).

Em 2017, uma matéria foi bastante difundida em sites especializados em criptomoedas e portais de notícias sobre economia. Em suas várias versões, noticiavam um estudo feito pelo economista holandês Alex de Vries sobre o consumo energético do sistema Bitcoin: a partir de alguns pressupostos sobre a quantidade de máquinas mineradoras e o "consumo médio por transação", de Vries havia calculado que a rede Bitcoin viria consumir uma quantidade de energia elétrica equivalente ao consumo anual de países como a Irlanda ou a Áustria, podendo chegar a quase 8 GW naquele ano. No estudo, publicado no ano seguinte na revista Jaule sob o título "Bitcoin's Growing Energy Problem" (DE VRIES, 2018), a metodologia empregava os valores nominais de consumo energético dos principais modelos de ASICs (máquinas especializadas no procedimento de mineração), a quantidade total de poder computacional mobilizada pela rede e os custos operacionais estimados em uma instalação de mineração, como os gastos com a exaustão do calor produzido em galpões com centenas ou milhares de máquinas. De Vries especulava, assim, que, com a média de 200 mil transações diárias efetuadas no sistema Bitcoin, cada transação consumisse algo em torno de 300 a 900kWh, a depender do volume diário.

Estima-se, a partir do estudo de De Vries, que o sistema *peer-to-peer* Bitcoin, sozinho, consuma atualmente 0,5% da produção de energia global[38], ou

38 Essas estimativas costumam ser controversas, pois variam em função dos métodos aplicados. Seriam 0,25% de acordo com "Bitcoin consumes more energy than Switzerland, according to new estimate", que se baseia no índice CBECI. Disponível em:

cerca de 70 TWh por ano (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 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 e a implementação de algoritmos capazes de otimizar o tamanho (em bytes) das transações e, assim, otimizar os custos por transação.

Atualmente, dois índices têm sido considerados por especialistas como os mais relevantes para aferir o consumo energético do sistema Bitcoin: o *Bitcoin Energy Consumption Index*, mantido pelo *Digiconomist* (projeto iniciado por Alex de Vries)[39], e o *Cambridge Bitcoin Electricity Consumption Index* (CBECI)[40], lançado em 2019 e mantido por pesquisadores do Centre for Alternative Finance da Universidade de Cambridge. No entanto, em função das diferentes metodologias empregadas, os valores atuais divergem consideravelmente.

https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison. Acesso em: 23 fev. 2024.

39 Disponível em: https://digiconomist.net/bitcoin-energy-consumption. Acesso em: 23 fev. 2024.

40 Cambridge Bitcoin Electricity Consumption Index (CBECI). Disponível em: https://www.cbeci.org. Acesso em: 23 fev. 2024.

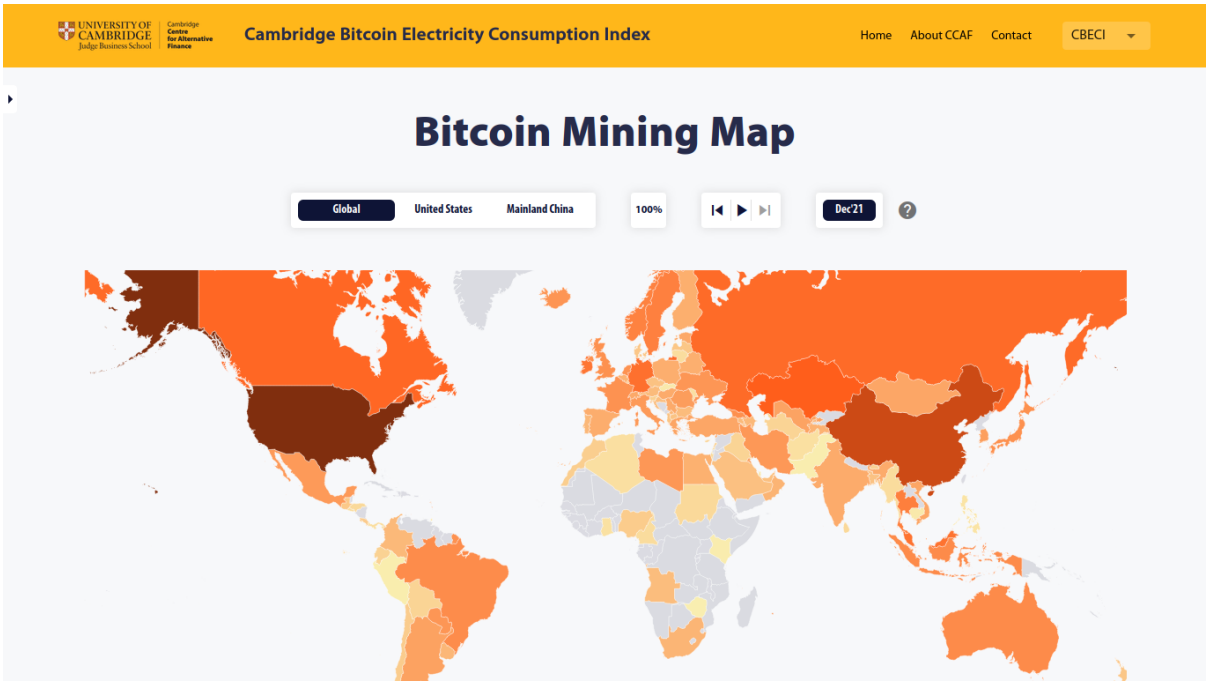

Figura 7: Mapa da distribuição geográfica do hashrate do sistema Bitcoin em dezembro de 2021 (https://ccaf.io/cbnsi/cbeci/mining_map)

Embora as análises não coincidam, elas refletem duas características importantes sobre os efeitos globais do procedimento de mineração do sistema Bitcoin. Em primeiro lugar, em função dos protocolos de comunicação baseados na criptografia e no pseudoanonimato, a contabilização do número efetivo de participantes da rede em um dado momento não é trivial, muito menos a distinção entre mineradores que mobilizam poucas ou muitas máquinas para a execução dos procedimentos de prova de trabalho exigidos na mineração. Em segundo lugar, essa característica difusa advém da própria topologia distribuída de redes tipo *peer-to-peer*, cuja totalidade circunstancial de participantes varia em função das conexões estabelecidas entre os pares, sem que haja um ponto privilegiado para esse tipo de investigação e mapeamento. A partir de qualquer ponto da rede é possível aferir uma série de métricas e estatísticas (como veremos no capítulo 3) que, mesmo apresentando desvios em relação às medições efetuadas em outros pontos da rede, compõem um quadro geral que pode ser sistematizado em função de diferentes metodologias de análise.

Com a especialização dos mineradores e o crescimento do preço do Bitcoin, que atingiria 20 mil dólares ao final do ano de 2017, as disputas políticas e ideológicas sobre modificações da rede se tornam cada vez mais acirradas, como veremos no capítulo 2. Assim, na "terceira era" da mineração, a ênfase recai sobre a consolidação desses grupos de mineradores como uma modalidade de centralização de poder econômico e computacional, modalidade esta favorecida pelas próprias regras de consenso deste sistema distribuído, e a despeito do paradigma de descentralização que orienta o código e as narrativas sobre a rede. Essas tensões e os processos de centralização e descentralização não são estanques: produzem alterações na topologia da rede e nas disputas políticas e econômicas sobre o sistema enquanto uma "moeda global".

Desse modo, como vimos, uma das inovações tecnológicas introduzidas pelo sistema *peer-to-peer* Bitcoin é o acoplamento do procedimento de emissão de moedas a um regime de validação de propriedade e escassez digital baseado em chaves criptográficas. No entanto, embora essa configuração algorítmica seja uma particularidade (e uma arbitrariedade) do sistema Bitcoin, um de seus efeitos, nos últimos anos, tem sido a concentração de poder computacional em agrupamentos de usuários especializados, cujo investimento de capital em instalações de máquinas especializadas e contratos de energia é o que garante parte do "lastro" do sistema enquanto uma rede global de transações, e é também o que fez emergir indústrias de hardware dedicado e estratégias energéticas geolocalizadas. Recentemente, cada vez mais empresas e fundos de investimentos institucionais têm alocado parte significativa de seu capital em criptoativos, acumulado centenas de milhares de *bitcoins* aos seus portfólios na expectativa de multiplicar seus patrimônios e de não ficar para trás na corrida ao "ouro digital".

1.3 IMPLICAÇÕES POLÍTICAS E ECONÔMICAS DE CONFIGURAÇÕES ALGORÍTMICAS

A formação de mercados em torno de sistemas descentralizados de transação de propriedades digitais, arranjos de pagamentos, especulação de valores e estruturas de dados de registro distribuído evidencia alguns processos característicos do capitalismo tecnocientífico e da proliferação da "forma ativo"

(*asset form*), em especial a dificuldade em delimitar com precisão os instrumentos que o constituem (BIRCH; MUNIESA, 2020). O funcionamento da política monetária do Bitcoin, o contexto de pós-crise de 2008 até os dias de hoje, o paradigma "inflação *versus* deflação", que é um dos principais pontos de oposição defendidos pelos entusiastas do sistema, e as especificidades das suas estruturas de dados, desencadearam uma série de desenvolvimentos tecnológicos e arranjos tecnopolíticos associados ao "ciberlibertarianismo" e o "anarcocapitalismo". De acordo com Edemilson Paraná, esse arranjo evidencia o caráter utópico das prescrições neoliberais, veiculadas aqui como "libertárias":

> o bitcoin é o desdobramento de uma combinação contraditória entre o desenvolvimento e intensificação do processo de neoliberalização das sociedades capitalistas e seus limites, problemas e promessas não realizadas, no contexto de esgotamento da crise do capitalismo pós-2008; o contorcionismo, em suma, de uma ideologia de modo a dar inteligibilidade ao mundo que a desafia (PARANÁ, 2020, p. 81).

É a partir das dinâmicas estabelecidas pelas "regras de consenso" do sistema (definições de estruturas de dados, modalidades de transação, processos de validação), e pelas relações que os participantes estabelecem com o sistema e entre si, que o "jogo" do Bitcoin é jogado cotidianamente desde 2009. Esses e outros acontecimentos constituem uma história comum sobre o funcionamento do sistema.

Ao definir estruturas de dados específicas – como modalidades de transação, blocos de transação, e correntes de blocos –, além de 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, sem a necessidade de autoridades centrais. A principal inovação do Bitcoin, como vimos, é esse mecanismo descentralizado de consenso emergente: o consenso não é atingido explicitamente ou num momento preciso, mas é um artefato emergente da interação assíncrona de milhares de máquinas seguindo um conjunto de regras simples, como uma espécie de "dispositivos coletivos de cálculo", descritos por Michel Callon e Fabian Muniesa (2005) a partir da ideia de "configurações algorítmicas"[41].

41 A discussão presente nessa seção se dá a partir de um artigo que apresentei na VII Reunião de Antropologia, Ciência e Tecnologia (ReACT) em 2019, intitulado "Algoritmos como ’máquinas de

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 porque 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; 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 (MIROWSKI; SOMEFUN, 1998, p. 343). E cada vez mais, como também argumenta Donald MacKenzie (2014), os próprios mercados financeiros e a maioria de seus atores são algoritmos.

---

cultura’: Notas sobre política e produção de consenso no sistema peer-to-peer Bitcoin" (CARDOSO, 2019).

No caso do Bitcoin, sua performatividade enquanto um sistema *tecnofinanceiro* é percebida por participantes e entusiastas como "deflacionária" e "distribuída", 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. A ideia de uma "economia das máquinas", aqui descrita em função das características das estruturas de dados, que impõem formas, ritmos, pulsos e uma temporalidade não-convencional, constitui as bases das várias imaginações de futuro e os horizontes daquilo que é possível fazer (ou "revolucionar") com um sistema como o Bitcoin.

Em especial, 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 (p. 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 (p. 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 entusiasmo 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, com proliferação de novos intermediários digitais (PATELIS, 2000). 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 para 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. Notadamente, Satoshi Nakamoto na mensagem 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.[42]

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*.

A ideologia que guia o Bitcoin não se faz na prática sem estar aterrada de maneira predatória no planeta. Afinal, o horizonte utópico da libertação de políticas monetárias centralizadas em bancos centrais, por meio de um sistema descentralizado, é profundamente dependente de altos níveis de extração de energia e da mobilização de infraestruturas materiais voltadas para a replicação intensiva de informação.

---

42 Mensagem de 11 de fevereiro de 2009. Disponível em: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source. Acesso em: 23 fev. 2024.

CAPÍTULO 2. CONSENSOS E DISPUTAS EM SISTEMAS DESCENTRALIZADOS

O desenvolvimento coletivo de um software como o Bitcoin é motivo de disputas e controvérsias que costumam se arrastar por muitos meses e ultrapassar os limites do repositório de código-fonte e dos dilemas técnicos pertinentes. Debates acirrados não costumam se restringir apenas às especificidades de um dado algoritmo ou aos detalhes e dificuldades da sua implementação em C++ (a linguagem de programação em que é escrito o código-fonte da implementação de referência do Bitcoin). Tais debates são eminentemente políticos, econômicos, sociais, ideológicos e, sobretudo, *tecnofinanceiros*. Essas dinâmicas evidenciam que a formação de um "consenso bruto" (*rough consensus*)[43], um procedimento de governança técnica e política, podem tanto estar restritas a algumas linhas de código, quanto podem transbordá-las por completo.

Um procedimento técnico importante para entender a resolução de disputas técnicas no interior de uma comunidade de programadores e desenvolvedores é o chamado *fork*, que, de modo geral, consiste na realização de uma cópia de um repositório de código e introdução as mudanças ou melhorias desejadas, produzindo assim uma derivação (ou *branch*) do código-fonte copiado. É também o procedimento que está no cerne da criação de milhares de criptomoedas e *tokens*, muitas das quais são produzidas por derivação de bases de código de outros sistemas[44]. No caso das criptomoedas, os *forks* podem servir à correção de problemas críticos em uma implementação, ou, o que se tornou bastante comum, após longas discussões e impasses em fóruns e listas de e-mail sobre os rumos de um projeto, podem resultar divisões de uma comunidade, uma cisão muitas vezes irreconciliável.

---

43 O termo *rough consensus* se refere aos processos de tomada de decisão e à prevalência de visões dominantes de um determinado grupo de trabalho, que independe da concordância individual de todos os participantes, tendo sido originalmente cunhado no âmbito da Internet Engineering Task Force (IETF): "We reject: kings, presidents and voting. We believe in: rough consensus and running code." Para uma descrição mais detalhada desse termo, ver: "RFC 7282 - On Consensus and Humming in the IETF". Disponível em: https://datatracker.ietf.org/doc/html/rfc7282. Acesso em: 23 fev. 2024.

44 O site https://mapofcoins.com, por exemplo, reúne em um imenso diagrama arborescente os ramos de derivação de centenas de criptomoedas a partir do código-fonte do Bitcoin. Acesso em: 23 fev. 2024.

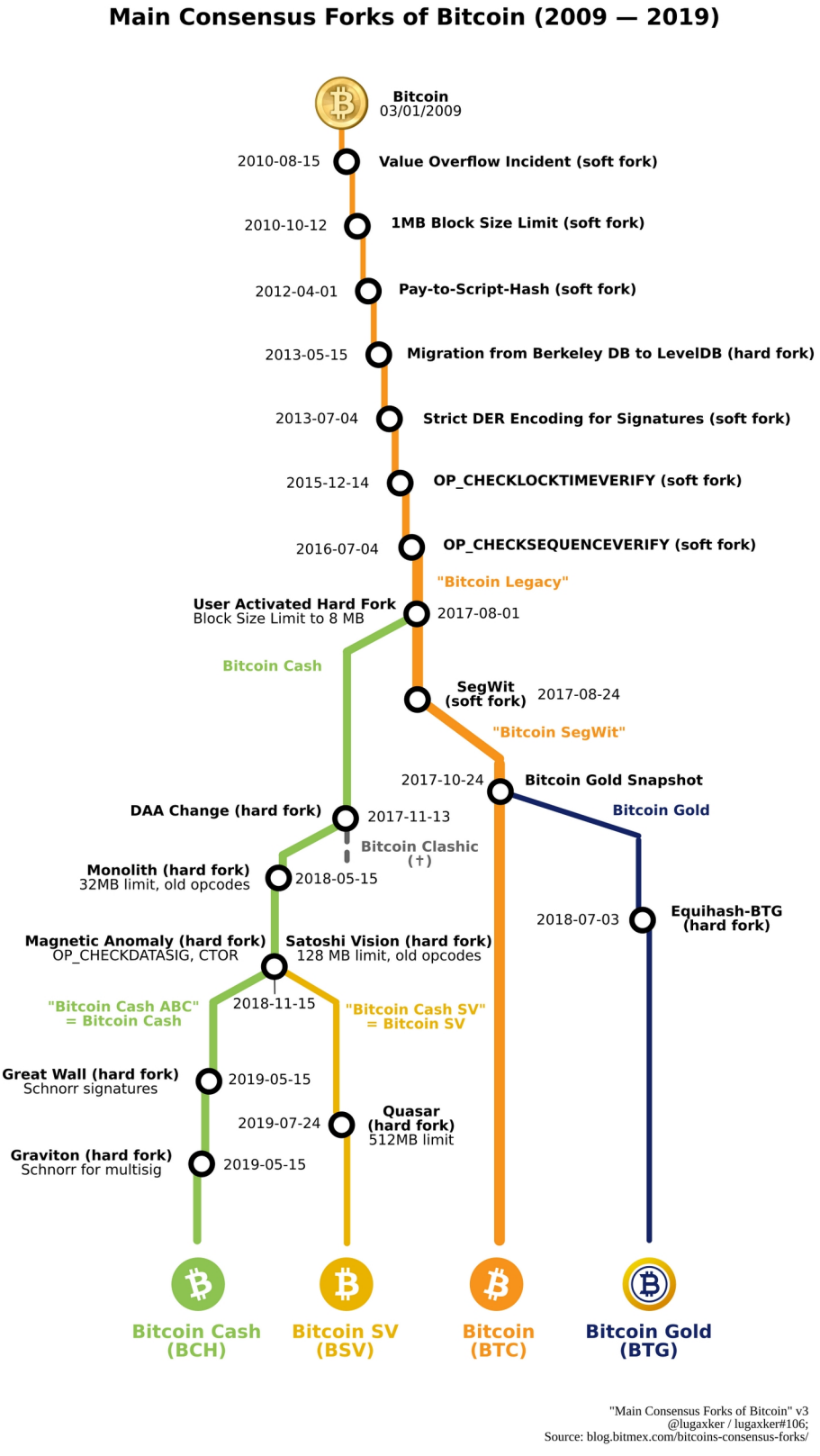

Figura 8: Diagrama com os principais forks no Bitcoin (BTC), que resultaram em diferentes criptomoedas, com suas próprias redes e incompatíveis entre si.

É possível que um software cujo código-fonte foi substancialmente alterado após um *fork* seja total ou parcialmente incompatível como a versão original da qual ele deriva, e as chances de incompatibilidades tendem a aumentar exponencialmente quando são comparadas certas derivações, ou linhagens de derivações, umas com as outras. Numa rede descentralizada ou distribuída, a introdução de incompatibilidades desse tipo é o suficiente para causar uma cisão ou ruptura entre os participantes que estão rodando a versão original e aqueles que estão rodando uma versão derivada. Quando isso ocorre em uma rede desse tipo, é dito que ela sofreu um *fork* – o mesmo nome do processo central da produção de código, justamente porque ilustra bem o fato de que as redes *forkadas* tomaram caminhos diferentes e muitas vezes irreversíveis e incompatíveis.

Assim, um grande motivo de disputas e debates acerca do desenvolvimento do Bitcoin se dá sobre o fato de que qualquer mudança no "núcleo duro" das regras de consenso pode ocasionar a cisão da rede que, a princípio, não é (ou não deve ser) controlada por ninguém. Uma parte dos participantes pode simplesmente não concordar com mudanças introduzidas, mesmo que a "maioria" (algo notoriamente difícil de estimar e calcular em redes desse tipo) decida por acatar aquelas alterações. Assim, as redes podem ser divididas e podem se tornar mutuamente incompatíveis. Modificações radicais desse tipo são chamados de *hard forks*, e são comuns no campo das criptomoedas, justamente por que as disputas entre participantes são muitas vezes insolúveis (brigas, ofensas, difamação, processos judiciais e a acirrada hostilidade pública costumam sedimentar as diferenças e discordâncias de modo irreparável).

Chama-se, portanto, *hard fork* uma modificação ou derivação do código que envolve alterações nas principais regras de consenso. Quando implementada, a modificação 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.

No entanto, uma outra forma de introdução de mudanças e funcionalidades é por meio de *soft forks*, de modo que as alterações, embora substanciais, possam manter algum grau de compatibilidade com as versões anteriores, evitando assim uma cisão completa da rede. Certas modificações (como aquelas do "núcleo duro") são muita vezes impossíveis por meio de *soft forks* e, por demandar ajustes muito delicados, implementações desse tipo, embora mais desejáveis, também costumam ser bastante controversas. Um *soft fork*, assim, 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 as funcionalidades introduzidas com a atualização de um software só possam ser executadas e/ou compreendidas pelos pares que de fato executarem a atualização, a maioria dos demais componentes permanecem compatíveis. Assim, 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 modificadas), ainda que possam não "entender" 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 recentes.

Um exemplo deste tipo de modificação foi um *soft fork* ocorrido no segundo ano de funcionamento do sistema. O *Value Overflow Incident*, também conhecido como "bug da inflação", ocorreu no bloco 74638 (15 de agosto de 2010): um *bug* no código-fonte permitiu a criação instantânea de bilhões de *bitcoins* por meio de uma transação especial que explorava uma falha na verificação do software. Em poucas horas, uma nova versão do software trazia a correção do problema, que consistia em rejeitar transações que explorassem essa falha: "although many unpatched nodes continued to build on the ’bad’ block chain, the ’good’ block chain overtook it at a block height of 74691 at which point all nodes accepted the ’good’ blockchain as the authoritative source of Bitcoin transaction history"[45]. Este é um caso especial em que um *soft fork* foi recebido como "consensual" e serviu para restituir a rede diante da

45 Disponível em: https://en.bitcoin.it/wiki/Value_overflow_incident. Acesso em: 23 fev. 2024.

violação das regras de consenso fundamentais (a política de emissão deflacionária e teto estabelecido é de 21 milhões de moedas). Embora a *blockchain* tenha sido bifurcada após a correção – uma versão contendo o bloco com bilhões de *bitcoins*, e uma outra versão com um bloco regular – a corrente mais longa de blocos (a que suprimia o erro), passou a ser adotada pela maioria dos participantes da rede e, algumas dezenas de blocos adiante, a corrente problemática foi descartada.[46]

Para citar um outro exemplo, o *User-Activated Soft Fork* (*UASF*), que ficou conhecido como *SegWit*, implementou funcionalidades significativas no protocolo, permitindo maior maleabilidade de transações e a expansão da capacidade dos blocos. A história e o motivo da implementação deste *soft fork*, em agosto de 2017, ilustra bem as dinâmicas da comunidade de programadores e os efeitos causados por essas disputas, tendo sido abordada em detalhes em "The Blocksize War: The Battle for Control Over Bitcoin's Protocol Rules" (BIER, 2021). Nesse caso, embora o *soft fork* tenha sido bem-sucedido, pois implementou as modificações desejadas, o conflito de interesses e a crise no interior da comunidade fizeram com que parte dos participantes optasse, preventivamente, por um *hard fork* deliberado, criando assim uma nova criptomoeda chamada "Bitcoin Cash", incompatível com a rede original do Bitcoin e motivo, até hoje, de diversas polêmicas.

Neste capítulo abordamos algumas das controvérsias que permeiam as comunidades de desenvolvedores e entusiastas do Bitcoin e enfatizam a dimensão agonística do ecossistema das criptomoedas. Na primeira seção, descrevemos como se dão as disputas internas à comunidade enquanto um projeto colaborativo, evidenciando a multiplicidade de atores e partes interessadas. A partir das mensagens trocadas em uma lista de e-mails, sobre a possibilidade de implementação de um melhoramento algorítmico no sistema Bitcoin, tomamos a controvérsia em torno do chamado *ASICBoost* como um exemplo etnográfico acerca dos modos de governança de projetos de software. A intenção de descrever esses

46 O comportamento de adotar sempre a corrente de blocos mais longa, pois é aquela que tem em seu histórico de produção a maior quantidade de poder computacional acumulado, é também uma das regras do sistema. Frequentemente, dois mineradores criam, quase ao mesmo tempo, blocos diferentes mas igualmente válidos: diante dessa bifurcação da corrente, os demais mineradores escolhem qualquer um dos blocos como referência e iniciam a produção do próximo bloco. Quando este é encontrado em um dos ramos, o bloco "órfão" é descartado em favor da corrente mais longa.

processos – comuns à maioria dos projetos de software livre e código aberto, mas aqui acirrados por questões de dinheiro e poder – é mostrar como o software é um artefato digital instável e dinâmico, uma obra coletiva que se desloca numa dada direção por meio de uma espécie de "consenso bruto" (*rough consensus*) entre os programadores e usuários. Na seção seguinte, procuramos descrever como as particularidades técnicas e ideológicas do sistema, ao longo de processos de especialização e radicalização de certos grupos de usuários e entusiastas, têm fomentado a imaginação de futuros específicos com relação às demais criptomoedas e ao sistema financeiro.

2.1 A CONTROVÉRSIA DO *ASICBOOST* E O PROBLEMA DA ESCALABILIDADE

Como mencionado no capítulo anterior, a política de emissão monetária entendida como "deflacionária" (por conta dos *halvings*) é uma das principais regras de consenso do sistema, mas não é a única. Aqui tomamos como ponto de partida a chamada "implementação de referência" do Bitcoin, isto é, o conjunto de arquivos de código-fonte que deriva diretamente da primeira versão criada por Satoshi Nakamoto[47]. Após mais de dez anos de desenvolvimento coletivo por partes de programadores anônimos e não-anônimos de todas as partes do mundo, o *corpus* de código, histórico de versões, requisições de modificação (*pull requests*) e propostas de melhorias (via documentos chamados *BIPs*), acumula todo desenvolvimento realizado e as disputas e debates sobre o que deve e o que não deve ser implementado no sistema.

Em um *whitepaper* publicado em 31 de março de 2016 na lista *bitcoin-dev*[48], o pesquisador e matemático Timo Hanke anunciava, em parceria com o pesquisador Sergio Lerner, apresentavam um "melhoramento algorítmico" para o processo de mineração do Bitcoin que ainda não havia sido discutido em público[49]. De acordo com seu artigo, que trazia especificações do processo, o chamado "*AsicBoost* is a

47 Disponível em: https://github.com/bitcon/bitcoin. Acesso em: 23 fev. 2024.

48 "Bitcoin Protocol Discussion", lista de e-mails para o desenvolvimento e discussão do protocolo do sistema Bitcoin. Disponível em: https://lists.linuxfoundation.org/mailman/listinfo/bitcoin-dev. Acesso em: 23 fev. 2024.

49 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. Acesso em: 23 fev. 2024.

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, p. 1). O processo é descrito por eles como um modo de otimizar os cálculos computacionais necessários à mineração:

> 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 uma máquina 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, significaria uma vantagem 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.

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.[50]

50 Peter Todd, "Re: [bitcoin-dev] AsicBoost", 1º de abril de 2016. Disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-April/012597.html. Acesso em: 23 fev. 2024.

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).[51]

Marek Palatinus, fundador da *pool* de mineração *Slush*[52], 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."[53]

Ao longo dos meses seguintes e até o lançamento da implementação de código aberto do *ASICBoost*, em outubro de 2018, as três perspectivas manifestadas acima, embora contraditórias, se mostraram mais ou menos acertadas.

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*). Em suma, tornou-se um consenso, em especial a partir de meados de 2015, que a arquitetura do sistema Bitcoin seria incapaz de 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 e, assim, provocar um *hardfork*. Porém, não havia consenso sobre

---

51 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. Acesso em: 23 fev. 2024.

52 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 (*hashrate*) – 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. 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 *hashrate* investido por usuário.

53 Marek Palatinus, "Re: [bitcoin-dev] AsicBoost", 6 de abril de 2016. Disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-April/012601.html. Acesso em: 23 fev. 2024.

como, nem quais alterações deveriam ser implementadas para solucionar os problemas identificados pelos participantes (BIER, 2021).

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.[54]

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 rápido).

---

54 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. Disponível em: https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki. Acesso em: 23 fev. 2024.

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. Duas posições se tornaram as mais eloquentes: de um lado, desenvolvedores, mineradores e fabricantes que viam num *hardfork* 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[55], de 22 de junho de 2015, em que o desenvolvedor Gavin Andresen propõe pela primeira vez um *hardfork* 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[56], escrito por Jeff Garzik, propunha o aumento dos blocos de 1MB para exatos 2MB.

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[57], uma proposta de extensão por *softfork* que ficou conhecida como *SegWit*. Essa proposta previa 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.

---

55 BIP 101: "Increase maximum block size". Disponível em: https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki. Acesso em: 23 fev. 2024.

56 BIP 102: "Block size increase to 2MB". Disponível em: https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki. Acesso em: 23 fev. 2024.

57 BIP 141: "Segregated Witness (Consensus layer)". Disponível em: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki. Acesso em: 23 fev. 2024.

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 então chamada "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."[58]

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?"[59]

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[60]. Propostas enviadas à lista por Hanke e Lerner passaram a ser vistas com alguma desconfiança[61], dada a suspeita de estarem

---

58 "Bitcoin Roundtable Consensus", Disponível em: https://medium.com/@bitcoinroundtable/bitcoin-roundtable-consensus-266d475a61ff. Acesso em: 23 fev. 2024. 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.

59 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. Acesso em: 23 fev. 2024.

60 Peter Todd, "Re: [bitcoin-dev] Drivechain proposal using $OP_{COUNTACKS}$". Disponível em: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-October/013175.html. Acesso em: 23 fev. 2024.

61 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. Acesso em: 23 fev. 2024.

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[62]. 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[63].

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 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**

62 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). Acessos em: 23 fev. 2024.

63 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. Acesso em: 23 fev. 2024.

> **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. (grifo nosso) [64]

O risco da centralização de poder de mineração, decorrente dessa implementação, nas mãos de alguns poucos mineradores se tornou o principal motivo de preocupação dos participantes. 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 *testnet*, 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.[65]

Ainda que os pesquisadores Timo Hanke e Sergio Lerner fossem os detentores da patente original[66], 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, conforme

64 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. Acesso em: 23 fev. 2024.

65 Bitmain, "Regarding Recent Allegations and Smear Campaigns", 07 de abril de 2017. Disponível em: https://blog.bitmain.com/en/regarding-recent-allegations-smear-campaigns. Acesso em: 23 fev. 2024.

66 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. Acesso em: 23 fev. 2024.

alegavam na mesma publicação: "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/].[67]

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*):

> 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.[68]

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",

67 Mensagem de Gregory Maxwell, citada acima. Ênfase minha.

68 Postagem da Bitmain, citada acima.

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[69]. 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[70]. Numa clara demonstração de força e, ironicamente, de centralização de recursos, as partes envolvidas mobilizavam todo seu aparato de mineração para "sinalizar" a concordância com essa posição[71].

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,

---

69 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. Acesso em: 23 fev. 2024.

70 "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. Acesso em: 23 fev. 2024.

71 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.

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[72] 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 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,

72 A *Blockchain Defensive Patent Licence* (BDPL) 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. Disponível em: https://blockchaindpl.org. Acesso em: 23 fev. 2024.

> **there may be no escaping the need for all mining equipment manufacturers to use it to remain competitive**.[73]

Com a mudança de licenciamento, fabricantes concorrentes, como a chinesa Halong Mining, passaram a aderir à "comunidade BDPL"[74], 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[75].

Com isso, a controvérsia do *ASICBoost* 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 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.

2.2 TENSÕES TOPOLÓGICAS E FUTUROS IMAGINADOS

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

---

73 "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. Acesso em: 23 fev. 2024.

74 Halong Mining, "BDPL Offering Announcement", 6 de março de 2018. Disponível em: https://halongmining.com/blog/2018/03/06/bdpl-offering-announcement. Acesso em: 23 fev. 2024.

75 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 também: https://braiins-os.org. Acesso em: 23 fev. 2024.

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).

Como vimos, 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 (ASICs). As implicações geopolíticas da formação desses aglomerados especializados – a maior parte deles localizados na China, sudeste asiático, em países da América do Sul, como o Paraguai e a Venezuela, e mais recentemente nos Estados Unidos – 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, comercialização de máquinas mineradoras e concentrações de poder.

Em meio a esses agrupamentos de usuários e entusiastas, destaca-se também um crescente movimento global de usuários ortodoxos *Bitcoin-only*, chamados *maximalistas*, que se organizam como um grupo radical difuso, cujas ficções de futuro imaginam cidades privadas povoadas por indivíduos soberanos e alimentadas por transações liquidadas na cadeia de blocos do Bitcoin. São usuários que rejeitam todas as outras criptomoedas, entendidas por eles como *scams* (golpes ou pirâmides financeiras) e que sonham com uma sociedade utópica que nasceria por meio de um processo especulativo e imparável a que eles se referem frequentemente como *hiperbitcoinização*.

Este fenômeno hipotético, embora altamente esperado, foi definido inicialmente em 2014 por Daniel Krawisz, então um proeminente *bitcoiner*, como "uma transição voluntária de uma moeda inferior para uma moeda superior", de modo que essa transição se daria por meio uma série de "atos individuais de empreendedorismo" (KRAWISZ, 2014, n.p). Para os *maximalistas*, que já celebram os primeiros indícios da suposta disrupção financeira em curso, este é o resultado mais desejável para o desenvolvimento do Bitcoin e para a adoção em larga escala dessa forma dinheiro eletrônico descentralizado.

Numa palavra, o *maximalismo bitcoiner* articula a ideia de que só pode haver uma única e verdadeira criptomoeda descentralizada – o próprio Bitcoin, a primeira e a mais difundida criptomoeda em operação. O *maximalismo* também se baseia na crença de que o Bitcoin, como um sistema descentralizado, como uma composição de algoritmos e máquinas de *mineração*, produz um tipo superior de dinheiro e um conjunto de regras monetárias melhores do que qualquer outra criptomoeda ou quaisquer moedas de estados-nação.

O termo "maximalismo" ganhou relevância geral nas comunidades digitais de criptomoedas após uma publicação no blog de 2014 do fundador da criptomoeda Ethereum, Vitalik Buterin, na qual ele criticava o "maximalismo dominante" do Bitcoin, referindo-se a esta perspetiva maximalista como "a ideia de que um ambiente de múltiplas criptomoedas concorrentes seria indesejável, que seria errado lançar ’mais uma moeda’ e que seria justo e inevitável que o Bitcoin venha a assumir uma posição de monopólio no cenário das criptomoedas."[76]

A crítica de Vitalik foi mais tarde apropriada e adotada pelos próprios *maximalistas* como uma posição virtuosa e moralmente superior em relação ao ecossistema das criptomoedas. Desde então, esse grupo se tornou bastante numeroso. No Twitter, por exemplo, é possível identificar representantes desta multidão radicalizada pelas suas fotos de perfil com olhos de *laser* vermelho *photoshopados* sobre seus avatares; pela repetição interminável e por vezes até sem sentido de *slogans* e *memes* sobre a superioridade absoluta do Bitcoin;

76 "On Bitcoin Maximalism, and Currency and Platform Network Effects". Vitalik Buterin, 20 de novembro de 2014. Disponível em: https://blog.ethereum.org/2014/11/20/bitcoin-maximalism-currency-platform-network-effects. Acesso em: 23 fev. 2024.

afirmações morais e comportamentais de inspiração cristã conservadora; afirmações sobre os supostos benefícios de dietas baseadas apenas em carne vermelha; e a glorificação da economia neoclássica, do liberalismo e do próprio capitalismo.

De certa forma, a infraestrutura técnica do Bitcoin é defendida pelos maximalistas como uma solução definitiva para a estrutura social e para a estrutura econômica. Segundo uma postagem mais recente de um maximalista no Twitter, "Bitcoin is an innovation on the order of agriculture, antibiotics, or the industrial revolution. I highly recommend buying some of humanity's best money while you can still exchange paper for it"[77], o que encapsula numa breve declaração alguns dos principais tropos da hiperbitcoinização como um processo revolucionário que já estaria em curso.

A publicação de "The Bitcoin Standard" (2018) por Saifedean Ammous em 2018 (que foi posteriormente traduzido para o português do Brasil em 2020) é uma das muitas publicações que estabeleceram e popularizaram ainda mais esta perspetiva como um movimento cultural emergente das comunidades digitais de usuários e entusiastas do Bitcoin. No Brasil, esse movimento é articulado principalmente em redes sociais como Twitter, YouTube e Telegram, de maneira difusa e numerosa, muitas vezes misturado às comunidades digitais de viés mais neoliberal, anarcocapitalista e outras comunidades de extrema direita. Essa sobreposição de grupos costuma se dar por meio de um conjunto pouco estruturado de imperativos econômicos e estratégias de investimento, impulsionadas pelo desejo de obter controle sobre seu próprio futuro financeiro por meio da autocustódia de criptoativos e da busca por uma autonomia financeira.

Embora a crença na inevitável hiperbitcoinização da economia mundial possa ser um fator comum entre os *maximalistas* do Bitcoin, no Brasil e em algumas das comunidades brasileiras, um dos principais pontos de convergência é a ampla rejeição de qualquer tipo de "regulação estatal", no sentido de que esse é um dos principais temas a que os entusiastas das criptomoedas e os *maxis*, como uma multidão, se opõem ativamente. Com a regulamentação das criptomoedas e dos criptoativos ainda em fase inicial no Brasil, como veremos no capítulo 3, a forte

77 Disponível em: https://twitter.com/coryklippsten/status/1537474450815234048. Acesso em: 23 fev. 2024.

oposição dos *bitcoiners* às propostas de regulamentação vem muitas vezes acompanhada de um impulso na direção de ficções e futuros imaginados em que o Bitcoin pode vir dominar o mundo, transcendendo as fronteiras financeiras dos Estados-nação, que são vistas como obstáculos ao "fluxo livre" ideal de transações digitais e estratégias de negociação.

Como vimos nas seções anteriores, a questão da confiança em intermediários ou entidades terceirizadas, como os bancos e outras instituições financeiras, juntamente com o risco iminente de desvalorização das moedas nacionais, são um dos principais temas abordados pelos entusiastas de criptomoedas e, de fato, a principal razão que levou à criação do próprio sistema Bitcoin. Devido à sua escassez programada, por meio de um calendário de emissão monetária bem definido, o Bitcoin é visto pelos seus defensores mais fervorosos como uma proteção contra o inevitável colapso econômico global. A crise hiperinflacionária prevista para todas as economias tradicionais é encarada como um importante ciclo de *feedback* positivo que impulsionaria os próximos picos de aumento de preços do Bitcoin, embalados também pelo "medo de ficar de fora" (*fear of missing out*, *FOMO*) desse acontecimento financeiro. Como um importante desenvolvedor de Bitcoin resumiu em um *tweet*:

> Q: What's your bitcoin trading strategy?
>
> A: Collect as much as possible before the rest of the world catches on.
>
> That's it, that's the trade.[78]

Essa ênfase específica na acumulação em vez da negociação, alimentada pelo "medo de perder" o *boom* da hiperbitcoinização, destaca uma das principais características da "síndrome maxi": se, em um futuro talvez próximo, todos os outros bens e *commodities* serão denominados e negociados por *bitcoins* e *sats*, não faria sentido negociá-los *agora* por qualquer outra coisa. Os ciclos de *feedback* positivo de acumulação, reforçados pela multidão de investidores, apesar das quedas de preço ou dos longos mercados em baixa, são o principal efeito que supostamente levará os *maxis* às suas desejadas utopias baseadas em Bitcoin.

78 Disponível em: https://twitter.com/lopp/status/1293157604697559046. Acesso em: 23 fev. 2024.

Em conversas online com *bitcoiners* brasileiros durante a pandemia, um *bitcoiner maximalista* me descrevia que a disrupção esperada da economia poderá ocorrer muito antes do previsto. Segundo ele, um autodenominado empresário e investidor na casa dos 20 e poucos anos, "a hiperbitcoinização da sociedade" ocorrerá inevitavelmente, uma vez que o Bitcoin é um ativo escasso diante da atual expansão agressiva das bases monetárias dos Estados-nação em todo o mundo, citando como exemplo o aumento exponencial dos preços do ouro em relação ao Marco alemão nas décadas de 1920 e 1930. "Gradualmente, e então de repente", como diz um dos *slogans* bastante comuns nesses grupos.

Como outro *bitcoiner* brasileiro me explicou certa vez, "o papel dos maximalistas", segundo ele, é essencial "para o próprio ecossistema do Bitcoin", pois é a sua própria ortodoxia que impõe os limites sobre as modificações que devem ser permitidas no protocolo, tanto quanto o estabelecimento de diretrizes e "melhores práticas" sobre a autocustódia de bitcoins (por exemplo, evitando serviços de terceiros e plataformas de troca de criptomoedas). Segundo ele, essas são práticas essenciais para garantir o domínio monetário do Bitcoin a longo prazo.

Além disso, também de acordo com a perspectiva dos maximalistas, tudo o que acontece na economia e no mundo é de alguma forma sempre "bom para o Bitcoin". Mesmo as quedas dos mercados, o colapso de esquemas de pirâmide de criptomoedas e de algumas *exchanges* digitais que se revelaram insolventes e quebraram; todos esses acontecimentos são enquadrados como eventos que "purificam" e pavimentam o caminho para a supremacia do Bitcoin. Embora, no curto prazo, a percepção de que virtualmente todos os projetos *cripto* sejam potencialmente *scams* (golpes) – o que resume o diagnóstico maximalista sobre o ecossistema –, a longo prazo é o Bitcoin e a "tecnologia blockchain" que irão prevalecer: após a esperada disrupção, com a derradeira descentralização dos processos e fluxos financeiros, em uma "inédita" topologia transacional, os problemas sociais e econômicos atuais serão depurados e superados em um novo arranjo societal.

A maioria dos *bitcoiners* com quem já conversei, e cujas discussões tenho acompanhado em comunidades online, nem sempre utilizam o conceito de

hiperbitcoinização *per se* para se referirem às suas realidades ou para dar sentido a estes supostos processos futuros. Na maior parte das vezes, eles se reúnem em torno dessas ficções futuras, mitos e dogmas/slogans relacionados, tanto quanto o fazem em torno da ação do preço da Bitcoin, como uma forma de dar sentido aos movimentos da economia mundial e às suas próprias realidades e escolhas pessoais. Implícita nesta disposição está a ideia de que a inflação monetária, através da "impressão de dinheiro", conduz a processos hiperinflacionários em que ativos escassos, como o ouro ou o Bitcoin, se valorizarão rapidamente devido às suas propriedades intrínsecas, tornando-os assim uma forma superior de dinheiro ("hard money" ou "sound money") em relação às moedas fiduciárias que, por sua vez, estariam, por definição, condenadas ao fracasso.

Uma vez que todas as *moedas fiduciárias* são frequentemente entendidas como "condenadas" por padrão, o Dólar americano (USD) e o Real brasileiro (BRL) não são exceção; e como todas as outras criptomoedas também estariam prestes a afundar "para zero" (pois são vistas como nada além do que esquemas pirâmide extravagantes e elaborados), há uma sensação de pressa e urgência, encapsulada no slogan comum *stack sats and stay humble* (onde *sats* é a menor unidade negociável de uma moeda, 1/100000000 de um bitcoin), que descreve um processo contínuo e disciplinado de acumulação gradual (*stacking*) de bitcoins. O acúmulo lento mas constante de *sats* é descrito como uma autodisciplina obrigatória para todos os *bitcoiners* dedicados, que retratam essa prática financeira como um exercício de soberania individual (um tópico bastante comum entre os "influenciadores digitais" de criptomoedas) e uma maneira de "comprar uma saída" (*to buy a way out*) quando o USD ou o BRL finalmente virarem pó.

Contudo, ainda que o slogan em questão também oriente a "manter a humildade" durante essa fase de acumulação, os *bitcoiners* esperam com isso fazer parte de uma nova elite financeira em formação. Embora no presente uma modesta pilha de *sats* possa não ser convertida em uma riqueza significativa, essas economias podem torná-los os futuros milionários de um mundo pós-hiperbitcoinizado. Se, de acordo com Elias Canetti, "o desejo de crescer é o primeiro e supremo atributo da multidão: ela quer se apoderar de todos ao seu alcance" (CANETTI, 1981, p. 16); e, neste caso, o crescimento dessa multidão é

frequentemente cultivado *contra* "as massas", contra daqueles que ainda estão "presos" ou que podem ficar para sempre "presos pelo sistema", e sobre as quais, num futuro esperado, eles poderão governar como uma seleta multidão de "remanescentes", mais poderosa, mais rica e apartada dos demais. Como afirma, por exemplo, um entusiasta do Bitcoin:

> Bitcoin is for the Remnant. Crypto is for the masses. The masses are generally on the wrong side of history because of the madness inherent in crowds. They only find themselves "right" when it's the default position. After the truth, forged forth by the Remnant, finally prevails. … By the time they're all finally using Bitcoin in the same way they breathe oxygen, the Remnant will be building cities and citadels, terraforming new lands, unlocking intergalactic energy and inventing cosmic teleportation. The Remnant are the 20% that make possible the 80% in the Pareto distribution.[79]

Portanto, a produção constante de "ficções futuras" (GUNKEL; HAMEED; O'SULLIVAN, 2017), de certa forma, é o que conduz essas comunidades digitais de entusiastas a futuros imaginados de "cidadelas Bitcoin", cidades privadas ou pequenos países habitados por uma multidão de indivíduos soberanos, paraísos repletos de armas, livres de impostos e livres de inflação, com que eles ativamente sonham, *memetizam* e anunciam. É a isso que, segundo eles, o Bitcoin inevitavelmente leva: a uma ruptura do social em direção a um mundo privado.

Aqui, a imaginação de futuro que emerge dos acoplamentos de milhões de robôs e sistemas criptográficos é uma imaginação que tem na guerra, na desconfiança mútua, e no individualismo os seus maiores referentes. Embora a esperada disrupção possa criar novas oportunidades para a organização social e econômica, as utopias maximalistas e os futuros imaginados que estão sendo criados no presente não são simplesmente fantasias ociosas disfarçadas de profecias autorrealizáveis, mas ficções futuras que têm potencial de criar novas realidades e influenciar o sistema financeiro global de maneiras inesperadas.

79 "Bitcoiners Are The Remnant", Aleksandar Svetski, 21 de setembro de 2021. Disponível em: https://bitcoinmagazine.com/culture/bitcoiners-are-the-remnant. Acesso em: 23 fev. 2024.

CAPÍTULO 3. A TROCA COMO PROPAGAÇÃO DE INFORMAÇÃO

O Bitcoin é frequentemente pensado como uma moeda digital, uma vez que, desde o início do projeto, pretende-se como um "sistema *peer-to-peer* de dinheiro eletrônico". Por isso, seu *status* como moeda (*currency*) é também motivo de polêmicas e disputas. Muitas narrativas mobilizam a tríade (neo)clássica das características que definem uma moeda: meio de troca, reserva de valor e unidade de conta. De acordo com Paraná, a partir do trabalho de Nigel Dodd (2018), a teoria que sustenta o Bitcoin parte do pressuposto de que, embora seja, como todo dinheiro, virtual, "o dinheiro obtém valor a partir de suas propriedades materiais como meio de troca" (PARANÁ, 2020, p. 94). Nesse sentido,

> uma imagem do dinheiro como uma coisa que deve ser mantida escassa de modo a proteger seu valor é o que sustenta, portanto, a lógica fundamental desta criptomoeda. Eis, então, o paradoxo apresentado por Dodd (2018): sendo nitidamente um processo social, o Bitcoin busca negar justamente aquilo que o constitui de modo mais intrínseco – seu caráter sociorrelacional, a comunidade de usuários e entusiastas que mobiliza, algo nitidamente perpassado por certas crenças e formas de confiança (PARANÁ, 2020, p. 95).

Um aspecto que chama a atenção nos debates entre os entusiastas das criptomoedas é a interdependência dos chamados "fundamentos técnicos" do sistema Bitcoin com um conjunto de "fundamentos ideológicos" característicos de certas variantes do neoliberalismo. Esses fundamentos ideológicos por vezes oscilam entre o "ciberlibertarianismo" e o "anarcocapitalismo" como ideologias político-econômicas basilares. Tratam-se de pressupostos a que adere, seja por convicção ou por inércia, uma parte hegemônica dos participantes das comunidades observadas, comumente sob o termo guarda-chuva *criptoeconomia* (VOSKUIL, 2020).

Entre os entusiastas defensores da posição de que "Bitcoin é moeda", um argumento comum descreve o Bitcoin, por definição, como um meio de troca, e também como "uma ótima reserva de valor", pois é um dos ativos que mais se valorizaram nos últimos anos, a despeito de sua alta volatilidade. No entanto, talvez não seja ainda uma boa unidade de conta, isto é, não costumamos ver preços denominados em *bitcoins*, mas isso, especulam os entusiastas, seria apenas uma

questão de tempo e se daria naturalmente com a maior adesão de usuários e comerciantes.

Os críticos dessas proposições tendem a atacar uma ou mais dessas características, notadamente porque há pouco comércio ("transações de fato") sendo realizado com *bitcoins*, sendo o uso mais comum aquele da especulação (*trade*) em casas de câmbio digitais (*exchanges*), cujo objetivo "final" para a maioria dos *traders* é resgatar seu lucro em dólar ou em reais. Um ponto de convergência, embora nunca consensual, é que, das três características, a "reserva de valor" parece de fato a mais promissora, tanto pela valorização a curto e médio prazo, quanto pelas estimativas a longo prazo, dada a curva de escassez prevista pelo sistema.

Como exemplo dessa questão, podemos mencionar um acontecimento específico: o "Pizza Day", celebrado todos os anos no dia 22 de maio, marca a data de quando foi registrada, no fórum BitcoinTalk, a primeira transação pública feita com bitcoins para a compra de uma mercadoria, isto é, seu primeiro uso como moeda[80]. Foram compradas duas pizzas grandes pelo valor de dez mil *bitcoins*, o que em 2010 conferia a uma unidade de bitcoin o valor de meio centavo de dólar, pois não havia, até então, mercados que negociavam a moeda e que pudessem estabelecer um preço de referência. Hoje, mais de dez anos depois, este episódio é contado como o caso das pizzas mais caras da história, uma vez que este montante somaria em valores atuais mais de 500 milhões de dólares.

Do quase despretensioso "dia da pizza" até o pico histórico do preço em novembro de 2021 (o chamado *all time high* ou ATH), quando uma unidade de bitcoin passou a ser negociado por mais de 69 mil dólares, muita coisa mudou. As primeiras grandes *exchanges* começam a surgir e se popularizar a partir de 2011, e desde então o preço passou a ser melhor "descoberto" (fabricado) nesses mercados. De acordo com levantamento do site Cointrader Monitor[81], que calcula o preço médio diário de negociação do Bitcoin a partir de uma média ponderada dos volumes das principais *exchanges* em operação no Brasil, em seu mais recente

80 "Pizza for bitcoins?" Disponível em: https://bitcointalk.org/index.php?topic=137.0. Acesso em: 23 fev. 2024.

81 Disponível em: https://cointradermonitor.com. Acesso em: 23 fev. 2024.

relatório mensal (de outubro de 2022), "as exchanges brasileiras declararam ter movimentado 27.664,47 Bitcoins de 1 a 31/10/2022, que equivale a aproximadamente R$ 2.882.485.027,92 (2,8 Bi)"[82]. Essa estimativa leva em consideração os volumes declarados de mais de 30 *exchanges*, sendo a chinesa Binance responsável por quase metade (47,53%) das negociações de bitcoins no Brasil durante o mês de outubro daquele ano.

As imensas oscilações e as mudanças na nascente indústria de mineração, efetuando a migração dos computadores domésticos para máquinas especializadas, bem como os desenvolvimentos de software e serviços em torno do Bitcoin e de outras criptomoedas que também começaram a circular, fizeram com que esses arranjos sociotécnicos se transformassem a ponto de se tornarem um fenômeno em escala global. Em especial, trata-se de um fenômeno de apreciação do Bitcoin não apenas como moeda (algo em constante disputa), mas como o carro-chefe de uma nova classe de ativos financeiros chamados de *criptoativos*, assim denominados ao longo de processos de financeirização e formalização de instrumentos financeiros específicos. Muitas vezes às margens das diretrizes regulatórias de muitos países, a especulação financeira passa a ser o principal motivo das transações realizadas nesses sistemas, sendo notável – e quase imediato – o emprego das mesmas ferramentas, tipos de gráficos e outras formas de visualização utilizadas nos mercados de ações, derivativos e FOREX para apreender a movimentação esses criptoativos.

Diversos artifícios gráficos, diagramas, metáforas e analogias são mobilizados para descrever um sistema complexo como o Bitcoin. Serviços como *blockchain explorers*[83] e *dashboards*[84], por exemplo, oferecem visualizações gráficas acerca do *status* da rede, bem como panoramas e representações gráficas sobre o

---

82 Volumes das exchanges de Outubro de 2022 - Blog CTM - Cointrader Monitor. Disponível em: https://blog.cointradermonitor.com/1125/volumes-das-exchanges-de-outubro-de-2022. Acesso em: 23 fev. 2024.

83 Há diversos serviços online para visualização da *blockchain* (blocos e transações) do Bitcoin e outras criptomoedas, como por exemplo https://mempool.space e https://blockchair.com.

84 *Dashboards*, como https://statoshi.info e https://bitcoin.clarkmoody.com/dashboard, oferecem gráficos e visualizações sobre dezenas de outras métricas possíveis de se aferir a partir de um nó da rede (*full node*).

funcionamento do sistema. Gráficos de preço e outros dispositivos de mercado são elementos externos ao sistema, porém fundamentais para seus diferentes modos de apreensão (CALLON; MILLO; MUNIESA, 2007; CALLON; MUNIESA, 2005) e, sobretudo, para o modo como as trocas são ali realizadas e entendidas.

Abordagens mais clássicas em antropologia tendem a definir a troca (*exchange*) simplesmente como uma transação entre pares, como é o caso da formulação de Chris Gregory (1982):

> Exchange, in its simplest form, can be defined as a transaction involving two transactors, A and B, and two objects, x and y. The discussion here is limited to the case where A and B are individuals or groups, and where the objects are things. (GREGORY, 1982, p. 41)

No caso das plataformas digitais, a troca se dá entre duas partes que não se conhecem, não se veem, não sabem se a outra parte é um humano ou um robô (o que, na prática, parece não ser de grande importância), e os objetos, trocados instantaneamente, são coisas ou ativos financeiros que também circulam como "moeda" neste e em outros mercados – o que, nas plataformas das corretoras, são representados por *tickers*: BTC, BRL, ETH, XRP, etc., com seus respectivos gráficos de evolução de preço nos pares de moedas disponíveis. O que há, na prática, é uma lista ordenada de intenções: "compro *X* bitcoins (BTC) por *Y* reais (BRL)", "vendo *W* BTC por *Z* BRL".

Isto é, a noção de propriedade digital vem atrelada, ou emaranhada, com outras noções, como as de posse e controle, além da própria ambiguidade da tradução, quase sempre intercambiável nesses contextos, do termo "propriedade" como *property* e *ownership*: "At the protocol level, the nature of Bitcoin's information space means that private keys function like a digital bearer instrument: *there is no inherent difference between possession, control and ownership*."[85] Notadamente, essa perspectiva já estava presente desde os primeiros debates sobre moedas digitais:

> Back in the late 1980s, Tim May asked the cypherpunk community, "What is a 'digital coin'?" Here was one answer: it was not a "coin" at

85 "The Nature of Bitcoin", Zane Pocock, 13 de fevereiro de 2020. Disponível em: https://medium.com/knox-blog/the-nature-of-bitcoin-66d4e285041b. Acesso em: 23 fev. 2024.

> all – not some discrete string of bits, some unit of data – but *a system for the collective verification of ownership, with no existence outside that system of verification*. No coin exists without a Bitcoin account that currently owns it; *the "coin" itself is the property of being owned*. (…) This is one of the implications of Nakamoto's premise: *"We define an electronic coin as a chain of digital signatures."* A coin cannot be separated from the history of the signed transactions in which it has been exchanged – in fact, *it is nothing but those transactions* (BRUNTON, 2019, pp. 161–162).

Assim, se no primeiro capítulo o sistema blockchain do Bitcoin é descrito a partir de aspectos técnicos e das dinâmicas impostas pelas "regras de consenso" e, no segundo, a partir de disputas sobre procedimentos técnicos, neste capítulo tomamos como base algumas das modalidades de produção de "imagens comuns" sobre esse sistema tecnofinanceiro, isto é, as diferentes formas como a troca é imaginada. Reunimos aqui diferentes perspectivas sobre os fundamentos do sistema Bitcoin e da chamada *criptoeconomia*, suas concepções subjacentes de política e economia, para descrever como os participantes percebem essas diferenças em relação aos sistemas convencionais. O objetivo desta abordagem é descrever como essas variações de ideologias neoliberais (ou *ciberlibertárias*) constituem as narrativas e as imaginações de futuro de programadores, entusiastas e investidores acerca de previsões sobre o "futuro da economia" e de profecias sobre o "futuro do dinheiro", do Estado e do próprio Capitalismo.

Na primeira seção, veremos como os *dashboards*, gráficos e outros dispositivos de mercado são interfaces indispensáveis para a produção de totalidades parciais do sistema, bem como as próprias plataformas das corretoras (*exchanges*) implementam esses dispositivos para a constituição de mercados de compra e venda de criptoativos. Na seção seguinte, abordamos como narrativas tomadas de empréstimo da antropologia e da economia servem como pano de fundo para a produção de sentido e de futuros imaginados sobre esses sistemas de dinheiro digital, e alguns dos movimentos mais recentes de instituições financeiras nacionais para a regulação desses sistemas.

3.1 TRANSAÇÕES NO SISTEMA BITCOIN: DASHBOARDS, GRÁFICOS E TRANSFERÊNCIA DE PROPRIEDADE

A multiplicidade de perspectivas sobre o *ecossistema cripto* decorre de uma característica das redes de tipo descentralizado ou distribuído. Ao permitirem conexões sem o intermédio de um servidor central, e sim por meio de protocolos de "descoberta" de pares, cada nó da rede se conecta a apenas alguns outros nós e estes, por sua vez, a vários outros. Desse modo, as conexões estabelecidas em diferentes regiões da rede diferem qualitativa e quantitativamente.

A velocidade e a estabilidade de uma conexão determinam a eficiência e a qualidade da transmissão de dados: caso uma conexão entre pares resulte em muitas perdas de informação ou em repetidas inconsistências de informação, o algoritmo de rede busca por outras conexões possíveis a partir de requisições que são replicadas pelos pares conhecidos até que se encontre melhores candidatos para a conexão. Embora as conexões entre nós (*nodes*) particulares possam ser localizadas em regiões específicas da rede, a multiplicação de conexões possíveis entre os pares permite que as informações por eles trocadas sejam propagadas rapidamente por um grande número de nós. Esta é uma característica de redes descentralizadas que implementam diferentes modalidades de protocolos de comunicação conhecidos como *gossip protocols* (NARAYANAN *et al.*, 2016, p. 67; TASCA; TESSONE, 2019, p. 13). À semelhança da comunicação boca a boca e da viralidade dos boatos em grupos e sociedades humanas, esse tipo de "espalhamento" de informação, embora possa incorrer em múltiplas repetições e redundâncias, é um método bastante eficiente de disseminação de informação. Parece interessante pensar os "gossip protocols" como ponto de comparação com a antropologia e discussões sobre a disseminação de fofocas e boatos, bem como os paradigmas de redes sociais (não as digitais) que servem de referência a estes algoritmos.

Por conta desse caráter difuso, outros métodos algorítmicos devem ser empregados para garantir a legitimidade da informação, por meio da verificação de identificações criptográficas (*hashes*) e procedimentos de validação a partir da comparação entre as informações que chegam pelos canais estabelecidos. Via de regra, um nó considerado "honesto" só repassa para seus pares aquelas

informações que estejam de acordo com o conjunto de regras estabelecido pelo protocolo de comunicação. Qualquer informação discrepante deve ser descartada e, caso um nó em particular incorra na propagação de informações inválidas, a conexão com ele deve ser interrompida em favor de um nó mais confiável. Como mencionamos na introdução, este é um problema clássico da matemática e da teoria de redes, popularmente conhecido como "o problema dos generais bizantinos" ou do consenso distribuído (LAMPORT; SHOSTAK; PEASE, 1982), e o mecanismo destinado a evitar o gasto duplo de moedas na rede do Bitcoin é uma implementação particular deste problema. Das diversas implementações possíveis para solucionar o problema de nós não-confiáveis ou de repetidas perdas de informação, a solução de Nakamoto propõe o uso intensivo da criptografia e do encadeamento de dados para minimizar esse tipo de falha e a possibilidade de ataques à rede.

Uma vez que todos os nós devem, idealmente, entrar em consenso sobre o histórico das transações efetuadas pelos participantes da rede, uma espécie de acordo pragmático é estabelecido a cada dez minutos por meio da construção de um bloco de transações que seja consistente com as regras do sistema. Conforme os pares verificam a validade do bloco proposto por um *minerador* e o replicam para seus pares, os mineradores passam então a construir novos blocos a partir de transações pendentes e com identificação criptográfica (*hash*) do bloco anterior recém produzido. Ao longo do tempo, a sempre crescente corrente de blocos (*blockchain*) se consolida como um registro distribuído de todas as transações válidas efetuadas e consolidadas.

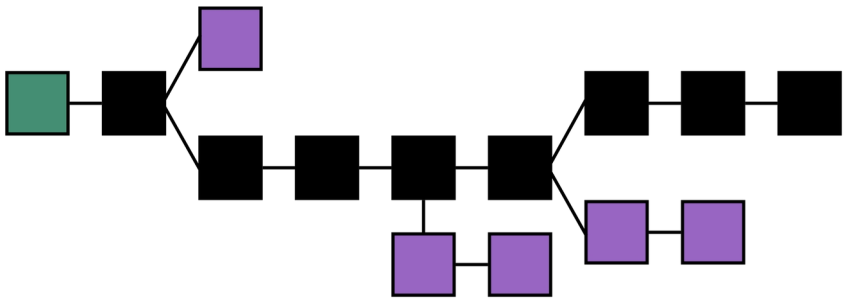

Figura 9: Representação de um segmento da blockchain. Em verde, um bloco anterior comum às ramificações. Os ramos em roxo serão descartados pelos da rede em favor da corrente mais longa, a dos blocos pretos. As transações dos blocos "órfãos" serão incluídas em outros blocos.

Nos intervalos de dez minutos entre a consolidação de um bloco e outro, diferentes regiões da rede possuem conjuntos distintos de informações sobre o estado atual das transações. O processo decisório sobre quais transações devem ser efetuadas antes das demais, ou descartadas por inconsistências, pode resultar na criação simultânea de diversos blocos de transação válidos e concorrentes, pois apontam para um bloco anterior em comum e validam transações diferentes. Essa bifurcação do registro é mitigada pela escolha, por parte dos nós, pela corrente de blocos "mais longa", o que, na prática, significa que aquela corrente de blocos possui uma maior quantidade de poder computacional acumulado, uma vez que um bloco, para ser *minerado*, demanda uma grande quantidade de poder computacional. A corrente "mais curta", um pequeno ramo desviante do registro de transações válidas, porém ainda não consolidadas de fato, é então descartada pelos demais nós em favor da outra, mais longa e "mais verdadeira", que passa então a ser replicada para embasar a construção dos novos blocos.

Assim, embora o consenso dos acontecimentos emerja como resultado desta série de procedimentos algorítmicos, o estado atual da rede é sempre uma função das conexões estabelecidas em cada região, da propagação dos dados entre os pares, e do fluxo contínuo de novas transações que devem ser validadas e agrupadas. Disso decorre que cada nó da rede, ainda que compartilhe de todo o histórico comum dos acontecimentos e esteja sujeito à aplicação sumária das mesmas *regras de consenso*, tem sempre uma perspectiva presente que diverge em maior ou menor grau dos demais. Ou seja, o *status* de uma máquina, a qualquer momento, reflete a perspectiva das relações estabelecidas com as outras máquinas, de modo que a diferença daquilo que ela *sabe* sobre a rede precisa ser sempre ajustada: o que converge será consolidado, e o que diverge será descartado ou mantido no limiar da indeterminação até que um novo estado de consenso venha a ser estabelecido.

Aferir o *status* a partir de um nó completo da rede (*full node*) pode ser tão simples quanto executar uma ação num terminal de comando ou consultar um resumo das informações exibidas pela interface gráfica do software Bitcoin. Diversas ferramentas e aplicações foram desenvolvidas para facilitar o acesso a esses dados,

como os chamados *block explorers*, sites que organizam e exibem a *blockchain* em uma interface legível para humanos, e os *dashboards*, que são aplicações que buscam sistematizar o maior número possível de informações em painéis, gráficos e estatísticas. Ambas as modalidades de ferramentas dependem do ponto de vista de um *full node* (ou mesmo de vários).

Na imagem abaixo, vemos a tela de um *dashboard* bastante conhecido entre usuários da rede interessados nas métricas *on-chain* consideradas mais relevantes: o atual poder computacional da rede (*hashrate*), a quantidade de transações contidas no último bloco produzido, a altura do último bloco (*block height*, a corrente de blocos também pode ser imaginada como uma pilha), o tamanho atual da *blockchain* (cerca de 628GB), a quantidade de transações à espera de validação (*mempool*), a quantidade de nós conhecidos, a dificuldade de mineração, etc.

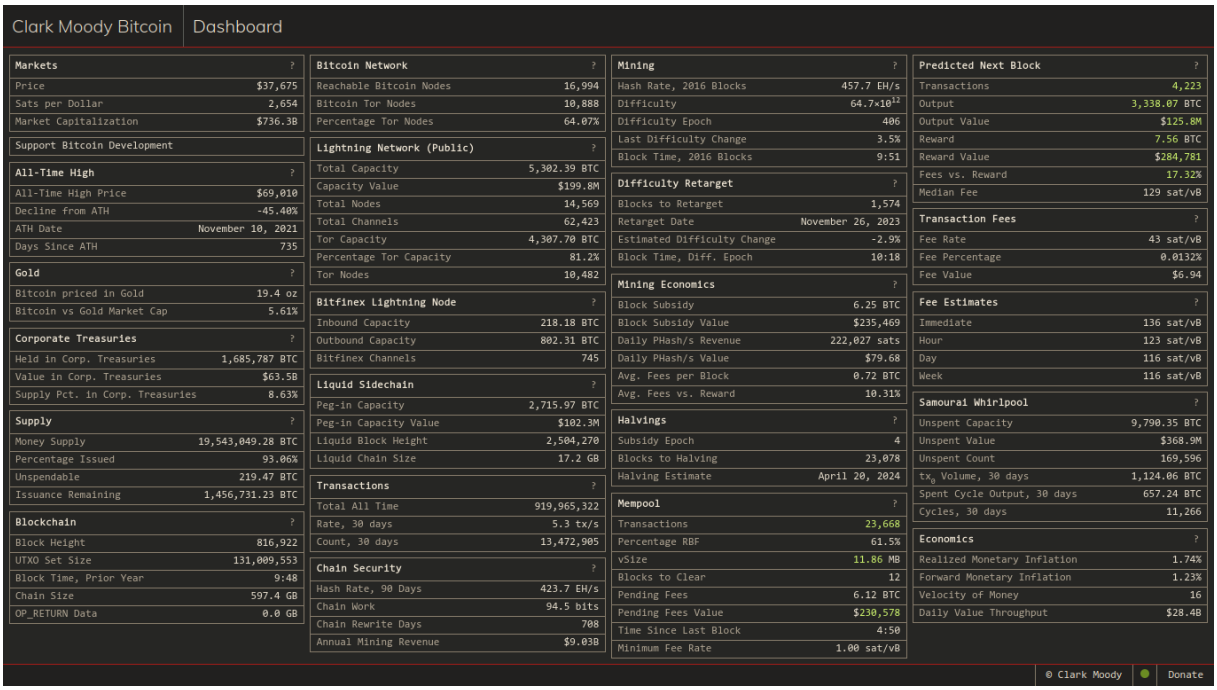

Figura 10: Tela inicial do dashboard de Clark Moody, pesquisador que o mantém online um dos mais completos e conhecidos pontos de referência sobre o sistema Bitcoin: https://bitcoin.clarkmoody.com/dashboard

Os dashboards oferecem os *status* de referência acerca da rede em um dado momento. Muitas dessas métricas são utilizadas em processos de tomada de decisão por parte dos participantes (por exemplo, saber a taxa média que está

sendo paga por transação em um dado momento do dia) e por parte de investidores e *traders* (por exemplo, se o *hashrate* diminui, pode significar que mineradores estão saindo do mercado, o que pode vir a impactar o preço atual). Essas informações internas ao sistema (métricas *on-chain*), junto com gráficos de preço, modelos de mercado e outras estatísticas externas (métricas *off-chain*), influem diretamente no comportamento dos agentes – e, de certo modo, como veremos adiante, por meio desse *feedback* estatístico, ajudam a consolidar esses referentes como fontes privilegiadas de informação.

Assim, pensando a partir da perspectiva dos *traders* em plataformas digitais (*exchanges*), esses mercados se fazem ver como conjuntos de gráficos mediados por telas. Para muitos usuários e investidores, boa parte da explicação técnica sobre o funcionamento das criptomoedas é muitas vezes irrelevante: mais do que um sistema distribuído de registro de transações, o Bitcoin e outras criptomoedas, para eles, são ativos digitais, cujas características que os definem são pensadas como "qualidades" que os tornarão mais ou menos valiosos no futuro. No mais das vezes, esses *players* não têm qualquer intenção de utilizar esses sistemas diretamente, tendo suas negociações mediadas por outras plataformas ou instrumentos financeiros oferecidos em certos mercados (por exemplo, derivativos de Bitcoin).

Para uma *exchange*, tal como parece ser o caso do mercado FOREX, importam mais os pares de moedas que estão sendo negociados, em especial seu preço relativo, as possibilidades de arbitragem em diferentes mercados e as chances de especular sobre sua volatilidade. O funcionamento do software e as configurações algorítmicas subjacentes às redes de criptomoedas costumam ser, assim, motivo de um interesse secundário. Do mesmo modo, estratégias de "análise técnica" (análise gráfica sobre os gráficos de preço de cada moeda), generalizadas para avaliação de múltiplos ativos, têm por objetivo minimizar impulsos psicológicos dos *traders* e padronizar estratégias de compra e venda durante períodos de "ação de preço" (*price action*), bem como estruturar narrativas que visam antecipar os movimentos dos mercados.

Há um forte componente retórico em torno desses métodos, muitas vezes mobilizados junto de ideologias empreendedoras, e "profecias autorrealizáveis": se o

mercado se conforma com a análise, a análise é precisa; se o mercado desvia do esperado, a análise foi malfeita ou enviesada pelos "desejos" dos operadores ou por "ruídos" de informação (BLACK, 1986). Em todo o caso, o mercado é tomado aqui, por esses *players* como uma entidade (quase) "perfeita", correspondendo com descrições da "hipótese dos mercados eficientes" (ou EMH, *Efficient-Market Hypothesis*)[86], que embasa vários desses estilos de análise gráfica (ORTIZ, 2014).

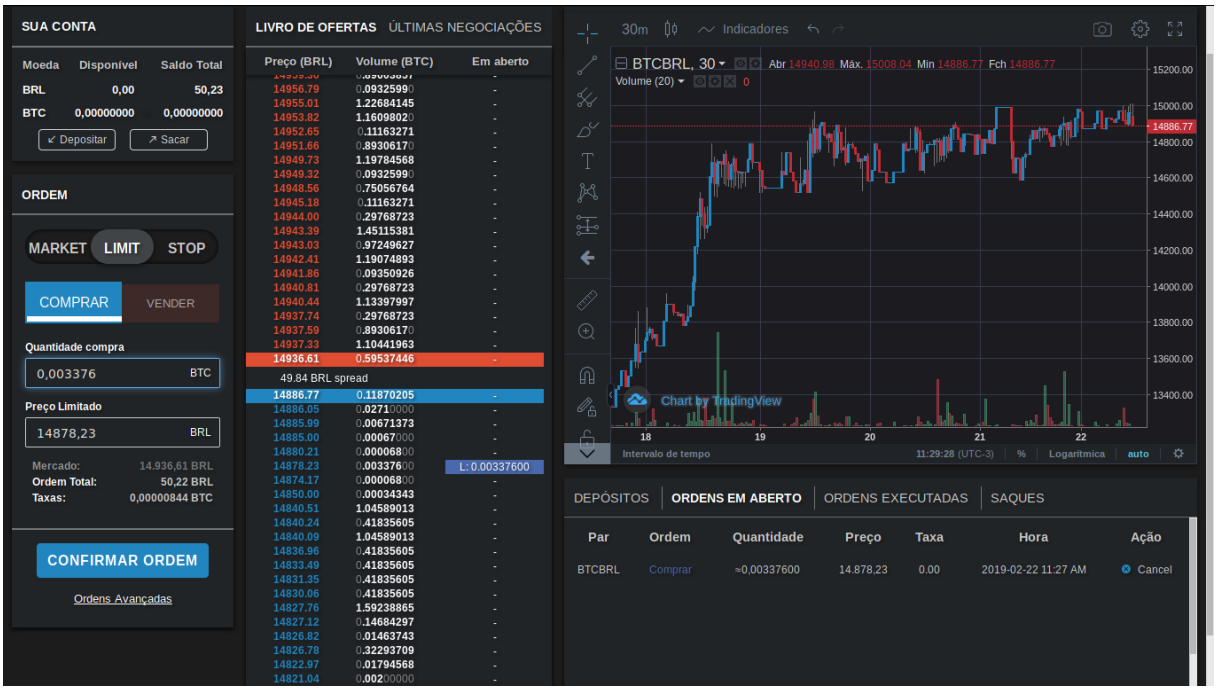

Figura 11: Dashboard principal da corretora Coinext em 2019.

A imagem acima é um *print* da tela do meu computador na manhã de 23 de fevereiro de 2019. Meu navegador está na página da corretora nacional Coinext[87], após eu ter *logado* com minhas credenciais (e-mail e senha). A interface consiste em três colunas e condensa num mesmo plano uma grande quantidade de informação.

86 A crítica de David Graeber em "Against Economics" (2019) menciona a EMH como uma hipótese falha pois "não-falseável", não por conta da discussão sobre a "precificação da informação", mas por causa do enlace da noção de "eficiência dos mercados" com o paradoxo, apontado por Robert Skidelsky (cujo livro "Money and Government: The Past and Future of Economics" é o motivo do texto de Graeber), de que é impossível verificar a hipótese dos mercados eficientes sem considerar as intervenções governamentais na economia pois estas, por sua vez, de acordo com a economia neoclássica, interferem na própria eficiência dos mercados e portanto deveriam ser reduzidas ou mesmo eliminadas.

87 Disponível em: http://coinext.com.br. Acesso em: 23 fev. 2024.

Esse é um modelo de interface bastante difundido entre corretoras e empresta diversas tecnologias dos mercados de ações: gráficos temporais de evolução do preço, livro de ofertas, relação de ordens abertas e executadas, balanços, histórico de negociações e um painel para criação de algumas modalidades de ordens de compra e venda.

Dentre as pouco mais de trinta corretoras nacionais, a Coinext está entre as dez maiores *exchanges* em volume diário de transações[88]. À época, optei por ela pois era uma das poucas que me permitia realizar o cadastro e as operações básicas apenas com meu e-mail e CPF, enquanto que a maioria das outras corretoras exigia, logo no início, o envio de um documento com foto e de uma *selfie* do usuário para autenticar sua identidade e tentar mitigar os registros de usuários com documentos falsos[89]. Neste caso, é possível depositar dinheiro ou criptomoedas na conta virtual da corretora e realizar compras e vendas sem a validação de documentos. No entanto, para a realização de saques, seja em Reais ou em Bitcoins, é necessário e inevitável "completar o cadastro": nome completo, telefone, endereço, documento com foto (RG ou CNH) e *selfie*. A validação dos documentos não era, na época, um processo automatizado e poderia demorar até 24 horas para ser efetivado por alguns dos funcionários da empresa.

A identificação do usuário é feita com a corretora e não há outra forma de identificação ou comunicação com os demais usuários da plataforma: só sabemos que eles existem pois podemos observar suas ações de compra e venda no livro de ofertas. Mais ainda, certas confirmações e cancelamentos de ordens com valores similares num curto intervalo de tempo são um indício da presença de *trading bots*. Como descendentes diretos dos algoritmos de HFT (*High Frequency Trading*, cf. MACKENZIE, 2014), os *trading bots* podem ser diversos programas e *scripts* – gratuitos, pagos ou mesmo maliciosos (*malwares*) – que se utilizam das APIs

88 Essas informações são baseadas no ranking do site https://www.cointradermonitor.com/preco-bitcoin-brasil que monitora as variações de preço das corretoras nacionais com base em dados públicos sobre os volumes de transação e livros de ofertas, em que baseia também um serviço gratuito de arbitragem de preços do Bitcoin entre as corretoras, mostrando que a variação pode chegar a centenas de reais entre uma e outra: https://www.cointradermonitor.com/arbitragem

89 Em 2017, quando me registrei numa *exchange* internacional (Bittrex), o procedimento de KYC (*Know Your Costumer*) era o mesmo: envio de documento com foto e *selfie* para a liberação das ações de compra e venda de criptomoedas.

(*Application Programming Interfaces*) públicas de corretoras para automatizar os processos de compra e venda, muitas vezes operando em paralelo em várias corretoras para encontrar vantagens nas diferenças de preço entre um mercado e outro (estratégia conhecida como "arbitragem").

Outro ponto importante é que a noção de que é possível apreender ou antecipar os movimentos dos mercados a partir da aplicação de regras simples de compra e venda, margens de lucro, *stop loss*, entre outras modalidades de "market making" e "market taking", é a mesma que orienta, há quase três décadas, a criação de *trading bots*, capazes não apenas de agir estritamente de acordo com regras bem definidas (a ausência de emoções e desejos é uma virtude das máquinas), mas também capazes de realizar dezenas, centenas ou mesmo milhares de operações de compra/venda em poucos segundos, numa temporalidade que nos é imperceptível mas que se mostra mais ou menos eficaz nos balanços do final do dia. Como argumenta MacKenzie (2014), cada vez mais os mercados (de futuros, derivativos, ações, FOREX e também criptomoedas) são ocupados, constituídos e mediados majoritariamente por robôs e algoritmos.

Os diversos modelos de precificação e o uso "estratégico" da análise técnica sobre gráficos de preço são elementos que constituem parte importante dessas técnicas e dispositivos como *tecnologias de imaginação*. As leituras de gráficos de preço e a percepção da rede enquanto um sistema financeiro descentralizado se baseiam nos históricos de transações de mercados digitais ou em eventos passados para evidenciar padrões que podem (ou não) se repetir. Isto é, modelos econômicos ou estratégias de análise não indicam nem prevêem o que de fato irá acontecer, mas informam e estimulam comportamentos econômicos específicos a partir de tendências e circunstâncias similares do passado (MACKENZIE, 2006). Aqui também a noção de "profecia autorrealizável" é recorrente, e muitas vezes o objetivo de um *trader*, seguindo "monasticamente" sua estratégia pessoal, é a de emular o desempenho de um bom robô (o que muitas vezes significa empregar um robô em seus próprios investimentos). Essas performances cruzadas entre *traders* e *bots*, ambos seguindo as mesmas regras em velocidades diferentes, parecem "confirmar" as profecias ditadas pela análise gráfica, uma vez que ela é o próprio modelo que orienta a ação desses *players* (MACKENZIE, 2019a).

Porém, ainda que tal performance chame a atenção de um observador do livro de ofertas, não há como saber se as demais ordens de compra e venda, mais discretas ou corriqueiras, mais volumosas ou comedidas, foram criadas por robôs ou humanos. Tudo se passa como se o ambiente virtual da plataforma estivesse livre de interferências externas e outras distrações. Lá, o *trader* silencioso contempla a ação do *preço puro* –

> "Price discovery automation" – a wave of electronic interventions that characterized financial markets all over the world and which culminated, sometimes quite resoundingly, with the abolition of open-outcry and face-to-face trading – was presented as both a unique contribution to the purification of price formation (i.e. the removal of the barriers that prevented the expression of the market in the form of truly transparent prices) and a blatant demonstration of the fact that *price formation is a technological service* (i.e. something that does not happen in and by itself, something explicitly manufactured, utterly unnatural). (MUNIESA, 2014, p. 62, grifos nossos)

É interessante notar como se dá a formação de preço em uma *exchange* de criptomoedas. Na imagem acima, a coluna do meio é o dinâmico livro de ofertas: os preços em azul são ordens de compra, ordenadas em ordem crescente; os preços em vermelho são as ordens de venda, em ordem decrescente. No centro do livro, o maior preço de compra e o menor preço de venda se encontram. A diferença entre esses preços é chamada *spread*. No instante em que capturei a imagem, o maior preço de compra era R$14.886,77 por 1 Bitcoin (e um volume de 0,11870205 bitcoins, ou seja, uma ordem de compra de aproximadamente R$1.767, desconsiderando as taxas de transação) e o menor preço de venda era R$14.936,61 por 1 Bitcoin (e um volume de 0,59537446 bitcoins, ou seja, uma ordem de venda de aproximadamente R$8.893, desconsideradas as taxas). O *spread* naquele momento era, portanto, de apenas R$49,84. Quanto mais usuários ativos, maior o volume de transações e mais rápida é a variação de preços conforme as ordens do livro vão sendo executadas, o que faz com que o *spread*, a diferença entre as ordens, não seja tão expressivo em um mercado movimentado. Em corretoras menores, onde o volume negociado é pequeno e a quantidade de usuários é menor, o *spread* dos preços pode chegar a várias centenas de reais, o que faz com que muitas ordens de compra ou venda demorem muito a sejam executadas e o mercado fique

praticamente "parado", registrando apenas os últimos preços negociados de quando em quando. Ao contrário, nas grandes corretoras é difícil acompanhar a velocidade de variação e execução das ordens em uma observação do seu livro de ofertas.

À direita do livro de ordens, o gráfico nos mostra a evolução recente do par BTC-BRL, usando "velas" (*candlesticks*) nas cores azul e vermelho para representar a oscilação do preço e os fechamentos positivos ou negativos a cada intervalo de 30 minutos, isto é, toda informação acumulada por aquele mercado nos últimos meses. O intervalo padrão da interface é de 15 minutos, e há vários outras opções de intervalos disponíveis: minutos, horas, dias, semanas, meses. O provedor do gráfico é a empresa Trading View[90], talvez um dos sites mais populares para visualização de gráficos do mercado financeiro global, trazendo gráficos interativos de uma infinidade de pares de moedas, ações ou ativos, bem como ferramentas de desenho e comentários sobre esses gráficos. Há anos, pares com Bitcoin e as principais criptomoedas foram inseridos na plataforma, que permite incorporar seus gráficos em páginas externas, sendo assim uma das principais ferramentas de *traders* e objeto de milhares de *lives* no Youtube sobre previsões de preços futuros e padrões gráficos complexos que podem antecipar os comportamentos e humores do mercado.

Fabian Muniesa (2014) argumenta que não apenas a automação da "descoberta de preço" (*price discovery*, mas na prática, *price fabrication*) tem caracterizado os mercados financeiros desde fins da década de 1970, como também todo um *vocabulário algorítmico* é mobilizado para descrever o curso das ações:

> How should agents be prevented from trading at "false" prices, whatever this means? And what should be done if more than one "true" price is found? Those questions call for a somewhat algorithmic formulation of the course of action. "If … then … go to … terminate". And this is precisely what economics has become, to a quite great extent, in the wake of the "machine turn" that characterized specialities such as experimental economics, operations research, mechanism design, auction theory and market microstructure (MUNIESA, 2014, p. 62).

Daí em diante, segundo Muniesa, nas décadas de 1980 e 1990, os mercados financeiros se tornam palco de uma série de iniciativas de "computer-

90 Disponível em: http://tradingview.com. Acesso em: 23 fev. 2024.

assisted liquidity enhancement (i.e. enabling more trading)" com a instalação de novos mercados eletrônicos:

> They challenged the very definition of what an "exchange" was supposed to be. They introduced into market regulatory parlance words that better described computer technologies than commercial transactions (i.e. 'system', 'data', 'access', 'execution', 'program', 'network'). They activated circumstantial (but crucially performative) associations between financiers, technologists and economists in the emerging business for market technologies (*idem*).

Sobre esse mesmo tema, de acordo com Pardo-Guerra, em sua arqueologia dos processos de automação dos mercados financeiros:

> the architects of electronic financial markets (…) are nevertheless capable of shaping their world by shifting the language of what was possible, desirable, and legitimate through the creation of myths. As Meyer and Rowan (1977) argued, with little entrepreneurial energy, actors can then assemble such myths "into a structure; and because these building blocks are considered proper, adequate, rational, and necessary, organizations must incorporate them to avoid illegitimacy". Infrastructural workers did not simply produce automated markets: they also fabricated the organizational building blocks and cultural vocabularies that rendered them a legitimate, almost necessary route for the future of finance; they crafted technologies of honor and community to justify their novel technology of consociation (PARDO-GUERRA, 2019, p. 166).

Isto é, ainda que em retrospecto a automação dos mercados financeiros possa parecer um processo "natural" de modernização e incorporação de novas tecnologias, movido pela racionalidade da eficiência e redução de custos, esses processos são, segundo Pardo-Guerra, "as a type of myth that structure and coordinate action across organizational fields by depicting what seem to be the legitimate 'rational means for the attainment of desirable ends' (*idem*, p. 165-166). As modalidades de transação oferecidas pelos mercados digitais não pretendem apenas replicar modalidades "tradicionais", mas principalmente instituir novos procedimentos de troca de informação e novas velocidades, por meio de uma transformação cultural promovida nesses próprios mercados, assim tornando indispensável tudo aquilo que é possível de ser implementado.

Na corretora Coinext, em 2019, havia três modalidades de transação, que costumam ser oferecidas em qualquer mercado digital: *market*, *limit* e *stop*. A

transação de tipo *market* cria uma ordem de compra ou venda a partir do preço do mercado naquele exato momento. A transação *limit* permite que o usuário defina o preço e a quantidade que deseja negociar. A transação *stop* é ativada somente se o mercado atinge um certo preço, podendo ser um gatilho para compras caso o preço suba, ou um meio de evitar perdas maiores caso o preço venha a cair rapidamente (*stop-loss*). Atualmente a maioria das corretoras implementa essas três modalidades de transação, embora também seja possível, em algumas plataformas, criar ordens mais complexas baseadas em diversos outros condicionantes.

De volta à imagem anterior, ao livro de ordens, vemos que a quinta linha abaixo da primeira, em azul, está destacada por uma *tag* azulada, o que sinaliza uma ordem de compra ainda *em aberto*. Esta é a minha ordem de compra. Cerca de uma hora antes do *print*, utilizando o aplicativo do meu banco no celular, transferi para a corretora Coinext, em uma conta de um banco que eu então desconhecia[91], o valor mínimo para um depósito: R$50. Na verdade, transferi exatos R$50,23 numa transação TED, pois este também é um processo aparentemente manual: cabe a alguém comparar os depósitos com o comprovante, que enviei à corretora por meio de um formulário que especifica o valor transferido e a modalidade de transação (DOC ou TED), e confirma o saldo; é mais fácil para o funcionário responsável por essa tarefa confirmar o depósito de "valores quebrados" em meio a tantos depósitos diários (prática que também era comum em outras corretoras, e que provavelmente já foi superada por outros meios de automação e pela instantaneidade das transações PIX, que à época não exista).

Cerca de meia hora após a transferência, meu saldo na corretora era de R$50,23. Criei, então, uma ordem de compra do tipo *limit*: decidi que 1 Bitcoin valia para mim, naquele momento, R$14.878,23. Por esse preço, usando todo meu saldo, conseguiria comprar 0,00337600 bitcoins. Mesmo ficando próximo do centro do livro,

91 Há uma série de relatos e inclusive processos contra os maiores bancos brasileiros por conta de congelamentos e cancelamentos de contas associadas com investidores ou mesmo com corretoras de criptomoedas. A maioria das corretoras costuma operar com contas em bancos pequenos, muitas vezes com duas ou três contas em bancos diferentes, pois esse parece ser um problema recorrente. As associações ABCB e ABCripto, que representam diversas das corretoras brasileiras, têm entrado na justiça com processos contra alguns desses cancelamentos. Vide, por exemplo, o caso da corretora Foxbit contra o banco Bradesco: https://portaldobitcoin.com/bradesco-vence-foxbit-na-justica-em-processo-sobre-fechamento-de-conta

tive que esperar um tanto: minha ordem de compra só foi executada uma hora mais tarde, quando o preço alcançou o valor que estipulei, consumiu a maioria das ordens na casa dos 14.800 reais, voltou a subir para a casa dos 14.900, e eventualmente rompeu a barreira dos 15.000, algumas horas depois. A partir de então, meu saldo na corretora passou a ser de 0,00337600 bitcoins – ou 337600 *satoshis*. Contudo, eu só poderia "sacar" essa quantia para uma carteira (*wallet*) particular, no meu computador ou no celular, após a validação da minha conta na corretora com um documento pessoal e uma *selfie*. Até lá, porém, poderia criar uma ordem de venda usando todo meu saldo ou parte dele, e estipular um preço maior para tentar vender meus *satoshis* e depois sacar o valor em reais, ou então utilizar essa nova quantia em reais para comprar mais *satoshis* no futuro por valor mais baixo, ou outras moedas, ou depositar mais reais ou criptomoedas e assim por diante[92]. Uma estratégia comum entre alguns investidores individuais com quem conversei era a de tentar sacar, em reais, a mesma quantia que foi depositada inicialmente, de modo a manter na corretora apenas o lucro proveniente da primeira operação, na expectativa de evitar perdas e multiplicar seus ganhos aos poucos (uma estratégia que funciona melhor em melhor durante períodos de alta, em que a curva de preço tende a subir).

Um aviso na plataforma indicava que as carteiras controladas pela corretora eram assinadas por empresas independentes, "contratadas e localizadas geograficamente em dois continentes", por meio de um método *multi-signature*, com vistas a tranquilizar seus clientes quanto às possibilidades de terem fundos

92 Todas as transações realizadas na corretora são taxadas. Cada corretora estipula suas próprias taxas. No caso desta, à época, 0,5% para ordens executoras (*taker*) e 0,25% para ordens executadas (*maker*). Além disso, há as taxas de transação no interior do sistema Bitcoin, pagas em *satoshis* para os mineradores que virão a confirmar minha transação de depósito (para uma carteira controlada pela corretora) ou saque (para uma carteira própria) em um bloco de transação. O cálculo dessa taxa é dinâmico, pois depende do tráfego da rede, e se dá em função do tamanho da transação, calculado em *satoshis/byte*. Uma transação tem em média 250 bytes de informação. No momento em que escrevo esta nota, estamos na altura do bloco número 564262, recém-minerado com 3064 transações (tamanho total: 1.125.174 bytes ou 1,07 megabytes), e um total de 0,13007488 bitcoins em taxas (pouco mais de 500 dólares), o que nos dá uma taxa média de 11 satoshis/byte. Interessante notar que, além dos 500 dólares em taxas, o minerador que criou este bloco recebeu a recompensa de 12,5 bitcoins recém-criados (cerca de 50 mil dólares). Somado com os valores das transações confirmadas, esse único bloco movimentou pouco mais de 14,1 milhões dólares. Vide em detalhes: https://blockchair.com/bitcoin/block/564262

roubados, que a própria corretora viesse a desaparecer do dia para a noite em um *exit scam*, de sofrerem ataques de *hackers* (ou alegarem terem sido *hackeados* para desaparecerem logo depois), ou de serem vítimas da traição de um alto funcionário. Carteiras *multi-sig*[93] garantem, em princípio, que os valores nela contidos só podem ser movidos caso a maioria ou todos os signatários da carteira concordem em fazê-lo por meio de assinaturas com chaves criptográficas privadas. Todavia, como diz o ditado popularizado pelo cientista da computação, autor e *Bitcoin evangelist* Andreas M. Antonopoulos: "Simple Rule: if you control the keys, it's your Bitcoin. If you don't control the keys, it's not your Bitcoin. Your keys, your Bitcoin. Not your keys, not your Bitcoin"[94]. Isto é, por mais que usuários mantenham "seus" bitcoins e outras criptomoedas em contas de corretoras, eles não possuem qualquer propriedade efetiva sobre esses valores até que tenham sido movidos de fato para uma carteira atrelada às suas próprias chaves privadas.

A noção de "chaves" ou "chaves criptográficas" se refere à criptografia assimétrica, um método criptográfico descrito pela primeira vez no final dos anos 1970 pelos pesquisadores R.L. Rivest, A. Shamir, and L. Adleman, e por isso conhecido pelas iniciais de seus sobrenomes, RSA (RIVEST; SHAMIR; ADLEMAN, 1978). Em linhas gerais, o método consiste em três algoritmos: 1) o gerador de chaves, que cria uma chave pública e uma chave privada; 2) o encriptador, que toma como parâmetro a chave pública do destinatário e a mensagem que se deseja enviar para produzir uma mensagem cifrada; e 3) o decriptador, que toma como parâmetro a chave privada do destinatário e a mensagem cifrada, para obter mensagem original. Somente a chave privada é capaz de decriptar a mensagem cifrada com a chave pública, pois ambas foram criadas pelo mesmo processo matemático. Esse sistema de chaves públicas e assinaturas[95] está na base do funcionamento dos

93 Vide https://en.bitcoin.it/wiki/Multisignature. Acesso em: 23 fev. 2024.

94 Andreas Antonopoulos em palestra em 7 de julho de 2017. Disponível em: https://www.youtube.com/watch?v=vt-zXEsJ61U. Acesso em: 23 fev. 2024.

95 Posso produzir uma assinatura para qualquer mensagem ou documento utilizando minha chave privada. Essa assinatura, junto do arquivo assinado, pode ter sua integridade verificada por qualquer um que conheça minha chave pública. Qualquer alteração no arquivo assinado ou na própria assinatura resulta numa verificação inválida. Esse é um método eficiente e utilizado de uma infinidade de maneiras para garantir a integridade e autenticidade de mensagens trocadas em rede.

endereços ("carteiras") do sistema Bitcoin e da maioria das outras criptomoedas – é, em verdade, o que justifica, junto dos *hashes*, o prefixo *crypto*.

Um *software* a que chamamos de carteira (*wallet software*, *wallet app* ou *web wallet*), a partir de uma senha conhecida apenas pelo usuário, pode gerar uma série de endereços – *grosso modo*, chaves públicas – que funcionam como carteiras ou contas: quando dizemos, por exemplo, que há 7 bitcoins em um determinado endereço, o que se passa de fato é que se supõe que o responsável por aquele endereço tenha a propriedade (*ownership*) das credenciais necessárias (a chave privada) para transferir aquela quantidade, ou parte dela, para a propriedade de qualquer outro endereço no futuro. Não há, na verdade, moedas ou partes de moedas que são enviadas de um lado para outro da rede. Quando uma transação entre pares é confirmada, aquilo que foi efetivamente trocado é a propriedade (ou titularidade) sobre uma quantidade alocada no registro distribuído (a *blockchain*). Sendo assim, toda transação é, de fato, uma transferência de propriedade, e todo *input* de uma transação é necessariamente o *output* de outra[96].

Toda uma linhagem de criptomoedas, começando pelo Bitcoin, se baseia nessa lógica, em que a "estrutura contábil" básica é a UTXO: *unspent transaction output*. Uma UTXO é de fato o "balanço" de um endereço: se tenho 3 bitcoins no meu endereço, isso significa que esses 3 bitcoins não foram gastos em nenhuma outra transação (portanto, *unspent*) e vêm de algum lugar considerado válido (ou são o *output* de outras transações que fizeram para o meu endereço ou são moedas criadas como recompensa pela mineração de um bloco). Se quero lhe pagar 1 bitcoin, eu realizo uma transação que utiliza todo meu balanço: lhe pago 1 bitcoin (que irá se tornar uma *unspent transaction output* no seu endereço, e portanto passa a ser sua propriedade), pago também as taxas de transação (digamos, 0,05 bitcoin para a mineração, que validará essa transação nos próximos blocos) e pago também

96 Vide, por exemplo, esta transação https://blockchair.com/bitcoin/transaction/385715053 (TXID: cbb0dec745440ff1e44636c2366d7045095884671e19bfb8554798a319aeb3c5), contida no bloco 564262, mencionado anteriormente, que move 7 bitcoins para um dado endereço, que transfere a quantia para outros dois endereços nos blocos seguintes: uma parte permanece não-gasta (*unspent*) e que a outra já foi gasta em novas transações: https://blockchair.com/bitcoin/transaction/618a89fa0024aa2d170a4d9d44ce18978b26a26e9c2a7e282438f7f02b773768#i=0.

o restante (1,95 bitcoin) de volta para mim mesmo. Toda transação destrói uma (ou mais) UTXOs e cria outras no mesmo ato.

Porém, quando realizo a "compra" dos meus 0,00337600 bitcoins, que constam agora no balanço na corretora, nada disso aconteceu. Não são as minhas chaves que controlam essa quantidade, ainda. O que há é que, no balanço interno da corretora, eles determinam que essa pequena quantidade, supostamente presente em carteiras controladas por eles, foi comprada por mim. Somente depois que eu validar minha conta e tentar realizar um "saque" dessa quantia para um endereço próprio – isto é, gerado num *software* em que eu controlo minhas próprias chaves –, e que a transação seja minerada em bloco, é que eu posso dizer, de fato, que esses 337600 satoshis são de minha propriedade, pois serão, caso tudo corra bem, uma UTXO cuja chave privada eu controlo. Essa é uma das grandes diferenças entre serviços de custódia (intermediários confiáveis) e sistemas *peer-to-peer* em que cada nó ou par opera como cliente *e* servidor, estabelecendo suas próprias conexões com a rede. De acordo com Brunton,

> You don't own a bitcoin – you don't have possession of the bits because there are no bits that constitute a given bitcoin to be possessed. Rather, *you hold the right in the ledger to claim a particular bitcoin and to assign that right to someone else*. (…) the right, the claim, is reassigned through a transaction update added to the ledger (BRUNTON, 2019, p. 162)

A ideia de que "bitcoins são moedas" decorre portanto de uma abstração estabelecida no código-fonte, na interface gráfica do sistema e em plataformas associadas, um artifício simbólico que, do ponto de vista das máquinas, não tem qualquer significado efetivo. Para além de um registro distribuído de todo o histórico de transações já realizadas, a *blockchain* é, mais precisamente, um sistema de encadeamento de assinaturas criptográficas que funcionam como registros de propriedades digitais: a *blockchain* registra todas as transações efetuadas na rede, o que de fato significa a atribuição de cada unidade (ou fração de unidades) em circulação à chaves criptográficas particulares, capazes de autorizar a transferência de sua titularidade a outra chave por meio de uma transação. Um *bitcoin*, portanto, é uma reivindicação (*claim*) sobre a propriedade de uma quantia discreta "não gasta": mais precisamente, um *bitcoin*, ou qualquer fração de *bitcoin*, consiste em um

unspent transaction output (*UTXO*) que pode vir a ser passado adiante na forma de uma "transação". Assim, aquilo que é trocado na rede não são "moedas", mas os direitos de movimentação, *como moedas*, sobre *outputs* ainda não gastos. Gastar uma moeda significa transferir os direitos de enviá-la para alguém: "bitcoin is the right to send fixed and non-replicable data to someone else privately in a public ledger" (ÇALIŞKAN, 2018, p. 7).

Quaisquer que sejam os modos de se conectar com o sistema *peer-to-peer* Bitcoin, o ponto importante é que o sistema não pode ser visto ou apreendido "totalmente" de ângulo nenhum: nem mesmo um nó da rede (um *full node*), que opera como um replicador de informações consideradas confiáveis de acordo com as regras do sistema, "enxerga" a totalidade circunstancial dos nós participantes. Quanto mais nos aproximamos dos meandros dos algoritmos, mais as máquinas, por meio de seus protocolos de comunicação, estabelecem entre si relações como fluxos de informação. E, quanto mais nos afastamos da minúcia da programação, tomando alguma distância de pontos particulares na direção do fenômeno coletivo da rede e dos mercados, mais as pessoas, as operadoras de máquinas e desejos, parecem estabelecer relações maquínicas com os aglomerados representados em gráficos dinâmicos de preço e nos *orderbooks* de corretoras digitais. Enquanto as máquinas transacionam entre si para estabelecer consensos, os "investidores" jogam o jogo das estratégias mecânicas diante das suas telas. Também a especulação, como um procedimento, torna o sistema acessível para muitos usuários, ao impor sobre suas partes um certo enquadramento que tanto procura imitá-lo, por meio de um modelos imaginados, quanto procura antecipá-lo, por meio de previsões e predições.

O sistema, assim, é continuamente visto a partir feixes de de transações e trocas, fluxos de informação organizados por *dashboards* e pensado como um sistema "perfeito" de preços. Esses artifícios se acoplam também a diferentes narrativas, ideologias e disputas de poder, bem como séries de explicações consideradas "canônicas" por diferentes comunidades organizadas de modo difuso. Os modos de regulação dessas trocas, tomam como referente um sistema financeiro mais amplo, ao qual esses novos mercados vão, cada vez, se amalgamando.

3.2 DO DINHEIRO DE PEDRA A ATIVOS FINANCEIROS DIGITAIS: IMAGINAÇÕES DO SISTEMA E A REGULAMENTAÇÃO DAS CRIPTOMOEDAS

O deslocamento das trocas entre humanos para as trocas entre máquinas traz tensões importantes com teorias econômicas clássicas, em que a troca é um fenômeno caracterizado por relações de afinidade e aliança. Porém, como vimos, estamos diante de redes de adversários em que no mais das vezes o lucro individual ou corporativo é o objetivo principal. Um fenômeno curioso por parte de alguns participantes e autores proeminentes nas comunidades criptomoedas é a mobilização de narrativas antropológicas como embasamento para narrativas ideológicas sobre a forma e a evolução do dinheiro. Essas apropriações vão desde as comparações das criptomoedas com *collectibles*, como conchas e as grandes pedras redondas da ilha de Yap, como veremos adiante. O breve artigo intitulado "Bitcoin Explained via Balinese Cockfights: The Similarities Are Uncanny", por exemplo, escrito por um antropólogo para uma publicação online, estabelece uma comparação entre o sistema de dinheiro eletrônico e a briga de galos balinesa descrita por Geertz (GEERTZ, 1972, 1981). O autor se vale da analogia com a arena de briga de galos para ilustrar os diversos níveis de interação e engajamento em uma comunidade, cada um com diferentes participantes e interesses, destacando assim as interações dinâmicas entre um grupo diverso de participantes da comunidade Bitcoin e, ao mesmo tempo, enfatizando sua natureza descentralizada e virtual.

> What is meant by "Bitcoin community" is itself hard to grasp, let alone visualise in place. That's because although it occasionally meets up in physical locations worldwide, this community is digitally native: members mostly inhabit Twitter, Reddit, Telegram groups, and Bitcointalk.org chatrooms. (…) So to help us imagine the Bitcoin community, a visual metaphor of the cockfight arena comes in handy: at its centre are the competing cryptocurrencies being discussed, in the first outside ring are the holders of the cryptocurrencies, and further out are the speculators.[97]

Alguns programadores e analistas do sistema Bitcoin teorizam sobre o funcionamento da rede a partir de certa literatura antropológica sobre a troca. Ao

97 "Bitcoin Explained via Balinese Cockfights: The Similarities Are Uncanny", 21 de agosto de 2020. Disponível em: https://hackernoon.com/bitcoin-explained-via-balinese-cockfights-the-similarities-are-uncanny-vp3q3xio. Acesso em: 23 fev. 2024.

refletir sobre as origens do dinheiro, o *cypherpunk* Nick Szabo, criador do *Bitgold*[98] (uma proposta de moeda digital, precursora do Bitcoin, porém nunca implementada), estabelece aproximações entre "formas primitivas de dinheiro", objetos sem uma "utilidade concreta", com o entendimento moderno de moeda, como meio de troca, reserva de valor e unidade de conta. Em "Shelling Out: The Origins of Money" (SZABO, 2005), um artigo bastante referenciado por entusiastas do Bitcoin, Szabo faz uma analogia entre moedas contemporâneas e "formas de dinheiro colecionáveis", tal qual os objetos trocados no circuito do Kula, descrito por Malinowski:

> by solving the double-coincidence problem an armshell or necklace would prove more valuable than its cost after only a few trades, but could circulate for decades. Gossip and stories that about prior owners of the collectibles further provided information about upstream credit and liquidity (*ibid*).

Outro caso interessante é sobre o "dinheiro de pedra" de Yap. Em dezembro de 2010, na seção de economia do veículo de comunicação NPR, o artigo "The Island of Stone Money"[99] trazia uma descrição do *stone money* de Yap, baseada na pesquisa do antropólogo Scott Fitzpatrick (2004; 2003), e que seria replicada à exaustão ao longo dos meses e anos seguintes em dezenas de artigos e postagens em portais de notícias sobre criptomoedas.

> "They often talk about the stones themselves not changing hands at all," Fitzpatrick says. "In fact, most of the time they wouldn't."
>
> So imagine there's this great big stone disc sitting in a village. One person gives it to another person. But the stone doesn't move. It's just that everybody in the village knows the stone now has a new owner.
>
> In fact, the stone doesn't even need to be on the island to count as money.

---

98 Postulado no final da década de noventa, o *Bitgold* pretendia resolver o mesmo problema que, mais tarde, o Bitcoin veio a implementar – isto é, o da troca digital sem intermediários, tendo como base a noção de escassez e custo de produção de metais preciosos e objetos colecionáveis, como conchas. Vide artigo de Szabo sobre o Bitgold. Disponível em https://unenumerated.blogspot.com/2005/12/bit-gold.html. Acesso em: 23 fev. 2024.

99 "The Island of Stone Money", Jacob Goldstein e David Kestenbaum, 10 de dezembro de 2010. Disponível em: https://www.npr.org/sections/money/2011/02/15/131934618/the-island-of-stone-money. Acesso em: 23 fev. 2024.

O artigo faz referência tanto ao livro de William Furness (1910) sobre a ilha de Yap, quanto ao ensaio de mesmo título de Milton Friedman (1991), que, por sua vez, cita largamente o capítulo VII de Furness ("Money and Currency") para estabelecer uma comparação com o "padrão ouro" ocidental:

> is there really a difference between the Federal Reserve Bank's believing that it was in a weaker monetary position because of some marks on drawers in its basement and the Yap Islanders' belief that they were poorer because of some marks on their stone money? (…) Or, for that matter, how many of us have literal personal direct assurance of the existence of most of the items we regard as constituting our wealth? Entries in a bank account, property certified by pieces of paper called shares or stocks, and so on and on (FRIEDMAN, 1991, p. 4).

Friedman conclui sua comparação, e o ensaio, ressaltando que a "crença" é parte fundamental das questões monetárias:

> What both examples – and numerous additional ones that could be listed – illustrate is how important "myth," unquestioned belief, is in monetary matters. Our own money, the money we have grown up with, the system under which it is controlled, these appear "real" and "rational" to us. The money of other countries often seems to us like paper or worthless metal, even when the purchasing power of individual units is high. (*idem*)

A primeira correlação, ainda que indireta, entre o Bitcoin e o "dinheiro de pedra" de Yap, creio, é feita num post de um blog em junho de 2011[100], que ressalta o que o seria uma das principais características do dinheiro, em especial do dinheiro digital: "money is a matter of belief, even faith: belief in the person paying us; belief in the person issuing the money he uses or the institution that honours his cheques or transfers"[101]. É somente em abril de 2014 que é estabelecida uma analogia direta entre Bitcoin e o "dinheiro de Yap". No blog "Bitcoins and Economy", Pepe Giménzes escreve uma postagem intitulada "Bitcoins & The Stone Money"[102], em que o ponto

100 "Bitcoin, the brave new currency", 26 de junho de 2011. Disponível em: http://www.internetsecuritydb.com/2011/06/bitcoin-brave-new-currency.html. Acesso em: 23 fev. 2024.

101 O que, na verdade, é uma citação do livro *The Ascent of Money: A Financial History of the World*, do historiador britânico Niall Ferguson.

102 Bitcoins & The Stone Money, 26 de junho de 2014. Disponível em: https://bitcoinsandeconomy.blogspot.com/2014/04/bitcoins-stone-money.html. Acesso em: 23 fev. 2024.

de comparação se dá sobre o contraste entre "posse" (*possession*) e "propriedade" (*ownership*) e a importância de um sistema de registro público – no caso de Yap, o registro oral sobre as pedras; no caso do Bitcoin, a *blockchain*:

> The phenomenon of rai stones teaches us that it is not necessary to hold a currency, possession is not important. It is sufficient that there is a public ledger that gives recognition to the owner. The Bitcoin protocol is a public accounting system where every transaction is recorded on the computers of people dedicated to keeping the system alive.

É essa analogia que irá se espalhar, como um *meme*, pela "criptosfera" (a "blogosfera" da "criptoeconomia" e o que é chamado por alguns de "crypto twitter", uma rede difusa de perfis pessoais de programadores, investidores e entusiastas que interage principalmente entre si)[103]. E um dos motivos é que ela está alinhada ao pressuposto generalizado de que o escambo precede a troca, ou de que as trocas são feitas (somente) em função de necessidades básicas ou aquisição de bens[104]. Portanto, a circulação se daria por "meios de troca", dos quais o dinheiro emerge como uma forma sofisticada de "máximo denominador comum" – "if no barter, there is no need for any medium of exchange" (FURNESS, 1910, p. 92).

O "dinheiro de pedra" de Yap se torna um exemplo tanto do "dinheiro primitivo" citado por Friedman, quanto uma modalidade primitiva de *blockchain*, como Vitalik Buterin, criador da criptomoeda Ethereum, cita ao relacionar o valor das pedras a partir das histórias que se contam sobre elas, como um registro público e coletivo mobilizado em sua criptomoeda como um tipo de "proof of stake" (BUTERIN, 2014). Outro autor famoso no meio das criptomoedas também incorpora as pedras de Yap em sua narrativa, nesse caso sob a chave da discussão sobre "inflação versus deflação"[105]:

---

103 As pedras *Rai*, para além da comparação conceitual, também serviram de inspiração para batizar a criptomoeda *RaiBlocks*, criada em 2015, que experimentou uma grande popularidade em seus primeiros anos. Em 2018, entretanto, após um *rebranding*, essa criptomoeda passou a se chamar Nano: https://nano.org.

104 Essa narrativa, é claro, é contestável sob várias perspectivas, como bem demonstra, entre outros, David Graeber (2011).

105 Bitcoin Magazine, "Lies, Deception And Unnatural Money", 13 de outubro de 2020. Disponível em: https://bitcoinmagazine.com/articles/lies-deception-and-unnatural-money. Acesso em: 23 fev. 2024.

> As Saifedean Ammous described in "The Bitcoin Standard," (AMMOUS, 2018) the Island of Yap thrived until Irishman David O'Keefe immigrated there and saw the immense opportunity to mass produce these stones using iron tools. The key here was that O'Keefe was able to make these stones at a quicker rate and to make them smaller, making them more transportable. Over time, the Rai Stone market was so flooded that the stones became worthless, and the value held by the islanders was wiped out.

Em artigos recentes, o próprio arqueólogo, autor da tese sobre Yap que desencadeou todas essas comparações, discorre precisamente sobre a relação entre o dinheiro de pedra de Yap e a *blockchain* do Bitcoin (FITZPATRICK, SCOTT M., 2018; FITZPATRICK, SCOTT M.; MCKEON, 2020). Em especial, para além de propriedades como escassez e o trabalho necessário para sua produção, o ponto central da comparação se dá em torno da noção a que já aludimos de um "regime de verdade" socialmente verificável: "Both oral and digital blockchains represent an 'unequivocal source of truth' where anyone within the system (island society or electronic realm) can know and observe the entire transaction history, enabling auditability" (FITZPATRICK, SCOTT M.; MCKEON, 2020, p. 15). Como argumentam Fitzpatrick e McKeon,

> *Rai* were considered extremely valuable, but given their size, weight, and relative fragility, they were not typically moved after being placed in a specific location. As a result, if a *rai* were gifted or exchanged, the new owner(s) of a disk may not have lived in close proximity to it. To ensure that ownership was known and indisputable, an oral ledger was used within communities to maintain transparency and security. (…) the processes by which both *rai* and Bitcoin were developed, transported, and maintained require sophisticated negotiations between partners to obtain access, mining of the resource, movement of the "coin" between nodes, and placement of ownership within a "block" that is known among all relevant parties. (p. 7, 10)

Assim, é interessante notar como, para os autores, a questão da demanda de energia é um elemento comum a estes sistemas: "both ancient and modern forms of consensus-based ledgers require immense power to operate" (p. 15). Isto é, as modalidades de troca em sistemas como estes implicam tanto um fluxo de informações quanto um gasto energético significativo para sua manutenção, algo que efetivamente aproxima as teorizações antropológicas e arqueológicas sobre

troca e as teorizações nativas dos *bitcoiners* sobre o ecossistema que participam. Notadamente, nos primeiros anos de funcionamento do sistema Bitcoin, o termo "electrical potlatch" foi mobilizado por um crítico ao fazer alusão ao gasto energético excessivo da mineração: "if you’re going to have a system like bitcoin, one could at least have an efficient system of this sort rather than a stupid one based on an *electrical potlatch*"[106]. As dimensões ecológicas dessa modalidade de produção e exploração, que aparecem aqui por meio da descrição material dos sistemas sociotécnicos constituídos a partir lógica de *mineração*, nos remetem novamente à apreensão do Bitcoin enquanto um sistema termodinâmico, operando intensas transformações de energia para a consolidação de sua infraestrutura técnica e material (ZIMMER, 2017).

Teorizações como as apontadas aqui parecem buscar *naturalizar* alguns dos pressupostos técnicos e econômicos do Bitcoin (e da economia neoclássica) num *corpus* muitas vezes autorreferente. Essas questões e comparações implicam diferentes imaginações de futuro e trazem consigo, implícita ou explicitamente, ideologias políticas bastante particulares. Ainda que os entusiastas mais ideológicos das criptomoedas comumente considerem como "refutada" a teoria marxista do valor-trabalho em favor de uma "teoria subjetiva do valor", defendida por autores da economia neoclássica, em especial aqueles da chamada Escola Austríaca, é curioso notar como parte do valor do sistema Bitcoin deriva de procedimentos de exploração e acumulação tão característicos do Capital. Tal ênfase numa "teoria subjetiva do valor", no mais das vezes, tende a eclipsar considerações ecológicas ou humanistas sobre os impactos e efeitos dessas atividades econômicas, em particular, e dos modos de produção capitalista, em geral. Tudo se passa como se a transição para um modo de produção *descentralizado* decorresse das inevitáveis lógicas de mercado e do subjacente determinismo tecnológico da transformação das infraestruturas de comunicação. Como também descreve Matan Shapiro acerca desses mercados, "’belief’ in the power of highly unstable decentralized markets is seen to liberate people from hegemonic economic and political structures" (SHAPIRO, 2024, p. 143).

106 Essa e outras posições estão compiladas no artigo "Bitcoin Is Worse Is Better" (2011). Disponível em: https://www.gwern.net/Bitcoin-is-Worse-is-Better. Acesso em: 23 fev. 2024.

Assim como o capital fragmenta e continuamente especializa seus modos de reprodução, estendendo cadeias de produção e circulação por meio da proliferação de intermediações, também os modos de circulação de ativos digitais produzem uma multiplicidade de novos intermediários. Essa espécie de "reorganização" dos modos de circulação do capital financeiro, embora ainda incipiente e bastante experimental sob a "forma criptomoeda", pretende à dissolução de intermediários "tradicionais" (como as instituições financeiras) e à sobreposição de fronteiras transnacionais por meio de plataformas digitais que conectam mercados locais e globais, o que, no mais das vezes, tende a acelerar e tornar mais eficientes os mesmos processos de acumulação e exploração.

É nesse sentido, por exemplo, que McKenzie Wark (WARK, 2019) delineia os processos históricos do capitalismo para situar o mundo contemporâneo das comunicações digitais como o cenário não da superação do modelo capitalista "tradicional", mas da intensificação dos processos de alienação, exploração e, em especial, da luta de classes, precisamente por conta da emergência de um par de "novas classes" que espelham e complexificam as relações antagônicas estabelecidas. A classe dos *vetorialistas*, segundo a autora, é aquela que emergiu nas últimas décadas como uma nova classe dominante, controlando as infraestruturas de comunicação, os fluxos de dados e os vetores da informação. Ao longo do mesmo processo, emergiu também a classe *hacker*, que engloba desde os trabalhadores do precarizado setor de serviços até as modalidades mais corriqueiras de "trabalho cognitivo" em plataformas digitais e redes sociais. É a partir daquilo que Wark identifica como uma assimetria informacional que se consolidam novas formas de acumulação, exploração da "mais-valia cognitiva" e mineração de dados, características dessa "etapa atual" do capitalismo – se é que, como ela sugere, isso ainda possa ser chamado capitalismo, uma vez que lhe parece possível que se trate de algo *pior*.

Em um trabalho anterior sobre o mesmo tema, Wark argumenta que a informação transforma a própria forma *commodity* e possibilita um novo nível de abstração: "it is not just that information helps run the old forces of production. Information itself becomes commodified. And in the process, it changes the commodity form itself" (WARK, 2017, p. 61). Similarmente, como argumentam Birch

e Muniesa (2020), ainda que os mercados e a lógica especulativa continuem exercendo um papel decisivo na constituição da "forma commodity" como um modelo universal para todas as coisas científicas e tecnológicas, a forma dominante do capitalismo tecnocientífico tornou-se o *ativo*, cujos contornos não são apenas aqueles dos mercados especulativos, mas do capital de investimento: "almost anything can be turned into an asset given the right techno-economic configuration" (p. 29). Dito de modo mais direto, nas palavras de um investidor entrevistado por Pardo-Guerra: "trading securities is pretty much a hundred percent information flow" (PARDO-GUERRA, 2019, p. 121).

A não-ambiguidade e o caráter sumário dos algoritmos parece coincidir com o fatalismo de um "realismo capitalista" (FISHER, 2009, n.p), onde, diante da aparente impossibilidade de se imaginar um sistema alternativo, parece não haver outra alternativa senão acelerá-lo. Outra imagem, que decorre desta, é a de uma dupla captura: de um lado, a captura do presente em função de um futuro imaginado, único e inevitável, operada pelos processos de financeirização e acelerada pelo desenvolvimento de sistemas, plataformas e novos instrumentos financeiros (BIRCH; MUNIESA, 2020); e, por outro lado, a captura do futuro em função do presente, por meio de processos de capitalização de recursos, redes, sistemas, energia, etc (MUNIESA *et al.*, 2017). Como viemos demostrando ao longo do texto, tais processos se retroalimentam e criam as condições de possibilidade para que ambos *rodem* (como software) tal como *daemons* em um sistema operacional[107].

Ao longo das dinâmicas desses mercados, processos de acumulação e especulação de criptoativos performam modelos econômicos e relações financeiras específicas, de modo a se inserirem no regime mais amplo dos processos de financeirização de ativos e instrumentos econômicos, investimentos e alocação de capital. Tais processos são baseados não apenas nos mercados que negociam *bitcoins* em moedas nacionais ou em outras criptomoedas, que corresponde à parte majoritária do mercado de criptoativos, mas também na produção de instrumentos

107 Um *daemon* é um programa ou processo que roda continuamente no *background*, monitorando e respondendo a alterações de um sistema, podendo controlar recursos, permissões de acesso e fluxos de informação.

financeiros e sistemas de pagamentos baseados na lógica descentralizada dessas redes.

A emergência dessa multiplicidade de arranjos financeiros é acompanhada por movimentos que são identificados por alguns participantes como "reações" ou "ataques" à sua *soberania monetária*, a saber, as iniciativas de regulação desses mercados por parte dos estados nacionais e de suas agências reguladoras, bem como a incidência de taxas sobre seus lucros e dividendos. No mais das vezes, o que é percebido por entusiastas e *players* do mercado como "reações" do sistema financeiro tradicional têm seguido na direção de enquadrar esses novos sistemas sob as legislações vigentes que visam coibir a lavagem de dinheiro e possibilitar a taxação dos rendimentos dos investidores. A generalização de uma noção abstrata de "moeda digital" em uma categoria mais ampla de "ativos digitais" é consequência do processo de inserção do Bitcoin e das demais criptomoedas no campo da economia financeira e dos processos de financeirização, uma vez que a proliferação de instrumentos financeiros baseados em criptomoedas multiplica as possibilidades imaginadas por usuários, entusiastas e investidores desse setor.

É nessa "zona cinza" de possibilidades e de normativas estabelecidas por agências reguladoras que os processos de regulação de criptoativos estão inseridos e em disputa, tanto sobre as possíveis nomenclaturas desses instrumentos, quanto sobre a efetividade da regulação em sistemas elaborados para minimizá-la ou contorná-la. Também é possível perceber como termos e conceitos vão sendo cunhados ou mobilizados para dar conta da proliferação de criptoativos como instrumentos financeiros que pertencem a uma nova classe de *ativos digitais*. Aqui interessa especialmente o encontro desses sistemas e mercados com instituições financeiras tradicionais e agências reguladoras, em que o esforço de nomeação desses fenômenos e a tentativa de regulação desses mercados é motivo de uma série de disputas.

O Brasil tem visto um aumento significativo na adoção de criptomoedas nos últimos anos, com um número crescente de indivíduos e empresas usando Bitcoin e outras criptomoedas para transações e principalmente como forma de investimento. Em levantamento recente, estima-se que o Brasil conta com cerca de 10 milhões de

investidores em criptoativos[108]. Durante a segunda onda da pandemia de COVID-19, no início de 2021, com centenas a milhares de mortes por dia, a Bolsa de Valores brasileira também estava batendo recordes em seus volumes de transações. O Índice Bovespa atingiu o seu máximo histórico no início de janeiro de 2021 e o Bitcoin esteve em alta por todas as semanas desde novembro de 2020, atingindo, alguns meses depois, o seu maior preço até então, sendo negociado cerca de 300.000 reais por moeda.

Desde 2018, o número de investidores individuais em criptomoedas no Brasil já era duas vezes maior do que o número de investidores individuais no mercado financeiro tradicional[109], com ambos os números crescendo continuamente até hoje. Essa natureza desarticulada entre catástrofe sociopolítica brasileira e a aparente exuberância das criptomoedas e das bolsas de valores são um dos aspectos mais marcantes da economia neoliberal e das políticas de austeridade que foram aplicadas pelo governo do ex-presidente Jair Bolsonaro e que foram amplamente apoiadas pelas elites brasileiras. Como diz David Graeber acerca do neoliberalismo, trata-se, na verdade, de "um projeto político disfarçado de um projeto econômico" (GRAEBER, 2018, p. xxii).

O *status* legal das criptomoedas ainda está longe de ser algo consolidado em muitos países, o que faz com que as adequações às legislações instituídas não sejam nem triviais, nem incontroversas. No caso brasileiro, ao longo dos últimos anos, a concepção sobre o que são criptomoedas e, posteriormente, *criptoativos* ou *ativos financeiros digitais*, passou por entendimentos distintos das agências reguladoras nacionais, alguns deles divergentes entre si. Há um histórico de decisões do Banco Central do Brasil (BACEN), da Comissão de Valores Mobiliários (CVM), da Receita Federal (RF) e das comissões da Câmara dos Deputados sobre a

108 "O perfil do investidor brasileiro de criptomoedas ainda é majoritariamente masculino (56%) e jovem, com os investidores de 18 a 34 anos configurando 53%. As classes A e B configuram 73% dos investidores e a maioria deles também é iniciante, com menos de dois anos de investimento (43%)." Dados citados na matéria "Mercado de criptomoedas ultrapassa número de investidores da bolsa de valores, aponta estudo", EXAME, 6 jul 2023. Disponível em: https://exame.com/future-of-money/mercado-de-criptomoedas-ultrapassa-numero-de-investidores-da-bolsa-de-valores-aponta-estudo. Acesso em: 23 fev. 2024.

109 "Brasil tem 10 milhões de investidores de criptoativos, e isso ainda é pouco", EXAME, 6 ago 2023. Disponível em: https://exame.com/future-of-money/brasil-tem-10-milhoes-de-investidores-de-criptoativos-e-isso-ainda-e-pouco. Acesso em: 23 fev. 2024.

pertinência e adequação de projetos de lei específicos sobre os mercados de criptomoedas no Brasil. Como ocorre à maioria dos países, no Brasil ainda não há uma legislação específica, mas sim um conjunto de deliberações, pareceres e ofícios circulares emitidos nos últimos anos pelo BACEN, CVM e RF, em que nenhuma dessas instituições tem (ou parece pretender ter) responsabilidade direta sobre o tema.

Dos projetos de lei que estiveram em tramitação no Brasil nos últimos anos, o mais significativo é o PL 2303/2015[110], de autoria do deputado Áureo Ribeiro, que inicialmente associava as então chamadas "moedas virtuais" a outros "arranjos de pagamento", como programas de milhagens aéreas. Ao longo de sua tramitação na Câmara dos Deputados, e tendo sido renumerado como PL 4401/2021 a partir de sua tramitação no Senado Federal, o projeto se consolidou como uma disposição sobre "diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais", sendo promulgado em 21 de dezembro de 2022, como a Lei Nº 14.478[111]. A alteração no Código Penal para "prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros" e outros "crimes contra o sistema financeiro nacional" e lavagem de dinheiro, passou também a incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições.

Cabe ressaltar também a Instrução Normativa Nº 1888[112], emitida pela Receita Federal em maio de 2019, que desde então obriga as exchanges digitais que operam no Brasil a reportar mensalmente todas as transações financeiras efetuadas dentro de suas plataformas. Essa decisão teve grande impacto nos "criptomercados" brasileiros, bem como entre os usuários mais ortodoxos, cujos

110 PL 4401/2021 (Nº Anterior: PL 2303/2015) – Portal da Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1555470. Acesso em: 23 fev. 2024.

111 Lei Nº 14.478, de 21 de dezembro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14478.htm. Acesso em: 23 fev. 2024.

112 Receita Federal - Instrução Normativa RFB nº 1888, de 03 de maio de 2019: "Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB)". Disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=100592. Acesso em: 23 fev. 2024.

temores sobre o aumento das obrigações do KYC (*Know Your Costumer*) e tributações do governo os direcionaram para uma oposição mais vocal contra qualquer tipo de intervenção estatal nos mercados digitais.

Por um lado, para muitos dos usuários desses sistemas, a regulação é vista como um problema imposto pelas burocracias estatais e instituições financeiras, como empecilhos aos sistemas de transação que, sem ela, seriam mais "livres" e "ideais". Por outro lado, há ao menos dois aspectos positivos que costumam ser levantados: dada a proliferação de golpes e esquemas de pirâmides financeiras[113], é a regulação (não especificamente dos mercados de criptomoedas em si, mas o estabelecimento de normativas jurídicas para o sistema financeiro) que garantiria ou restringiria o alcance e a disseminação desses golpes; o outro aspecto, considerado positivo até mesmo entre alguns usuários mais ortodoxos, é que somente por meio de certas normativas de regulação o Capital institucional passaria a entrar nesses mercados, garantindo maior liquidez e fazendo elevar os preços das criptomoedas negociadas.

Em um artigo intitulado "Bitcoin: The Cryptopolitics of Cryptocurrencies", David Golumbia argumenta que uma das principais funções da regulação exercida por bancos centrais é a garantia de certa estabilidade dos ativos enquanto uma reserva de valor, uma vez que mercados "absolutamente desregulados" tendem a resultar em ciclos extremos de explosão e recessão (GOLUMBIA, 2014, n.p):

> Precisely because it is outside of regulatory structures, Bitcoin is particularly prone to the kinds of hoarding, dumping, and manipulation that characterize all instruments that lack central bank control and regulatory oversight by bodies like the SEC. Contrary to the advocates' claims, unregulated securities instruments are everywhere in contemporary finance; there is convincing evidence that the inability of the Commodities Futures Trade Commission to establish regulatory authority over CDOs and CMOs is the proximate cause for the economic crisis of 2008. Now the lack of regulation of

113 O Relatório Final da Comissão Parlamentar de Inquérito da Câmara dos Deputados, de outubro de 2023, conhecida como "CPI das Pirâmides Financeiras", traz os resultados da investigação de operações fraudulentas na gestão de empresas do mercado financeiro, em especial aquelas que negociavam criptomoedas, e define as chamadas "pirâmides financeiras" como "esquemas engendrados para extrair irregularmente recursos de terceiros". Disponível em: https://journaliststudio.google.com/pinpoint/search?collection=f8e9b82249b6449c. Acesso em: 23 fev. 2024.

> Bitcoin means that hoarders (as of Dec 2013, half of all Bitcoins were owned by approximately 927 people, such fight-the-power revolutionaries as the Winklevoss twins of Facebook infamy among them) can use all sorts of sophisticated trading methods to manipulate the market. (*idem*)

Para investidores mais experientes, o atrativo mais imediato das criptomoedas, *tokens* e NFTs (*Non-fungible tokens*) é o que parece ser, à primeira vista e para muitos incautos, um *bug*: esquemas de pirâmide e a proliferação de *criptos* com nenhuma utilidade prática, mas com alto desempenho de *marketing* e propaganda, é o que as tornam atrativas para aqueles que, como num jogo, desejam ser mais rápidos que os demais para comprar grandes quantidades e vendê-las antes de uma queda abrupta. Como em uma loteria, em que a "sorte grande" é no mais das vezes extremamente improvável, quanto mais tempo for possível *surfar* na parte ascendente do gráfico de preço, melhor; quanto mais próximo do *crash* for possível pular fora, maior o lucro. Um interlocutor, quando perguntado se não o incomodava o fato de a maioria das *criptos* serem golpes, esquemas de pirâmide ou fraudes, me respondeu de forma breve: "já ganhei uma boa grana com isso."

É importante ressaltar, no entanto, que processos de regulação não se dão apenas por força de instituições financeiras e estatais. Os próprios processos de produção de software e os mecanismos de *feedback* implementados pelo sistema regulam disrupções e controlam com maior ou menor rigor o comportamento dos participantes humanos e maquínicos. No caso das máquinas, como vimos, o problema do consenso emergente é um modo de regulação algorítmica bastante efetivo, que se vê replicado, como se incidisse de volta, na comunidade de desenvolvedores, onde conflitos de interesses costumam ser frequentes e intensos. Porém, um outro fenômeno, mais próximo das dinâmicas de formação de mercado, é o da autorregulação da comunidade sobre seus próprios participantes, por meio de políticas de reputação social dos vendedores individuais (chamados no Brasil de "vendedores P2P"), que negociam diretamente com outras pessoas; da militância ideológica de influenciadores e participantes de comunidades, que "regulam" o consenso "libertário" por meio de *memes*, *slogans* e catecismos próprios contra participantes considerados "estatistas" ou "esquerdistas"; e por meio de outros grupos de afinidade e posições políticas correlatas, em que conjuntos de preceitos

"libertários", "capitalistas" e "individualistas" são incentivados e disseminados. A própria discordância sobre se criptomoedas são, de fato, "moeda", "reserva de valor" ou "mecanismos de câmbio" é algo que retroalimenta essas comunidades e reflete, também, tanto a posição ambígua dos órgãos reguladores sobre essa questão, quanto a posição mais "conservadora" em aplicar o *corpus* legal vigente sem grandes ressalvas sobre as particularidades desses sistemas.

Portanto, além de serem vistas como um empecilho ou um cerceamento de suas liberdades, seja pela limitação do escopo de atividades legais, seja pela tributação de transações e dividendos, diretrizes de regulação são muitas vezes vistas como problemáticas por conta de sua falta de clareza. Há ambiguidades sobre a definição correta de criptoativos, sobre quais leis e regulamentos atuais devem ser aplicados e sobre qual agência reguladora deve aplicá-los. Em geral, cabe aos utilizadores assumir os riscos de operar com estes novos instrumentos financeiros, lidar com eventuais perdas de capital, evitar esquemas financeiros "suspeitos" e observar as orientações legislativas gerais sobre transações financeiras em território nacional. Segundo um interlocutor, em vez de regular os casos comuns, as agências regulatórias optam "sempre" por acumular regulações sobre "as exceções", dificultando assim tanto o entendimento de não-especialistas sobre que é ou não é legal, quanto aumentando os custos de empreendimentos, uma vez que tais "regulações por exceção" impõem obstáculos muitas vezes desnecessários e demandam, de investidores e empreendedores, custos adicionais com advogados, consultoria jurídica e tributária. Embora esses limites nem sempre sejam claros ou impostos, eles em geral recaem sobre empresas e entidades terceirizadas, como intermediários e *exchanges* de criptomoedas, uma vez que os próprios sistemas em que operam, por sua natureza distribuída, não podem ser delimitados ou regidos como os mercados tradicionais podem ou gostariam.

Por fim, o embate com esforços regulatórios governamentais e a oposição ideológica às políticas monetárias em curso costumam se dar, no mais das vezes, mais como uma resistência à interdição do jogo especulativo do que como uma percepção real de captura dessas redes e sistemas por entidades estatais. Ainda que mercados e tecnologias não-reguladas sejam comumente percebidos por instituições estatais como ameaças que devem ser contidas e moderadas, tais

movimentos refletem também o interesse nas tecnologias para fortalecimento do próprio sistema financeiro, como é o caso de experimentos com a "tecnologia *blockchain*" empregada nos sistemas de criptomoedas para o desenvolvimento de alternativas e melhorias do sistema financeiro tradicional por meio da elaboração de novas plataformas e experimentação com os chamados sistemas DLT (*Distributed Ledger Technologies*) (CARDOSO; MORAWSKA VIANNA, 2019).

CONSIDERAÇÕES FINAIS

Esta tese teve como objetivo produzir uma descrição das relações, atores e sistemas sociotécnicos que constituem as economias político-materiais da circulação de criptomoedas na formação de mercados, infraestruturas e assimetrias sobre as quais se estabelecem esses ativos digitais. Assim, procuramos nos capítulos anteriores delinear as imaginações de futuro que decorrem da elaboração e transação de instrumentos financeiros como criptoativos, e as ideologias tecnocráticas e neoliberais cujos princípios estão implementados na própria materialidade desses sistemas. Os efeitos desses processos e o desenvolvimento de modos de governança coletiva, produção de software e troca de valores digitais evidenciam como as dimensões ideológica e técnica se entrelaçam na produção do sistema *peer-to-peer* Bitcoin.

Descrevermos aqui o sistema Bitcoin e o ecossistema mais amplo de outras criptomoedas a partir dos principais procedimentos algorítmicos que os constituem enquanto sistemas sociotécnicos de dinheiro eletrônico e, ao mesmo tempo, enquanto redes *peer-to-peer* de registro distribuído para a transação de valores digitais. Ao longo da descrição, evidenciamos também os efeitos político-econômicos da circulação de criptomoedas na formação de mercados e infraestruturas sobre as quais se estabelecem esses ativos. Com base no que viemos chamando de relações *tecnofinanceiras*, que constituem as criptomoedas enquanto sistemas sociotécnicos de dinheiro eletrônico, descrevemos conjuntos de procedimentos técnicos, aglomerados materiais e configurações algorítmicas, agenciados por *players* humanos e máquinas, no estabelecimento de sistemas de transação de propriedades digitais, especulação de valores e registro de dados em redes de tipo distribuído e descentralizado. A abordagem dos fundamentos ideológicos da criptoeconomia, orientada pela noção cibernética de *feedback* nos permitiu articular uma descrição sobre como essas ideologias influenciam o próprio aparato sociotécnico que dá corpo às criptomoedas por meio de implementações técnicas e efeitos de rede específicos.

Procuramos neste trabalho analisar as economias político-materiais subjacentes aos mercados de criptoativos, as imaginações de futuro que decorrem da elaboração de instrumentos financeiros codificados em software e reunir um

conjunto diverso de ideias e pressupostos deste campo em função de duas perspectivas mais amplas: aquela da técnica e da política dos algoritmos que constituem sistemas digitais, e aquela que diz respeito aos processos de financeirização, tal como abordados pela literatura da antropologia e da sociologia econômica.

No primeiro capítulo, o sistema Bitcoin foi descrito a partir de suas dimensões técnica e ideológica, de modo a evidenciar os procedimentos que o constituem enquanto uma moeda percebida por seus usuários como "deflacionária". Com a descrição do chamado *halving*, o mecanismo responsável pela redução gradual dos subsídios da mineração, enfatizamos como a diagramática do gráfico de emissão monetária do Bitcoin produz uma imagem comum desse sistema tecnofinanceiro, bem como de ecossistemas derivados. A questão sobre a produção do consenso distribuído em sistemas descentralizados foi abordada enquanto um problema antropológico, a partir das interfaces da antropologia da técnica e da ciência, com o intuito de descrever os movimentos, fluxos e as paisagens sociotécnicas que constituem o ecossistema das criptomoedas, marcados por articulações dinâmicas em torno de mercados e comunidades virtuais.

No segundo capítulo, descrevemos controvérsias específicas relativas à descentralização em sistemas digitais, buscando apresentar o sistema do Bitcoin do ponto de vista das disputas que ocorrem nas comunidades de desenvolvedores do Bitcoin enquanto um projeto de software e, de modo mais amplo, evidenciando a multiplicidade de atores e partes interessadas nessas disputas. Tais processos de especialização e radicalização desses grupos têm fomentado a hipótese da *hiperbitcoinização* enquanto um mito funcional que deriva das temporalidades específicas do sistema, de perspectivas radicais sobre o sistema financeiro, e das materialidades algorítmicas do Bitcoin, informadas por agendas políticas, econômicas e ideológicas específicas.

No último capítulo, tratamos do problema da troca como fluxo ou propagação de informação a partir de diferentes perspectivas sobre os fundamentos do sistema Bitcoin, da chamada *criptoeconomia* e suas concepções subjacentes de política e economia. Evidenciamos como as interfaces produzidas por *dashboards*, gráficos e

outros dispositivos de mercado são instrumentos indispensáveis para a produção de totalidades parciais do sistema. Narrativas tomadas de empréstimo da antropologia e da economia são também frequentemente articuladas para a produção de sentido e de futuros imaginados sobre esses sistemas de dinheiro digital. Um dos objetivos foi mostrar como essas variações de ideologias neoliberais ou *ciberlibertárias* constituem as narrativas e as imaginações de futuro de programadores, entusiastas e investidores acerca de previsões sobre o "futuro da economia" e de profecias sobre o "futuro do dinheiro", do Estado e do próprio Capitalismo.

Sendo a primeira e mais difundida criptomoeda em operação, o sistema *peer-to-peer* Bitcoin constitui um campo complexo de investigação antropológica sobre troca de valores, implementação técnica e os modos de governança de uma criptomoeda que, em oposição às moedas fiduciárias nacionais, pretende-se global, transnacional e descentralizada. Este trabalho pretende, assim, contribuir para a pesquisa sobre sistemas descentralizados a partir da perspectiva dos algoritmos, dos seus participantes e de suas economias político-materiais, em que movimentos, fluxos e as paisagens sociotécnicas que constituem esses sistemas são marcados por articulações dinâmicas em torno de mercados, comunidades e infraestruturas.

REFERÊNCIAS

ALABI, Ken. Digital Blockchain Networks Appear to Be Following Metcalfe's Law. *Electronic Commerce Research and Applications*, v. 24, p. 13, jul. 2017.

AMMOUS, Saifedean. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. [S.l.]: Wiley, 2018.

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, 2016a.

ANTONOPOULOS, Andreas M. *The Internet of Money Volume Two*. Vereinigte Staaten von America: Merkle Bloom LLC, 2016b.

ASSANGE, Julian *et al. Cypherpunks - Liberdade e o Futuro Da Internet*. 1a. ed. [S.l.]: Boitempo Editorial, 2013.

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

BEER, Stafford. What Is Cybernetics? *Kybernetes*, v. 31, n. 2, p. 209–219, mar. 2002.

BIER, Jonathan. *The Blocksize War: The Battle for Control Over Bitcoin's Protocol Rules*. [S.l.]: Independently Published, 2021.

BIRCH, Kean; MUNIESA, Fabian (Eds.). *Assetization: Turning Things into Assets in Technoscientific Capitalism*. Cambridge, Massachusetts: The MIT Press, 2020.

BLACK, Fischer. Noise. *The Journal of Finance*, v. 41, n. 3, p. 528–543, jul. 1986. Disponível em: <http://doi.wiley.com/10.1111/j.1540-6261.1986.tb04513.x>. Acesso em: 23 mar. 2020.

BOELLSTORFF, Tom. *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human*. [S.l.]: Princeton University Press, 2008.

BRATTON, Benjamin H. *The Stack: On Software and Sovereignty*. Cambridge, Massachusetts: MIT Press, 2015. (Software Studies).

BRUNTON, Finn. *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency*. Princeton, NJ: Princeton University Press, 2019.

BUTERIN, Vitalik. *Proof of Stake: How I Learned to Love Weak Subjectivity*. Disponível em: <https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/>. Acesso em: 16 jun. 2018.

CADENA, Marisol De la *et al.* Anthropology and STS: Generative Interfaces, Multiple Locations. v. 5, n. 1, p. 39, 2015.

ÇALIŞKAN, Koray. Data Money: The Socio-Technical Infrastructure of Cryptocurrency Blockchains. *SSRN Electronic Journal*, p. 20, 2018. Disponível em: <https://www.ssrn.com/abstract=3372015>. Acesso em: 19 jul. 2019.

CALLON, Michel. *The Laws of the Markets*. 1. ed. Oxford, United Kingdom: Blackwell Publishers/Sociological Review, 1998.

CALLON, Michel; MILLO, Yuval; MUNIESA, Fabian (Eds.). *Market Devices*. Malden, MA: Blackwell Pub, 2007. (Sociological Review Monographs).

CALLON, Michel; MUNIESA, Fabian. Economic Markets as Calculative Collective Devices. *Organization Studies*, v. 26, n. 8, p. 1229–1250, ago. 2005. Disponível em: <http://journals.sagepub.com/doi/10.1177/0170840605056393>. Acesso em: 10 abr. 2019.

CANETTI, Elias. *Crowds and Power*. New York: Continuum, 1981.

CARDOSO, Bruno Campos. Algoritmos Como "Máquinas de Cultura": Notas Sobre Política e Produção de Consenso No Sistema Peer-to-Peer Bitcoin. *Anais da VII Reunião de Antropologia da Ciência e da Tecnologia*, v. 4, n. 4, 2019. Disponível em: <http://ocs.ige.unicamp.br/ojs/react/article/view/2678>.

CARDOSO, Bruno Campos. Governança Digital e o Processo de "Mineração": Especialização e Controvérsias No Sistema Peer-to-Peer Bitcoin. *31ª*

Reunião Brasileira de Antropologia, 2018. Disponível em: <https://www.31rba.abant.org.br/simposio/view?ID_SIMPOSIO=48>.

CARDOSO, Bruno Campos. Towards Hyperbitcoinization: Bitcoin Maximalism as Speculative Fiction. In: SHAPIRO, MATAN (Ed.). *Crypto Crowds: Singularities and Multiplicities on the Blockchain*. Critical Interventions: A Forum for Social Analysis. Oxford, United Kingdom: Berghahn Books, 2024. p. 23–39.

CARDOSO, Bruno Campos; MORAWSKA VIANNA, Catarina. *Algorithms and Politics in Brazilian Finance: The Formation of a Cryptocurrencies Market*. [S.l: s.n.]., 2019

CHAUM, David. Blind Signatures for Untraceable Payments. 1983, [S.l: s.n.], 1983. p. 199–203.

CHAUM, David. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM*, v. 28, n. 10, p. 1030–1044, 1985.

CHUN, Wendy Hui Kyong. On ”Sourcery,” or Code as Fetish. *Configurations*, v. 16, n. 3, p. 299–324, 2008.

CLARK, Andy. *Natural-Born Cyborgs: Minds, Technologies, and the Future of Human Intelligence*. [S.l.]: Oxford University Press, 2003.

CLARKE, Arthur C. *Profiles of the Future: An Inquiry into the Limits of the Possible*. New York: Harper & Row, 1973.

DE VRIES, Alex. Bitcoin’s Growing Energy Problem. *Joule*, v. 2, n. 5, p. 801–805, mai. 2018. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S2542435118301776>. Acesso em: 27 mai. 2018.

DIFFIE, Whitfield; HELLMAN, Martin E. New Directions in Cryptography. *IEEE Transactions on Information Theory*, v. 22, n. 6, p. 644–654, 1976.

DODD, Nigel. The Social Life of Bitcoin. *Theory, Culture & Society*, v. 35, n. 3, p. 35–56, mai. 2018. Disponível em: <http://journals.sagepub.com/doi/10.1177/0263276417746464>. Acesso em: 25 jul. 2019.

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

FISHER, Mark. *Capitalist Realism: Is There No Alternative?* [S.l.]: Zero Books, 2009.

FITZPATRICK, Scott. Banking on Stone Money. *Archaeology*, v. 57, n. 2, p. 18–23, 2004.

FITZPATRICK, Scott M. *Banking on Stone Money: The Influence of Traditional "Currencies" on Blockchain Technology*. [S.l: s.n.]., 2018

FITZPATRICK, Scott M. *Stones of the Butterfly: Archaeological Investigation of Yapese Stone Money Quarries in Palau, Western Caroline Islands, Micronesia*. 2003. tese de doutorado – University of Oregon, 2003.

FITZPATRICK, Scott M.; MCKEON, Stephen. Banking on Stone Money: Ancient Antecedents to Bitcoin. *Economic Anthropology*, v. 7, n. 1, p. 7–21, jan. 2020. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sea2.12154>. Acesso em: 28 abr. 2020.

FLUSSER, Vilém. *Filosofia Da Caixa Preta: Ensaios Para Uma Futura Filosofia Da Fotografia*. [S.l.]: Relume Dumará, 2002.

FORSYTHE, Diana E; HESS, David J. *Studying Those Who Study Us: An Anthropologist in the World of Artificial Intelligence*. [S.l.]: Stanford University Press, 2002.

FOUCAULT, Michel. *Microfísica Do Poder*. [S.l.]: Rio de Janeiro: Edições Graal, 1979.

FRIEDMAN, Milton. *The Island of Stone Money*. [S.l.]: Hoover Institution, Stanford University, 1991. (Domestic Studies Program).

FURNESS, Willam Henry. Money and Currency. *The Island of Stone Money: Uap of the Carolines*. Philadelphia: J. B. Lippincott Co., 1910. p. 94–106.

GEERTZ, Clifford. *A Interpretação das Culturas*. Rio de Janeiro: LTC, 1981.

GEERTZ, Clifford. Deep Play: Notes on the Balinese Cockfight. *Daedalus*, v. 101, n. 1, p. 1–37, 1972.

GLOERICH, Inte; LOVINK, Geert; DE VRIES, Patricia (Eds.). *MoneyLab Reader 2: Overcoming the Hype*. Amsterdam: Institute of Network Cultures, 2018. Disponível em: <https://networkcultures.org/blog/publication/moneylab-reader-2-overcoming-the-hype/>. (INC Reader, 11).

GOLUMBIA, David. *Bitcoin: The Cryptopolitics of Cryptocurrencies*. Disponível em: <https://harvardpress.typepad.com/hup_publicity/2014/02/bitcoin-the-cryptopolitics-of-cryptocurrencies-david-golumbia.html>. Acesso em: 3 jan. 2019.

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

GRAEBER, David. *Against Economics*. Disponível em: <https://www.nybooks.com/articles/2019/12/05/against-economics/>. Acesso em: 23 mar. 2020.

GRAEBER, David. *Bullshit Jobs: A Theory*. [S.l.]: Simon & Schuster, 2018.

GRAEBER, David. *Debt: The First 5,000 Years*. New York: Melville House, 2011.

GRAEBER, David. *Direct Action: An Ethnography*. [S.l.]: AK Press, 2009.

GRAEBER, David. *Toward An Anthropological Theory of Value: The False Coin of Our Own Dreams*. [S.l.]: Palgrave, 2001.

GREGORY, Christopher A. *Gifts and Commodities: Exchange and Western Capitalism Since 1700*. 1. ed. London: Academic Press, 1982. Disponível em: <http://gen.lib.rus.ec/book/index.php?md5=0217b339549e6d626bc310754c8dfcf0>.

GUNKEL, Henriette; HAMEED, Ayesha; O'SULLIVAN, Simon (Eds.). *Futures and Fictions*. Repeater Books paperback original ed. London: Repeater, 2017. (Cultural Studies Philosophy).

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

HELMREICH, Stefan. *Silicon Second Nature: Culturing Artificial Life in a Digital World*. [S.l.]: University of California Press, 1998.

HORST, Heather A.; MILLER, Daniel. *Digital Anthropology*. [S.l.]: Berg, 2012.

HU, Tung-Hui. *A Prehistory of the Cloud*. [S.l.]: The MIT Press, 2015.

INGOLD, Tim. *Being Alive: Essays on Movement, Knowledge and Description.* [S.l.]: London: Routledge, 2011.

INGOLD, Tim. *The Life of Lines*. [S.l.]: Routledge, 2015.

INTRONA, L. D. Algorithms, Governance, and Governmentality: On Governing Academic Writing. *Science, Technology & Human Values*, v. 41, n. 1, p. 17–49, 2016.

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>.

KNOX, Hannah; WALFORD, Antonia. Digital Ontology. *Fieldsights*, Theorizing the Contemporary. 24 mar. 2016. Disponível em: <https://culanth.org/fieldsights/series/digital-ontology>.

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

KRAWISZ, Daniel. *Hyperbitcoinization*. Disponível em: <https://nakamotoinstitute.org/mempool/hyperbitcoinization/>. Acesso em: 17 nov. 2022.

KURBALIJA, Jovan. *Uma Introdução à Governança Da Internet*. Cadernos C ed. [S.l.]: Comitê Gestor da Internet no Brasil, 2017.

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. *Ciência Em Ação: Como Seguir Cientistas e Engenheiros Sociedade Afora*. São Paulo: Editora Unesp, 2012.

MACKENZIE, Adrian. *Cutting Code: Software and Sociality*. New York: Peter Lang, 2006. (Digital Formations, v. 30).

MACKENZIE, Donald. A Material Political Economy: Automated Trading Desk and Price Prediction in High-Frequency Trading. *Social Studies of Science*, v. 47, n. 2, p. 172–194, abr. 2017. Disponível em: <http://journals.sagepub.com/doi/10.1177/0306312716676900>. Acesso em: 14 ago. 2019.

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

MACKENZIE, Donald. *An Engine, Not a Camera: How Financial Models Shape Markets*. Cambridge, Mass.: MIT Press, 2006.

MACKENZIE, Donald. How Algorithms Interact: Goffman's «Interaction Order» in Automated Trading. *Theory, Culture & Society*, v. 36, n. 2, p. 39–59, mar. a2019. Disponível em: <http://journals.sagepub.com/doi/10.1177/0263276419829541>. Acesso em: 14 ago. 2019.

MACKENZIE, Donald. *Material Markets: How Economic Agents Are Constructed*. Oxford ; New York: Oxford University Press, 2009. (Clarendon Lectures em Management Studies).

MACKENZIE, Donald. Pick a Nonce and Try a Hash. *London Review of Books*, v. 41, n. 8, p. 35–38, 18 abr. b2019. Disponível em: <https://www.lrb.co.uk/v41/n08/donald-mackenzie/pick-a-nonce-and-try-a-hash>. Acesso em: 25 jul. 2019.

MACKENZIE, Donald; MUNIESA, Fabian; SIU, Lucia. *Do Economists Make Markets?: On the Performativity of Economics*. New Jersey: Princeton University Press, 2007.

MALINOWSKI, Bronislaw. *Os Argonautas Do Pacífico Ocidental*. [S.l.]: Abril Cultural, 1978. (Os Pensadores, XLIII).

MASSUMI, Brian; FISH, Stanley; JAMESON, Fredric. *Parables for the Virtual: Movement, Affect, Sensation*. [S.l.]: Duke University Press, 2002. (Post-Contemporary Interventions).

MAUSS, Marcel. *Sociologia e Antropologia*. [S.l.]: São Paulo: Cosac Naify, 2003.

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

MIROWSKI, Philip. *Never Let a Serious Crisis Go to Waste: How Neoliberalism Survived the Financial Meltdown*. London ; New York: Verso, 2013.

MIROWSKI, Philip; NIK-KHAH, Edward M. *The Knowledge We Have Lost in Information: The History of Information in Modern Economics*. New York City: Oxford University Press, 2017.

MIROWSKI, Philip; SOMEFUN, Koye. Markets as Evolving Computational Entities. *Journal of Evolutionary Economics*, v. 8, n. 4, p. 329–356, 1998. Disponível em: <https://EconPapers.repec.org/RePEc:spr:joevec:v:8:y:1998:i:4:p:329-356>.

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. Disponível em: <https://doi.org/10.1038/s41558-018-0321-8>.

MORABITO, Vincenzo. *Business Innovation Through Blockchain: The B3 Perspective*. [S.l.]: Springer International Publishing, 2017.

MUNIESA, Fabian *et al. Capitalization: A Cultural Guide*. [S.l.]: Presses des Mines, 2017.

MUNIESA, Fabian. *The Provoked Economy: Economic Reality and the Performative Turn*. [S.l.]: Routledge, 2014.

MUNN, Nancy D. *The Fame of Gawa: A Symbolic Study of Value Transformation in a Massim (Papua New Guinea) Society*. Durham: Duke University Press, 1992. (The Lewis Henry Morgan Lecture).

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.

NARAYANAN, Arvind; CLARK, Jeremy. Bitcoin's Academic Pedigree. *ACM Queue*, v. 15, n. 4, p. 1–28, 2017. Disponível em: <https://queue.acm.org/detail.cfm?id=3136559>.

ORTIZ, Horacio. The Limits of Financial Imagination: Free Investors, Efficient Markets, and Crisis: The Limits of Financial Imagination. *American Anthropologist*, v. 116, n. 1, p. 38–50, mar. 2014. Disponível em: <http://doi.wiley.com/10.1111/aman.12071>. Acesso em: 10 jan. 2021.

PARANÁ, Edemilson. *Bitcoin: A Utopia Tecnocrática Do Dinheiro Apolítico*. São Paulo, SP: Autonomia Literária, 2020.

PARDO-GUERRA, Juan Pablo. *Automating Finance: Infrastructures, Engineers, and the Making of Electronic Markets*. Cambridge, United Kingdom ; New York, NY: Cambridge University Press, 2019.

PATELIS, Korinna. *The Political Economy of the Internet*. 2000. 296 f. PhD thesis, Dept. of Media and Communications – Goldsmiths College University of London, London, 2000. Disponível em: <https://www2.aueb.gr/users/patelis/PHDTELIO.pdf>.

RIVEST, Ron L.; SHAMIR, Adi; ADLEMAN, Leonard. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, v. 21, n. 2, p. 120–126, 1 fev. 1978. Disponível em: <http://portal.acm.org/citation.cfm?doid=359340.359342>. Acesso em: 6 fev. 2019.

SEAVER, Nick. Algorithms as Culture: Some Tactics for the Ethnography of Algorithmic Systems. *Big Data & Society*, v. 4, n. 2, p. 12, dez. 2017. Disponível em: <http://journals.sagepub.com/doi/10.1177/2053951717738104>. Acesso em: 26 mar. 2019.

SEGATA, Jean; RIFIOTIS, Theophilos. *Políticas Etnográficas No Campo Da Cibercultura*. [S.l.]: Editora Letradágua, 2016.

SHAPIRO, Matan (Ed.). *Crypto Crowds: Singularities and Multiplicities on the Blockchain*. Oxford, United Kingdom: Berghahn Books, 2024. Disponível em: <https://www.berghahnbooks.com/title/ShapiroCrypto>. (Critical Interventions: A Forum for Social Analysis, 21).

SOUZA, Rebeca Hennemann Vergara De; SOLAGNA, Fabrício; LEAL, Ondina Fachel. As Políticas Globais de Governança e Regulamentação Da Privacidade Na Internet. *Horizontes Antropológicos*, v. 20, n. 41, p. 141–172, jun. 2014.

SZABO, Nick. Shelling Out: The Origins of Money. 2005. Disponível em: <https://nakamotoinstitute.org/shelling-out/>.

SZABO, Nick. Trusted Third Parties Are Security Holes. 2001. Disponível em: <https://nakamotoinstitute.org/trusted-third-parties>.

TASCA, Paolo; TESSONE, Claudio J. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger*, v. 4, 15 fev. 2019. Disponível em: <http://ledger.pitt.edu/ojs/index.php/ledger/article/view/140>. Acesso em: 16 fev. 2019.

VOSKUIL, Eric. *Cryptoeconomics: Fundamental Principles of Bitcoin*. 1.2. ed. Hanoi: Bowker Identity Services, 2020.

WARK, McKenzie. *Capital Is Dead: Is This Something Worse?* London ; New York: Verso, 2019.

WARK, McKenzie. What If This Is Not Capitalism Any More, but Something Worse? NPS Plenary Lecture, APSA 2015, Philadelphia, PA. *New Political Science*, v. 39, n. 1, p. 58–66, 2 jan. 2017. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/07393148.2017.1278846>. Acesso em: 20 jul. 2020.

WEINER, Annette. *Inalienable Possessions: The Paradox of Keeping-While Giving*. [S.l.]: University of California Press, 1992.

WIENER, Norbert. *Cybernetics: Or, Control and Communication in the Animal and the Machine*. Second edition, 2019 reissue ed. Cambridge, MA: The MIT Press, 2019.

WINNER, Langdon. Cyberlibertarian Myths and the Prospects for Community. *ACM SIGCAS Computers and Society*, v. 27, n. 3, p. 14–19, 1 set. 1997. Disponível em: <https://www.langdonwinner.com/other-writings/2018/1/15/cyberlibertarian-myths-and-the-prospects-for-community>. Acesso em: 8 jan. 2019.

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.

ZHANG, Xing-Zhou; LIU, Jing-Jie; XU, Zhi-Wei. Tencent and Facebook Data Validate Metcalfe's Law. *Journal of Computer Science and Technology*, v. 30, n. 2, p. 246–251, mar. 2015.

ZIMMER, Zac. Bitcoin and Potosí Silver: Historical Perspectives on Cryptocurrency. *Technology and Culture*, v. 58, n. 2, p. 307–334, 2017. Disponível em: <https://muse.jhu.edu/article/662979>. Acesso em: 7 mai. 2022.